

# **NIST SPECIAL PUBLICATION 1800-28**

# Data Confidentiality: Identifying and Protecting Assets Against Data Breaches

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

William Fisher R. Eugene Craft Michael Ekstrom Julian Sexton John Sweetnam

February 2024

**FINAL** 

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-28

The first draft of this publication is available free of charge from: https://www.nccoe.nist.gov/data-confidentiality-identifying-and-protecting-assets-against-data-breaches



# Data Confidentiality: Identifying and Protecting Assets Against Data Breaches

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

> William Fisher National Cybersecurity Center of Excellence NIST

> > R. Eugene Craft Michael Ekstrom Julian Sexton John Sweetnam The MITRE Corporation McLean, Virginia

> > > FINAL

February 2024



U.S. Department of Commerce Gina M. Raimondo, Secretary

National Institute of Standards and Technology Laurie E. Locasci, NIST Director and Under Secretary of Commerce for Standards and Technology

# **NIST SPECIAL PUBLICATION 1800-28A**

# Data Confidentiality:

Identifying and Protecting Assets Against Data Breaches

Volume A: Executive Summary

William Fisher National Cybersecurity Center of Excellence NIST

R. Eugene Craft Michael Ekstrom Julian Sexton

John Sweetnam

The MITRE Corporation McLean, Virginia

February 2024

FINAL

This publication is available free of charge from: <u>https://doi.org/10.6028/NIST.SP.1800-28</u>



# **Executive Summary**

#### **CHALLENGE**

An organization must protect its information from unauthorized access and disclosure. Data breaches large and small can have far-reaching operational, financial, and reputational impacts on an organization. In the event of a data breach, data confidentiality can be compromised via unauthorized exfiltration, leaking, or spills of data to unauthorized parties, including the general public.

It is essential for an organization to identify and protect assets to prevent breaches. And in the event a data breach occurs, it is essential that an organization be able to detect the ongoing breach themselves, as well as begin to execute a response and recovery plan that leverages security technology and controls.

#### **BENEFITS**

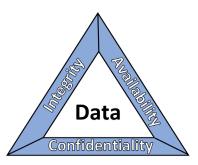
The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed this guide to help organizations implement strategies to prevent data confidentiality attacks. This NIST NCCoE Cybersecurity Practice Guide demonstrates how organizations can develop and implement appropriate actions to identify and protect data against a confidentiality cybersecurity event. It includes numerous technology and security recommendations to improve your organization's cybersecurity posture.

#### This practice guide can help your organization:

- Identify assets that may be affected by a data breach incident.
- Identify risks that may lead to data breaches.
- Implement protective technologies for your assets to prevent data breaches

#### **APPROACH**

This is part of a series of projects that seek to provide guidance to improve an organization's data security in the context of the CIA triad. The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability. This practice guide focuses on **data confidentiality**: the property that data has not been disclosed in an unauthorized fashion. Data confidentiality concerns data in storage, during processing, and while in transit. (Note: These definitions are from <u>NIST</u> <u>Special Publication (SP) 800-12 Rev 1, *An Introduction to Information Security*.)</u>



This guide applies data confidentiality principles through the lens of the NIST Cybersecurity Framework version 1.1. Specifically, this practice guide focuses on the Cybersecurity Framework Functions of Identify and Protect to provide guidance on how to prevent data confidentiality attacks. It informs organizations of how to **identify** and **protect** assets, including data, against a data confidentiality attack, and in turn understand how to manage data confidentiality risks and implement the appropriate safeguards. A complementary project and accompanying practice guide (SP1800-29) addresses data confidentiality through the lens of **detecting**, **responding**, and **recovering** from a data confidentiality attack.



The NCCoE developed and implemented an example solution that incorporates multiple systems working in concert to identify and protect assets and data against data confidentiality cybersecurity events. This document highlights both the security and privacy characteristics of the example solution by considering common data security use cases an organization might seek to address and by enumerating problematic data actions that might impact privacy.

Collaborator	Security Capability or Component
Avrio Software (now known as Aerstone)	Data Management
Cisco	Policy Enforcement, User Access Control
Dispel	Network Protection
FireEye	Logging
PKWARE	Data Protection
Qcor	Data Protection
Strongkey	Data Protection
Symantec, a Division of Broadcom	Browser Isolation

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

#### **HOW TO USE THIS GUIDE**

Depending on your role in your organization, you might use this guide in different ways:

**Business decision makers, including chief information security and technology officers** can use this part of the guide, *NIST SP 1800-28A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

**Technology, security, and privacy program managers** who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-28B: Approach, Architecture, and Security Characteristics,* which describes what we built and why, including the risk analysis performed and the security/privacy control mappings.

**IT professionals** who want to implement an approach like this can make use of *NIST SP 1800-28C: How-To Guides*, which provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

#### **SHARE YOUR FEEDBACK**

You can view or download the guide at <u>https://www.nccoe.nist.gov/projects/building-blocks/data-</u><u>security/dc-detect-identify-protect</u>. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at <u>ds-nccoe@nist.gov</u>.

#### **COLLABORATORS**

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

# **NIST SPECIAL PUBLICATION 1800-28B**

# Data Confidentiality: Identifying and Protecting Assets Against Data

Breaches

Volume B: Approach, Architecture, and Security Characteristics

William Fisher National Cybersecurity Center of Excellence NIST

R. Eugene Craft Michael Ekstrom Julian Sexton John Sweetnam

The MITRE Corporation McLean, Virginia

February 2024

**FINAL** 

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-28

The first draft of this publication is available free of charge from: <a href="https://www.nccoe.nist.gov/data-confidentiality-identifying-and-protecting-assets-against-data-breaches">https://www.nccoe.nist.gov/data-confidentiality-identifying-and-protecting-assets-against-data-breaches</a>



#### DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-28B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-28B, 62 pages, (February 2024), CODEN: NSPUE2

#### **FEEDBACK**

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at <u>ds-nccoe@nist.gov</u>.

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence National Institute of Standards and Technology 100 Bureau Drive Mailstop 2002 Gaithersburg, MD 20899 Email: <u>nccoe@nist.gov</u>

#### NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit <u>https://www.nccoe.nist.gov/</u>. To learn more about NIST, visit <u>https://www.nist.gov.</u>

#### **NIST CYBERSECURITY PRACTICE GUIDES**

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

#### ABSTRACT

Attacks that target data are of concern to companies and organizations across many industries. Data breaches represent a threat that can have monetary, reputational, and legal impacts. This guide seeks to provide guidance concerning the threat of data breaches, exemplifying standards and technologies that are useful for a variety of organizations defending against this threat. Specifically, this guide seeks to help organizations identify and protect assets, including data, against a data confidentiality attack.

#### **KEYWORDS**

asset management; cybersecurity framework; data breach; data confidentiality; data protection; identify; malicious actor; malware; protect; ransomware

#### ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Jason Winder	Avrio Software (now known as Aerstone)
Dylan Buel	Broadcom Software
Sunjeet Randhawa	Broadcom Software
Paul Swinton	Broadcom Software
Trey Doré	Cisco
Matthew Hyatt	Cisco
Randy Martin	Cisco
Peter Romness	Cisco
Bryan Rosensteel	Cisco
Micah Wilson	Cisco
Ben Burke	Dispel
Fred Chang	Dispel
Matt Fulk	Dispel
lan Schmertzler	Dispel
Kenneth Durbin	FireEye
Tom Los	FireEye
J.R. Wikes	FireEye
Jennifer Cawthra	NIST
Joe Faxlanger	PKWARE

Name	Organization
Victor Ortiz	PKWARE
Jim Wyne	PKWARE
Steve Petruzzo	Qcor
Billy Stewart	Qcor
Norman Field	StrongKey
Patrick Leung	StrongKey
Arshad Noor	StrongKey
Lauren Acierto	The MITRE Corporation
Spike Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Brian Johnson	The MITRE Corporation
Lauren Lusty	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Julie Snyder	The MITRE Corporation
Lauren Swan	The MITRE Corporation
Anne Townsend	The MITRE Corporation
Jessica Walton	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product

components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Avrio Software (now known as Aer- stone)	Avrio SIFT
Cisco Systems	Duo
Dispel	Dispel
FireEye	FireEye Helix
Qcor	Qcor ForceField
PKWARE	PKWARE PKProtect
StrongKey	StrongKey Tellaro
Symantec, a Division of Broadcom	Symantec Web Isolation

#### **DOCUMENT CONVENTIONS**

The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms "should" and "should not" indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms "may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

#### **PATENT DISCLOSURE NOTICE**

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL. No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

# Contents

1	Sun	nmary	
	1.1	Challe	nge2
	1.2	Solutio	n3
	1.3	Benefi	ts3
2	Hov	v to U	se This Guide3
	2.1	Туроді	aphic Conventions4
3	Арр	roach	
	3.1	Audier	ıce5
	3.2	Scope	6
	3.3	Assum	ptions6
	3.4	Privacy	Considerations6
	3.5	Risk As	sessment8
		3.5.1	Security Risk Assessment
		3.5.2	Privacy Risk Assessment9
	3.6	Techno	ologies9
4	Arcl	hitect	ıre12
5	Sec		A Privacy Characteristic Analysis13
5	<b>Sec</b> 5.1	urity 8	
5		<b>urity 8</b> Assum	& Privacy Characteristic Analysis13
5	5.1	<b>urity 8</b> Assum	<b>A Privacy Characteristic Analysis</b> 13 ptions and Limitations
5	5.1	urity 8 Assum Securit	<b>Privacy Characteristic Analysis</b>
5	5.1	Assum Securit 5.2.1	<b>A Privacy Characteristic Analysis</b>
5	5.1	Assum Securit 5.2.1 5.2.2	A Privacy Characteristic Analysis
5	5.1	Assum Securit 5.2.1 5.2.2 5.2.3	A Privacy Characteristic Analysis
5	5.1	Assum Securit 5.2.1 5.2.2 5.2.3 5.2.4	A Privacy Characteristic Analysis
5	5.1	Assum Securit 5.2.1 5.2.2 5.2.3 5.2.4 5.2.5	A Privacy Characteristic Analysis       13         ptions and Limitations       13         ry Scenarios       13         Exfiltration of Encrypted Data       14         Spear Phishing Campaign       15         Ransomware       15         Accidental Email       17         Lost Laptop       17
5	5.1	Assum Securit 5.2.1 5.2.2 5.2.3 5.2.4 5.2.5 5.2.6 5.2.7	A Privacy Characteristic Analysis       13         ptions and Limitations       13         ry Scenarios       13         Exfiltration of Encrypted Data       14         Spear Phishing Campaign       15         Ransomware       15         Accidental Email       17         Lost Laptop       17         Privilege Misuse       18         Eavesdropping       19         Y Scenarios       20
5	5.1 5.2	Assum Securit 5.2.1 5.2.2 5.2.3 5.2.4 5.2.5 5.2.6 5.2.7	A Privacy Characteristic Analysis13ptions and Limitations13cy Scenarios13cy Scenarios13Exfiltration of Encrypted Data14Spear Phishing Campaign15Ransomware15Accidental Email17Lost Laptop17Privilege Misuse18Eavesdropping19
5	5.1 5.2	Assum Securit 5.2.1 5.2.2 5.2.3 5.2.4 5.2.5 5.2.6 5.2.7 Privacy	A Privacy Characteristic Analysis       13         ptions and Limitations       13         ry Scenarios       13         Exfiltration of Encrypted Data       14         Spear Phishing Campaign       15         Ransomware       15         Accidental Email       17         Lost Laptop       17         Privilege Misuse       18         Eavesdropping       19         Y Scenarios       20
5	5.1 5.2	Assum Securit 5.2.1 5.2.2 5.2.3 5.2.4 5.2.5 5.2.6 5.2.7 Privacy 5.3.1	A Privacy Characteristic Analysis13ptions and Limitations13cy Scenarios13Exfiltration of Encrypted Data14Spear Phishing Campaign15Ransomware15Accidental Email17Lost Laptop17Privilege Misuse18Eavesdropping19V Scenarios20User Login with Multifactor Authentication21

5.3.5	User Web Browsing with Browser Isolation Solution	34
6 Future B	uild Considerations	36
Appendix A	List of Acronyms	37
Appendix B	Glossary	39
Appendix C	References	43
Appendix D	Security Control Map	45
Appendix E	Privacy Control Map	49

# **List of Figures**

Figure 1-1 Data Security Project Mapping	1
Figure 3-1 Cybersecurity and Privacy Risk Relationship	7
Figure 4-1 High Level Architecture	12
Figure 5-1 Multifactor Authentication Data Flow Diagram	22
Figure 5-2 Virtual Desktop Interface Data Flow Diagram	25

# **List of Tables**

Table 3-1 Products and Technologies	10
Table 5-1 Exfiltration of Encrypted Data Security Scenario	14
Table 5-2 Spear Phishing Campaign Security Scenario	15
Table 5-3 Ransomware Security Scenario	15
Table 5-4 Accidental Email Security Scenario	17
Table 5-5 Lost Laptop Security Scenario	17
Table 5-6 Privilege Misuse Security Scenario	18
Table 5-7 Eavesdropping Security Scenario	19
Table 5-8 User Login with Multifactor Authentication Data Actions	23
Table 5-9 User Login with Multifactor Authentication Problematic Data Action	24
Table 5-10 Virtual Desktop Interface Data Actions	26
Table 5-11 Virtual Desktop Interface Problematic Data Actions	27
Table 5-12 Data Management Data Action	29

Table 5-13 Data Management Problematic Data Actions	30
Table 5-14 Logging Data Actions	32
Table 5-15 Logging Problematic Data Actions	33
Table 5-16 Browser Isolation Data Actions	34
Table 5-17 Browser Isolation Problematic Data Actions	35
Table 6-1 Security Control Map	45
Table 6-2 Privacy Control Map	49

# **1** Summary

In our data-driven world, organizations must prioritize cybersecurity and privacy as part of their business risk management strategy. Specifically, data confidentiality remains a challenge as attacks against an organization's data can compromise emails, employee records, financial records, and customer information—impacting business operations, revenue, and reputation.

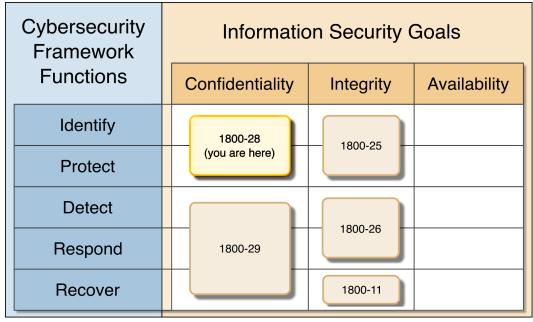
Confidentiality is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information"[1]. Data confidentiality makes sure that only authorized users can access data and use it in an authorized manner. Ensuring data confidentiality should be a priority for any organization regardless of industry. A loss of data confidentiality can be of great impact to not just the company or organization, but also to the individuals who have trusted the organization with their data.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed an example solution to address data security and privacy needs. This project fits within a larger series of Data Security projects that are organized by the elements of the Confidentiality, Integrity, Availability (CIA) triad, and the NIST Cybersecurity Framework's (CSF) Core Functions: Identify, Protect, Detect, Respond, and Recover.



**Note:** This project was initiated before the release of the DRAFT NIST CSF 2.0 and thus does not include the newly added GOVERN function. The DRAFT NIST CSF 2.0 defines Govern as "Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy". The govern function cuts across the other CSF functions. Though this document focuses on technical capabilities, it's intended that those capabilities would support an organizational governance function in managing data confidentiality attack risk.

Figure 1-1 Data Security Project Mapping



The goals of this NIST Cybersecurity Practice Guide are to assist organizations in identifying and protecting their assets and data in order to prepare for and prevent a data confidentiality event. This guide will help organizations:

- Inventory data storage and data flows
- Protect against confidentiality attacks against hosts, the network and enterprise components
- Protect enterprise data at rest, in transit, and in use
- Configure logging and audit capabilities to meet organizational requirements
- Implement access controls to sensitive data
- Implement authentication mechanisms for host and network access
- Enumerate data flows and problematic data actions in line with the NIST Privacy Framework

In addition to the guidance provided in these documents, NIST has many resources available to help organizations to identify and protect data:

- NIST Special Publication 1800-25, Data Integrity: Identifying and Protecting Assets Against Ransomware and other Destructive Events [2]
- NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops [5]
- NIST Special Publication 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security [6]
- NIST Privacy Framework [7]
- NIST Cybersecurity Framework [8]
- NIST Interagency Report 8374, Ransomware Risk Management: A Cybersecurity Framework Profile
   [9]
- NIST Special Publication 800-160, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach [10]

#### 1.1 Challenge

Data confidentiality is a challenge because all data exists to be accessible by some number of authorized people or systems. Data access can lead to a data breach when access is achieved or given to an unauthorized person or system. Challenges for an organization to maintain data confidential result from the sheer volume of an organization's data, the many ways users can access the data (on-site versus remote, computer versus mobile device), and the potential for the compromise of valid user credentials being used by unauthorized users.

NIST SP 1800-28 focuses on applying the Identify and Protect Functions of the NIST Cybersecurity Framework to address the challenges related to categorizing authorized and unauthorized data access. This document helps organizations address identifying potential breaches of data confidentiality as well as protecting against the resulting losses.

Additional challenges arise when defining what it means to "identify" or "protect" data. In the NCCoE's previous work on Data Integrity (1800-25 [2], 1800-26 [3], and 1800-11 [4]), it was possible to define recovery as a rollback of the compromised data to a point in time before it was altered. With respect to a loss of data confidentiality, there is no such process by which to "undo" the effects of such a loss—

once digital data is in the hands of an unauthorized user, there is no guaranteed method by which to get all copies of the data back. This leaves an organization and the affected individuals with non-technical mitigations for the consequences of the breach (financial, reputational, etc.), as well as the ability of the organization to apply the lessons learned to technical improvements earlier in the timeline to prevent against future breaches.

#### **1.2 Solution**

The NCCoE developed this two-part solution to address considerations for both data security and data privacy to help organizations manage the risk of a data confidentiality attack. The work in 1800-29 addresses an organization's actions during and after a loss of data confidentiality (the remaining NIST CSF Functions of Detect, Respond, and Recover) while this guide's focus is on the needs prior to a loss of data confidentiality (by focusing on the NIST CSF Functions Identify and Protect). The solution utilizes commercially available tools to provide relevant capabilities such as automated data sensitivity detection, access controls for data, encryption of potential confidential data, and multifactor authentication, among others.

#### **1.3 Benefits**

Organizations can use this guide to help:

- Evaluate their data confidentiality concerns
- Determine if their data security needs align with the data confidentiality challenges identified in this guide
- Conduct a gap analysis to determine the distance between the current state and desired state of the organization's data confidentiality protections
- Perform a feasibility assessment for implementing the protections described in this guide
- Determine a business continuity analysis to identify potential impacts on business operations as a result of a loss of data confidentiality.

# 2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the data confidentiality capabilities described in this document. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-28A: Executive Summary
- NIST SP 1800-28B: Approach, Architecture, and Security Characteristics what we built and why (you are here)
- NIST SP 1800-28C: How-To Guides instructions for building the example solution

Depending on your role in your organization, you might use this guide in different ways:

**Business decision makers, including chief security and technology officers,** will be interested in the *Executive Summary, NIST SP 1800-28A*, which describes the following topics:

- challenges that enterprises face in identifying vulnerable assets and protecting them from data breaches
- example solution built at the NCCoE
- benefits of adopting the example solution

**Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-28B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.5, <u>Risk Assessment</u>, provides a description of the risk analysis we performed
- Section 3.6, <u>Security Control Map</u>, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-28A*, with your leadership team members to help them understand the importance of adopting standards-based solutions to protecting against losses in data confidentiality.

**IT professionals** who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-28C*, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a security architecture that protects against data breaches. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, <u>Technologies</u>, lists the products we used and maps them to the cybersecurity and privacy controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to <u>ds-nccoe@nist.gov</u>.

#### 2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the NCCoE Style Guide.
Bold	names of menus, options, command buttons, and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on- screen computer output, sample code examples, and status codes	mkdir
Monospace Bold	command-line user input contrasted with computer output	service sshd start
<u>blue text</u>	link to other parts of the doc- ument, a web URL (uniform resource locator), or an email address	All publications from NIST's NCCoE are available at <u>https://www.nccoe.nist.gov</u> .

# **3** Approach

The NCCoE is developing a set of data confidentiality projects mapped to the five Functions of the NIST Cybersecurity Framework Core. This project centers on identifying and protecting vulnerable data from attack. Our commercial collaboration partners have volunteered to provide the products that provide this example solution for the problems raised in each of our use cases. Through this collaboration, our goal is to create actionable recommendations for organizations and individuals trying to solve data confidentiality issues.

#### 3.1 Audience

The architecture of this project and accompanying documentation targets three distinct groups of readers. The first is those personally managing, implementing, installing and configuring IT security solutions for their organization. The walkthroughs of installation and configuration of the chosen commercial products, as well as any of our notes on lessons learned, work to ease the challenge of implementing security best practices. This guide also serves as a starting point for those addressing these security issues for the first time, and a reference for experienced admins who want to do better.

The second group are those tasked with establishing broader security policies for their organizations. Reviewing the threats each organization needs to account for and their potential solutions allows for more robust and efficient security policy to be generated with greater ease.

The final group are those individuals responsible for the legal ramifications of breaches of confidentiality. Many organizations have legal obligations to take steps to proactively protect the personal data or personally identifiable information (PII) of individuals they process. The ramifications

for failing to adequately protect PII can have severe consequences for both individuals and follow on consequences for the organizations as a whole.

This guide will allow potential adopters to assess the feasibility of implementing data confidentiality best practices within the IT systems of their own organization.

#### 3.2 Scope

This document provides guidance on identifying potentially sensitive data and protecting against a loss of data confidentiality. Refer to Figure 1-1 to understand how this document fits within the larger set of NCCoE Data Security projects, as organized by the CIA triad and the functions of the NIST Cybersecurity Framework Core.

#### 3.3 Assumptions

The technical solution developed at the NCCoE and represented in this guide does not incorporate the non-technical aspects of managing the confidentiality of an organization's data. The non-technical components could include (but are not limited to):

- applicable legal requirements based on pertinent jurisdictions
- corporate or other superseding policies relevant to confidentiality and privacy
- standard operating procedures in the event of a loss of data confidentiality
- public relations strategies

This project is guided by the following assumptions:

- The solution was developed in a laboratory environment and is limited in the size and scale of data.
- Only a subset of products relevant to data confidentiality are included in this project, as such organizations should consider the guiding principles of this document when evaluating their organization's needs against the product landscape at the time of their IT implementation.

#### 3.4 Privacy Considerations

Because privacy risks may arise as a result of a loss of confidentiality of data, this guide includes privacy considerations. This section gives a primer for why privacy is important to protect, the relationship between privacy and cybersecurity risk, as well as NIST's approach to privacy risk assessment.

In today's digital landscape, consumers conduct much of their lives on the internet. Data processing, which includes any operations taken with data, including the collection, usage, storage, and sharing of data by organizations, can result in privacy problems for individuals. Privacy risks can evolve with changes in technology and associated data processing. How organizations treat privacy has a direct bearing on their perceived trustworthiness. Recognizing the evolving privacy impacts of technology on individuals, governments across the globe are working to address their concerns through new or updated laws and regulations.

Following an open and transparent development process, NIST published the NIST Privacy Framework, Version 1.0 to help organizations better identify and manage their privacy risks, build trust with customers and partners, and meet their compliance obligations. The Privacy Framework Core provides

privacy outcomes that organizations may wish to achieve as part of a privacy risk management program. The Privacy Framework also discusses privacy engineering objectives that can be used to help organizations prioritize their privacy risk management activities. The privacy engineering objectives are:

- Predictability: Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system
- Manageability: Providing the capability for granular administration of data, including collection, alteration, deletion, and selective disclosure
- Disassociability: Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system

It is important for individuals and organizations to understand the relationship between cybersecurity and privacy. As noted in Section 1.2.1 of the *NIST Privacy Framework* [8], having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. Figure 3-1 illustrates this relationship, showing that some privacy risks arise from cybersecurity risks, and some are unrelated to cybersecurity risks.

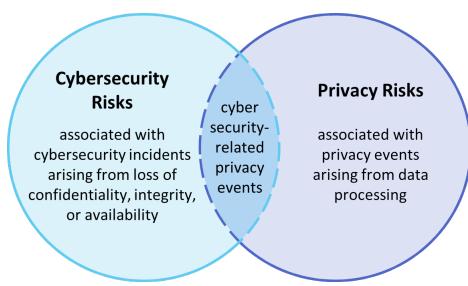


Figure 3-1 Cybersecurity and Privacy Risk Relationship

Though a data confidentiality breach may lead to privacy problems for individuals, it is important to note that privacy risks can arise without a cybersecurity incident. For example, an organization might process data in ways that violates an individual's privacy without that data having been breached or compromised through a security incident. This type of issue can occur under a variety of scenarios, such as when data is stored for extended periods, beyond the need for which the information was initially collected.

Privacy risks arise from privacy events—the occurrence or potential occurrence of problematic data actions. The NIST Privacy Framework defines problematic data actions as data actions that may cause an adverse effect for individuals. Problematic data actions might arise by data processing simply for mission or business purposes. Privacy risk is the likelihood that individuals will experience problems resulting from data processing, and the impact should they occur [16]. As reflected in the overlap of Figure 3-1, analyzing these risks in parallel with cybersecurity risks can help organizations understand the full

consequences of impacts of data confidentiality breaches. <u>Section 5.3</u> demonstrates scenarios where privacy risks may arise and potential mitigations.

Based on the reference architecture, this build considered the data actions that potentially cause problematic data actions.

#### 3.5 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [12]—material that is available to the public. The Risk Management Framework (RMF) [13] guidance proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

#### 3.5.1 Security Risk Assessment

Security risk assessments often discuss the consideration of threats to an information system. NIST SP 800-30 Revision 1 defines a threat as "[a]ny circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service". Threats are actions that may compromise a system's confidentiality, integrity, or availability [11]. Threats evolve, and an organization needs to perform its own analysis when evaluating threats and risks that the organization faces.

The following threats were considered during the development of the data confidentiality solution:

- exfiltration by malicious outsider actor
- exfiltration by malicious internal actor (privilege misuse)
- ransomware with threat to leak data
- non-malicious insider actor (accidental email)
- misplaced hardware

For a threat to be realized, a system, process or person must be vulnerable to a threat action. A vulnerability is a deficiency or weakness that a threat source may exploit, resulting in a threat event. Vulnerabilities may exist in a broader context. That is, they may be found in organizational governance structures, external relationships, and mission/business processes.

Organizations should consider impact if a data confidentiality breach occurs including potential decline in organizational trust and credibility affecting employees, customers, partners, stakeholders as well as financial impacts due to loss of proprietary or other sensitive information.

#### 3.5.2 Privacy Risk Assessment

This build also incorporates privacy as part of the build risk assessment. It is important for organizations to address privacy risk as part of a comprehensive risk management process. The build utilized the NIST Privacy Framework [7] and Privacy Risk Assessment Methodology (PRAM) [14] to identify and address privacy risks.

As part of identifying privacy risks in this build, problematic data actions were correlated to observed privacy risks. In many cases, the security capabilities in this build will help mitigate privacy risks, but organizations should use caution to implement these capabilities in a way that does not introduce new privacy risks.

Section 5.3 discusses problematic data action and privacy considerations for this build.

#### 3.6 Technologies

Table 3-1 Products and Technologies lists the technologies used in this project and provides a mapping among the generic application term, the specific product used, and the security control(s) that the product provides. Refer to Table 6-1 Security Control Map for an explanation of the NIST Cybersecurity Framework Subcategory identifiers. Table 3-1 also provides the Privacy Framework Subcategory identifiers. Table 3-1 also provides the Privacy Framework Subcategory identifiers.

#### Table 3-1 Products and Technologies

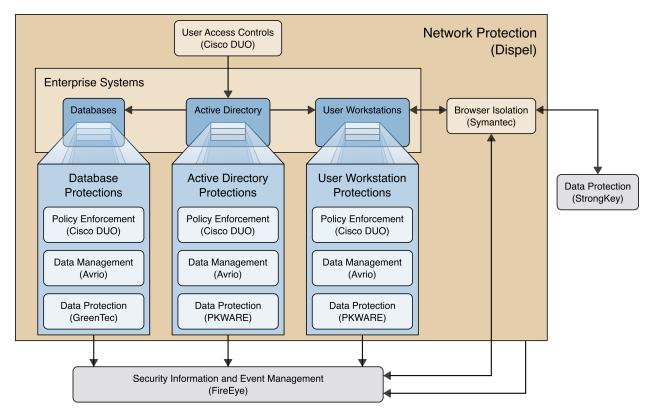
Component	Product	Capability	NIST Cybersecurity Framework Subcatego- ries	NIST Privacy Frame- work Subcategories
Data Management	Avrio SIFT v1.0.5.R5	• Discovers, tags, and protects sensitive files across the network	ID.AM-2, PR.DS-1, PR.DS-3	ID.IM-P1, PR.DS-P1, PR.DS-P3
Data Protection	Qcor Forcefield v1.9h	<ul> <li>Protects data at-rest from unauthorized access and malicious modification</li> </ul>	PR.DS-1	PR.DS-P1
	PKWARE PKProtect v16.40.0010	Provides data encryption at-rest     and in-transit	PR.DS-1, PR.DS-2	PR.DS-P1, PR.DS-P2
	StrongKey Tellaro	<ul> <li>Provides a Web API (application programming interface) for encryption and tokenization, key management, and strong authentication</li> </ul>	PR.AC-7, PR.DS-2	PR.AC-P6, PR.DS-P2
User Access Con- trols	Cisco Duo	Provides multi-factor authentication	PR.AC-1, PR.AC-4, PR.AC-7	PR.AC-P1, PR.AC-P4, PR.AC-P6
Browser Isolation	Symantec Web Isola- tion	<ul> <li>Provides isolation of web browsers to protect from risky traffic</li> <li>Protects from malware and phishing threats</li> <li>Provides a privacy toggle that allows for user browsing data to be anonymized.</li> <li>Provides a login banner to inform individuals of data collection practices with web browsing</li> </ul>	PR.AC-5, PR.DS-2	PR.AC-P5, PR.DS-P2, CT.DP-P2, CM.AW-P3
Policy Enforcement	Cisco Duo	<ul> <li>Provides policy control on a global or per-application basis</li> </ul>	PR.IP-5	PR.PO-P4

Component	Product	Capability	NIST Cybersecurity Framework Subcatego- ries	NIST Privacy Frame- work Subcategories
Logging	FireEye Helix	<ul> <li>Provides a baseline for normal enterprise operations</li> <li>Provides logs and enables incident response</li> </ul>	ID.RA-1, ID.RA-2, ID.RA- 3, PR.PT-1	CT.DM-P8
Network Protec- tion	Dispel	Provides remote access to network	PR.AC-3, PR.AC-5	PR.AC-P3, PR.AC-P5

# **4** Architecture

This section presents the high-level architecture and a set of capabilities used in our data confidentiality reference design that identifies and protects assets from unauthorized access and disclosure.





Each of the capabilities implemented plays a role in mitigating data confidentiality attacks:

- Data Management allows discovery and tracking of files throughout the enterprise.
- Data Protection involves encryption and protection against disclosure of sensitive files.
- Access Controls allows organizations to enforce access control policies, ensuring that only authorized users have access to sensitive files.
- **Browser Isolation** protects endpoints in the organization from malicious web-based malware by sandboxing and containing executables downloaded from the internet.
- **Policy Enforcement** ensures that endpoints in the organization conform to specified security policies, which can include certificate verification, installed programs, and machine posture.
- **Logging** creates a baseline of a normal enterprise activity for comparison in the event of a data confidentiality event.
- Network Protection ensures that hosts on the network only communicate in allowed ways, preventing side-channel attacks and attacks that rely on direct communication between hosts.
   Furthermore, it protects against potentially malicious hosts joining or observing traffic (encrypted or decrypted) traversing the network.

These capabilities work together to provide the functions Identify and Protect for the reference architecture. The data management capability provides data inventory and asset management for files in the enterprise; helps identify potentially sensitive files; and works with the data protection capability to ensure potentially sensitive files are properly protected in the event of a breach. Because organizations can be large and new sensitive files may be created daily, it is important to have the capability to automate identification and protection of files at least partially. The data protection capability and access controls prevent data from being read by unauthorized parties. By ensuring that only the correct users and systems have access to data, and that data is protected in-use and at-rest, it becomes more difficult for adversaries to steal and disclose sensitive data.

The policy enforcement, network protection, and browser isolation capabilities work together to protect endpoints such as laptops and desktops against common attack vectors. Malicious websites distributing malware first pass through the browser isolation capability, which sandboxes webpages to ensure that malware downloaded via malicious webpage cannot spread to the user or enterprise's system. Network segmentation uses network layer policies to group endpoints into segments based on business needs. If an endpoint is infected, network segmentation can limit impact by preventing malware from spreading between segments. Policy enforcement ensures that systems remain up to date with organizationally defined security policies. All of these functions feed into logging capabilities and provide organizations with an understanding of their baseline of normal activity. These logs inform the organization of its security posture before an event, so that the organization can adjust its policies as new information about threats becomes available and take appropriate action.

# **5** Security & Privacy Characteristic Analysis

The following section is intended to help organizations understand the extent to which the project meets its objective of demonstrating technologies and capabilities to help organizations mitigate data confidentiality risk. To support this, we developed several scenarios which organizations may consider when conducting their security and privacy risk analysis. For each scenario we discuss how our architecture might help mitigate or limit security and privacy risks.

#### 5.1 Assumptions and Limitations

The following analysis has the following limitations:

- It is neither a comprehensive test of all security and privacy components, nor a red-team exercise.
- It cannot identify all weaknesses or risks.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

#### 5.2 Security Scenarios

Our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. Each scenario lays out a potential cybersecurity event and discusses the responsibilities of an organization with respect to each event, and how the security

capabilities of our architecture would help an organization address the Cybersecurity Framework Functions of **Identify** and **Protect** for that event.

Below is a list of the scenarios created to test the security capabilities of this architecture.

NOTE: The below scenarios map to the DRAFT NIST CSF 2.0. For a mapping to the NIST CSF 1.1 please see Security Control Map in Appendix D.

#### 5.2.1 Exfiltration of Encrypted Data

 Table 5-1 Exfiltration of Encrypted Data Security Scenario

Description	An organization has unknowingly acquired a compromised machine from an outside source and has attached the machine to its trusted network. This machine periodically scans a certain part of the filesystem, which it has deemed to be potentially sensitive, and encrypts and uploads the contents to a malicious web host. Because the machine was assumed to be trusted due to human error, the delivery of this malware into the system is difficult to detect; it must be detected and stopped after it has already started running.
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-5, ID.RA-5, PR.AA-01, PR.AA-02, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-04
Organizational Response	In this scenario, the organization accepts an infected machine onto its network. As an example, this could be hardware ordered from a third-party vendor, potentially having been refurbished or modified before delivery to the organization. Because the organization connects the machine directly to the network, the acquisition of the malware happens immediately and without warning. It falls to the organization to protect sensitive data from this breach, as well as be able to identify the traffic generated by the malware as anomalous.
Identify	The <b>Data Management</b> capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk of targeting and the impact to the enterprise in the event of compromise.
Protect	The <b>Data Protection</b> capability provides encryption for sensitive data which has been identified as important, protecting it from unauthorized access in the event of an exfiltration attack.
	Another important aspect of the Protect function is the documentation of audit logs, with respect to sensitive data. The <b>Logging</b> capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase to discover anomalies in network traffic and lead to the discovery of malicious exfiltration.

#### 5.2.2 Spear Phishing Campaign

Table 5-2 Spear Phishing Campaign Security Scenario

Description	An unknown user has successfully launched a spear phishing attack, and in the process retrieved an authorized user's login and password. This user has access to several of the organization's databases, allowing them to both view and manipulate the data contained within. This exposes proprietary data to theft and manipulation/deletion.
Associated DRAFT CSF 2.0 Subcategories	PR.AA-01, PR.AA-02, PR.AA-03, PR.DS-01, PR.DS-02, PR.PS-01, PR.PS-04, DE.CM-09
Organizational Response	In this scenario, someone at the organization with privileged credentials has had their credentials compromised through a spear phishing email. The user may report this themselves if they retroactively realize it was a phishing attack, or they may not. The organization will need to deal with a privileged user account with access to the database being used by a malicious actor and is responsible for protecting assets from the compromised account.
Identify	Though identifying assets is an important function, in this scenario we are specifically focusing on the ability of a compromised user to access an in- use database, and do not have a specific need to identify the database as part of the scenario's resolution, since the target is known.
Protect	The <b>Data Protection</b> capability provides write-protection against alteration or deletion of saved data, as well as protection against reading the data through encryption of data-in-use.
	Another important aspect of the Protect function is the management of access permissions. The <b>User Access Controls</b> capability allows the database to be protected by a second layer of authentication separate from the user's username and password. In the event of compromised credentials, the database is less likely to be impacted if two factors of authentication are required.
	Furthermore, acquisition of user credentials does not necessarily imply that a user's physical system has been stolen. <b>Policy Enforcement</b> can take advantage of this by authenticating the hardware, software and/or firmware that is being used by the account at time of access. This is typically done by digital certificates, hash values, or other forms of attestation that are stored in hardware-backed security mechanisms. This serves to ensure that a stolen username and password is not enough to compromise critical resources.

#### 5.2.3 Ransomware

 Table 5-3 Ransomware Security Scenario

Description	An employee of the company makes a mistake while entering the URL of
	their company's email provider. This mistake takes them to an identical
	login page, but it is hosted by a malicious actor. When they enter their

	credentials on the login page, the page records their credentials, and forwards them to the actual login page, as if the credentials were mistyped. The malicious actor later uses these credentials to login as the employee. They download and run a malicious ransomware executable as the user. The ransomware executable uploads sensitive files to the malicious host website, which displays a notice that unless a ransom is paid, the sensitive files will remain publicly visible.
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-5, ID.RA-5, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01, PR.PS-01, PR.PS-04
Organizational Response	In this scenario, someone at the organization with privileged credentials has had their credentials compromised through a malicious webpage disguised as the organization's email provider. The user may or may not report the attack, though there may be clues as to its existence - a user with account troubles and traffic going to a domain name very similar to the organization's domain might be enough to send up red flags if noticed. Regardless, the organization will need to deal with a privileged user account being used to download malware and hold the confidentiality of sensitive files ransom.
Identify	The <b>Data Management</b> capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk of targeting and the impact to the enterprise in the event of compromise.
Protect	The <b>Data Protection</b> capability provides encryption for sensitive data, protecting it from unauthorized access in the event of an exfiltration attack. Even if the data is stolen and released, encryption prevents the data from being used or read.
	Another important component of the Protect function is the documentation of audit logs, with respect to sensitive data. The <b>Logging</b> capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase to discover anomalies in network traffic and user behavior, potentially allowing for the detection of a malicious actor accessing the user's workstation outside of normal hours.
	<b>Browser Isolation,</b> in tandem with <b>Network Protection,</b> will prevent downloads of malicious files from websites and unknown ports, limiting the attacker's ability to acquire their ransomware program after the system has been compromised. While the ability to download malicious programs onto the workstation may not completely stop determined attackers, it increases the difficulty and time required for the attack, allowing more time for Detection and Respond activities by the defending organization.

#### 5.2.4 Accidental Email

Table 5-4 Accidental Email Security Scenario

Description	A user of the organization accidentally cc's an individual on an email. This email has an attachment containing proprietary information which the cc'd individual is not cleared for. The individual copied on the email is considered a disgruntled employee, and when he sees this email, immediately downloads and saves these files.
Associated DRAFT CSF	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-5, ID.RA-5, PR.AA-01, PR.AA-02,
2.0 Subcategories	PR.AA-03, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01, PR.PS-04
Organizational Response	In the event of an accidental information leak via email, it is not unlikely that the event will be reported. Since there are multiple parties involved who are not malicious, it is possible that one of them will report the incident. Regardless of whether it is reported, however, the organization should be able to track the transfer of sensitive data to the unauthorized employee's system, and also prevent that employee from reading it.
Identify	The <b>Data Management</b> capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise in the event of an information leak.
Protect	<ul> <li>The Data Protection capability provides encryption for sensitive information, protecting it from unauthorized access even if it is accidentally sent to unauthorized users.</li> <li>Another important component of the Protect function is documentation of audit logs, with respect to sensitive data. The Logging capability provides a baseline for normal enterprise activity. This baseline can be used as a</li> </ul>
	comparison point in the Detect phase for reporting on data which has been transferred onto the systems of unauthorized users.

#### 5.2.5 Lost Laptop

Table 5-5 Lost Laptop Security Scenario

Description	A user has lost their work laptop, which contains proprietary information. It is unknown if the laptop was targeted for its data and access credentials by a malicious actor, or if the incident was an unfortunate accident. For the purposes of this scenario, we assume the user of the laptop has reported the missing system on their own.
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-05, ID.AM-07, PR.AA-01, PR.AA-03, PR.DS-01, PR.DS-09, PR.PS-03
Organizational Response	In the event of a lost laptop, it is likely that the loss will be reported by the user, as the user will directly lose their ability to work. Although some aspects of this event are easier because of the user's knowledge of the system, it is important for the organization to determine the data that was on the laptop, the security posture of the laptop, and the access the laptop

	provided to the organization's network, so that the loss can be accurately assessed, and further data loss can be prevented.
Identify	The Data Management capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise in the event of a compromise.
	The Policy Enforcement capability can be used to force computers connecting to organizational resources to meet requirements regarding which programs are installed. While this capability typically falls under the Protect function, knowing the security posture of assets in the enterprise is an important Identify function. When policy enforcement is used to ensure the presence of encryption capabilities, for example, the enterprise has some assurance that data on the workstation has not been compromised.
Protect	The Data Protection capability provides encryption for the laptop and prevents sensitive data from being read.
	Another important aspect of the Protect function is the management of access permissions. The User Access Controls capability allows the network to be protected by two layers of authentication. Although the laptop may be compromised, requiring user account credentials as well as a second factor of authentication protects the network from further compromise.
	Policy Enforcement can be used to force computers connecting to organizational resources to meet requirements regarding which programs are installed, which helps to ensure that lost or stolen machines will have adequate data protection and user access control in place to prevent the loss of data in the event of a lost or stolen laptop.

### 5.2.6 Privilege Misuse

Table 5-6 Privilege Misuse Security Scenario

Description	A malicious insider navigates to one of the organization's shared drives, and finds sensitive information stored there. Looking to sell this information to competitors, the insider copies the information to his personal USB (universal series bus) drive. The insider also prints these files.
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-05, ID.AM-07, ID.RA-03, PR.AA-03, PR.AA-05, PR.AA-06, PR.DS-01, PR.DS-02, PR.DS-09, PR.PS-04, PR.IR-01
Organizational Response	It is unlikely that a malicious insider will advertise their misdoings; it falls to the organization to discover the insider behavior and protect assets from them. Through proper access control and encryption of sensitive files, organizations can hinder the insider's attempt to exfiltrate useful data. It is unlikely that an organization will be able to completely stop a determined insider through technical means; however, organizations should use the technical capabilities they have to limit the exfiltration, while also gathering

	information about the extent of the loss to aid in the pursuit of legal resolutions to the incident.
ldentify	The <b>Data Management</b> capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise in the event of a compromise. In the event of a malicious insider attempting to exfiltrate data, it is important to know which data was accessible on the machines accessed by the insider, as well as the sensitivity levels of the affected data.
Protect	The <b>Data Protection</b> capability provides encryption for sensitive data, protecting it from unauthorized access. While a malicious insider may be able to decrypt data relevant to their work role, irrelevant data which is encrypted and managed properly will be significantly less useful to the insider.
	Another important capability within the Protect Function is the management of access permissions. The <b>User Access Controls</b> can prevent unauthorized users from accessing sensitive files in the first place, preventing copying and printing functionality.
	While user access controls and data protection ensure that the user only has access to some data, ultimately, malicious insiders tend to have some level of access to data due to their role in the organization. <b>Logging</b> provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase for reporting on data which has been exfiltrated from the organization. In the event of exfiltration by a malicious insider, logs can help determine what data was accessed and printed and can aid the organization in recovering from the exfiltration, potentially in non-technical ways, such as through the legal system or law enforcement.

# 5.2.7 Eavesdropping

Table 5-7 Eavesdropping Security Scenario

Description	A malicious outsider has gained access to the network traffic of the organization. They possess the capability to intercept and hijack internal communications via man-in-the-middle attack. A user begins uploading a sensitive proposal for a new project. The malicious outsider is able to intercept and view these files.
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-03, ID.AM-07, PR.AA-05, PR.AA-06, PR.DS-01, PR.DS-02, PR.PS-04, PR.IR-01
Organizational Response	In this scenario, an organization will likely be able to see the introduction of a new device on the network. In this example, a user's sensitive upload is stolen while it is in transit. The user may see warnings about HTTPS or invalid certificates due to the nature of the attack, and the organization may notice anomalous traffic going through the new device on the network. The organization is responsible for identifying the new device as

	malicious, protecting data intercepted by it through encryption, and mitigating its ability to communicate with trusted enterprise machines.
Identify	The Data Management capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise. In this scenario, a new project proposal is created - the data management capability is used to identify the creation of new sensitive data and track it throughout the enterprise.
Protect	The Data Protection capability provides encryption for sensitive data, protecting it from unauthorized access. While a malicious third party on the network may be able to intercept the data in transit, encryption prevents the third party from being able to read the intercepted data.
	Another important component of the Protect Function is the documentation of audit logs, with respect to sensitive data. The Logging capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase for noticing anomalous network activity, such as a malicious host on the network acting as a proxy between two systems.
	Network Protection is also an important capability for protecting network traffic from malicious adversaries. Using network segmentation, zero trust, and moving target defense capabilities, unrecognized devices can be prevented from identifying, reconnoitering, and accessing the network or communicating with trusted hosts.

#### 5.3 Privacy Scenarios

The following section describes scenarios an organization may consider when conducting their privacy risk assessment. Based on the reference architecture used in this project each scenario is examined for data actions that give rise to potential privacy problems for individuals. Each table documents problematic data actions taken from the NIST Catalogue of Problematic Data Actions and Problems [16], and lists privacy mitigations mapped to the NIST Privacy Framework [7]. For the privacy risks analyzed, consideration was given to how the data is processed. The specific privacy risks found within the scenarios are derived from the architecture components and the data flows used in this build, but to the extent possible, generalized for organizations using similar components and capabilities.

Organizations may collect information affecting privacy when implementing cybersecurity or privacybased controls. For example, an organization might implement multi-factor authentication (MFA) using information such as mobile phone number. Even though collecting this information helps to protect systems and data by supporting capabilities like non-repudiation and system auditing, it may also generate privacy risks.

When implementing cybersecurity or privacy-based controls, organizations should consider the benefit a user realizes, both from use of a service and securing that service before processing information

affecting privacy. This benefit can be weighed against the risk posed to both individuals and the organization should a privacy event occur.

For example, using MFA mentioned above, users may feel compelled to provide information affecting privacy, such as their personal phone number for SMS (short messaging service) authentication, to gain access to systems or services. However, if the user is accessing publicly available information, the risk of the misuse of information from collecting personal phone numbers may be greater than the security benefit for protecting the low-sensitivity information. Additionally, if given the option, users may elect to use alternative authentication methods that are less privacy-invasive, such as using a work phone number over a personal number or a hardware MFA authenticator over SMS authentication. The NIST Privacy Risk Assessment Methodology (PRAM) refers to this problematic data action, where the user is compelled to provide information disproportionate to the purpose or outcome of the transaction, as induced disclosure.

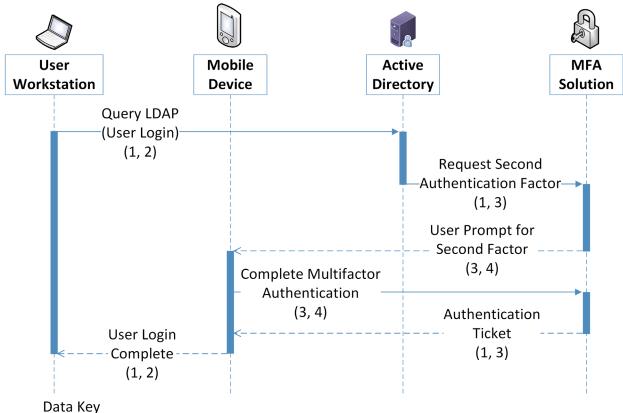
Organizations should consider these types of risks as they design and implement systems. As demonstrated in the scenarios below, risk mitigations should be implemented within the design to limit privacy risks. These privacy risk mitigations might include the following, among others:

- Understand where and how information is processed, including collection practices and system components that store and transmit this information (data flows and mapping)
- Understand the risks and benefits of collecting different data elements to determine if it should not be collected
- Keep data only as long as needed for its function and destroy or de-identify it otherwise using proper data lifecycle management practices and in accordance with applicable laws and policies
- Keep personal data segregated in a different repository, when practicable
- Encrypt data at rest, in transit, and in use
- Use role-based access controls
- Consider what measures should be taken to address predictability and manageability before deciding whether data can be used beyond its initial expected and agreed upon use
- Implement privacy-enhancing technologies to increase disassociability while retaining confidentiality and the capability to process data for mission or business purposes

### 5.3.1 User Login with Multifactor Authentication

Phishing-resistant multifactor authentication is a security best practice. The architecture recommends the use of a password, pin (personal identification number) or biometric with an asymmetric cryptographic key for authentication. However, it is common practice for organizations to offer a variety of MFA solutions. This can include user-owned mobile devices, which may impact privacy risk [17].

Figure 5-1 Multifactor Authentication Data Flow Diagram



- 1. Username
- 2. Client IP Address
- 3. Transaction Identifier
- 4. Mobile device information (Cellular number)

Table 5-8 User Login with Multifactor Authentication Data Actions

Data Type	Data Action	Privacy Impact	
Username	Username is stored by the user workstation and transferred across the authentication process to help identify the transaction.	Usernames potentially contain inferable PII such as user's first and last names.	
Client IP Ad- dress	The client IP (Internet Protocol) address is stored by the user workstation, and transferred as part of communica- tions where it is an endpoint.IP addresses can be used to derive PII such as location.		
Transaction Identifier	The transaction identifier is generated by active directory and transferred to the MFA solution and the mobile device.		
Mobile device information	The mobile device information is stored by the MFA solu- tion and the mobile device and transferred as a part of the communication between the mobile device and MFA solu- tion.	Information about a user's mobile device, such as device type and version, can be used to infer privacy-impacting in- formation such as the cost of their personal devices. Fur- thermore, user cell-phone numbers used in certain MFA transactions are PII.	

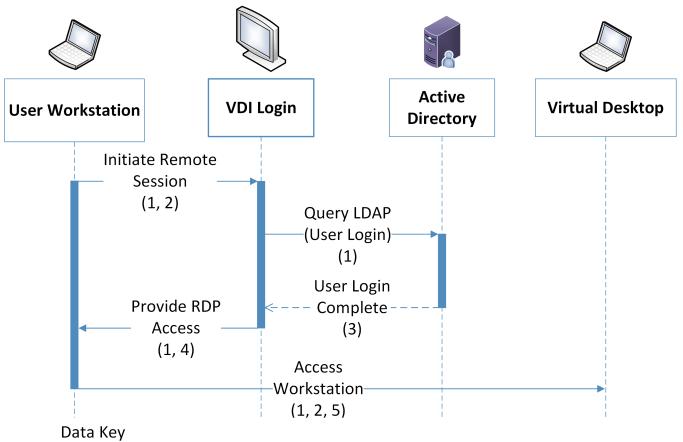
 Table 5-9 User Login with Multifactor Authentication Problematic Data Action

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
User authentication may use a mobile device as an au- thenticator, which can be personally or organizationally owned.	Mobile devices are a popular option for au- thentication processes. Personal information can be transferred in the process of authen- ticating. This can in- clude phone number and location infor- mation. Users' non- work activity may be tracked by an organiza- tion.	Context: Authentication processes that utilize personally owned mobile devices can require the use of information that is personal to the user, such as phone numbers and other metadata. The tracking could extend beyond the work environment or even within the work environment be disproportionate to the security needs leading to unanticipated revelations about user activities or degradation of the dignity or autonomy of users. Problematic Data Action: Unanticipated Revela- tion, Induced Disclosure Problem: Loss of Autonomy: Users have no control over what information is shared in this scheme. Users may not feel comfortable using their own per- sonal information as a security feature for an or- ganizational service. Loss of Trust: Users may not feel comfortable with their personal phone numbers and device information being shared with third-party appli- cations and Software as a Service providers.	<ul> <li>Predictability: Organizations should inform users of information that is viewed and collected by login tools, such as through privacy notices when devices are enrolled. System administrators should have limited access to user authentication information.</li> <li>Manageability: Organizations that leverage user's personal devices for user login processes should consider tools that give the users optionality for registering different types of authenticators, including those that do not use personal devices and information. In this build, Duo offers a variety of authentication options, such as a hardware-based authenticator.</li> <li>Organizations should audit tools to determine what information they are using and collecting.</li> <li>Disassociability: Organizations should explore capabilities and configurations that allow for the de-identification of phone numbers and other personal information, such as the capability to replace a phonenumber with placeholder text or privacy-enhancing cryptographic techniques to limit the tracking of users.</li> </ul>

# 5.3.2 Authentication to Virtual Desktop Interface Solution

The reference architecture in this document demonstrates a Virtual Desktop Interface (VDI) solution to facilitate secure access to organizational resources and data. Organizations may allow users' personal devices to access corporate resources using the VDI solution. Organizations should consider the privacy risk of installing VDI software on personally owned devices, information revealed by the VDI protocol, and monitoring of user activity while in the virtual environment.

Figure 5-2 Virtual Desktop Interface Data Flow Diagram



- 1. Username
- 2. Client IP address
- 3. Token identifier
- 4. One-time password
- 5. Client time zone, computer name

 Table 5-10 Virtual Desktop Interface Data Actions

Data Type	Data Action	Privacy Impact
Username	The username is stored by the user workstation and active directory. It is transferred as part of the authentication process.	Usernames potentially contain inferable PII such as user's first and last names
Client IP Ad- dress	The Client IP Address is stored on the user workstation, and transferred as part of transactions and connections it generates.	IP addresses can be used to derive PII such as user's general location
Token Identifier	A Token Identifier is generated by Active Directory in support of the authentication process and transferred to the VDI.	Token identifiers can be used to re-identify other infor- mation affecting privacy that occur as part of transactions.
One-time pass- word	A One-time Password is generated by the VDI to authenti- cate the RDP (remote desktop protocol) connection and is transferred to and stored on the user workstation.	
Client Time Zone	The Client Time Zone is stored by the user workstation and transferred as part of an RDP connection to the virtual desk-top.	Along with IP addresses, time zones specifically provide in- formation about a user's location
Client Computer Name	The Client Computer Name is stored by the user work- station and transferred as part of an RDP connection to the virtual desktop.	User's personal device names can include inferable PII, such as personal names and device locations.

 Table 5-11 Virtual Desktop Interface Problematic Data Actions

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
User logs into a Vir- tual Desktop Inter- face solution from a personally or or- ganizationally owned device.	Central login platforms can be connected to by a variety of devices, which may be person- ally owned by the user. Information that can be associated with the user, such as their de- vice information or lo- cation, may be trans- mitted to security tools as part of the authenti- cation process.	Context: Users operating under a BYOD or re- mote work scheme may not expect that certain data is under organizational purview. This can include their location, personal device metadata, and operating hours. Problematic Data Action: Surveillance, Unantici- pated Revelation Problem: Loss of Trust. Users may not feel comfortable with this information being shared with third- party applications, or the company in general. Dignity Loss. Users may have information, such as their physical location and work hours, re- vealed to organizations in an undesired fashion.	<ul> <li>Predictability: Users should be informed of information that is viewed and collected by login and network access tools such as Dispel, through either a login banner or other alert mechanism. Use privacy enhancing technologies and techniques to de-identify user, user ID and IP address like obfuscation, communication anonymization, data minimization, and pseudonymization, among others.</li> <li>Manageability: Organizations that include user's personal devices in day-to-day operation should audit tools to determine what information they are using and collecting and who has access rights</li> <li>Confidentiality: Organizations should mandate strict access control for the management and configuration of user login services, such as with MFA.</li> <li>Availability: Organizations that utilize central login platforms as their entry should consider the robustness of their platforms and systems. A loss of access to these systems can lead to an inability for users to access their data.</li> </ul>

# 5.3.3 Automated Data Movement with Data Management Solution

The reference architecture uses data management technology that allows for the scanning files for highly sensitive information and establishment of policy that automatically moves sensitive content to secure storage. Files with detected PII or other sensitive information may be moved in ways that are unexpected to the user, potentially creating privacy concerns.

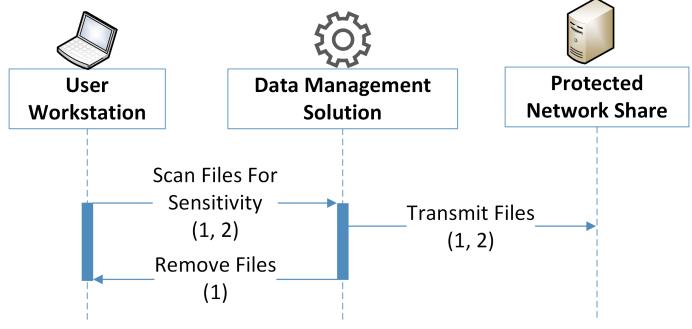


Figure 5-3 Data Management Data Flow Diagram

Data Key

- 1. File metadata (Name, Date of Modification, File Type, Author)
- 2. File contents

Table 5-12 Data Management Data Action

Data Type	Data Action	Privacy Impact
File metadata	File metadata is stored on the user workstation, along with file contents. It is transferred along with file contents to the Data Management Solution and the Protected Network Share as part of the data movement operation. It is also used to identify data for deletion by the Data Management Solution.	File metadata can include information affecting privacy that is not derivable from file contents, such as the file name, date of modification, and author. This can be used to derive information such as active work hours and can lead to false assumptions about an individual
File contents	File contents are stored on the user workstation and trans- ferred through the Data Management Solution to the Pro- tected Network Share.	The privacy impact of file contents rely heavily on the data being used by an enterprise. This information can include SSNs, credit card information, health data, and other PII. Privacy impact and regulatory burden should be specifically considered and analyzed by organizations implementing these sorts of security solutions.

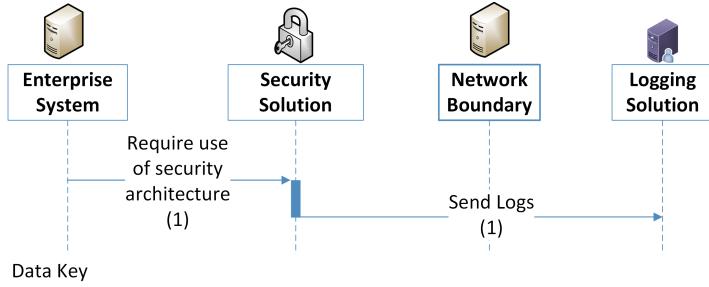
 Table 5-13 Data Management Problematic Data Actions

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
Data generated in areas moderated by data management solutions are potentially duplicated, moved, or deleted in compliance with organizational policy.	Movement of data by external tools can lead to information being placed in unexpected or unintended places. This can lead to user confusion and a loss of trust in the organization, as well as data being made vulnerable to discovery and exfiltration	Context: Moving data from the place in which it was created or saved can create confusion for users and expose information in ways the user did not intend. Problematic Data Action: Appropriation, Unanticipated Revelation Problem: Loss of Trust. Users may be uncomfortable working in protected zones if they do not trust that their data will be kept under their control. Loss of Autonomy. Users may see involuntary data movement as a loss of their ability to govern the data they generate.	<ul> <li>Predictability: Zones under the purview of data management and protection tools should be clearly defined and expressed to the user, such as through clearly understood network share names. Notice should be given to users who are impacted by the data management solution, such as by leaving a stub file at the original location.</li> <li>Manageability: Organizations seeking to include these capabilities should make sure they use solutions that can be configured to mitigate their inherent privacy risk.</li> <li>Confidentiality: Tools that provide the ability to analyze and move data should only be governed by system administrators. The automatic movement of data should only move data to locations only accessible by the user who created the original data or to folder with equal or more stringent access rights than the originating location. Furthermore, data locations are protected by IDAM (identity and access management controls) controls such as MFA.</li> </ul>

# 5.3.4 Monitoring by Logging Solution

This reference architecture generates logs used to aid in response and recovery activities. These logs are essential for proper data management and incident response. However, organizations should consider the privacy of information collected by logs when they are created, transmitted, and stored.





1. Usernames, IP addresses, web traffic history

The utilization of the security architecture, and the logs their user generates, can interact with and generate information that affects privacy. The use of a logging solution requires that data and metadata about user's activity be generated and stored in an additional location. Depending on the details and scope of the logging tool, this can extend the effective domain of information that affects privacy used by those tools. Some examples of information affecting privacy utilized in such transactions is given below:

#### Table 5-14 Logging Data Actions

Data Type	Data Action	Privacy Impact
IP Addresses	IP Addresses are stored and transferred by enterprise sys- tems as well as the logging solution. They are transferred by and through the security solutions.	IP addresses can be used to determine rough locations for user-owned machines. Additionally, IP Addresses can be common across logs from many security tools, allowing for anonymized data to be re-identified.
Device Identifi- ers	Device Identifiers are stored and transferred by enterprise systems as well as the logging solution. They are transferred by and through the security solutions.	Under certain circumstances, device Identifiers, such as MAC (media access control) addresses, can be used to iden- tify individuals from data that has been de-identified, or al- low for privacy-impacting correlations to be made between data logs.

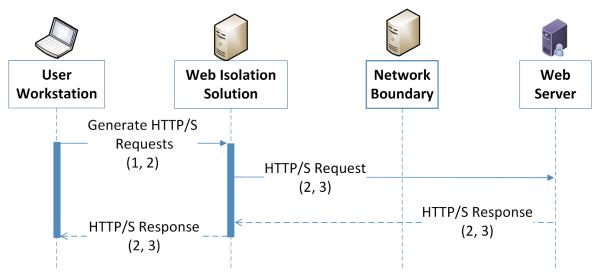
Table 5-15 Logging Problematic Data Actions

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
Security tools gen- erate metadata that is transferred to a logging solu- tion, either directly or via an on-site forwarder.	The security system passively creates data about users, their data, and their activities. This information is transmitted across the network and stored re- motely.	Context: Logging systems can contain private data. These logs are transmitted off the device or system in which they were created to other sys- tems where log information is aggregated. The privacy impact of each log and the aggregation of logs must be considered. Furthermore, this infor- mation is exposed to admin user who have access to either the individual or aggregated logs. Problematic Data Action: Unanticipated Revela- tion, Re-identification, Surveillance Problem: Loss of trust. Users may not expect the scope of information created and tracked by logs, even if they understand the scope of the security infra- structure. Dignity Loss. Embarrassing or undesired privacy information may be inferred about individuals whose actions generate logging information.	<ul> <li>Predictability: The existence of monitoring systems should be disclosed to users upon their access to organizational systems, such as through a login banner. Use privacy enhancing technologies and techniques to de-identify user ID and IP address like obfuscation, communication anonymization, data minimization, and pseudonymization, among others.</li> <li>Manageability: Organizations should evaluate how logs can be configured to collect the least amount of information necessary in order to meet security needs, especially when security tools are aggregating log information across multiple systems.</li> <li>Disassociability: Organizations should consider de-identification functions for log creation, transmission, storage and aggregation. For example, privacy-relevant information such as the user's name can be disassociated from their IP address or device identifier when collecting log information.</li> <li>Confidentiality: Tools that generate or store logs should have strict access control applied to them such as MFA.</li> </ul>

# 5.3.5 User Web Browsing with Browser Isolation Solution

Web isolation solutions must have governance over all user web traffic to be effective. This can generate privacy concerns to users by increasing the risk of their browsing data being misused.

Figure 5-5 Browser Isolation Data Flow Diagram



Data Key

- 1. Client IP Address
- 2. User browsing metadata (Target IP address, URL, Session information)
- 3. User browsing contents

Table 5-16 Browser Isolation Data Actions

Data Type	Data Action	Privacy Impact
Client IP Ad- dress	IP Addresses are stored on the User Workstation and sent by network con- nections to and from it.	IP addresses can be used to derive PII such as a user's general location
User brows- ing metadata	User browsing metadata is generated on the user workstation and sent to and from the user workstation, as well as to and from the web isolation solution to the web server.	HTTP/S traffic, even when encrypted, re- lies on unencrypted metadata such as time stamps, source IPs, and destination IPs. These materials can be used to gen- erate information that affects privacy, such as a specific user's browsing habits.
User brows- ing contents	User browsing contents are generated on the user workstation as well as the web server. They are sent back and forth be- tween the web server and the web isola- tion solution and delivered back to the user workstation.	Tools that can view and inspect the con- tents of a user's web browsing session could further impact user privacy. This can include a user accessing their bank and checking balance information, ac- cessing information from their healthcare provider, and so on.

 Table 5-17 Browser Isolation Problematic Data Actions

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
Data from user web browsing flows through web isolation solutions, centralizing infor- mation about em- ployee web brows- ing.	Web monitoring tools are used to detect ma- licious web traffic pat- terns or access re- quests to unsafe do- mains but may also collect and transmit in- formation that affects the user's privacy.	<ul> <li>Context: User browsing data can reveal information affecting privacy, such as personal health or financial information. Administrators can centrally view user browsing metadata at this location. This information may also be forwarded to other third-party tools.</li> <li>Problematic Data Action: Surveillance, Unanticipated Revelation</li> <li>Problem: Loss of Trust. Users may perceive the monitoring of their web traffic as a form of surveillance which may negatively impact the trust they have in their IT systems and/or organization.</li> </ul>	<ul> <li>Predictability: Users should be informed on the capabilities of web monitoring and related tools, such as through a login banner. Use privacy enhancing tech- nologies and techniques to de-identify user ID and IP address like obfuscation, communication anonymization, data minimization, and pseudonymization, among others.</li> <li>Manageability: Organizations seeking to use web monitor tools should assess their privacy preserving capabilities. In this reference architecture Symantec Web Isolation provides a privacy toggle that allows for user browsing data to be anonymized.</li> <li>Disassociability: Organizations should employ de-identification options for data when appropriate. In this reference ar- chitecture the privacy toggle provided by Symantec Web Isolation was enabled, which anonymized user browsing data.</li> <li>Confidentiality: Organizations should mandate strict access controls for secu- rity tools that can impact user privacy, including the use of MFA.</li> </ul>

# **6 Future Build Considerations**

As shown in <u>Figure 1-1</u>, the NCCoE Data Security work that remains to be addressed within the framework of the CIA triad is Data Availability. The Data Security team plans to evaluate the current landscape of Data Availability challenges that organizations face and determine future relevant projects to address those needs.

Appendix A	List of Acronyms
ΑΡΙ	Application Programming Interface
BYOD	Bring Your Own Device
CIA	Confidentiality Integrity Availability
CIS	Center for Internet Security
CNSSI	Committee on National Security Systems Instruction
COBIT	Control Objectives for Information and Related Technologies
CRADA	Cooperative Research And Development Agreement
CSC	Critical Security Controls
CSF	Cybersecurity Framework
FIPS	Federal Information Processing Standard
FIPPS	Fair Information Privacy Principles
НТТР	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDAM	Identity and Access Management
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISA	International Society of Automation
ISO	International Organization for Standardization
ІТ	Information Technology
ITL	Information Technology Laboratory
MAC	Media Access Control
MFA	Multi Factor Authentication
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NIST IR	NIST Interagency or Internal Report
PDA	Problematic Data Action
PII	Personally Identifiable Information
PIN	Personal Identification Number
PRAM	Privacy Risk Assessment Methodology
RDP	Remote Desktop Protocol
RMF	Risk Management Framework
SMS	Short Messaging Service
SP	Special Publication
URL	Uniform Resource Locator
USB	Universal Series Bus

Virtual Desktop Interface

VDI

Appendix B	Glossary
Access Control	The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).
	SOURCE: Federal Information Processing Standard (FIPS) 201-3
Adversary	Person, group, organization, or government that conducts or has the intent to conduct detrimental activities.
	SOURCE: CNSSI 4009-2015
Asset	A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
	SOURCE: Committee on National Security Systems Instruction (CNSSI) 4009-2015
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
	SOURCE: FIPS 200
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
	SOURCE: CNSSI 4009-2015
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose.
	SOURCE: NIST SP 800-53 Rev. 5
Control	The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature.
	SOURCE: NIST SP 800-160 Vol. 2 Rev. 1

Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
	SOURCE: FIPS 200
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted.
	SOURCE: CNSSI 4008-2015
Data Action	A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.
	SOURCE: NIST Privacy Framework Version 1.0
Disassociability	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system.
	SOURCE: NISTIR 8062
Encrypt	Cryptographically transform data to produce cipher text.
	SOURCE: CNSSI 4009-2015
Enterprise	An entity of any size, complexity, or positioning within an organizational structure.
	SOURCE: NIST SP 800-72
Event	Any observable occurrence in a network or system.
	SOURCE: CNSSI 4009-2015
Exfiltration	The unauthorized transfer of information from an information system.
	SOURCE: CNSSI 4009-2015
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
	SOURCE: FIPS 200

Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
	SOURCE: FIPS 200
Key Management	The activities involving handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.
	SOURCE: CNSSI 4009-2015
Manageability	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure.
	SOURCE: NISTIR 8062
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
	SOURCE: CNSSI 4009-2015
Mitigation	A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities.
	SOURCE: NIST SP 1800-160 Vol. 2 Rev. 1
Multi-Factor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
	SOURCE: CNSSI 4009-2015
Phishing	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
	SOURCE: CNSSI 4009-2015
Predictability	Enabling reliable assumptions by individuals, owners, and operators about PII and its processing by a system.
	SOURCE: NISTIR 8062

Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
	SOURCE: FIPS 200
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
	SOURCE: NIST SP 800-53
Security Policy	A set of rules that governs all aspects of security-relevant system and system component behavior.
	SOURCE: NIST SP 800-53 Rev. 5
Spear Phishing	A colloquial term that can be used to describe any highly targeted phishing attack.
	SOURCE: CNSSI 4009-2015
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
	SOURCE: NIST SP 800-53 Rev. 5
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
	SOURCE: FIPS 200

# Appendix C References

- W. Barker, Guideline for Identifying an Information System as a National Security System, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, Gaithersburg, Md., Aug. 2003, 17 pp. Available: <u>https://doi.org/10.6028/NIST.SP.800-59</u>.
- [2] T. McBride et. al, Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-25, Gaithersburg, Md., Dec. 2020, 488 pp. Available: <u>https://doi.org/10.6028/NIST.SP.1800-25</u>.
- [3] T. McBride et. al, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-26, Gaithersburg, Md., Dec. 2020, 441 pp. Available: <u>https://doi.org/10.6028/NIST.SP.1800-26</u>.
- T. McBride et. al, Data Integrity: Recovering from Ransomware and Other Destructive Events, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-11, Gaithersburg, Md., Sep. 2020, 377 pp. Available: <u>https://doi.org/10.6028/NIST.SP.1800-11</u>.
- [5] M. Souppaya and K. Scarfone, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-83 Revision 1, Gaithersburg, Md., July 2013, 36 pp. Available: <u>https://doi.org/10.6028/NIST.SP.800-83r1</u>.
- [6] M. Souppaya and K. Scarfone, Guide to Enterprise Telework, Remote Access, and Bring Your Own Devise (BYOD) Security, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 2, Gaithersburg, Md., July 2016, 43 pp. Available: https://doi.org/10.6028/NIST.SP.800-46r2.
- [7] NIST. *Privacy Framework*. Available: <u>https://www.nist.gov/privacy-framework</u>.
- [8] NIST. *Cybersecurity Framework*. Available: <u>http://www.nist.gov/cyberframework</u>.
- [9] W. Barker et. al, Ransomware Risk Management: A Cybersecurity Framework Profile, NIST Interagency Report 8374, Gaithersburg, Md., Feb. 2022, 23 pp. Available: <u>https://doi.org/10.6028/NIST.IR.8374</u>.
- [10] R. Ross et. al, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 2 Revision 1, Gaithersburg, Md., Dec. 2021, 309 pp. Available: <u>https://doi.org/10.6028/NIST.SP.800-160v2r1</u>.
- [11] Joint Task Force Transformation Initiative, Guide for Conducting Risk Assessments, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, Gaithersburg, Md., Sep. 2012, 83 pp. Available: <u>https://doi.org/10.6028/NIST.SP.800-30r1</u>.

- Joint Task Force, Risk Management Framework for Information Systems and Organizations, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2, Gaithersburg, Md., Dec. 2018, 164 pp. Available: <u>https://doi.org/10.6028/NIST.SP.800-37r2</u>.
- [13] NIST. *Risk Management Framework*. Available: <u>https://csrc.nist.gov/projects/risk-management/about-rmf</u>.
- [14] NIST. *Privacy Risk Assessment Methodology*. Available: <u>https://www.nist.gov/privacy-framework/nist-pram</u>.
- [15] S. Brooks et. al, An Introduction to Privacy Engineering and Risk Management in Federal Systems, NIST Interagency Report 8062, Gaithersburg, Md., Jan. 2017, 41 pp. Available: <u>https://doi.org/10.6028/NIST.IR.8062</u>.
- [16] NIST. Catalog of Problematic Data Actions and Problems. Available: <u>https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md</u>.
- [17] NIST Cybersecurity Center of Excellence, Mobile Device Security, Bring Your Own Device Practice Guide, NIST SP 1800-22, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf.
- [18] NIST Privacy Framework Repository, <u>https://www.nist.gov/privacy-framework/resource-repository.</u>

# Appendix D Security Control Map

The following table lists the NIST Cybersecurity Framework Functions, Categories, and Subcategories addressed by this project and maps them to relevant NIST standards, industry standards, and controls and best practices.

Table 6-1 Security Control Map

	Cyberse	curity Framework v1.1	Standards & Best Practices	
Function	Category Subcategory		Informative References	
IDENTIFY (ID)	Asset Manage- ment (ID.AM)	ID.AM-2: Software platforms and appli- cations within the organization are in- ventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5	
	Risk Assess-	ID.RA-1: Asset vulnerabilities are identi- fied and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA- 7, CA-8, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	
	ment (ID.RA)	ID.RA-2: Cyber threat intelligence is re- ceived from information sharing forums and sources	CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI- 5, PM-15, PM-16	

	Cyberse	curity Framework v1.1	Standards & Best Practices
Function	Category	Subcategory	Informative References
		ID.RA-3: Threats, both internal and ex- ternal, are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM16
		PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443- 2-1:2009 4.3.3.5.1 ISA 62443-3- 3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
PROTECT (PR)	Identity Man- agement, Au- thentication and Access Control (PR.AC)	PR.AC-3: Remote access is managed	IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443- 2-1:2009 4.3.3.6.6 ISA 62443-3- 3:2013 SB 1 13 SB 2 6 ISO/IEC
		PR.AC-4: Access permissions and au- thorizations are managed, incorporat- ing the principles of least privilege and separation of duties	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2- 1:2009 4.3.3.7.3 ISA 62443-3- 3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC- 2, AC-3, AC5, AC-6, AC-14, AC- 16, AC-24

	Cyberse	curity Framework v1.1	Standards & Best Practices
Function	Category	Subcategory	Informative References
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443- 2-1:2009 4.3.3.4 ISA 62443-3- 3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
	sets are authenticated (e.g., single-fac- tor, multi-factor) commensurate withDSS05.0the risk of the transaction (e.g., individ- uals' security and privacy risks and4.3.3.6.		CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9
	Data Security	PR.DS-1: Data-at-rest is protected	CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC- 12, SC-28
	(PR.DS)	PR.DS-2: Data-in-transit is protected	CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12

Cybersecurity Framework v1.1 Standards & Best			Standards & Best Practices
Function	Category	Subcategory	Informative References
		PR.DS-3: Assets are formally managed throughout removal, transfers, and dis- position	CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800- 53 Rev. 4 CM-8, MP-6, PE-16
	Information Protection Processes and Procedures (PR.IP)	PR.IP-5: Policy and regulations regard- ing the physical operating environment for organizational assets are met	CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443- 2-1:2009 4.3.4.3.9 ISA 62443-3- 3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800- 53 Rev. 4 CP-4, CP-6, CP-9
	Protective Technology (PR.PT)	PR.PT-1: Audit/log records are deter- mined, documented, implemented, and reviewed in accordance with policy	CIS CSC 1, 3, 5, 6, 14, 15, 16 CO- BIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3- 3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family

# Appendix E Privacy Control Map

The following table lists the NIST Privacy Framework Functions, Categories, and Subcategories addressed by this project and maps them to relevant NIST standards, industry standards, and controls and best practices.

NOTE: The International Organization for Standardization (ISO) standard 27701 references were not mapped by NIST, but by an external organization. They are available at the NIST Privacy Framework Repository [18] and provided here for convenience. The Fair Information Privacy Principles (FIPPS) references are provided to aid understanding of the Privacy Control Map.

Table 6-2 Privacy Control Map

Privacy Framework 1.0			Standards and Best Practices
Function	Category	Subcategory	Informative Refences
<b>IDENTIFY-P (ID-P):</b> Develop the organizational understanding to manage privacy risk for indi- viduals arising from data pro- cessing.	<b>Inventory and Mapping</b> ( <b>ID.IM-P</b> ): Data processing by systems, products, or services is understood and informs the management of privacy risk.	<b>ID.IM-P1:</b> Systems/prod- ucts/services that process data are inventoried.	FIPPS 7: Purpose Specification/Use Limitation NIST SP 800-37 Rev. 2: Task P-10 NIST SP 800-53 Rev. 5: CM-8 (10), CM-12, CM-13, PM-5 NIST IR 8062 NIST PRAM: Worksheet 2 ISO/IEC 27701:2019 7.2.8, 8.2.6
<b>CONTROL-P (CT-P):</b> Develop and Optional (Risk Based) ap- propriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	Data Processing Manage- ment (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individ- uals' privacy, increase manageability, and enable the implementation of pri- vacy principles (e.g., indi- vidual participation, data quality, data minimiza- tion).	<b>CT.DM-P8:</b> Audit/log records are determined, documented, and reviewed in accordance with policy and incorporating the principle of data minimiza- tion.	FIPPS 4: Minimization NIST SP 800-53 Rev. 5: AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU- 14, AU-16 NIST IR 8062 ISO/IEC 27701:2019 6.9.4.1, 6.9.4.2, 6.15.1.3

	Privacy Framework 1.0		Standards and Best Practices
Function	Category	Subcategory	Informative Refences
	Disassociated Processing (CT.DP-P): Data processing solutions increase disasso- ciability consistent with the organization's risk strategy to protect individ- uals' privacy and enable implementation of privacy principles (e.g., data mini- mization).	<b>CT.DP-P2:</b> Data are processed to limit the identification of in- dividuals (e.g., de-identification privacy techniques, tokeniza- tion).	FIPPS 7: Purpose Specification/Use Limitation NIST SP 800-53 Rev. 5: AC-23, AU- 3(3), IA-4(8), PE-8(3), SA-8(33), SI- 12(1), SI-12(2), SI-19 NIST SP 800-63-3 NIST SP 800-188 (draft) NIST SP 800-188 (draft) NIST IR 8053 NIST IR 8062 ISO/IEC 27701:2019 7.4.2, 7.4.4
	Data Processing Aware- ness (CM.AW-P): Individu- als and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mecha- nisms are used and main- tained to increase predict- ability consistent with the organization's risk strategy to protect individuals' pri- vacy.	<b>CM.AW-P3:</b> System/prod- uct/service design enables data processing visibility.	FIPPS 7: Purpose Specification/Use Limitation NIST SP 800-53 Rev. 5: PL-8, PT-5(1), SA-17, SC-42(4) NIST IR 8062 ISO/IEC 27701:2019 7.3.2, 7.3.3, 8.3.1
<b>PROTECT-P (PR-P):</b> Develop and Implement appropriate data processing safeguards.	Data Protection Policies, Processes, and Procedures (PR.PO-P): Security and privacy policies (e.g., pur- pose, scope, roles and re- sponsibilities in the data processing ecosystem, and	<b>PR.PO-P4:</b> Policy and regula- tions regarding the physical op- erating environment for organi- zational assets are met.	FIPPS 5: Quality and Integrity FIPPS 7: Purpose Specification/Use Limitation NIST SP 800-53 Rev. 5: PE-1 ISO/IEC 27701:2019 All of 6.8

Privacy Framework 1.0		Standards and Best Practices	
Function	Category	Subcategory	Informative Refences
	management commit- ment), processes, and pro- cedures are maintained and used to manage the protection of data.		
	Identity Management, Au- thentication, and Access Control (PR.AC-P): Access to data and devices is lim- ited to authorized individu- als, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	<ul> <li>PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.</li> <li>PR.AC-P3: Remote access is managed.</li> </ul>	FIPPS 8: Security NIST SP 800-53 Rev. 5: IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA- 11, IA-12 NIST SP 800-63-3 ISO/IEC 27701:2019 6.6.2.1, 6.6.2.2, 6.6.4.2 FIPPS 8: Security FIPS Publication 199
			NIST SP 800-46 Rev. 2 NIST SP 800-53 Rev. 5: AC-1, AC-17, AC-19, AC-20, SC-15 NIST SP 800-77 NIST SP 800-113 NIST SP 800-114 Rev. 1 NIST SP 800-121 Rev. 2 ISO/IEC 27701:2019 6.6.2.1, 6.6.2.2
		<b>PR.AC-P4:</b> Access permissions and authorizations are man- aged, incorporating the princi- ples of least privilege and sepa- ration of duties.	FIPPS 8: Security NIST SP 800-53 Rev. 5: AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 NIST SP 800-162

Privacy Framework 1.0		Standards and Best Practices	
Function	Category	Subcategory	Informative Refences
		<b>PR.AC-P5:</b> Network integrity is protected (e.g., network segregation, network segmentation).	FIPPS 8: Security NIST SP 800-53 Rev. 5: AC-4, AC-10, SC-7, SC-10, SC-20
		<b>PR.AC-P6</b> : Individuals and de- vices are proofed and bound to credentials and authenticated commensurate with the risk of the transaction (e.g., individu- als' security and privacy risks and other organizational risks).	FIPPS 8: Security NIST SP 800-53 Rev. 5: AC-14, AC-16, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11, IA-12, PE-2, PS-3 NIST SP 800-63-3
	Data Security (PR.DS-P): Data are managed con- sistent with the organiza- tion's risk strategy to pro- tect individuals' privacy	<b>PR.DS-P1:</b> Data-at-rest are pro-tected.	FIPPS 8: Security NIST SP 800-53 Rev. 5: MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC- 28 NIST SP 800-175B
	and maintain data confi- dentiality, integrity, and availability.	<b>PR.DS-P2:</b> Data-in-transit are protected.	FIPPS 8: Security NIST SP 800-53 Rev. 5: SC-8, SC-11 NIST SP 800-175B
		<b>PR.DS-P3:</b> Systems/prod- ucts/services and associated data are formally managed throughout removal, transfers, and disposition.	FIPPS 8: Security NIST SP 800-53 Rev. 5: CM-8, MP-6, PE-16, PE-20

# **NIST SPECIAL PUBLICATION 1800-28C**

# **Data Confidentiality:**

Identifying and Protecting Data Against Data Breaches

Volume C: How-To Guides

William Fisher National Cybersecurity Center of Excellence NIST

R. Eugene Craft Michael Ekstrom Julian Sexton John Sweetnam The MITRE Corporation McLean, Virginia

February 2024

FINAL

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-28

The first draft of this publication is available free of charge from: <u>https://www.nccoe.nist.gov/data-confidentiality-identifying-and-protecting-assets-against-data-breaches</u>



#### DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCOE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

While NIST and the NCCOE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise, and the impact should the threat be realized before adopting cybersecurity measures such as this recommendation.

National Institute of Standards and Technology Special Publication 1800-28C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-28C, 86 pages, (February 2024), CODEN: NSPUE2

#### **FEEDBACK**

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at <u>ds-nccoe@nist.gov</u>.

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence National Institute of Standards and Technology 100 Bureau Drive Mailstop 2002 Gaithersburg, MD 20899 Email: <u>nccoe@nist.gov</u>

### NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit <u>https://www.nccoe.nist.gov/</u>. To learn more about NIST, visit <u>https://www.nist.gov.</u>

### **NIST CYBERSECURITY PRACTICE GUIDES**

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

#### ABSTRACT

Attacks that target data are of concern to companies and organizations across many industries. Data breaches represent a threat that can have monetary, reputational, and legal impacts. This guide seeks to provide guidance around the threat of data breaches, exemplifying standards and technologies that are useful for a variety of organizations defending against this threat. Specifically, this guide identifies risks associated with the loss of data confidentiality, and mitigations to protect against those risks.

#### **KEYWORDS**

asset management; cybersecurity framework; data breach; data confidentiality; data protection; identify; malicious actor; malware; protect; ransomware

### **ACKNOWLEDGMENTS**

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Jason Winder	Avrio Software (now known as Aerstone)
Trey Doré	Cisco
Matthew Hyatt	Cisco
Randy Martin	Cisco
Peter Romness	Cisco
Bryan Rosensteel	Cisco
Micah Wilson	Cisco
Ben Burke	Dispel
Fred Chang	Dispel
Matt Fulk	Dispel
lan Schmertzler	Dispel
Kenneth Durbin	FireEye
Tom Los	FireEye
J.R. Wikes	FireEye
Jennifer Cawthra	NIST
Joe Faxlanger	PKWARE
Victor Ortiz	PKWARE
Jim Wyne	PKWARE
Steve Petruzzo	Qcor
Billy Stewart	Qcor

Name	Organization
Norman Field	StrongKey
Patrick Leung	StrongKey
Arshad Noor	StrongKey
Dylan Buel	Symantec, a division of Broadcom
Sunjeet Randhawa	Symantec, a division of Broadcom
Paul Swinton	Symantec, a division of Broadcom
Spike Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Brian Johnson	The MITRE Corporation
Lauren Lusty	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Julie Snyder	The MITRE Corporation
Lauren Swan	The MITRE Corporation
Anne Townsend	The MITRE Corporation
Jessica Walton	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Avrio	Avrio SIFT
Cisco Systems	DUO

Technology Partner/Collaborator	Build Involvement
Dispel	Dispel
FireEye	FireEye Helix
Qcor	Qcor ForceField
PKWARE	PKWARE PKProtect
StrongKey	StrongKey Tellaro
Symantec, a Division of Broadcom	Symantec Web Isolation

### **DOCUMENT CONVENTIONS**

The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms "should" and "should not" indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms "may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

### PATENT DISCLOSURE NOTICE

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

# Contents

1	Intr	oduct	ion	1
	1.1	How t	o Use this Guide	1
	1.2	Build (	Overview	2
	1.3	Турод	raphic Conventions	3
	1.4	Logica	Il Architecture Summary	3
2	Pro	duct I	nstallation Guides	5
	2.1	FireEy	e Helix	5
		2.1.1	Installing the Communications Broker - CentOS 7	5
		2.1.2	Forwarding Event Logs from Windows 2012 R2	7
	2.2	Symar	ntec Cloud Secure Web Gateway	9
		2.2.1	Configure Web Security Service	10
		2.2.2	Install Proxy Certificates and enabling TLS/SSL Interception	13
		2.2.3	Configure Symantec Web Security Service Proxy	17
	2.3	PKWA	RE PKProtect	23
		2.3.1	Configure PKWARE with Active Directory	24
		2.3.2	Create a New Administrative User	26
		2.3.3	Install Prerequisites	27
		2.3.4	Install the PKProtect Agent	29
		2.3.5	Configure Discovery and Reporting	32
	2.4	Strong	gKey Tellaro	37
		2.4.1	Python Client for StrongKey – Windows Executable Creation and Use	37
	2.5	Qcor F	ForceField	41
		2.5.1	Installation and Usage of ForceField	41
	2.6	Avrio	SIFT	44
		2.6.1	Configuring Avrio SIFT	44
	2.7	Cisco	Duo	47
		2.7.1	Installing Cisco Duo	47
		2.7.2	Registering a Duo User	54
	2.8	Dispel		55
		2.8.1	Installation	55
		2.8.2	Configuring IP Addresses	57
		2.8.3	Configuring Network	59

		2.8.4	Adding a Device	60
	2.9	Integra	ation: FireEye Helix and Symantec SWG	63
		2.9.1	Configure Fireye Helix to Collect Logs from Symantec SWG	63
	2.10	Integra	ation: FireEye Helix and PKWARE PKProtect	66
		2.10.1	Configure the Helix Communications Broker	67
		2.10.2	Configure PKWARE PKProtect to Forward Events	67
	2.11	Integra	ation: FireEye Helix and Cisco Duo	69
		2.11.1	Configure Fireye Helix to Collect Logs from Cisco Duo	69
	2.12	Integra	ation: FireEye Helix and QCOR ForceField	72
		2.12.1	Configure an SFTP server on Windows	73
		2.12.2	Configure the Linux Machine to Download and Send Logs to the Helix Communications Broker	74
	2.13	Integra	ation: FireEye Helix and Dispel	75
	2.14	Integra	ation: Avrio SIFT and PKWARE PKProtect	75
		2.14.1	Configuring PKWARE PKProtect	75
	2.15	Integra	ation: Dispel and Cisco Duo	79
App	pend	lix A	List of Acronyms	80

# **1** Introduction

The following volumes of this guide show information technology (IT) professionals and security engineers how we implemented this example solution. We cover all of the products employed in this reference design. We do not re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our lab environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

## 1.1 How to Use this Guide

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the ability to identify threats to and protect from a loss of data confidentiality. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-28A: Executive Summary
- NIST SP 1800-28B: Approach, Architecture, and Security Characteristics what we built and why
- NIST SP 1800-28C: How-To Guides instructions for building the example solution (you are here)

Depending on your role in your organization, you might use this guide in different ways:

**Business decision makers, including chief security and technology officers,** will be interested in the *Executive Summary, NIST SP 1800-28A*, which describes the following topics:

- challenges that enterprises face in identifying vulnerable assets and protecting them from data breaches
- example solution built at the NCCoE
- benefits of adopting the example solution

**Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-28B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.5, Risk Assessment, describes the risk analysis we performed.
- Appendix D, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary, NIST SP 1800-28A*, with your leadership team members to help them understand the importance of adopting a standards-based solution to identify threats to and protect from a loss of data confidentiality

**IT professionals** who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-28C*, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution to identify threats to and protect from a loss of data confidentiality. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6 Technologies, lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to <u>ds-nccoe@nist.gov</u>.

### **1.2 Build Overview**

The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively identify sensitive data and protect against a loss of data confidentiality in various Information Technology (IT) enterprise environments. This work also highlights standards and technologies that are useful for a variety of organizations defending against this threat. The servers in the virtual environment were built to the hardware specifications of their specific software components.

The NCCoE worked with members of the Data Confidentiality Community of Interest to develop a diverse (but non-comprehensive) set of security scenarios against which to test the reference implementation. These are detailed in Volume B, Section 5.2.

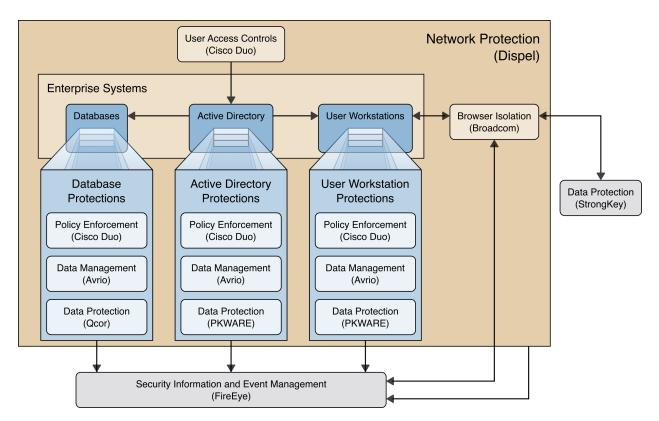
## **1.3 Typographic Conventions**

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that	For language use and style guidance, see
	are not hyperlinks; new terms;	the NCCoE Style Guide.
	and placeholders	
Bold	names of menus, options,	Choose File > Edit.
	command buttons, and fields	
Monospace	command-line input, onscreen	mkdir
	computer output, sample code	
	examples, and status codes	
Monospace Bold	command-line user input	service sshd start
	contrasted with computer	
	output	
<u>blue text</u>	link to other parts of the	All publications from NIST's NCCoE are
	document, a web URL, or an	available at <a href="https://www.nccoe.nist.gov">https://www.nccoe.nist.gov</a> .
	email address	

The following table presents typographic conventions used in this volume.

#### **1.4 Logical Architecture Summary**

The architecture described is built within the NCCoE lab environment. Organizations will need to consider how the technologies in this architecture will align technologies their existing infrastructure. In addition to network management resources, such as a border firewall, the architecture assumes the presence of user workstations, an active directory system, and databases. The diagram below shows the components of the architecture and how they interact with enterprise resources.



- Data Management (Avrio) allows discovery and tracking of files throughout the enterprise.
- Data Protection (GreenTec, StrongKey, PKWARE) involves encryption and protection against disclosure of sensitive files.
- User Access Controls (Cisco Duo) allows organizations to enforce access control policies, ensuring that only authorized users have access to sensitive files.
- Browser Isolation (Symantec SWG) protects endpoints in the organization from malicious webbased threats by utilizing multi-layered content inspection to block threats and remote isolation of content from high-risk and unknown sites.
- **Policy Enforcement (Cisco Duo)** ensures that endpoints in the organization conform to specified security policies, which can include certificate verification, installed programs, and machine posture.
- Security Information and Event Management (FireEye Helix) creates a baseline of a normal enterprise activity for comparison in the event of a data confidentiality event. This function includes the collection, aggregation, and analysis of logs throughout the enterprise, including logs from other security tools, to provide a better picture of the overall health of the enterprise before a breach should occur.
- Network Protection (Dispel) ensures that hosts on the network only communicate in allowed ways, preventing side-channel attacks and attacks that rely on direct communication between hosts.
   Furthermore, it protects against potentially malicious hosts joining or observing traffic (encrypted or decrypted) traversing the network.

For a more detailed description of our architecture, see Volume B, Section 4.

# **2** Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution. This implementation guide is split into sections for each product and integrations between these products, aiming to present a modular architecture where individual capabilities and products can be swapped out or excluded depending on the needs of the organization. Organizations can choose to implement a partial architecture based on their own risk assessments and data protection requirements.

#### 2.1 FireEye Helix

FireEye Helix is a security incident and event management system used for collecting and managing logs from various sources. In this build, Helix is primarily used to manage events and alerts generated by data collected from across the enterprise. This build implemented a cloud deployment of Helix, and as such, much of the documentation provided will be integrating a cloud deployment with various products and components of the enterprise.

In this setup, we detail the installation of a communications broker, which will be used to collect logs from the enterprise and forward them to the cloud deployment. This installation took place on a CentOS 7 Virtual Machine.

#### 2.1.1 Installing the Communications Broker- CentOS 7

- 1. Acquire the Helix Communications Broker for CentOS 7.
- 2. Navigate to the folder containing the installer, and run

> sudo yum localinstall ./cbs-installer\_1.4.2-9.x86\_64.rpm

- 3. Log on to the Helix web console.
- 4. Navigate to **Dashboards** > **Operational**.
- 5. Click **Download Certificate**.
- 6. Click Download. This will download a "bootstrap.zip" file.
- 7. Copy the zip file to the Helix Communications Broker certificate directory.

> sudo cp bootstrap.zip /opt/tap-nxlog/cert

- 8. Navigate to the certificate directory.
  - > cd /opt/tap-nxlog/cert
- 9. Extract the zip file you just copied.
  - > sudo unzip ./bootstrap.zip
- 10. If prompted, select "Yes" to overwrite any previous certificate files.
- 11. Navigate to one folder above.
  - > sudo cd ..

#### 12. Run the setup script.

> sudo ./setup.sh

- 13. Enter the name of the CentOS machine.
- 14. Enter the receiver URL provided in the Helix welcome email.

	administrator@localhost:/opt/tap-nxlog	-	•	>
File Edit View Se	earch Terminal Help			
LOGSENDER SETU				
	der's identification number			
	7937007088510978			
	helix-centos.dc.ipdrr			
	() Managed Comm. Broker			
	() Cloud Collector			
	60			
Receiver URL				
	/opt/tap-nxlog/cert/			
	storage location			
	/opt/tap-nxlog/conf/			

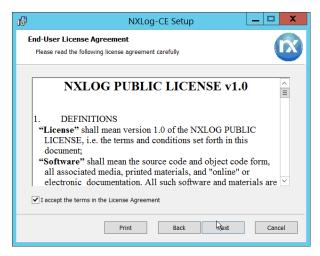
- 15. Select Add Routes and press Enter.
- 16. Select syslog.
- 17. Select tcp.
- 18. Select the Internet Protocol (IP) address of the machine where logs should be sent.
- 19. Enter 512 for the port number where logs should be sent.

administrator@localhost:/opt/tap-nxlog					-		×				
File	Edit	View	Search	Terminal	Help						
[ IN	PUT	SOURCE	SETUP:	:ADD —							
In			(X) (_) (_)		J						
		ol Typ Interf	(X) ()								
			( ) (x) ( )	192.16	8.122.1 8.1.206 0.1						
In			512								
								Cancel		OK	

- 20. Select OK and press Enter.
- 21. Review the configuration, then select **OK** and press **Enter**.
- 2.1.2 Forwarding Event Logs from Windows 2012 R2
  - 1. Acquire **nxlog-ce-2.10.2150.msi** from <u>http://nxlog.org/products/nxlog-community-edi-tion/download</u>.
  - 2. Run nxlog-ce-2.10.2150.msi.

1 <del>6</del>	NXLog-CE Setup	_ 🗆 X
	Welcome to the NXLog	CE on your computer. Click
	Back	<u>l</u> ext Cancel

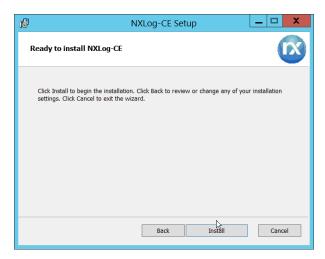
- 3. Click Next.
- 4. Check the box next to I accept the terms in the License Agreement.



5. Click Next.

ß	NXLog-CE Setup
	Destination Folder Click Next to install to the default folder or click Change to choose another.
	Install NXLog-CE to:
	C:\Program Files (x86)\nxdog\ Change
	Back Next

6. Click Next.



7. Click Install.

16	NXLog-CE Setup	_ 🗆 X
	Completed the NXLog-CE Click the Finish button to exit the Setup	Wizard.
	Back Figis	h Cancel

- 8. Click Finish.
- 9. Navigate to C:\Program Files (x86)\nxlog\conf and open nxlog.conf.

10. Copy the nxlog.conf file provided below.

```
Panic Soft
#NoFreeOnExit TRUE
define ROOT C:\Program Files (x86)\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
<Extension syslog>
  Module
            xm syslog
</Extension>
<Input in>
  Module im_msvistalog
# For windows 2003 and earlier use the following:
# Module im_mseventlog
</Input>
<Output out>
  Module om_tcp
Host 192.168.1.206
  Port
            512
           to_syslog_snare();
  Exec
</Output>
<Route 1>
          in => out
  Path
</Route>
```

- 11. Restart the **nxlog** service.
- 12. You can verify that this connection is working by checking the logs in *data\nxlog.log*, and by noting an increase in events on the Helix Dashboard.

#### 2.2 Symantec Cloud Secure Web Gateway

This installation and configuration guide for Symantec SWG uses a cloud instance of Web Isolation. In this guide, Web Isolation is used to isolate threats to the user through the browser. It does this through the use of a web proxy, which captures traffic and assigns a threat level to it, and based on administrative policy decides whether to serve the page to the user. In doing so, threats from the web can be mitigated through shared intelligence and isolated execution of the page before it reaches the user's desktop.

#### 2.2.1 Configure Web Security Service (WSS)

1. Login to the Symantec portal by navigating to <a href="https://portal.threatpulse.com/">https://portal.threatpulse.com/</a>.

S Web Security Service - Product S × +		~	_ □	X
← → C ( â portal.threatpulse.com		É	* .	:
left web Security Service				
Product Configuration				
Products will be available for use after completion of their initial configuration. Please select a product to configure.				
Product 👃	Configuration Status	Action	Progres	s
Web Security	🍄 Not Configured	Configure	0%	
Protection Suite	🕌 Not Purchased			
Hosted Reporting	🕌 Not Purchased			
CASB	🞽 Not Purchased			
			_	
Exit / Logout			Contin	iue

- 2. Click **Configure** next to Protection Suite.
- 3. Select WSS Portal.
- 4. Select Monitor.

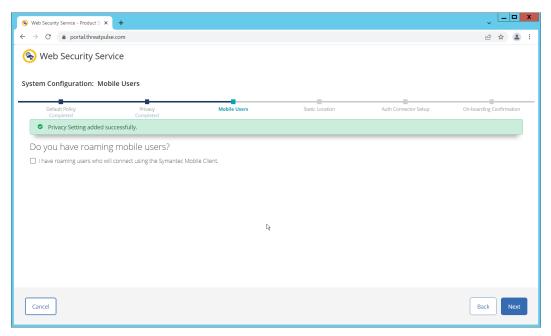
🛞 Web Security Service - Proc	luct Sc × +	v [-]	□ ×
$\leftarrow$ $\rightarrow$ C $\textcircled{a}$ portal.t	hreatpulse.com	止 ★	<b>a</b> :
🛞 Web Securit	y Service		
System Configuration	n: Default Policy		
Default Policy	Privacy	Mobile Users Static Location Auth Connector Setup On-boarding Confirma	ation
Where do you plar	n to manage your clou	ud policy?	•
Policy Source:	• WSS Portal	Configure and manage your policy from the WSS portal	ι.
	O Management Center	Configure and manage your policy from your Management Center and deploy your policy to your appliances and to WSS as enforcemen points	ıt
What policy profile	do you want to use?		
Choose the policy prof	ile that corresponds with y	your security requirements. You can fully customize your policy behavior after the On-Boarding process.	
Default Policy Profile:	<ul> <li>Monitor</li> </ul>	Protects against security threats, monitors all other traffic.	
	O Standard	Protects against security threats, adult content and illegal activity. $$\natural_{\rm f}$$	L
	O High	Protects against all Standard plus additional legal liability and security risks.	Ŧ
Cancel		Back	Next

5. Click Next.

6. Select **Suppress User/Group, Device Info, Client IP, Geolocation**. (Note: If you are planning to use this tool for network monitoring of organizational users, a less strict privacy policy may be preferable; however, for this build, we are using Web Isolation primarily for external threats.)

😣 Web Security Service - Produc	tt Sc × +				~ <b>— — </b> X
$\leftarrow$ $\rightarrow$ C $\oplus$ portal.thm	eatpulse.com				🖻 🖈 😩 📋
🛞 Web Security	Service				
System Configuration:	Privacy	_		_	
Default Policy Completed	Privacy	Mobile Users	Static Location	Auth Connector Setup	On-boarding Confirmation
<ul> <li>Default policy add</li> </ul>	led successfully.				
Configure Privac	у				
What data do you w	ant to log?				
To address privacy requi	rements, Personally Identifiable Inform	nation (PII) can be suppress	ed in access logs. Specific traffic report	ing is not available for any data th	at is suppressed.
Choose what data is colle and locations after the O		Default Privacy Setting, wh	ich applies to all traffic. You can config	ure different privacy settings for s	pecific users, groups, IPs,
Default Privacy Setting:	Suppress User/Group, Device Info, Clie	nt IP, Geolocation 🔹	Note: User, Client IP, and Geolocation r	eporting is not available with this set	ting
L				l≩	
Who can access you	ir account?				
Control whether Support	t Operators from Symantec can access	your account to assist with	troubleshooting and support.		*
Cancel					Back

- 7. Click Next.
- 8. Indicate whether you have mobile users.



9. Click Next. Indicate whether your users connect from a static location.

Security Service - Product Ser	Register Your Web Security Ser	vic ×   +			~ <u> </u>
$\leftarrow$ $\rightarrow$ C $($ portal.threatput	ulse.com				e 🖈 😩 :
left Security Set Security Set	rvice				
System Configuration: Sta	atic Location				
Default Policy Completed	Privacy Completed	Mobile Users Completed	Static Location	Auth Connector Setup	On-boarding Confirmation
Do you want to con	nect from a static loca	ition?			
Yes, my users will connect f	rom a static location.				
	R				
Cancel					Back Next

10. Click **Next**. Indicate whether you want to configure an Auth Connector.

🛞 Web Security Service - Product S	< . Register Your Web Security Ser	vic ×   +			~ <u> </u>
$\leftrightarrow$ $\rightarrow$ C $\bullet$ portal.threatput	Ilse.com				☞ ☆ 😩 :
🛞 Web Security Ser	rvice				
-					
System Configuration: Au	th Connector Setup				
Default Policy	Privacy	Mobile Users	Static Location	Auth Connector Setup	On-boarding Confirmation
Completed	Completed	Completed	Completed	Auth connector betup	on bourding commutor
Do you want to con	figure an Auth Connec	ctor to automatically in	nport Users and Gro	ups from your Active D	irectory?
Yes, I want to configure an I	Auth Connector				
		R			
Cancel					Back Next

11. Click Next.

S Web Security Service - Product S 🗙	Register Your Web Security Service	vic ×   +			~ <mark>- • ×</mark>
$\leftarrow$ $\rightarrow$ C $\bullet$ portal.threatpu	lse.com				ie 🛧 😩 :
🛞 Web Security Ser					
System Configuration: On	-boarding Confirmation				
Default Policy Completed	Privacy Completed	Mobile Users Completed	Static Location Completed	Auth Connector Setup Completed	On-boarding Confirmation
<ul> <li>Users and Groups statu</li> </ul>	us added successfully.				
You have succe	essfully completed the	on-boarding configu	ration. k		
Cancel				Bac	k Go To Product Setup

#### 12. Click Go To Product Setup.

🛞 Web Security Service - Product S 🗴 🧶 Register Your Web Security Servi 🗴 🕇 🕇		~	_	X
← → C		Ē	*	:
left web Security Service				
Product Configuration				
Products will be available for use after completion of their initial configuration. Please select a product to configure.				
Product ↓	Configuration Status	Action	Progress	5
Web Security	Configured		100%	
Protection Suite	🕌 Not Purchased			
Hosted Reporting	🕌 Not Purchased			
CASB	🞽 Not Purchased			
ha da				
			_	
Exit / Logout			Contin	ue

13. Click Continue.

# 2.2.2 Install Proxy Certificates and enabling TLS/SSL Interception

1. Click the **Policy** tab.

🚱 Web Sec	urity Servi	ce × +		<
← → C		portal.threatpulse.com/#policyConfig landin	9	iê 🛧 🔲 😩
Solution (Second Second		ecurity Service 🧧	👼 🛛 Julian S	exton Julian Sexton Admin
		icy o neral, traffic is processed top to bottom u	*Pending changes	Activate Policy
<b>u</b> <sup>2</sup>		Client	Traffic sent to WSS: Locations Agents Bypassed Traffic	
器	•	Cloud Firewall Service 🔒	Control and report on all traffic in your network	
ē	•	Authentication Policy	Configure authentication type by source and destination	
	•	Secure Web Gateway	₽ <sub>€</sub>	
1		TLS/SSL Interception*	Intercepting selected traffic	
ŵ		Threat Protection	9 rules	
ŝ		Content Filtering	5 rules	
		Proxy Restrictions	Off	
		Search Restrictions	Off	
	•	Data Loss Prevention	Block requests that contain sensitive information	
<>		CASB Gatelets 🔒	Gain visibility into and control of thousands of cloud apps and servers Link CloudSO	CASB

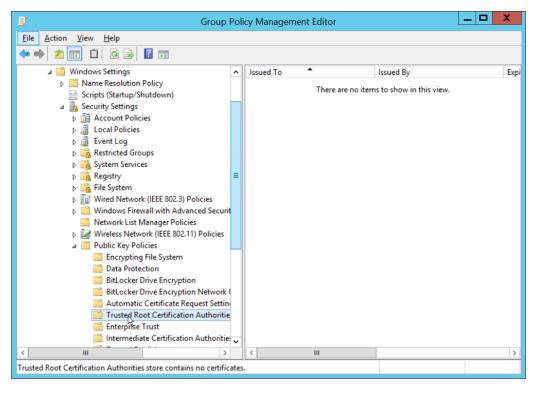
- 2. Click TLS/SSL Interception.
- 3. Enable TLS/SSL interception by clicking the toggle.

🛞 Web S	ecurity Service × +		_ <u></u>
$\leftarrow \   \rightarrow$	C  portal.threatpulse.com/#policyConfig ssl		ie 🖈 🗖 😩 i
	Web Security Service  Policy / TLS/SSL Interception ~		Julian Sexton Julian Sexton
	TLS/SSL Interception Enabling TLS/SSL Interception allows you to co encrypted traffic that is not intercepted. Enabled*	ntrol and report on encrypted traffic. Some policy, including content ana	Activate Policy
윪	TLS/SSL Interception Certificate	Install on endpoint browsers	0 •
E 1		e on all endpoint browsers in your network before enabling TLS/SSL Inte	rrception for the best end-user experience.
¢	TLS/SSL Interception Policy	5 rules	0 -
	OCSP Validation	Disabled	0 -
<>			

- 4. Download the certificate here. You can either install this individually in the Trusted Root Certification Authorities store on individual machines or follow the below steps to distribute the certificate via Group Policy.
- 5. Open the Group Policy Management Console.
- 6. Right click the **Domain** and select **Create a GPO in this domain, and Link it here...**.

Ν	ew GPO
Name: WSS Certificate	
Source Starter GPO:	¥
	OK Cancel

- 7. Enter a name and click OK.
- 8. Right click the newly created GPO and click Edit....



- 9. Navigate to Computer Configuration > Policies > Window Settings > Security Settings > Public Key Policies, and right click Trusted Root Certification Authorities.
- 10. Click Import.
- 11. Click Next.
- 12. Select the certificate you just downloaded.

	Certificate Import Wizard
Fi	le to Import
	Specify the file you want to import.
	File name:
	C:\Users\Administrator\Documents\CertEmulationCA\crt Browse
	Note: More than one certificate can be stored in a single file in the following formats:
	Personal Information Exchange- PKCS #12 (.PFX,.P12)
	Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)
	Microsoft Serialized Certificate Store (.SST)
	h.
	v

13. Click Next.

📀 😼 Certificate Import Wizard	
Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a locati the certificate.	
<ul> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store</li> </ul>	
Certificate store:	
Trusted Root Certification Authorities Brows	e
$\searrow$	
Next	Cancel

14. Click Next.

📀 🤗 Certificate Import Wizard		X
Completing the Certifi	cate Import Wizard	
The certificate will be imported after	r you click Finish.	
You have specified the following set	ttings:	
-	Trusted Root Certification Authorities	
Content File Name	Certificate C:\Users\Administrator\Documents\CertEmulationC/	4
<	III >	
	N	
	R.	
	Finish Car	ncel

- 15. Click Finish.
- 16. Click OK.

## 2.2.3 Configure Symantec Web Security Service Proxy

1. Navigate to the **Connectivity** tab.

	ectivity	Julian Sexton Julian Sexton Admin
2	Connectivity 🛛	
LI	Locations	1 location
器	Agents	Agents that send traffic to the service
æ	Setup and Configuration	R.
<u>ا</u>	Bypassed Traffic	8 domains
¢	PAC Files	Configure PAC files to facilitate Explicit Proxy and SEP connections
	WSS Agent	WSS Agent settings and installer for Windows & Mac devices
	Symantec Endpoint Security	Setup instructions for SEP with Seamless identification and agents for both iOS and Android

2. Click Locations.

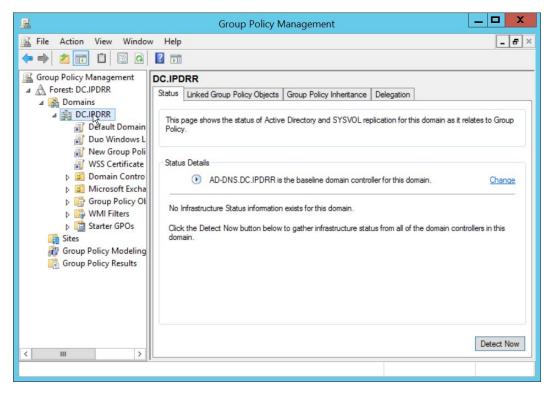
🛞 Web Se	ecurity Service × +					~	_ □	X	
$\leftrightarrow$ $\rightarrow$ (	C  portal.threatpulse.com/#connectivity location	ons				iê ☆		) E	
	Web Security Service ②				Julia	n Sexton Julian	Admin	~	
	Locations 🛛								
	In order to direct traffic from Explicit Proxy locations, please set your browser's PAC file to: https://pfms.wss.symantec.com/v1/pac?tenant=								
∎ *	+ Add Location Edit Delete	<b>2</b> Refresh 7/15/2022,	12:49:15 PM		Search			Q	
	□ Location Name ↓ IP Address / Dev	vice ID Access Method	Agent Configuration	References		Data Center Con	nections		
Æ		Explicit Proxy	Inactive	1 reference(	s)	🗢 gusas1			
l	≪ <   Page 1 of 1   >	» C				Displaying loc	ations 1 - 1	of 1	
¢									
<>									

- 3. Click Add Location.
- 4. Enter a name for the Location.
- 5. Select Proxy Forwarding for Access Method.
- 6. Enter any public IP addresses of your organization, to ensure that traffic sent through the WSS (Web Security Service) proxy is redirected to the proper dashboard.

	Security Service	× + threatpulse.com/#connectivity/locations			<ul> <li>-□ ×</li> <li></li></ul>
	Web Sect	Add Location 🛛			Julian Sexton 🗸
	Location	Location Name: * DC IPDRR	Estimated Users: 🍁	Less than 50 👻	
ū	http:	Access Method: * Proxy Forwarding 👻	Country: 🛊	United States 👻	
	+ Add	Proxy Forwarding	Time Zone: 🍁	Eastern Time (America/New_Yc 🛛 💌	Q
쁆	Local	We've noticed that your IP address is:	Address Line 1:		er Connections
Æ		IP Address:	Address Line 2:		ar connections
E	~	Agent Configuration	Zip / Postal Code:		/ing locations 1 - 1 of 1
¢		The following options require WSS Agent v7.x or higher Keep agents active at this location	Comments:		
		Selective intercept ()		255 of 255 characters left	
<>				Cancel Save	

7. Click Save.

- This page will now provide a URL to a PAC file that can be distributed to browsers across the organization via GPO. If you wish to create a custom PAC file, you can navigate to Connectivity > PAC Files.
- 9. Open the Group Policy Management Console.



10. Right click the Domain and select Create a GPO in this domain, and Link it here....

	New GPO	X
Name: WSS Proxy		
Source Starter GPO: (none)		~
	OK Cance	el

11. Enter a name and click OK.

<u>E</u>	Group Policy Manageme	ent		_ 🗆 🗙
🔜 File Action View Window	/ Help			- 8 ×
Group Policy Management ▲ ▲ Forest: DC.IPDRR ▲ ▲ Domains ▲ ➡ Domains ▲ ➡ DC.IPDRR ➡ Default Domain ➡ Duo Windows L	WSS Proxy           Scope         Details         Settings         Delegation           Links         Display links in this location:         DC.IPDRR           The following sites, domains, and OUs are linked to         Display links in this location:         DC.IPDRR			~
WSS Certificate	Location  DC.IPDRR	Enforced No	Link Enabled Yes	Path DC.IPDRR
<ul> <li>Image: Second Sec</li></ul>	Security Filtering The settings in this GPO can only apply to the follow Name	wing groups, use	ers, and computers:	×
द्धि Sites 波 Group Policy Modeling 武 Group Policy Results	Add Remove	Properties		
< III >	WMI Filtering This GPO is linked to the following WMI filter: <pre></pre>	~	Open	

- 12. Right click the newly created GPO and click Edit....
- 13. Navigate to User Configuration > Preferences > Control Panel Settings.

<u>I</u>	Group Policy M	lana	gement Ed	litor			_	X
File Action View Help								
🧇 🏟 🖄 🗊 🖥 🗐 👼 🧔	🗟 🚺 🖬 🗟 🛇 🕇							
WSS Proxy [AD-DNS.DC.IPDRR]     ▲	🏘 Internet	Se	etting	gs				
			Name	Or	der			
<ul> <li>K. User Configuration</li> <li>Policies</li> <li>Preferences</li> <li>Windows Settings</li> <li>Control Panel Setting</li> <li>Data Sources</li> <li>Devices</li> <li>Folder Options</li> <li>Folder Options</li> <li>Local Users and C</li> <li>Network Options</li> <li>Power Options</li> <li>Printers</li> <li>Regional Options</li> <li>Scheduled Tasks</li> <li>Start Menu</li> </ul>	Processing 2	3		There are no i	items t	to show in this vie	w.	
< III >	Preferences (Extended ) Stand	lard J	/					
Internet Settings	<u>/</u> /							

- 14. Right click Internet Settings and select New > Internet Explorer 10 Properties.
- 15. Click the Connections Tab.

	ms	Advanced		Common
General	Security	Privacy	Conten	t Connections
Sei	tup.	met connection, Network settings		Setup
				Add
				Add VPN
				Remove
	ttings if you nee	ed to configure a	proxy	Settings
	dial a connectio	n		
Dial wh	enever a netwo	ork connection is	not prese	nt
Always	dial my default	t connection		
Current	None			Set default
	Network (LAN) :	settings		LAN settings
LAN Settin		/ to dial-up conne or dial-up setting		Chitactunga

16. Click Local Area Network (LAN Settings).

Local Area Network (LAN) Settings
Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings Use automatic configuration script Address:
Proxy server Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections). Address: Port: Advanced
Bypass proxy server for local addresses OK Cancel
OK Cancel

- 17. Select the **Address** field.
- 18. Press **F6** to enable it (it is enabled if the box has a solid green underline.
- 19. Enter the PAC file URL from earlier in the **Address** field.

Local Area Network (LAN) Settings
Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings Use automatic configuration script Address: https://pfms.lwss.symantec.com/v1/pac:
Proxy server Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections). Address: Port: Advanced Bypass proxy server for local addresses
OK Cancel

#### 20. Click **OK**.

	New Inter	net Explorer	10 Prop	erties X
Progra	ms	Advanced		Common
General	Security	Privacy	Conten	t Connections
Set	up.	rnet connection, Network settings		Setup
				Add
				Add VPN Remove
	tings if you ne connection.	ed to configure a	proxy	Settings
O Never of	lial a connectio	n		
Dial who	enever a netw	ork connection is	not preser	nt
Always	dial my defaul	t connection		
Current	None			Set default
	letwork (LAN)	settings		LAN settings
		y to dial-up conne or dial-up setting:		
	ок	Cancel	Ар	ply Help

- 21. Click OK.
- 22. To verify that traffic is going through Isolation, you can visit the following test website, and substitute 1-10 for the threat level: <u>http://testrating.webfilter.bluecoat.com/threatrisk/level/7</u>.

$\leftarrow$	$\rightarrow$ C	0.8	estrating.webfilter.bluecoat.com/threatrisk/level/1					ជ			) =
`	- 4		can any second control and any second					3		0	
	🗹 Sy	mantec.									
	A Div	vision of Broadcom									
	То	at Datin									
	IE	st Ratin	iy								
	This is	s a Symantec test ra	ting page with a threat risk level of								
	1 - \	Very Safe									
	Top vi	eited sites with long	history of good behavior								
	TOP VI	sited sites with long	history of good benavior								
	Inspector	Console Debugger	Network {} Style Editor	ory 🗄 Storage 🕇	Accessibility	BBB Application			9 9	Û	•••
	Filter URLs		11 + Q	All HTML CSS	S JS XHR	Fonts Images Media W	S Other	Disable C	ache No Th	rottling	•
tus	Method	Domain	File	Initiator	Туре	Transferred	Size	0 ms	80 ms	160 r	ms
0	GET	🔏 testrating.webfilter.blu	1	document	html	12.42 KB	12.16 KB	16 ms			
9	GET	🔏 testrating.webfilter.blu	analytics.js	script	js	cached	409 B		0 ms		
0	GET	Ø www.google-analyt		script	js	cached	45.19 KB		0 ms		
3	GET	K testrating.webfilter.blu		img	xml	cached	116 B		0 ms		
3	GET		96f62f549352cef6d2fb7c71ac9133d0.woff	font	xml	456 B	142 B		16 ms		
			8fb10297f2a424aad242e8813d159cb0.woff		xml		142 B			-	
8	GET		_utm.gif?utmwv=5.7.2&utms=2&utmn=697801032&utmhn=testrat	font	gif	619 B 455 B	35 B 141 B		16	ms 16 ms	
9 4	GET		98b25ed8f8a57633895435395edf05d4.ttf 482f0f1dd35ec8ec8ee38fcad322d6f1.ttf	font	xml	455 B	141 B		_	16 ms	
3	GEI	M testrating.webhiter.blu	4821011dd35ec8ec8ec8ec88tcad322db11.ttf	tont	xml	455 B	141 8			15 ms	5
	ſ	.45 KB / 14.80 KB transferred	Finish: 156 ms   DOMContentLoaded: 59 ms   load: 167 ms						L	_   🗖	1
	ſ	webfilter.bluecoat.cor × -	+ estrating.webfilter <b>bluecoat.com</b> /threatrisk/level/7	ocurity los				☆		<b>- -</b>	
	testrating.	webfilter.bluecoat.co × -	estrating webfilter bluecoat.com/threatrisk/level/7 I Not Connect: Potential S a detected a potential security threat and did not cont e requires a secure connection. can you do about it? sue is most likely with the website, and there is nothing are on a corporate network or using anti-virus software.	tinue to isolation-ins ng you can do to rese re, you can reach ou	stances.wss. olve it.			\$2			
<b>)</b>	testrating.	webfilter.bluecoat.co × -	estrating webfilter bluecoat.com/threatrisk/level/7 Standard Connect: Potential Standard and the standard stan	tinue to isolation-ins ng you can do to rese re, you can reach ou	stances.wss. olve it.			쇼	L		
•	testrating A	webfilter.bluecoat.co ×	testrating, webfilter bluecoat.com/threatrisk/level/7 testrating, webfilter Or Performance Or Mem	inue to isolation-ins ng you can do to reso re, you can reach ou oblem. ory 🔁 Storage 🕇	stances.wss. olve it.		ance.			0	9
	testrating.   testrating.    testrating.    testrating.   testrating.   testrating.   testrating.   testrating. testrating.testrating. testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testrating.testratin	webfilter.bluecoat.co ×	testrating.webfilter.bluecoat.com/threatrisk/level/7 testrating.webfilter.bluecoat.com/testrating.webfilter.bluecoat.com/testrating.webfilter.bluecoat.com/testrating.webfilter.bluecoat.com/testrating.webfilter.bluecoat.com/testrating.webfilter.bluecoat.com/testrating.webfilter.bluecoat.com/testrating.bluecoat.com/testrat	inue to isolation-ins ng you can do to ress re, you can reach ou oblem. ary estronge t All HTML css	olve it. Accessibility	pport teams for assista	/S Other [	] Disable 0	Cache No Ti	C	D   9 \$
	testrating x     ∴	webfilter.bluecoat.co: X =	estrating webfilter bluecoat.com/threatrisk/level/7 A Not Connect: Potential S c detected a potential security threat and did not cont e requires a secure connection. can you do about it? sue is most likely with the website, and there is nothir are on a corporate network or using anti-virus softwa n also notify the website's administrator about the pr motor N Network ① Style Editor @ Performance ① Mem III + @ File	inue to isolation-ins ag you can do to resu re, you can reach ou oblem. ary Storage <b>†</b> <b>O</b> All HTML CS Initiator	olve it. Accessibility s JS XHR Type	pport teams for assista	/S Other [ Size		Cache No Ti 320 m	0	D   9 \$
	testrating.     ∴	webfilter:bluecoat.co × webfilter:bluecoat.co ×	estrating.webfilter.bluecoat.com/threatrisk/level/7 estrating.webfilter.bluecoat.com/threatrisk/level/7 Not Connect: Potential S c detected a potential security threat and did not cont e requires a secure connection. can you do about it? sue is most likely with the website, and there is nothir are on a corporate network or using anti-virus softwa are on a corporate ne	inue to isolation-ins Ing you can do to ress re, you can do to ress re, you can areach ou oblem. ory Storage Tr Storage Tr Mark HTML CSS Mark HTML HTML CSS Mark HTML HTML CSS Mark HTML HTML HTML CSS Mark HTML HTML HTML HTML HTML HTML HTML HTML	olve it. Accessibility	poport teams for assista     Application     Fonts Images Media W     Transferred     36.61 K8	/S Other [ Size 35.47 KB	] Disable 0	Cache No Ti 320 ms	C Interesting	D   g¢
	testrating A	webfilter.bluecoat.cor × webfilter.bluecoat.cor ×	t  estrating webfilter bluecoat.com/threatrisk/level/7 estrating webfilter bluecoat.com/threatrisk/level/7 estrating webfilter bluecoat.com/threatrisk/level/7 estrational security threat and did not cont e requires a secure connection. can you do about it? sue is most likely with the website, and there is nothir are on a corporate network or using anti-virus softwa are on a corporate network or using are on a corporate n	inue to isolation-ins Ing you can do to reso re, you can reach ou oblem. ory Storage * Mi HTML CSS Instator document 6 uoigt	olve it. Accessibility s JS XHR Type	pport teams for assistance of the second sec	/S Other [ Size 35.47 KB 0 B	] Disable 0	Cache No Ti 320 ma 312 ma	C 1	D   g¢
	testrating X	webfilter.bluecoat.cor × webfilter.bluecoat.cor × Dic Firefor websit What The is: If you You ce Console Debugger Domain Sconsole Debugger Domain Sisolation-inflances.vs Sisolation-inflances.vs	estrating webfilter bluecoat.com/threatrisk/level/7 estrating webfilter bluecoat.com/threatrisk/level/7 estrating webfilter bluecoat.com/threatrisk/level/7 estration accord a potential security threat and did not context erequires a secure connection. can you do about if? sue is most likely with the website, and there is nothir are on a corporate network or using anti-virus softwa n also notify the website's administrator about the pr motor  N Network () Style Editor () Performance () Mem III + Q File 7 basesabatonyibver11554+386299059579bac2095342a7720182 dagrostica/tver11554+386	inue to isolation-ins g you can do to ress re, you can reach ou oblem. ory E Storage T Ministor document 0 cropt 7.7 (sorpt)	olve it. Accessibility s JS XHR Type	Ppport teams for assistation Fonts Images Media W Transferred 3.6.61 KB 0.8 0.8	ANCE. /S Other [ Size 35.47 KB 0 B 0 B	] Disable 0	Cache No Ti 320 m 312 ms	Ti ms	D   9 \$
tus	➡ testrating.x → C ■ Inspector ♥ Filter URLS Method GET GET	webfilter:bluecoat.co × Webfilter:bluecoat.co × Dic & 1 Firefor Websil What The is: If you Console Debugger Dornain K testrating.webfilter.blu B isolation-instances.w B isolation-instances.w B isolation-instances.w	estrating.webfilter.bluecoat.com/threatrisk/level/7 estrating.webfilter.bluecoat.com/threatrisk/level/7 Not Connect: Potential S cdetected a potential security threat and did not cont e requires a secure connection. can you do about it? sue is most likely with the website, and there is nothir are on a corporate network or using anti-virus softwa an also notify the website's administrator about the p notor notor N Network () Style Editor () Performance () Mem III + Q Fie 7 base-sadonjklver=1.15.54+386.29059579bos2095342a7720182 diagnostics/lytver=1.15.54+386.	inue to isolation-ins gyou can do to ress re, you can reach ou oblem. Stanger tr document 77 (scrept) 77 (scrept)	stances.wss.	Popport teams for assista     Application     Fonts Images Media W     Transferred     36.61 K8     0 8     0 8     0 8	AS Other [ Size 35.47 KB 0 B 0 B	] Disable 0	Cache No Ti 320 m 312 m	C 1	D   g¢
2 1 1 2 3	testrating A	<ul> <li>webfilter.bluecoat.cor ×</li> <li>Nebfilter.bluecoat.cor ×</li> <li>Nebfilter.bluecoat.cor ×</li> <li>Dictor</li> <li>Fireforio</li> <li>websit</li> <li>What</li> <li>The iso</li> <li>Hyou</li> <li>Console</li> <li>Debugger</li> <li>Console</li> <li>Debugger</li> <li>Console</li> <li>Debugger</li> <li>Console</li> <li>Debugger</li> <li>Console</li> <li>Debugger</li> <li>Domain</li> <li>isolation-instances.vs</li> <li>isolation-instances.vs</li> <li>isolation-instances.vs</li> <li>isolation-instances.vs</li> </ul>	+ estrating, webfilter bluecoat.com/threatrisk/level/7  A Not Connect: Potential S c detected a potential security threat and did not cont is requires a secure connection. can you do about it? sue is most likely with the website, and there is nothir are on a corporate network or using anti-virus softwa n also notify the website's administrator about the pr more	inue to isolation-ins ag you can do to resu oblem. ary Storage T Nall HTML CSS Initiator document 0 sorigt 7.7 (scrept) 7.7 (scrept) 7.7 (scrept)	Accessibility S JS XHR Type html	Popport teams for assistance     Application     Fonts Images Media W     Transferred     S661 K8     O 8     O 8     O 8     O 8     Cached	XS Other [ Sce 5.47 KB 0 B 0 B 0 B 0 B 0 B 0 B	] Disable 0	Cache No T 320 mp 912 m 0 m	71 ms 79 ms 5	0
?	➡ testrating.x → C ■ Inspector ♥ Filter URLS Method GET GET	webfilter.bluecoat.cor × webfilter.bluecoat.cor ×		inue to isolation-ins ng you can do to ress re, you can reach ou oblem. ory E Storage T Mail HTML CSS Initiator document 77 (script) 77 (script) 77 (script) 77 (script)	stances.wss.	Popport teams for assista     Application     Fonts Images Media W     Transferred     36.61 K8     0 8     0 8     0 8	AS Other [ Size 35.47 KB 0 B 0 B	] Disable 0	Cache No Ti 320 m 312 m	71 ms 79 ms 5	D   g¢
tus	➡ testrating.X → C ■ Inspector ▼ Filter URLS Method GET GET GET	webfilter:bluecoat.co × Webfilter:bluecoat.co × Dic 2 at Firefor  websit What The is: If you Console Debugger Console Debugger Dornain K testrating webfiter:blu K isolation-instances.w K isolation-instances.w	+ estrating, webfilter bluecoat.com/threatrisk/level/7  A Not Connect: Potential S c detected a potential security threat and did not cont is requires a secure connection. can you do about it? sue is most likely with the website, and there is nothir are on a corporate network or using anti-virus softwa n also notify the website's administrator about the pr more	inue to isolation-ins ag you can do to resu oblem. ary Storage T Nall HTML CSS Initiator document 0 sorigt 7.7 (scrept) 7.7 (scrept) 7.7 (scrept)	Accessibility S JS XHR Type html	Popport teams for assistation  Forts Images Media W  Transferred  3661 K8  08  08  08  08  08  08  08  08  08	XS Other [ Sze 35.47 KB 0 B 0 B 168.25 KB	] Disable 0	Cache No T 320 mp 912 m 0 m	71 ms 79 ms 5	D   9 \$

23. On this test URL (tested July 2022), levels 5-7 will go through isolation, and you will be able to see the isolation traffic from the network tab in developer mode (F12) on the browser. Levels 8-10 will be blocked by the content filter, and levels 1-4 will not go through isolation or content filtering.

#### **2.3 PKWARE PKProtect**

This installation and configuration guide for PKWARE PKProtect uses a physical PKWARE server, and as such will not delve into the installation of server components. In this guide, PKWARE is used to automatically perform data inventory and data protection functions. PKWARE provides users with the ability to store encrypted files for retrieval later, requiring the use of user credentials to access them.

#### 2.3.1 Configure PKWARE with Active Directory

1. Login to the PKWARE web portal using the administrative credentials.

🖻 🖅 🗖 Login	$\times$ + $\sim$ $>$			-		×
$\leftrightarrow$ $\rightarrow$ $\circlearrowright$ $\textcircled{a}$	Certificate error https://192.168.1.43/mds/SuperUser/Login	□ ☆	դ≞	h	Ŀ	
PKWA	D <b>E</b> *					Help
PAVA						
Authorization R	equired					
	Username:					
	Password:					
	Login					
	PKWARE Enterprise Manager 18.5.203 - <u>About</u> - pkwarevm 8/20/20 11:00:04 AM					
	TRANSE Encloses manager roundor - <u>maxim</u> - paracerin of each - indoles an					

- 2. Once logged in, you can and should change the password to this administrative account by clicking Change Password in the top right corner.
- 3. Navigate to System > Domain.

E +5 System - Domain X + ✓		-	□ ×
← → Ů ŵ 🔺 Certificate error https://192.168.1.43/mds/SuperUser/System/Domain	∿≡	h	ie
DEALA DE Actions			Help
PKWARE       Actions * System Basics Advanced         Dashboard Archive Events       1			Log out Change
Status Database Elasticsearch Network			Password
Domain SNMP SSL Package Log			
Domain			
This system is not currently joined to a domain Join Domain			
PKWARE Enterprise Manager 18.5.203 - <u>About</u> - pkwarevm 8/20/20 11:02:01 AM			

- 4. Click Join Domain.
- 5. Enter the Kerberos Realm, NetBIOS Domain, as well as the username and password of an administrative user on the domain.

E System - Domain × + ~			-	
- → ♡ ⋒ ▲ Certificate error https://192	.168.1.43/mds/SuperUser/System/Domain	□ ☆	t≡ l~	. <i>ie</i>
Actions	System Basics Advanced			Help
PKWARE <sup>®</sup> Actions <sup>®</sup> Dashboa	rd Archive Events			Log out
				Change Password
	Database Elasticsearch Network			Password
Domain	SNMP SSL Package Log			
Join Windows Domain				
Kerberos Realm	dc.ipdrr			
NetBIOS Domain	dc			
User	Administator			
Password				
Password				
	Debug Output			
	Join Domain Cancel	L.	D	
PKWARE Enter	prise Manager 18.5.203 • About • pkwarevm 8/20/20 11:02:01 AM			

6. Click Join Domain.

#### 2.3.2 Create a New Administrative User

1. Navigate to Advanced > Admins.

							Search:	
Username/UPN		Type 🔅	Role 🕴	MFA	API 🕴	Last API 🕴	Last Login	
Ultimate Sys Admin		Local User	Super Sys Admin	n/a	n/a	n/a	n/a	
Administrator@DC.IP	DRR	Domain User	Super Sys Admin	No	No	(never)	2/10/21 12:47:00 PM	Edit EnableAPI Delete
			PKWARE Ente	nprise Manager 18.5.203	- <u>About</u> - pikwarevm 2/10	0/21 2/45/12 PM		

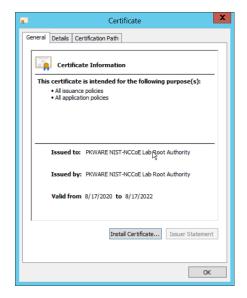
- 2. Click Add Domain User.
- 3. Enter the username of a user on the domain that should be able to login through the PKWARE management portal (this is meant for administrators only).
- 4. Select the level of permissions the user should have.

S Advanced - Admins	x m Discovery x +	_ 🗆 X
← → C ▲ Not secure	192.168.1.43/mds/SuperUser/Advanced/Admins	🖈 🛛 Update 🔅
<b>PKWARE</b> "	Actions System Basics Advanced Dashboard Archive Events Licenses Admins Data Center Cluster MFA Performance Reports	Help Log out Change Password
Add Domain User		
	Domain User Administratore (Administratore DC LPOBD) Role Security Admin  Save Cancel	
	PRIAR Entropole Vanger 16.303 - <u>doog</u> - staatem 2/1021 2-6512 PK	

5. Click Save.

#### 2.3.3 Install Prerequisites

- 1. If needed for your environment, you may need to install certificates locally before agents can connect to PKProtect ask your PKWARE representative if this is necessary for your environment.
- 2. Double click the certificate you wish to install.



- 3. Click Install Certificate...
- 4. Select Current User.



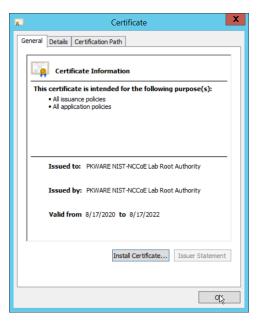
- 5. Click Next.
- 6. Click Browse.
- 7. Select Trusted Root Certification Authorities.

	X
Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store	
Certificate store: Trusted Root Certification Authorities Browse	
Next Cancel	

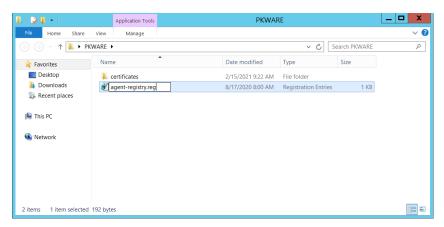
8. Click Next.



9. Click Finish.



- 10. Click **OK.**
- 11. Repeat steps 1 through 10 but select Personal instead of Trusted Root Certification Authorities.
- 12. Repeat steps 1 through 11 for each certificate that needs to be installed.



- 13. Rename agent-registry.txt to agent-registry.reg.
- 14. Double click the file (must have administrator privileges).



15. Click Yes.



- 16. Click OK.
- 17. Restart the machine to apply these changes.

#### 2.3.4 Install the PKProtect Agent

1. Run the PKProtect Installation executable.

🔂 Smartcry	ot 16.40.0010 - InstallShield Wizard
	Welcome to the InstallShield Wizard for Smartcrypt 16.40.0010
4	The InstallShield(R) Wizard will install Smartcrypt 16.40.0010 on your computer. To continue, click Next.
	WARNING: This program is protected by copyright law and international treaties.
	< Back Next > Cancel

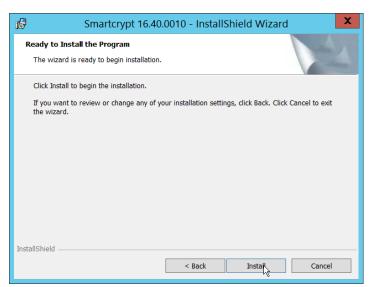
- 2. Click Next.
- 3. Select I accept the terms in the license agreement.

B Smartcrypt 16.40.0010 - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
PKWARE, INC.
PKWARE LICENSE AGREEMENT
(Software Subscription/ Products)
This PKWARE Agreement ("Agreement") is made by and between Licensor and Licensee, as defined below. This Agreement governs the subscription licensing of Software, the sale of Products and the provision of services related to the Licensor's PKWARE solution. For perpetual license terms for PKWARE software, visit https://legal.pkware.com.
BY ACCESSING, USING, OR INSTALLING ALL OR ANY PART OF THE SOFTWARE, PRODUCTS, OR SERVICES AS APPLICABLE, LICENSEE EXPRESSLY AGREES TO AND CONSENTS TO BE BOUND BY ALL OF THE TERMS OF THIS AGREEMENT. INCLUSIVE OF ALL SCHEDULES AND EXHIBITS HERETO. IF
• I accept the terms in the license agreement
$\bigcirc$ I do not accept the terms in the license agreement
InstallShield
< Back Next Cancel

- 4. Click Next.
- 5. Select Typical.

18	Smartcrypt 16.40.0010 - InstallShield Wizard
Setup Type Choose the s	etup type that best suits your needs.
Please select	a setup type.
• Typical	All program features will be installed. (Requires the most disk space.)
O Custom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield ——	< Back Next > Cancel

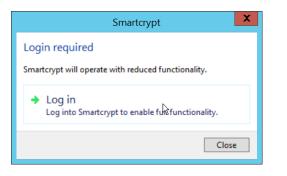
6. Click Next.



7. Click Install.

🔂 Smartcryp	t 16.40.0010 - InstallShield Wizard
	InstallShield Wizard Completed
A	The InstallShield Wizard has successfully installed Smartcrypt 16.40.0010.
	< Back Finish Cancel

8. Click Finish.



- 9. If a window to login is not automatically shown, you can right click the PKProtect icon in the Windows taskbar and click Login.... If a window is automatically shown, click Log in.
- 10. Login using the username of the account in the domain, in email format (such as administrator@domain.id).

8	Smartcrypt: Smartcrypt Manager Entry
Enter the	address of your Smartcrypt Manager:
https://p	kwarevm.dc.ipdrr/mds
	k,
	OK Cancel

- 11. Enter the address of the PKWARE server.
- 12. The PKWARE agent will now run in the background.

#### 2.3.5 Configure Discovery and Reporting

1. On the PKWARE dashboard, log in as an administrative user, and navigate to **Archive > Discov**ery.

- C	A Not secure   192.168.1.43/mds/5			
ЖИ		em Basics Advanced Dashboard Archive Events		Help Log Change Passw
	Fonces Disc	Remediations Classification Communities Assignments Lockers Accounts		
	Deployments	Devices Reporting Support		
mart Filte	er Bundles			
			Search:	۵
Туре 🔺	Filter Name	Bundle Patterns		
Discovery	HIPAA - Diagnosis Lexicon and	Social Security Number US (1 or more)	Drugs Dictionary (5 or more)	Edit Clone Delete
Discovery	Social Security Numbers	FDA Firms Dictionary (5 or more) CD-9 Codes Dictionary (5 or more) CD-10 Codes Dictionary (5 or more)	ctionary (5 or more)	Lui Cione Delete
Discoverv	PCI-DSS - Credit Cards and Social	All Supported Credit Cards (1 or more)	Social Security Number US (1 or more)	Edit Clone Delete
biscovery	Security Numbers	National Insurance Number UK (1 or more)		Lan shore exists
Discovery	Personally Identifiable Information	Social Security Number US (1 or more)	ID US (1 or more) Address US (10 or more)	Edit Clone Delete
howing 1 to	o 3 of 3 entries			
Add Biscove	ery Add Redaction Patterns Ir	mport Bundle Pack Export Bundle Pack		
iscovery	Global Settings			
	gent Scanning Priority Low			
Version	Detection Time Frame (Days) 1			

- 2. Click Add Discovery.
- 3. Enter a name for the discovery rule.
- 4. Select a pattern for the rule to discover. In this case, we are setting up a rule to detect social security numbers in files for reporting/remediation.
- 5. The Threshold field refers to how many of those patterns must be present in a document for the rule to be applied.

S Archive - Discovery	x an Discovery x   +	_ <b>D</b> X
$\leftarrow \rightarrow C $ A Not	t secure   192.168.1.43/mds/SuperUser/Archive/Discovery	🖈 🛛 Update 🔅
PKWAI	Actions System Basics Advanced Dashboard Archive Events Policies Discovery Remediations Classification Communities Assignments Lockers Accounts Deployments Devices Reporting Support	Help Log out Change Password
Discovery Smart		
	Filter Name SSN Discovery	
Pattern Social Security Number	rus v 1 -	
Add	k	
Exclusions		
	Patterns	
Inclusions		
	Patterns	
Save Cancel		
	POURAE Enterprise Manager 15.523 - <u>About</u> - pisaeterin 2/10/1 22036 PM	

- 6. Click Save.
- 7. Navigate to **Archive > Remediations.**

S Archive - Remediations	× an Discovery >	<   +	
← → C ▲ Not se	cure   192.168.1.43/mds/SuperUser/Archive/Re	emediations	☆ 😫 Update 🔋
PKWAR	Actions System Basics Advance     Policies Discovery Remediation:     Deployments Devices Reporting	Classification Communities Assignments Lockers Accounts	Help Log out Change Password
Remediation Action	s		
None Add	D <sub>6</sub>		
		POINAE Enterprise Manager 183.203 - <u>About</u> - privareum 2/10/21 22753 PM	

- 8. Click Add.
- 9. Enter a name for the remediation.

S Archive - Remediations	x 🖬 Discovery x   +	_ <b>_</b> X
← → C ▲ Not secur	e 192.168.1.43/mds/SuperUser/Archive/Remediations	🖈 😫 Update 🔅
PKWARE	Actions System Basics Advanced Dashboard Archive Events Searching – Policies Discovery Remediations Classification Communities Assignments Lockers Accounts Deployments Devices Reporting Support	Help Log out Change Password
Remediation Action		
	Report and Encrypt	
Comment		
	Report Discovery Events      Froypt      Report Successful Encryptions     Report Encryption Failures      Algorithm ASS (256-bit)      Key(s)      This list is prioritized from left to right. The first key a user has access to will be used for encryption operations.     If a user does not have access to any of the keys in the list, their Personal Smartkey will be used.      Classify     Before you can use redaction, you must add at least one Redaction Smart Filter Bundle      Delete     Do Nothing	
Pre Command 🗟		
Command	□ Ignore Filesystem Events	ĥ
Post Command		

- 10. Check the box next to Report Discovery Events.
- 11. Check the box next to Encrypt.
- 12. Ensure that AES (256-bit) is selected.
- 13. Click Save.

			ties Assignments Lockers Accounts		Change Pas
emediation Actions					
Name		Comment	Types	Search:	
Report and Encrypt	R.		Report, Encrypt	(none)	Edit Delete
Add		POWARE Ero	erprise Manager 18.5.203 - <u>About</u> - pixearevin 2/10/21 2:2947 PM		

14. Navigate to Archive > Assignments.

S Archive - A	ssignments 🗙 📾	Discovery	×   +						
- > G	A Not secure   192.168	.1.43/mds/SuperUser/Arch	ive/Assignments						☆ 😫 Update
PKV		tions System Basics Ac licies Discovery Remedi ployments Devices Rep	ations Classificati		Events hities Assignments Lockers Accounts				Help Log o Change Passwo
Assignments									
							Sear	ch:	•
Order 🔺	Name	Users / Groups	Platform	Mode	Locations	Re- Encryption	Compliant	Not Compliant	
≡ 1	Domain Users Desktop Encrypt	Domain Users [DC.IPDRR]	Windows	Encrypt	\${USERPROFILE}\Desktop\Encrypt	Disabled	1	٥	Status Edit Reset Delete Disable
Showing 1 t	to 1 of 1 entries								
Add									
				PKWARE I	nterprise Manager 18.5.203 - <u>About</u> - pixwarevm 2/10/21 2:29:5	5 PM			

15. Click Add.

S Archive - Assignments × an C	Discovery X +	_ 0
→ C 🔺 Not secure   192.168.1.	43/mds/SuperUser/Archive/Assignments	🖈 🕒 Update
PKWARE	ns System Basics Advanced Dashboard Archive Events les Discovery Remediations Classification Communities Assignments Lockers Accounts organets Devices Reporting Support	Help Log out Change Password
Assignment		
Name	Report and Encrypt SSN	
Platform	Windows	
Mode	Discovery	
Users / Groups	Domain Users [DC.IPDRR]	
Local Path(s)	\$(USERPROFILE)	
Whitelist		
Blacklist	SKAVPOATAYL SKLOCALAPPOATAYL *.acm *aii *.axii *.bmp *dli *.aps *.exe *.thv *.indd *.jpg *.git *.mov *.mp3 *.mp4 *.png *.pid *.pat *.axi *.tmp *.xxxv	w *.ocx *.ost
~	Enable Scan-Only Mode	
	Scan-only mode disables the local file system watcher in the Agent.	
	Instead of reacting to real-time file system events, the Agent will perform traditional folder scans.	
	Agents earlier than 16.30 do not support scan-only mode.	
Sweep Interval (seconds)	36001 Zeport Compliance and Status	
	Report Advanced File Attributes	
	Z Exclude Hidden Files	
	Z Exclude System Files	
Remediation Actions		

- 16. Enter a name for the Assignment.
- 17. Select the Platform for this assignment to run on.
- 18. Select Discovery for the Mode.
- 19. Enter the names of the Active Directory users or groups this rule should apply to.
- 20. Enter the folders for this rule to search in Local Paths.
- 21. Use Whitelist and Blacklist to specify file types that should or should not be considered.
- 22. Enter the interval for this rule to run in Sweep Interval.

S Archive - Assignments X	)iscovery ×   +		_ <b>D</b> X
← → C ▲ Not secure   192.168.1.	43/mds/SuperUser/Archive/Assignments		☆ \varTheta (Update :
Whitelist			
Blacklist	\$(APPDATA)\* \$(LOCALAPPDATA)\* *.acm *.ai *.avi *.bmp *.dll *.e *.tmp *.wav	ps ".exe ".flv ".indd ".jpg ".jpg ".gif ".mov ".mp3 ".mp4 ".png ".psd ".pst ".raw ".o	cx *.ost
	Enable Scan-Only Mode		
	Scan-only mode disables the local file system watcher in the Agent.		
	Instead of reacting to real-time file system events, the Agent will per	form traditional folder scans.	
	Agents earlier than 16.30 do not support scan-only mode.		
Sweep Interval (seconds)	3600		
	Report Compliance and Status		
	Report Advanced File Attributes		
	Z Exclude Hidden Files		
	Exclude System Files		
Remediation Actions Smart Filter Bun	dles	Remediation Action	
	No data avail	able in table	
Showing 0 to 0 of 0 entries			
Agents earlier than 15 70 will only use th	ne first Remediation Action shown above		
	le inst vernediation Action shown above		
Attd			
Save Cancel			
	PKWARE Enterprise Manager 18.5.203 -	About - okwarevm 2/10/21 2:29:55 PM	

- 23. Under Remediation Actions, click Add.
- 24. Select the Discovery rule created earlier under Smart Filter Bundles.

25. Select the Remediation Action created earlier under Remediation Action.

S Archive - Assignments × 🚥 🕻	iscovery x   +		_ <b>D</b> X
← → C ▲ Not secure   192.168.1.	43/mds/SuperUser/Archive/Assignments		🖈 \varTheta (Update :)
Local Path(s)	\$(USERPROFILE)		
Whitelist			
Blacklist		peg *.gif *.mov *.mp3 *.mp4 *.png *.psd *.pst *.rav	v *.ocx *.ost
	tmp *way     Denable Scan-Only Mode		
	Scan-only mode disables the local file system watcher in the Agent.		
	Instead of reacting to real-time file system events, the Agent will perform traditional folder scans.		
	Agents earlier than 16.30 do not support scan-only mode.		
Sweep Interval (seconds)	3600		
	Report Compliance and Status		
	Report Advanced File Attributes		
	Zexclude Hidden Files		
	Z Exclude System Files		
Remediation Actions			
Smart Filter Bundles		Remediation Action	
SSN Discovery	4	Report and Encrypt	Delete
Showing 1 to 1 of 1 entries			
Add			
Save Cancel			
	PKWARE Enterprise Manager 18.5.203 - <u>About</u> - pixwarevm 2/10/21 2:29:55 PM		-

#### 26. Click Save.

27. This rule will now run automatically, reporting and encrypting files that match its discovery conditions.

### 2.4 StrongKey Tellaro

StrongKey is a Representational State Transfer (REST) Application Programming Interface (API) providing various security services. In this project, we primarily make use of its file encryption capabilities in the context of data protection. Because it is a web service, there is not much installation required on the enterprise side, and the bulk of the setup is acquiring credentials to communicate safely with the API. In this build, Strongkey will primarily be used for integration with other products, to encrypt sensitive data generated by products in formats that may be otherwise difficult to encrypt.

## 2.4.1 Python Client for StrongKey – Windows Executable Creation and Use

- 1. Ensure that the following script (see end of section) is filled out with information specific to your enterprise, including the variables skdid, skuser, and skpass.
- 2. Save the file as strongkey-client.py.
- This example will demonstrate how to create an executable from the script below. Download Python 3.8.0 from the Python website: https://www.python.org/downloads/release/python-380/. Specifically, download the Windows x86 executable installer. The 32-bit version will provide better access to Active Directory packages and interfaces.
- 4. Run the installer.
- 5. Check the box next to Add Python 3.8 to PATH.



6. Click Install Now.

\$	Python 3.8.0 (32-bit) Setup
	Setup was successful
2	Special thanks to Mark Hammond, without whose years of freely shared Windows expertise, Python for Windows would still be Python for DOS. New to Python? Start with the <u>online tutorial</u> and <u>documentation</u> .
-	See <u>what's new</u> in this release.
python windows	
windows	Close

- 7. Click Close.
- 8. Open a PowerShell window.
- 9. Run the following command to install pyinstaller.
  - > pip install pyinstaller
- 10. Run the following command to install requests.
  - > pip install requests

- 11. From the PowerShell window, navigate to where you saved strongkey-client.py.
- 12. Run the following command to build the client into an executable.

```
> pyinstaller --onefile .\strongkey-client.py
```

- 13. A folder called **dist** will be created. In this folder will be an executable named strongkey-client.exe.
- 14. To encrypt a file in place (i.e., overwrite the file with encrypted contents), run the following command:
  - > ./strongkey-client.exe -encrypt -overwrite --infile sensitive.txt
- 15. To encrypt a file and save it to a new location, run the following command:

```
> ./strongkey-client.exe -encrypt --outfile encrypted.txt --infile sensi-
tive.txt
```

16. To decrypt a file in place (i.e., overwrite the encrypted file with plaintext contents), run the following command:

> ./strongkey-client.exe -decrypt -overwrite --infile sensitive.txt

17. To decrypt a file and save it to a new location, run the following command:

import requests

```
> ./strongkey-client.exe -decrypt --outfile decrypted.txt --infile en-
crypted.txt
```

18. This client can be configured to run on a schedule, or be iterated over a directory of files, depending on the needs of the organization. Because the client is Python and StrongKey is REST API based, the script is adaptable to various architectures and can be deployed widely across the enterprises, to fill in gaps that the enterprise may have in its data protection capabilities.

```
import json
import argparse
skdid = # Note: Users should reference a separate file for this ID
skuser = # Note: Users should reference a separate file for the username
skpass = # Note: Users should reference a separate file for the password
encurl = "https://demo4.strongkey.com/skee/rest/encrypt"
decurl = "https://demo4.strongkey.com/skee/rest/decrypt"
def buildrequest(fname, encrypt):
  req = \{\}
  req["svcinfo"] = {
      "did": skdid,
      "svcusername":skuser,
      "svcpassword":skpass
  }
  if (encrypt):
      req["encinfo"] = {
         "algorithm": "AES",
         "keysize":256,
         "uniquekey":True
      }
```

```
req["fileinfo"] = {
      "filename": name
   }
   req["authzinfo"] = {
       "username": "encryptdecrypt",
      #"userdn": "cn=encryptdecrypt,did="+skdid+",ou=users,ou=v2,ou=SKCE,ou=Stron-
qAuth, ou=Applications, dc=strongauth, dc=com",
      "authgroups": "cn=EncryptionAuthor-
ized, did="+skdid+", ou=groups, ou=v2, ou=SKCE, ou=StrongAuth, ou=Applications, dc=stron-
gauth,dc=com",
      "requiredauthorization": 0
   }
   reg["svcinfo"] = json.dumps(reg["svcinfo"])
   req["fileinfo"] = json.dumps(req["fileinfo"])
   if (encrypt):
      req["encinfo"] = json.dumps(req["encinfo"])
   req["authzinfo"] = json.dumps(req["authzinfo"])
   return req
def encrypt(filename,output,overwrite):
   req = buildrequest(filename, True)
   with open(filename, mode='rb') as f:
      files = [('filedata', f)]
      p = requests.request("POST", encurl, headers={}, data=req, files=files)
   print(p)
   p.raise for status()
   if (p.status code == 200):
      output = filename if overwrite else output
      with open(output, mode='wb') as o:
         o.write(p.content)
def decrypt(filename,out,overwrite):
   req = buildrequest(filename, False)
   with open(filename, mode='rb') as f:
      files = [('filedata', f)]
      p = requests.request("POST", decurl, headers={}, data=req, files=files)
   p.raise for status()
   if (p.status code == 200):
      output = filename if overwrite else out
      with open(output, mode='wb') as o:
          o.write(p.content)
parser = argparse.ArgumentParser(description='Encrypt or decrypt a file using
Strongkey.')
group = parser.add mutually exclusive group (required=True)
group.add_argument("-encrypt", action='store_true')
group.add argument("-decrypt", action='store true')
group = parser.add_mutually_exclusive_group(required=True)
group.add argument("-overwrite", action='store true')
group.add argument("--outfile", type=str)
parser.add_argument("--infile", type=str, required=True)
a = parser.parse args()
if (a.overwrite is True):
```

```
overwrite = True
out = ""
elif (a.outfile is not None):
out = a.outfile
overwrite = False
if (a.encrypt is True):
   encrypt(a.infile, out, overwrite)
elif (a.decrypt is True):
   decrypt(a.infile, out, overwrite)
```

# 2.5 Qcor ForceField

ForceField is a Write-Protected File System (WFS) combining hardware device security and encryption. In this build, ForceField is primarily used to backup data while maintaining confidentiality through encryption. In this build, we used ForceField for the protection of a transactional database that needs to maintain both the confidentiality and integrity of prior transactions, while still affording the ability to use that data in new transactions.

# 2.5.1 Installation and Usage of ForceField

- 1. Either a Compact Disk (CD) or zip file will be provided by Qcor containing the WFS API and associate utilities. Copy the contents of \*GreenTec*\*Release* onto the C: drive of the Qcor ForceField server.
- 2. Add the destination folder to the command line PATH variable if necessary. To do this, from the start menu search for **Environment Variables**.

				Edit User Varia	ible	)
Variable	Value					
Path	;C:\Program Files\Azure Data Studio\bi.		Variable name:	Path		
TEMP	%USERPROFILE%\AppData\Local\Temp					
ТМР	%USERPROFILE%\AppData\Local\Temp		Variable value:	Studio\bin;C:\Gree	nTec\ForceFie	eld; <mark>C:\Pro</mark>
				C	ж	Cancel
I	New Edit Dele	4-				
		te				
		te	_			
/stem variables		te	-			
ystem variables						
Variable	Value					
Variable CLASSPATH					- 	
Variable CLASSPATH ComSpec	C:\Windows\system32\cmd.exe					
Variable CLASSPATH ComSpec FP_NO_HOST_C	C:\Windows\system32\cmd.exe NO				* • *	
Variable CLASSPATH ComSpec FP_NO_HOST_C NUMBER_OF_PR	C:\Windows\system32\cmd.exe NO 32					
Variable CLASSPATH ComSpec FP_NO_HOST_C	C:\Windows\system32\cmd.exe NO					
Variable CLASSPATH ComSpec FP_NO_HOST_C NUMBER_OF_PR	C:\Windows\system32\cmd.exe NO 32					

3. Double click the **Path** variable and add the path to the WFS API.

<b>CN.</b>	Administrator:	Command Pron	npt 📕	a x
C:\Users\Administra	tor.DC>wfsdir 2			^
*				
ForceField(tm) Dir h, Apr 9 2022 at 2 Copyright (C) 2020 Licensed to GreenT	ectory List for Writ 0:48:29 -2021. All Rights R ec-USA, Inc.	e-Protected File eserved.	System (WFS) Vers	sion 1.9
Note: Must be exe (Linux))	cuted with elevated ;	permissions (e.g.	. admin (Windows)	or root $\equiv$
ST_Parms: * Warnin	g * Unable to locat	e wfs.conf file,	taking default pa	arms
ForceField(tm) FS VOLUME <	> *** HARDWARE-ENFO	RCED DATA SECURIT	Y <del>***</del> ACTIVE O	N THIS W
* *				
* SerialNum S2ZWJ9 25167	JG300194 has NOT bee JG300194 has BEEN EN forced or Finalized,	FORCED from 99904		
STuerify: <del>***</del> Fix < t be applied.	-fix) Option NOT Spe ERIFIED OK. Searche			
CrDate CrTime Ver Ext FILEN 	FileSize Blo AME	cks Start 	End	Dir 
 20210520	213	 8 10009	8 100015	99984
20210520 14:59:46	213 ers_Administrator.DC	8 10001 Deskton Pirates		99976
20210630 12:16:20	26 e_Mottos.txt	8 10002		99968
20221017 12:52:14 1 2 *		8 10003	100039	99960
20221017 12:56:23 1 3 *	242	8 10004	100047	99952
20221017 12:58:47 1 4 *	157	8 10004	100055	99944
20221026 11:42:00 1 5 *	157	8 10005	6 100063	99936
20221116 12:20:26 1 1 listi	157 ngs.txt	8 10006	64 100071	99928
20221116 12:21:41 1 2 listi	157 ngs.txt	8 10007	2 100079	99920
20221116 12:22:01 1 3 listi	157 ngs.txt	8 10008	100087	99912
20221116 12:26:30	157 ngs.txt	8 10008	8 100095	99904
USAGE STATISTICS: TB), Remaining=1.00 Drive 2		otal Disk Size=1.	.0002 (TB), Used=0	0.0001 <
	DATA: TB	Blocks	Percent	
	USED : 0.00000 AVAIL: 1.00015 TOTAL: 1.00015	88 1953425039 1953425127	0.00000 100.00000	
	DI RBLKS : GB	Blocks	Percent	
	USED : 0.00001 AVAIL: 0.00639 TOTAL: 0.00640	11 12482 12493	0.08805 99.91195	
				$\sim$

4. Verify that the drives of the Qcor WFS server have been formatted to work with ForceField with wfsdir command line utility that was just installed. The drives may be pre-formatted. Use the

following command to determine whether a drive is formatted. In place of "N", enter the number of the drive to check.

> wfsdir N

5. *If the hard drive(s) have not been formatted,* use the wfsx command line tool to format your drive. **Note:** Once performed, the formatting cannot be undone. The following instructions are copied from the WFS User Guide.

> wfsfx <devicename> <options>

devicename is the device identifier of the disk to be formatted. For Windows, this is the Windows disk number that may be found via the Windows Disk Manager (e.g. 1, 2, etc.). For Linux, this is the physical device name (e.g. /dev/sdb/).

options may be:

-DirX Or -x power of 10> (optional power of 10 for max number of files, default is 10)
1 will format for 1,243 files, 10 will allow 12,489 files, 100 allows 124,993 files, 1000 allows
1,249,930 files

-vuser <username> specifies a volume user name, DO NOT FORGET THIS USE NAME IF USED!

-vpass <password> specifies a volume password, DO NOT FORGET THIS PASSWORD IF USED!

-cache ONIOFF will turn on or off the disk drive internal cache (default is ON).

-verifywrite ONIOFF will turn write verify on or off for the WFS volume (default is OFF). The write verify status may be toggled ON or OFF using the WFScache utility. NOTE: turning write verify ON may significantly degradel/O performance.

6. Files can then be copied into or out of the designated drives using the wfscopy command line tool. The following instructions are copied from the WFS User Guide.

> wfscopy <source-file> <destination-file> <count>

One of the files must be a native Operating System (OS) file system file, and the other file must be a WFS file. **source-file** is the name of the input file and may be a native OS filename, or a WFS filename. **desti-nation-file** is the name of the input file and may be a native OS filename, or a WFS filename. **count** is the optional number of bytes to copied. count defaults to all records.

Examples of wfscopy using Windows:

```
> wfscopy testfile.txt 1:*
```

The above command will copy the file named testfile.txt from the local directory to disk number 1 with the same name. If the WFS file does not previously exist, then it is created. If the WFS file does previously exist, then the data is appended to the existing WFS file as a new file extension.

> wfscopy 2:Contracts.pdf c:\myfolder\Contracts.pdf

The above command will copy all records from all extensions of the WFS file named Contract.pdf from the disk, as identified as 2 by the Windows Disk Manager, to the Windows file C:\myfolder\Contracts.pdf record by record.

```
> wfscopy 4:myfile.txt con:
```

The above command will display the contents of the WFS file myfile.txt from disk 4 onto the console. This is similar to using the type command in the Windows command line.

# 2.6 Avrio SIFT

Avrio SIFT is a data inventory and management capability designed to enforce data policies. The installation of Avrio SIFT is typically done in a managed fashion by the vendor, and the deployment seen in the NCCoE lab may not resemble other deployments. In the case of a Docker deployment, configuration to the base Avrio installation can be made by modifying the docker-compose file. Otherwise, it will be assumed that Avrio has been installed and configured properly for the enterprise by the vendor.

# 2.6.1 Configuring Avrio SIFT

- 1. Navigate to the SIFT dashboard (default address: http://IP-address:8080/sift/) and login.
- 2. Click Configuration.
- 3. Under Enclaves, enter two locations. First, the path to the public Windows share, and second, the path to the one protected by PKProtect. We will use this second path later in the integration between PKProtect and SIFT. In this example, DCIPDRR is the path to the public share, and PRO-TECTED is the path to the one protected by PKProtect. Enter user accounts that can access each share. In production, it is recommended to create a separate user account for SIFT to use to access these shares.

×	SIFT   Secure Integrated File Tagg × 🕲 Archive	e - Lockers x +	~ <u> </u>
÷	→ C ▲ Not secure   192.168.1.198.8	3080/sift/blacklist/networks	
	🔗 SIFT Request 🗸 Confi	guration Reports Analyze Access v 🎍 Use	er, Admin 🗸
			_
	Configuration	Enclaves	_
	Enclaves	SMB S3 Sharepoint	
	Keywords		
	File Types	Name UNC Path Username Password	- 11
	Classifications	DCIPDRR X [\AD-DNS\TOP-SECRET-SF] DC\Administrator	
	Rich Text	PROTECTED X (\192.168.1.80\SECRET DC\Administrator	
	Batch Scanning	+ Add new enclave	_
	Video		
	Scan Mode	SAVE CHANGES	
	Profiles		
	Language		
	Import/Export		
	Machine Learning		
	File Status		
			-

- 4. Click Save Changes.
- 5. Click **Keywords** on the left menu.
- 6. Click Add new keyword.

 Enter the keyword under Name, and an Alias (if desired). Check the box next to any enclaves that are allowed to have this keyword – SIFT will be able to move files matching it to the enclaves you check the box for.

O A Not secure   192.1	168.1.198:8080/sift/blacklist/keywords				ዸ ☆ 🛛
SIFT Request ~	Configuration Reports Analyze	Access ~			L User, Admin ∽
Configuration	Keyword Restrictions				
Enclaves	Word List	Alias	Move To	Enclaves	
Keywords				DCIPDRR	PROTECTED
File Types	Select All				
Classifications	MALABAR	alias	PROTECTED ~	0	
Rich Text					
Batch Scanning		L <sub>6</sub>			
Video					
Scan Mode					
Profiles					
Language					
Import/Export					
Machine Learning					

8. Select the PROTECTED enclave under **Move To**.

- 9. Click Save Changes.
- 10. Click File Types.
- 11. Designate file types that are allowed to exist under each enclave.

SIFT   Secure Integrated File Tagg × 🕲 Archive - Lu		~ <mark>- □ ×</mark>
← → C ▲ Not secure   192.168.1.198:8080	)/sift/blacklist/filetypes	i£ ☆ 🛛 😩 :
🤣 SIFT Request 🗸 Configura	ation Reports Analyze Access -	💄 User, Admin 🗸
	PNG	
	PPT	
	PPTX	
	RTF	
	TAR	
	TIFF Dg	
	ТХТ	
	XLS	
	XLSX	
	XML	
	ZIP	
	SAVE CHANGES	
	© 2016 - Aerstone Labs   development - 1.0.5.R5	,

- 12. Click Save Changes.
- 13. Click Classifications.

- \_ **□** × SIFT | Secure Integrated File Tagg × SIFT | Secure Integrated File Tagg × × | + ← → C ▲ Not secure | 192.168.1.198:8080/sift/blacklist/classifications 🖻 ☆ 🔲 🏩 : 🔗 SIFT 👤 User, Admin 🗸 Classification Restrictions Configuration Enclaves Classification Enclaves Keywords DCIPDRR PROTECTED File Types Select All Classifications < TOP SECRET Rich Text SECRET Batch Scanning UNCLASSIFIED Video Scan Mode + Add new classification Profiles Language Import/Export Machine Learning File Status
- 14. Designate the classifications that are allowed to exist under each enclave.

- 15. Click Save Changes.
- 16. On the top click **Request** > **New Request**.
- 17. Click Batch.
- 18. Select UNC Path for Source Type.
- 19. Select the enclave to scan for sensitive files.
- 20. Select **Move** for **Scan Type**. (Note that if you select **Scan** for **Scan Type**, it will scan files and tell you they are sensitive and whether they can be moved but will not attempt to move them. This is useful for debugging.)
- 21. Select **Delete** for **Move Action**, or another action depending on the needs of your organization. Selecting Delete will remove the sensitive file from the public share and move it to the protected one.
- 22. Set Scan Subfolders to ON.
- 23. Enter a description for the scan.
- 24. Set the frequency of the scan. Note that the efficiency of the scan will likely depend on the size of the organization, and it may be more desirable to scan once an hour rather than once a minute.

SIFT   Secure Integrated File Tagg × 🕲 Archive -	Lockers ×   +		~ <u>- □ ×</u>
← → C ▲ Not secure   192.168.1.198:808	80/sift/batch/create		🖻 🖈 🔲 😩 🗄
🔗 SIFT Request 🗸 Configur	ration Reports Analyze		L User, Admin ∽
New Request Type	Initiate Batch Request		
File	Source Type	UNC Path ~	
Batch Rescan	Source Enclave	DCIPDRR	]
	Scan Type	Move	
	Move Action	Delete ~	
	Scan Subfolders	ON	
	Description*	Move Files	
			s
	Scheduled Time	Every minute ~ 0 0/1 *** ?	
		SUBMIT	

- 25. Click Submit.
- 26. Now, you can verify that files that are added to the public share with sensitive keywords are moved to the share designed to hold sensitive files.

### 2.7 Cisco Duo

Cisco Duo is a Multi-Factor Authentication and Single Sign-On tool. In this project, Dispel is used to control access to internal systems through virtualization, and Duo is used as a multifactor authentication solution between Dispel and those internal systems. This ensures that even if a Dispel virtual machine becomes compromised, there is still significant access control between that machine and the internal enterprise machines.

In the following section, we demonstrate the installation of Cisco Duo on an internal system in such a way that Remote Desktop Protocol (RDP) and local login to that system are protected by multifactor authentication.

### 2.7.1 Installing Cisco Duo

- 1. Begin by logging into the system you wish to protect with Duo.
- 2. Then connect to the internet, if not connected already, and go to the Duo Admin login page at <a href="https://admin.duosecurity.com/">https://admin.duosecurity.com/</a>.

Admin Login
Enter your admin credentials
Email address
Save my email address for next time Not recommended for public or shared computers
Continue
Continue

3. Login with your admin credentials and dual factor authentication until the admin dashboard is reached.

DUO	Q Search for users, groups, applications, or devices					MITRE	MITRE   IC	D: 2636-3111-77	Michael Ekstrom 🗸
Dashboard	Dashbo	ard							Add New 🗸
Policies	Dashbu	Jaru							Add New V
Applications	Users								
Users	0	0	5	1	Administrators				
Groups	Bypass Users	Locked Out	Inactive						
2FA Devices	View	View	View	2	2FA Devices				
Administrators	4 Licenses	Remaining		1	Groups				
Reports	6 Total Use	rs		471	Remaining Telepho	nv Credits			
Settings Billing					rtentaning rerepite	ing orouno			
Need Help? <u>Upgrade your plan</u> for support.									
opgrade your plan for support.									

- 4. Click **Applications** in the sidebar.
- 5. Click **Protect an Application**.

<b>DU</b> e	Q Search for users,	groups, applications, or devices	MITRE MITRE	ID: 2636-3111-77 Michael Ekstrom ~
Dashboard	Dashboard > Application	ons		
Policies	Applicati	000		Protect an Application
Applications	Applicati	0115		Protect an Application
Protect an Application				
Users				$\sim$
Groups	Manage your u experience, all	pdate to the new Universal Prompt		
2FA Devices	experience, an	in one place.	all is the second	×
Administrators	See My Progress	Get More Information		
Reports				
Settings	4	0		
Billing	All Applications	End of Support		
Need Help?			Export 🛩	Q Search

- 6. Search for, or scroll down to, **Microsoft RDP**.
- 7. Click **Protect**.

DUO	Q Search for users, groups, applications, or devices	MITRE	MITRE   ID: 2636-3111-77	Michael Ekstrom 🗸
Dashboard	Dashboard > Applications > Protect an Application			
Policies	Protect an Application			
Applications	Fiblect all Application			
Protect an Application	RDP			
Users				
Groups	Application	Protection Type		
2FA Devices				
Administrators	Microsoft RDP	2FA	Documentation 🗗	Protect
Reports				

8. The next screen will provide policy configuration options, as well as the **Integration Key**, **Secret Key**, and **API hostname**, which are required information for the next step. Either keep this window open or copy down those three pieces of information.

Applications Protect an Application Users Groups	Dashboard > Applications > M <b>Microsoft RE</b> See the RDP documentation (	Authentication Log	Remove Application		
2FA Devices Administrators Reports	Details	DIZQ2S5DXMVCA2FBVEMM	Сору		Reset Secret Key
Settings Billing	Secret key		Сору		
Need Help? <u>Upgrade your plan</u> for support. Versioning Core Authentication Service:	API hostname	Don't write down your secret key or share it with anyone.	Сору		

- 9. Download the **Duo Authentication for Windows Logon** installer package, located at <u>https://dl.duosecurity.com/duo-win-login-latest.exe</u>.
- 10. Run the downloaded EXE file.



11. Click Next.

#### 12. Copy the API Hostname into the labeled field.

	Sun 🖯 Microsoft RDP 2 - Application X 🖯 Duo Authentication for Windom.	Buo Authentication for Windows Logon x64 - InstallShield Wizard     X     Duo Connectivity Check     Please enter the hostname for your integration to verify connectivity
Details		API Hostname:
Integration key	DI8SZS91SLPZGWEEHZWG	[api-9d22a89:dusecurity.com] This hostname can be found in the <u>Duo Admin Panel</u> under Applications, configure or select a Microsoft RDP application.
Secret key	Copy Don't write down your secret key or share it with anyone.	Configure manual proxy for Duo traffic (Uses System settings if unspecified) Proxy Host: Proxy Port: Proxy Port:
API hostname	api-9d22ea89.duosecurity.com	
Policy		InstallShield <back next=""> Cancel</back>

- 13. Click Next.
- 14. Copy in the Integration and Secret Keys into the relevant fields and click Next.

🕼 Duo Authentication for Windows Logon x64 - InstallShield Wizard	×
Duo Security Account Details	
Please enter the keys provided by Duo Security	
Integration Key:	
DI8SZS91SLPZGWEEHZWG	
Secret Key:	
These keys can be found in the <u>Duo Admin Panel</u> under Applications, configure or select a Microsoft RDP application.	
Please refer to the Duo Windows Logon <u>documentation</u> for more information.	
<pre>Instalishield  <back next=""> Cancel</back></pre>	

- 15. Click Next.
- 16. Configure Duo's integration options according to the needs of your organization. Note that **Bypass Duo authentication when offline** will allow users to skip the two-factor authentication when offline, which increases the availability of their files but may increase risk.

🕼 Duo Authentication for Windows Logon x64 - InstallShield Wizard	Х
Duo integration options	
Configure the integration below	
Bypass Duo authentication when offline (FailOpen)	
Enable this option to allow user logon without completing two-factor authentication if the Duo Security cloud service is unreachable. If you plan to enable offline access with MFA consider disabling FailOpen to prevent un-enrolled users from logging in.	
Use auto push to authenticate if available Automatically send a Duo Push or phone call authentication request after primary credential validation.	
Only prompt for Duo authentication when logging in via RDP	
Leave this option unchecked to require Duo two-factor authentication for local logon and RDP sessions. If enabled, local logons do not require 2FA approval.	
Please refer to the Duo Windows Logon <u>documentation</u> for more information. InstallShield	
< Back Next > Cancel	

#### 17. Click Next.

### 18. Leave Enable Smart Card support unchecked.

<ul> <li>Protect smart card login with Duo Both smart card and username/password primary login is followed by Duo two-factor authentication.</li> <li>Enable smart card login without Duo Allow use of the Windows smart card login provider as an alternative to</li> </ul>		Enable Smart Card support
	(	Both smart card and username/password primary login is followed by Duo
Allow use of the Windows smart card login provider as an alternative to		Enable smart card login without Duo
password login with Duo two-factor authentication.		Allow use of the Windows smart card login provider as an alternative to password login with Duo two-factor authentication.

#### 19. Click Next.

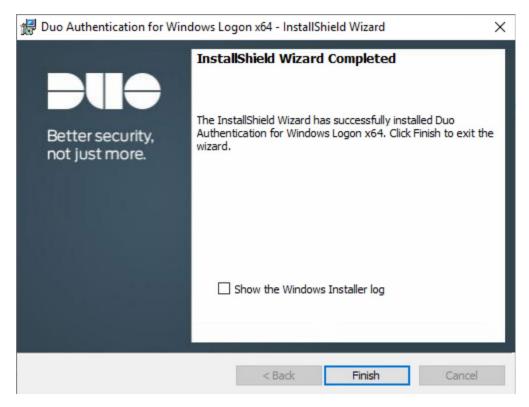
20. Leave Enable UAC Elevation Protection unchecked.

🖟 Duo Authentication for Windows Logon x64 - InstallShield Wizard	Х
Duo integration options	
Configure User Elevation Protection	2
Enable UAC Elevation Protection	
Enable Duo two-factor authentication for password protected UAC prompts.	
Protect User Elevation only	
Protect UAC Prompts Only. Disables MFA for Local and RDP sessions	
Protect User Elevation while offline Enable Duo two-factor authentication for password protected UAC prompts when Offline access is enabled.	
Allow Offline enrollment during User Elevation Allow for offline access enrollment during password protected UAC prompts when Offline access is enabled.	
Please refer to the Duo Windows Logon documentation for more information.	
installShield	
< Back Next > Cancel	

#### 21. Click Next.

🖟 Duo Authentication for Windows Lo	gon x64 - InstallShield Wizard	Х
Ready to Install the Program The wizard is ready to begin installation	n.	
Click Install to begin the installation.		
If you want to review or change any o exit the wizard.	f your installation settings, dick Ba	ck. Click Cancel to
InstallShield		
	< Back Install	Cancel

### 22. Click Install.



- 23. Click Finish.
- 24. Installation should now be complete. Users registered on the Duo Dashboard with a linked phone will be allowed access to the system.

### 2.7.2 Registering a Duo User

1. Login to the Duo Admin Dashboard.

ÐUƏ	<b>Q</b> Search for users, groups, applications, or devices				MITRE	MITRE   ID: 2636-3111-77	Michael Ekstrom 🗸
Dashboard	Dashbo	bard					Add New 🗸
Policies							
Applications	Users						User
Users	-	-	_				Application
Groups	0	0	5	1	Administrators		Group
2FA Devices	Bypass Users View	Locked Out View	Inactive View	2	2FA Devices		
Administrators Reports	4 Licenses	Remaining		1	Groups		
	6 Total Use	rs		463	Remaining Telephony Credits		
Settings				-+03	Remaining relephony credits		
Billing							

- 2. Click Add New > User from the drop-down menu on the right.
- 3. Enter a username for the user.

Policies Applications	Add User	
Users	Most applications allow users Learn more about adding use	s to enroll themselves after they complete primary authentication. $\operatorname{crs} \square^{*}$
Add User		
Pending Enrollments		
Bulk Enroll Users	Username	userName
Import Users		Should match the primary authentication username.
Directory Sync		
Bypass Codes		
Groups		Add User
2FA Devices		

- 4. Click Add User.
- 5. This will lead you to that user's information page, where additional information (full name, email, phone number) and Duo authenticators (phone numbers, 2 Factor Authentication (2FA) hardware tokens, WebAuthn, etc.) can be associated with that username. Note: A user will not be able to log into a Duo protected system unless the user is registered and has an authentication device associated with their username.

### 2.8 Dispel

Dispel is a network protection and user access tool that we used to provide a Virtual Desktop Infrastructure (VDI) capability. A typical deployment of Dispel is done in a largely managed fashion, with a specific deployment being tailored to a network setup. The deployment in the NCCoE laboratory may not be the best setup for any given network. The NCCoE deployment was done on an Ubuntu host with Wide-Area Network (WAN) and Local-Area Network (LAN) interfaces, placing the device in-line between the enterprise systems and the external network.

### 2.8.1 Installation

- 1. Deploy an Ubuntu machine with the provided specifications, ensuring that a provided ISO is attached to the device.
- 2. Login with username "dispel" and the password provided.

```
dispelwicket login: dispel
Password:
Linux dispelwicket 4.19.195-amd64-vyos #1 SMP Thu Feb 17 12:52:59 UTC 2022 x86_6
4
Welcome to VyOS!
Check out project news at https://blog.vyos.io
and feel free to report bugs at https://phabricator.vyos.net
You can change this banner using "set system login banner post-login" command.
VyOS is a free software distribution that includes multiple components,
you can check individual component licenses under /usr/share/doc/*/copyright
dispel@dispelwicket:~$
```

3. Begin the installation process

> install image

dispel@dispelwicket:~\$ install image Welcome to the Dispel Wicket ESI install program. This script will walk you through the process of installing the Dispel Wicket ESI image to a local hard drive. Would you like to continue? (Yes/No) [Yes]:

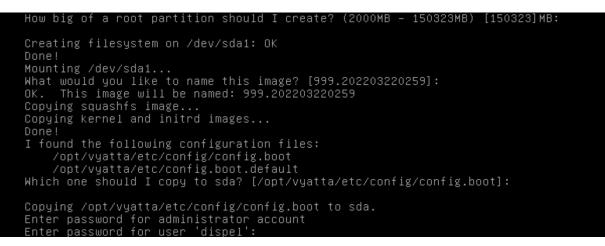
4. Press enter on the following three prompts, modifying any default options as desired.

```
Would you like to continue? (Yes/No) [Yes]:
Probing drives: OK
Looking for pre-existing RAID groups...none found.
The image will require a minimum 2000MB root.
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted? If
you have already setup your partitions, you may skip this step
Partition (Auto/Parted/Skip) [Auto]:
I found the following drives on your system:
sda 150323MB
Install the image on? [sda]:
This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]:
```

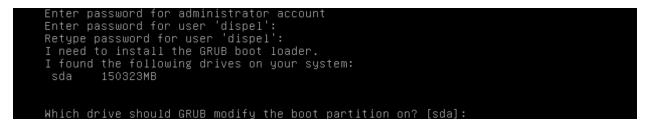
5. Type yes before pressing enter to rewrite the current volume.

```
This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]: yes
How big of a root partition should I create? (2000MB – 150323MB) [150323]MB: _
```

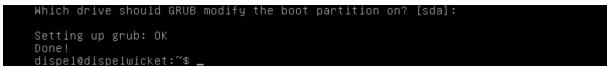
6. Press enter on the remaining prompts, modifying any default options as desired.



7. Enter and re-enter a new password for the user dispel



8. Press enter one final time to finish the installation



- 9. Power off the machine, remove the provided ISO, and power it back on.
- 10. Log in with the user "dispel" and the new password set in step 9.

UNAUTHORIZED USE OF THIS SYSTEM IS PROHIBITED!
Hint: Num Lock on
dispelwicket login: dispel Password: Linux dispelwicket 4.19.195–amd64–vyos #1 SMP Thu Feb 17 12:52:59 UTC 2022 x86_6 4 Welcome to VyOS!
Check out project news at https://blog.vyos.io and feel free to report bugs at https://phabricator.vyos.net
You can change this banner using "set system login banner post–login" command.
VyOS is a free software distribution that includes multiple components, you can check individual component licenses under /usr/share/doc/*/copyright
disnel@disnelwicket:~\$

11. Type in the command > ifconfig | grep inet. Verify the output to make sure it matches the desired network configuration. If not, see the next section.

```
dispel@dispelwicket:~$ ifconfig | grep inet
inet addr:10.33.53.194 Bcast:10.33.53.207 Mask:255.255.255.240
inet6 addr: fe80::250:56ff:fead:223e/64 Scope:Link
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
dispel@dispelwicket:~$
```

# 2.8.2 Configuring IP Addresses

1. Login to the device with the user "dispel".

UNAUTHORIZED USE OF THIS SYSTEM IS PROHIBITED! Hint: Num Lock on dispelwicket login: dispel Password: Linux dispelwicket 4.19.195-amd64-vyos #1 SMP Thu Feb 17 12:52:59 UTC 2022 x86\_6 4 Welcome to VyOS! Check out project news at https://blog.vyos.io and feel free to report bugs at https://phabricator.vyos.net You can change this banner using "set system login banner post-login" command. VyOS is a free software distribution that includes multiple components, you can check individual component licenses under /usr/share/doc/\*/copyright dispel@dispelwicket:~\$

2. Type in the command > configure.

```
dispel@dispelwicket:~$ configure
[edit]
dispel@dispelwicket# _
```

3. Type in the command > del interfaces ethernet eth0, or whichever interface you are currently modifying.

```
dispel@dispelwicket# del interfaces ethernet ethO
[edit]
dispel@dispelwicket# _
```

 Type in the command > set interfaces ethernet eth0 address followed by the desired IP address in CIDR notation, modifying for the desired interface as appropriate.

```
dispel@dispelwicket# set interfaces ethernet eth0 address 192.168.2.213/28
[edit]
dispel@dispelwicket# _
```

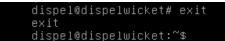
5. Type in the command > commit.

```
dispel@dispelwicket# commit
[edit]
dispel@dispelwicket#
```

6. Type in the command > save.

```
dispel@dispelwicket# save
Saving configuration to '/config/config.boot'...
Done
[edit]
dispel@dispelwicket# _
```

7. Type in the command > exit.



## 2.8.3 Configuring Network

The following instructions are to modify a Dispel wicket device to forward traffic to a different routing device. This may be desirable for some network setups.

1. Type in the command > configure to the Dispel wicket device after logging in.



2. Type in the command > set protocols static route 0.0.0/0 next-hop followed by the IP address of the router you wish to forward to.

dispel@dispelwicket# set protocols static route 0.0.0.0/0 next-hop 192.168.1.1 [edit] dispel@dispelwicket#

3. Type in the command > commit.

```
dispel@dispelwicket# commit
[edit]
dispel@dispelwicket#
```

4. Type in the command > save.

```
dispel@dispelwicket# save
Saving configuration to '/config/config.boot'...
Done
[edit]
dispel@dispelwicket# _
```

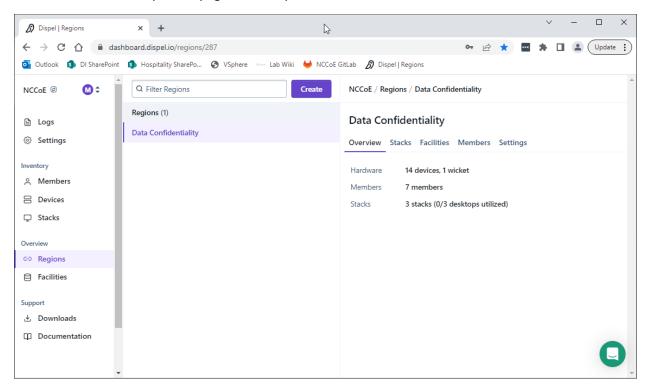
5. Type in the command > exit.

```
dispel@dispelwicket# exit
exit
dispel@dispelwicket:~$
```

- 6. On the designated router or firewall, ensure User Datagram Protocol (UDP) is allowed from the Dispel device on the provided port. For the NCCoE deployment, port 1194 was utilized. A target destination for the traffic will be provided by Dispel.
- Modify the IP addresses of the south-side network interface to properly align with your network. See the "Configuring IP Addresses" section above.

# 2.8.4 Adding a Device

- 1. On the workstation in question, ensure that ping and RDP are accessible, including allowing such connections through a local firewall.
- 2. Authenticate to the Dispel webpage with the provided credentials.



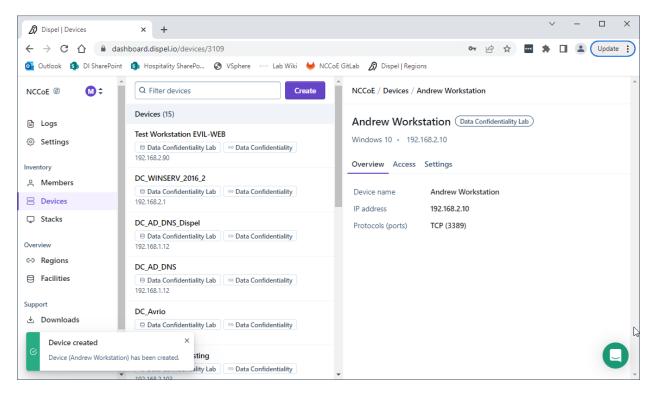
3. Click on the **Devices** page on the sidebar and click **Create**.

Dispel   Devices	× +					~	-		×
$\leftrightarrow$ $\rightarrow$ C $\triangle$ $$ dash	hboard.dispel.io/devices/create	07	È	☆	••••]	*		Update	e :)
💁 Outlook 🔹 DI SharePoint	🔹 Hospitality SharePo 🔇 VSphere 🛛 🖙 Lab Wiki 🤟 NCCoE GitLab 💋 Dispel   Regions								
NCCoE @ M ¢	B Data Confidentiality Lab     S Data Confidentiality 192.168.2.1     NCCoE / Devices / Create								-
🖹 Logs	DC_AD_DNS_Dispel       Add device         Data Confidentiality Lab       Adding a device allows you to control access to it.								
Inventory 은 Members	DC_AD_DNS     Facility*            □ Data Confidentiality Lab <ul> <li>         ○ Data Confidentiality 192.168.1.12         </li> </ul> <li>Select a Facility</li>	\$							
B Devices	DC_Avrio Wicket*								
🖵 Stacks	Data Confidentiality Lab     No wickets found     Name*								
Overview	DC_Cisco_Duo_Testing								
E Facilities	○ Data Confidentiality 192.168.2.103 Make								
Support	DC_CISCO_STEALTHWATCH_FLOW_C								
🕁 Downloads	<ul> <li>□ Data Confidentiality Lab</li> <li>∞ Data Confidentiality 192.168.1.64</li> <li>Model</li> </ul>								
Documentation	DC_CISCO_STEALTHWATCH_MANAGI								
	B Data Confidentiality Lab							C	

4. Under the Add Device window, fill out all fields, including Facility, Wicket, Name, Make, Model, IP, and Protocol.

Dispel   Devices	× +	∨ - □ X
← → C ☆ ●	dashboard.dispel.io/devices/create	🕶 🖻 🖈 🖬 🌲 🔲 😩 Update 🔋
o Outlook 🗿 DI SharePe	oint 🛐 Hospitality SharePo 🔇 VSphere 🚥 Lab Wiki 🦊 N	CCoE GitLab 🔊 Dispel   Regions
NCCoE © 🚺 🗘	Q Filter devices  Create	NCCoE / Devices / Create
	Devices (14)	Make
🖹 Logs	Test Workstation EVIL-WEB	Windows
Settings	B Data Confidentiality Lab	Model
Inventory	DC WINSERV 2016 2	10
	Data Confidentiality Lab     So Data Confidentiality	ID*
Devices	192.168.2.1	192.168.2.10
🖵 Stacks	DC_AD_DNS_Dispel	152,100,2,10
Overview	<ul> <li>⊟ Data Confidentiality Lab</li> <li>∞ Data Confidentiality</li> <li>192.168.1.12</li> </ul>	Protocol Ports
⇔ Regions	DC AD DNS	TCP 💠 3389 ×
Facilities	Data Confidentiality Lab     Solution     Solution	+ Add protocol
Support	DC_Avrio	Ports can be written as ranges in a comma-separated list. For example: "100,200-300" is the port 100 and the range 200-300.
🗄 Downloads	Data Confidentiality Lab     So Data Confidentiality	example: 100,200-300 is the port 100 and the range 200-300.
Documentation	192.168.1.198	Add device
	DC_Cisco_Duo_Testing	
	Data Confidentiality Lab     So Data Confidentiality	

5. Click Add Device.



6. Under Access for that device, search for the user(s) that will have access to that device. Verify they have the correct access settings.

Dispel   Devices	× +	∨ - □ X
$\leftrightarrow$ $\rightarrow$ C $\triangle$ $\stackrel{\circ}{\bullet}$ da	shboard.dispel.io/devices/352/access	🕶 🔄 🏚 🔳 😩 🗍 Update 🔅
outlook 🗿 DI SharePoin	it 🤹 Hospitality SharePo 🔇 VSphere 🚥 Lab Wiki 🦊 NO	CoE GitLab 🔊 Dispel   Regions
NCCoE © M ≎	DC_DISPEL_UBUNTU_1     Data Confidentiality Lab      Data Confidentiality     192.168.1.240	NCCoE / Devices / Test Workstation EVIL-WEB / Access
🗎 Logs	DC_HELIX_CENTOS	Test Workstation EVIL-WEB (Data Confidentiality Lab)
Settings	☐ Data Confidentiality Lab ○ Data Confidentiality 192.168.1.206	192.168.2.90
Inventory	DC_HELIX_UBUNTU	Overview Access Settings
은 Members	⊟ Data Confidentiality Lab  Solution Solutin Solution Solution Solution Solution	Q. Andrew
B Devices		
🖵 Stacks	B Data Confidentiality Lab     So Data Confidentiality	Device access (ACLs) (0) ····
Overview	192.168.2.40	
C→ Regions	DC_PRODUCT	
Facilities	Bata Confidentiality Lab	
	DC VICTIM WIN10_1	
Support	Data Confidentiality Lab     So Data Confidentiality	
🕁 Downloads	192.168.1.93	
Documentation	Andrew Workstation	
		ļ U

7. If a user is not already a member of the region, click **Members** in the sidebar and click **Invite.** Fill out relevant information for this individual and click **Invite this Member.** 

# 2.9 Integration: FireEye Helix and Symantec SWG

In this integration the output of the web isolation tool, Symantec SWG, will be forwarded to our Security Information and Event Management (SIEM), FireEye Helix. In this guide, we will aim to forward most logs to our SIEM, which can collect, analyze, and report on these logs to better maintain awareness of our systems and provide a single interface for analyzing the health of the system. Logs from SWG will allow us to see statistics on the number of threats that have been blocked, as well as any administrative changes made to the SWG product.

# 2.9.1 Configure Fireye Helix to Collect Logs from Symantec SWG

- 1. Navigate to the Symantec dashboard, and login.
- 2. Navigate to Account Configuration by clicking the gear icon on the left sidebar.

🛞 Web Secu	urity Service × / Trellix IAM	× +	✓ _ □ x
← → C	portal.threatpulse.com/#account landing		ie 🖈 🗖 😩 i
	eb Security Service @	Julian Sexton Julian Sexton	
	Account Configuration 🛛		*
ū	General		
品	Products & Licensing	View account information and licensed products	
æ	Data Retention & Privacy	Configure how WSS handles PII and other data $I_{\widehat{\mathbf{k}}}$	
1.	Administrators & Access Control		
ŵ	Administrators	Manage access to your account	
	Account Auditing	View account activity	
	API Credentials	Integrate external systems with WSS	
	Reporting Settings		
<>	Log Export	Download traffic logs	*

- 3. Click API Credentials.
- 4. Click Add.
- 5. Check the boxes next to **Reporting Access Logs**, **Location Management**, **Audit Logs**, **Agent Con-fig Management**, and **Egress IP**.
- 6. Set an **Expiration Date** for the credential (1 year recommended).
- 7. Copy the Username and Password provided, as you will not be able to retrieve these once you create the credential.

🛞 Web	Security Service	× / Trellix IAM × +				V		×
$\leftarrow \rightarrow$	C 🔒 portal	threatpulse.com/#accountlapiCredentials				6 \$		:
	Web Sect	itu Capileo 🦉			Julian Sextor	Julian	Sexton ~	
		Edit API Key 🛿			×			
	API Cr	Create API Credentials to integrate external systems with the WSS.	Access:	🌲 🗹 Reporting Access Logs	0			
	Create A	Username:		Location Management	0			
a	+ A			Audit Logs	0			
윮	🗆 St	Password: *******		Agent Config Management	0			
66	() Er	Expiry: Time-based Never		Egress IP	Ð			
Æ								
E		Expiry Date: 09/13/23 🛗 00:00 💌	Comments:					
	Er Er		R					
(i)			0	255 of 255 characters left				
	1000			e saved, the token cannot be displayed again you have a copy.	Ensure			
	S B							
	1			Cancel	Save			
<>								

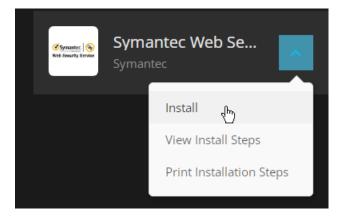
8. Click Save.

🛞 Web Security :	Service ×	HELIX   Trellix	×	+							✓	_ □	X
$\leftrightarrow$ $\rightarrow$ G (	apps.fireeye.com/hel	lix/id/hexspz443/								ß	*		÷
<b>Trellıx</b>	HELIX			Dashboards 🗸	Investigate 💙	Explore 💙	Configure 🔨	Manage	<ul> <li>DOC-NIST-I</li> </ul>	NC 🔁	Q .	•	
							Lists						
Summary Dashboard								Rules 🖨 Print As PDF					
A dashboard tailored to all users. Use this view to get a quick synopsis of what's going on in your environme								Trellix	dashboard, it i	s not edital	ole. Lear	n More 🗹	
Asset-Based /	lert Correlations	View All	Overall Risk Sco	ore 🔞			Searches				w All Cor	relations	
Asset		Risk Score					Network						
	No Entities to display.						Cloud Conn.	. œ					
Recent Alerts			0 08/15 08/16 00	917 0818 0819 0820 0	9/21 08/22 08/23 08/24	08725 08725 08727 087	28 08/29 08/30 08/ View Alert		าน อมาน อมาน อมาน อมาน อ Recent Alerts	9/07 09/08 09/09	09/10 09/1	09/12 09/1	3
Risk	Name			Origin	Events	Last Updated						1	
o Medium	SYSTEM MONITORING [I	Events Missing for I	ay - ms_windo	fireeye rule	1 hit	a year ago						,	

9. On the Helix Dashboard, click **Configure > Cloud Connect**.

Neb:	Security Service	×   🖊 HELIX   Trel	lix ×	/ Helix Cloud Integra	ations   FireEye × +	)			· - •
C  helix-integrations.cloud.aws.apps.fireeye.com/#/?filters=%58%5D									
Cloi	ud Conne	ct							
dd and	l manage cloud con				• • •	ο ο ι	ast Update: 2022-09-12T13		Add Claud Canadatia
lelix.							ast Opdate: 2022-09-12113	.05:22-04:00	Add Cloud Connectio
	Name	Vendor	Identifier	Sensor ID	Helix ID	Status	Created <sup>⑦</sup>	Last Event 🔊	Last Poll 🔊
	All ~	All ~	Search 1 records	Search 1 records	Search 1 records	All ~			
	Duo Auth	Duo Security	DI4ERNLR0C3L2I	1654094729300	hexspz443	•	3 months ago	3 months ago	an hour ago
ows per	Page 10 25 50							1 - 1 of 1	
2022 Tr									

- 10. Click Add Cloud Connection.
- 11. Click the arrow next to Symantec Web Security Service.



12. Click Install.

♦ Web Security Service × / / HELIX   Trellix	× / Helix Cloud Integrations   FireEye × +				~ <mark>- □ ×</mark>
$\leftarrow$ $\rightarrow$ C ( helix-integrations.cloud.aws.apps.fireeye.com	m/#/install/symantec_web_security_service				🖻 🖈 🗖 😩 i
Trellix   Cloud connect					(U)
Your Integration Instruction	IS				
(1)					(2)
Setup					Verify Integration
Step 1: Setup		Helix Instan	ice: hexspz443 🗸		Submit and Verify
	vord', please go to the Symantec Web Security Service docs	and follow th	e instructions. Do	wnload Audit	
Logs with REST API Documentat					
	<ol> <li>Input Required</li> </ol>				
	Username				
	Username matches the expected format.				
	Password		k.		
	Password matches the expected format.				
© 2022 Trellix					

13. Enter the username and password from the credential created earlier.

Web Security Service X / HELIX   Trellix X / Helix Cloud Integrations   FireEys X +	~		x
← → C ● helix-integrations.cloud.aws.apps.fireeye.com/#/install/symantec_web_security_service	₿☆		:
Trelin   CLOUD CONNECT		JU	
Your Integration Instructions		2) ntegration	
Step 2: Verify Integration Previous Step	o Ba	ck to Home	
Your data has now been submitted and we will verify that Helix is receiving data. Successful Integration Your Helix instance is now ingesting data from this integration, you may close this window or return home.			
© 2022 Trellix			

- 14. Click Submit and Verify.
- 15. Click **Back to Home**. You will now be able to see events from Symantec SWG in Helix.

# 2.10 Integration: FireEye Helix and PKWARE PKProtect

In the following section, PKWARE PKProtect, which has been configured to identify and encrypt sensitive data, will be configured to forward these events to FireEye Helix. Logs from PKWARE PKProtect will allow us to monitor the use of encryption throughout the enterprise, and catch any suspicious

decryptions that may indicate a breach. This section assumes the Helix Communications Broker has already been installed.

### 2.10.1 Configure the Helix Communications Broker

16. On the CentOS system with the Helix Communications Broker installed, run the following commands:

```
> cd /opt/tap-nxlog
> sudo ./setup.sh
```

- 17. Select Add Routes and press Enter.
- 18. Select bsd.
- 19. Select tcp.
- 20. Select the IP address of the network interface which should receive logs.
- 21. Enter 513 for the port.

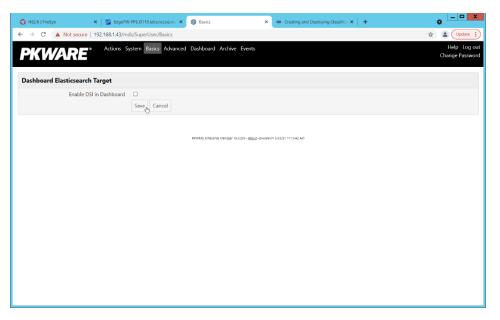
administrator@localhost:/opt/tap-nxlog	-	•	×
File Edit View Search Terminal Help			
_ INPUT SOURCE SETUP::ADD			
Input Type ( ) syslog ( ) json (X) bsd			
Protocol Type ( ) udp (X) tcp ( ) ssl			
Input Interface ( ) 192.168.122.1 (X) 192.168.1.206 ( ) 127.0.0.1			
Input Port 513			
	Cancel	OK	

- 22. Select **OK** and press **Enter**.
- 23. Select OK and press Enter.

#### 2.10.2 Configure PKWARE PKProtect to Forward Events

- 1. Navigate to the PKWARE PKProtect web portal.
- 2. Click the **Basics** link at the top of the page.
- 3. Scroll down to the Data Security Intelligence section.
- 4. Next to Dashboard Elasticsearch Target, click Internal.

- 5. Uncheck the box next to **Use Internal Elasticsearch**.
- 6. Uncheck the box next to **Enable DSI in Dashboard**.



- 7. Click Save.
- 8. In the **Data Security Intelligence** section, click **Internal** next to **Target**.
- 9. Select Syslog TCP RFC-3164 for Target.
- 10. Enter the URL and port of the Helix Communications Broker that was just configured.

🔿 HEUX   FireEye 🗙 🛛 🚮 EdgeFW-PFS.	0115.Jabs.ncco: 🗙 🕲 Basics 🗙 📾 Creating and Deploying Clas: 🗙 New Tab	×   +	• ×
← → C ▲ Not secure   192.168.1.43/mds	/SuperUser/Basics		🖈 😩 Update 🔅
PKWARE Actions Sys	Basics Advanced Dashboard Archive Events		Help Log out Change Password
Data Security Intelligence Target			
Target	Syslog TCP RFC+3164		
Url	192.168.1.206.513		
	Save Cancel		
	PORIOTE Enterprise Hangger 18.5.20 - <u>Janu</u> l - şinveneven 5.55.07 1 5.9635 PM		

- 11. Click Save.
- 12. Verify that PKWARE logs now show up in Helix.

# 2.11 Integration: FireEye Helix and Cisco Duo

In this integration, FireEye Helix will be configured to collect logs from Cisco Duo. Cisco Duo is our multifactor authentication mechanism and acts as source of information both for detecting breaches and for detecting insider threats. Information about a login, such as the username, time, location, are all useful in the event of a breach. Furthermore, they are useful as a baseline for user activity, which can be used as a comparison point for detecting unusual behavior.

## 2.11.1Configure Fireye Helix to Collect Logs from Cisco Duo

- \_ 🗆 X × 🖌 HELIX | Trellix O Applications - MITRE - Duo × + 10 \$ Search for users, groups, applications, or devices MITRE MITRE | ID: 2636-3111-77 Michael Ekstrom 🗸 Dashboard Dashboard > Applications Device Insight Applications Policies Applications Manage your update to the new Universal Single Sign-On Prompt experience, all in one place. Users Groups Get Started Get More Information Endpoints 2FA Devices 5 0 All Applications End of Support Trust Monito Q Search Export ~ Reports Application Policy Settings Name 🔺 Туре Group Policies Billina Admin API Admin API
- 1. On the Cisco Duo dashboard navigate to Applications.

2. Click Protect an Application.

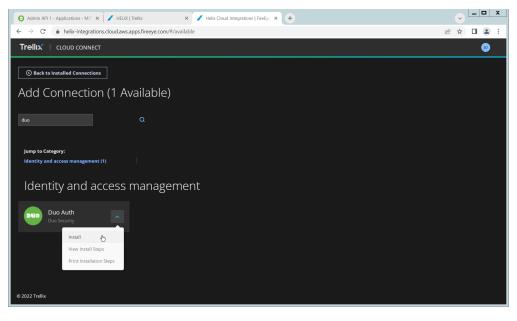
Protect an Application - Applicati     ×	/ HELIX   Trellix × +			<ul> <li>-</li> <li>-</li> </ul>	x
$\leftrightarrow$ $\rightarrow$ C $(a)$ admin-9d22ea8	39.duosecurity.com/applications/protect/types			🖻 🌣 🔲 😩	÷
<b>Bile</b>	A Search for users, groups, applications, or devices	MITRE	MITRE   ID: 2636-3111-77	Michael Ekstrom $\checkmark$	Í
Dashboard	Dashboard > Applications > Protect an Application				
Device Insight	Protect an Application				
Policies	Protect all Application				
Applications	Filter by keywords: VPN, Microsoft, SAML				
Protect an Application	Anniliantian	Durte dian Ture			
Single Sign-On	Application	Protection Type			
Users Groups	1Password	2FA	Documentation ⊡	Protect	
Endpoints					
2FA Devices	AWS Directory Service	2FA	Documentation 🗗	Protect	
Administrators					
Trust Monitor	Admin API	2FA		Protect	
Reports					
Settings	Aeries SIS	2FA	Documentation 🗗	Protect	
Billing	Aeries				
Need Use 2					

3. Click Admin API.

Helix Integration - Applications - × / HELIX   Trellix	X / Helix Cloud Integrations   FireEye X +
← → C 🔒 admin-9d22ea89.duosecurity.com/application	ons/DI4ERNLROC3L2IZTYAJZ 🖻 🖈 🗖 😩 🗄
Read Release Notes If Permissions	Grant administrators
	Permit this Admin API application to add, modify, and delete administrators and administrative units.
Account ID	Grant read information
2636-3111-77	Permit this Admin API application to read information and statistics generally used for reporting purposes.
Deployment ID	r onne uno roman n'i approation le road monnation uno diatableo generally adea le reporting perpedeo.
DUO62 Ef	Grant applications
Helpful Links	Permit this Admin API application to add, modify, and delete applications.
Documentation C	Grant settings
User Guide If	Grant settings Permit this Admin API application to read and update global account settings.
Knowledge Base D	Permit uns Admini API application to read and opdate global account settings.
	✓ Grant read log
Level Up: Training & Certification Ef	Permit this Admin API application to read logs.
Community 🗗	
	Grant read resource
	Permit this Admin API application to read resources such as users, phones, and hardware tokens.
	Grant write resource
	Permit this Admin API application to add, modify, and delete resources such as users, phones, and hardware tokens.
Networks for API access	Specify networks using a comma-separated list of IP addresses, IP ranges, or CIDRs. These must be public IP addresses, and not local or private IP addresses. If you leave this blank, access to the API will be allowed from all networks.
	Allow access to the API from these networks only:
	Example: 192.0.2.8, 198.51.100.0-198.51.100.20, 203.0.113.0/24

- 4. Scroll down and check the boxes next to Grant administrators, Grant read information, Grant applications, Grant settings, Grant read log, Grant read resource, and Grant write resource
- 5. Click Save.
- 6. Login to the Helix dashboard.
- 7. Navigate to **Configure** > **Cloud Connect**.

- 8. Click See Available Connections.
- 9. Type "Duo" in the Search box.



10. Click the Arrow next to the Cisco Duo integration and click Install.

Admin API 1 - Applications - MI	T 🗙 🖊 HELIX   Trellix 🛛 🗙 🕂			✓ - □ ×
$\leftarrow$ $\rightarrow$ C $\oplus$ admin-9d2	2ea89.duosecurity.com/applications/DI4ERNLR0C3L2IZTYA	Z		🖻 🖈 🔲 😩 🗄
Due	Q Search for users, groups, applications, or device	тім	RE MITRE   ID: 2636-3111-77	Michael Ekstrom $\sim$
Dashboard Device Insight	Successfully added Admin API to protect	ad applications. Add another.		
Policies	Dashboard > Applications > Admin API 1			
Applications Protect an Application	Admin API 1		ŀ¢	Remove Application
Single Sign-On	Setup instructions are in the Admin API document	tation 🗹.		
Users	The Admin API allows you to programmatically creater	te, retrieve, update, and delete users, phones, i	hardware tokens, admins, application	s, and more.
Groups Endpoints	Details			Reset Secret Key
2FA Devices	Integration key	Сору		
Administrators Trust Monitor	Secret key	Сору		
Reports	Don't write down you	secret key or share it with anyone.		
Settings	API hostname	Сору		
Billing	Settings			

11. Copy the **Integration Key**, **Secret Key**, and **API hostname** (not including duosecurity.com) to the appropriate fields on the Helix Cloud Connect page.

\varTheta Admin API 1 - Applications - MIT 🗙 📝 HELIX   Trellix	× / Helix Cloud Integrations   FireEye × +		✓ - □ ×
$\leftarrow$ $\rightarrow$ C $($ helix-integrations.cloud.aws.apps.fireeye.cd	om/#/install/duo		🖻 🖈 🔲 😩 🗄
Your Integration Instruction	าร		
roar meegrador mod action			
1			2
Create API Key			Verify Integration
Step 1: Create API Key		Helix Instance: hexspz443 🗸 Previous S	tep Submit and Verify
	rity admin console by following these instructions. Enter	the integration key, secret key, and API hostr	lame
below and click Submit and Verify			
	<ol> <li>Input Required</li> </ol>		
	Integration Key		
		•	
	Base64 client ID		
	Secret Key		
	Base64 secret Display hidden value		

#### 12. Click Submit and Verify.

• Helix Integration - Applications - X               • Helix Integration - Applications - X               • Helix Integration - Applications - X <th>-□ x</th>	-□ x
← → C 🔒 helix-integrations.cloud.aws.apps.fireeye.com/#/install/duo	☆ 🛛 😩 :
Trellix   Cloud Connect	U
Your Integration Instructions	- 2
Create API Key Ver	rify Integration
Step 2: Verify Integration	Back to Home
Your data has now been submitted and we will verify that Helix is receiving data. Successful Integration Your Helix instance is now ingesting data from this integration, you may close this window or return home.	
© 2022 Trellx	

13. If successful, you should see a screen about the integration being successful.

#### 2.12 Integration: FireEye Helix and QCOR ForceField

In this integration, we will configure the collection of logs from ForceField, our database encryption solution, into FireEye Helix. Detailed logs describing encryption and decryption are useful for determining how much of an enterprise is encrypted, and statistics and records in this area can prepare the organization for the event of a breach. For the purposes of this guide, we will assume ForceField is running on a Windows Server, and we would like to transfer files from this server to a Linux server. If you are using a Linux server for ForceField, you can skip to the configuration of rsyslog to forward logs directly to the Helix Comm Broker.

## 2.12.1Configure an Secure File Transfer Protocol (SFTP) server on Windows

In this section, we will configure an SFTP server on the Windows system to allow for encrypted, automated download of Forcefield's logs onto a Linux server. We have specifically elected not to use Windows Server Message Block (SMB) for this scenario because we would like to demonstrate an encrypted transfer of logs from Windows to Linux. We chose SFTP over FTPS because automation of File Transfer Protocol Secure (FTPS) would at some point require a plaintext password, while SFTP can default to the system's Secure Shell (SSH) capabilities.

Once on Linux, rsyslog can be configured to use TLS for encrypted transfer according to the needs of the organization.

- 1. Download OpenSSH from here (<u>https://github.com/PowerShell/Win32-OpenSSH/releases</u>). During the creation of this guide, version V8.9.1.0p1-Beta was used.
- 2. Extract to C:\Program Files\OpenSSH.
- 3. In a Powershell window, navigate to the folder you extracted it to, and run the following command to install the server.

powershell.exe -ExecutionPolicy Bypass -File ./install-sshd.ps1

4. Run the following command to open the firewall port for OpenSSH.

Run New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH SSH Server' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22 -Program "C:\Windows\System32\OpenSSH\sshd.exe"

- 5. Open services.msc and start the OpenSSH SSH server.
- Create a file called authorized\_keys in C:\Users\<Your Username>\.ssh. If needed, create the .ssh folder (Windows will not allow you to create it by default naming the folder .ssh. will allow you to bypass this restriction.)
- Generate a key using ./ssh-keygen. Copy the contents of the generated public key (.pub file) into the authorized\_keys file created earlier. The private key should be placed in the ~/.ssh folder on the Linux machine.
- 8. Right click the **authorized\_keys** file and click **Properties**.
- 9. Click Disable Inheritance.
- 10. Select Convert inherited permissions into explicit permissions on this object.
- 11. Using the remove button, remove all accounts other than SYSTEM from the list. Ensure that the SYSTEM account has full control.
- 12. Under C:\ProgramData\ssh, open sshd\_config.
- 13. Comment out these lines by adding '#' characters before each line, like so:

#Match Group administrators

# AuthorizedKeysFile \_\_PROGRAMDATA\_\_/ssh/administrators\_authorized\_keys

14. Add the following lines to the **sshd\_config** file to ensure that RSA public key authentication is allowed.

PubkeyAuthentication yes

PubkeyAcceptedKeyTypes=+ssh-rsa

- 15. Add the directory C:\Program Files\OpenSSH to the system path this is necessary so that the server can find the sftp-server.exe file.
- 16. Add the following lines to sshd\_config file to configure the SFTP server.

```
ForceCommand internal-sftp
ChrootDirectory C:\GreenTec\ForceField\log
```

- 17. Alternatively, if it's preferable to set the root directory somewhere else and move the log file, you can also do that. To edit the log file location, simply open C:\GreenTec\Forcefield\wfs.conf and change Logpath to a different directory, and update ChrootDirectory to point to that.
- After doing this, you should be able to authenticate over SSH to the server. If the authentication fails, you can check the logs in Event Viewer on the server, under Applications and Services Logs
   > OpenSSH > Operational to see the reason for the failure.

#### 2.12.2Configure the Linux Machine to Download and Send Logs to the Helix Communications Broker

19. On the Linux server, we can use sftp to download the file. Ensure that you replace the username and hostname with the username and hostname of your actual SSH server.

sftp administrator@forcefield.dc.ipdrr:/ForceField.log /tmp/ForceField.log

20. For automation purposes, we can use cron jobs to automatically download this file at regular intervals. Use crontab to edit the list of cron jobs.

Crontab -e

21. Enter the interval and command for sftp in the crontab file. The following line will download the log file once an hour. Ensure that you replace the username and hostname with the username and hostname of your actual SSH server.

0 \* \* \* \* sftp administrator@forcefield.dc.ipdrr:/ForceField.log
/tmp/ForceField.log

- 22. Next, we will use **rsyslog** to forward this log file to the Helix Comm Broker.
- 23. Open **/etc/rsyslog.conf**, and add the following line, using the IP and port of the Helix Comm Broker. (Note that putting a single '@' symbol here indicates UDP. Use two, such as '@@' for TCP.)

\*.\* @192.168.1.206:514

24. Create a file /etc/rsyslog.d/forcefield.conf and enter the following lines in it.

```
sudo nano /etc/rsyslog.d/forcefield.conf
$ModLoad imfile
$InputFilePollInterval 10
```

```
$PrivDropToGroup adm
$InputFileName /tmp/ForceField.log
$InputFileTag FORCEFIELD
$InputFileStateFile Stat-FORCEFIELD
$InputFileFacility local8
$InputRunFileMonitor
$InputFilePersistStateInterval 1000
```

\$ModLoad imfile \$InputFilePollInterval 10 \$PrivDropToGroup adm \$InputFileName /tmp/ForceField.log \$InputFileTag FORCEFIELD \$InputFileStateFile Stat-FORCEFIELD \$InputFileSeverity forcefield \$InputFileFacility local8 \$InputRunFileMonitor \$InputFilePersistStateInterval 1000

25. Restart rsyslog.

sudo service rsyslog restart

# 2.13 Integration: FireEye Helix and Dispel

In this integration, we configure the collection of logs from Dispel, our network protection solution. Because Dispel controls access from users to enterprise systems, it is important to have an overview of its actions through log collection and reporting. Dispel personnel can perform this integration by simply providing them with the protocol, port, and IP address of the Helix Communications Broker and allowing them to configure it on the on-premise Dispel wicket.

#### 2.14 Integration: Avrio SIFT and PKWARE PKProtect

When used together, SIFT and PKProtect can protect sensitive data accidentally dropped into public shares on the enterprise. In <u>Section 2.6</u>, we detail how to configure SIFT to detect sensitive data in a Windows Share and move it to a location designated for sensitive information. Now, we will demonstrate how to ensure that location is protected by PKProtect, which will automatically encrypt the data.

#### 2.14.1 Configuring PKWARE PKProtect

- 1. Navigate to the PKProtect dashboard and login.
- 2. Navigate to Archive > Discovery.

	Policies Di: Accounts I	stem Basics Advanced Dashboard Archive Events <sup>928</sup> icovery Remediations Classification Communities Assignments Lockers Þeployments Devices Support	Help Log ( Change Passwo
mart Filt	er Bundles	Search:	•
Туре 🔺	Filter Name	Bundle Patterns	
Discovery	HIPAA - Diagnosis Lexicon and Social Security Numbers	Social Security Number US (1 or more)         National Insurance Number UK (1 or more)         FDA Drugs Dictionary (5 or more)           FDA Firms Dictionary (5 or more)         ICD-9 Codes Dictionary (5 or more)         ICD-10 Codes Dictionary (5 or more)	Edit Clone Delete
Discovery	PCI-DSS - Credit Cards and Social Security Numbers	All Supported Credit Cards (1 or more)         International Bank Account Number (1 or more)           Social Security Number US (1 or more)         National Insurance Number UK (1 or more)	Edit Clone Delete
Discovery	Personally Identifiable Information	Social Security Number US (1 or more)         National Insurance Number UK (1 or more)         Tax ID US (1 or more)           Address US (10 or more)	Edit Clone Delete
Discovery	SSN Discovery	Social Security Number US (1 or more)	Edit Clone Delete
Discovery	Word Dictionary	Custom: Custom Dictionary Names (1 or more)	Edit Clone Delete

- 3. Click Pattern Dictionary.
- 4. Enter a name for these patterns in the **Name** field.
- 5. Enter keywords to match in the **Keywords** field.

🛃 SIFT   Secure Integrated File Tag; X 🔇 Archive - Discovery X +	. 🗆 X
← → C 🔺 Not secure   https://pkwarevm.dcipdrr/mds/SuperUser/Archive/Discovery	I 🖪 E
	lp Log out
Policies Discovery Remediations Classification Communities Assignments Lockers Chang	e Password
Accounts Deployments Devices Support	
Pattern - Dictionary	
Name Custom Dictionary Names	
Keywords malabar drake butfalo calcutta	
Choose File No file chosen Load Dictionary	
Match Whole Phrase     Match Case	
Save Cancel	
PXINARE Enterprise Manager 18.5.2019 - <u>About</u> - phaserem 17.51/23 54/634 PM	

- 6. Click Save.
- 7. Click Add Discovery.
- 8. Under **Pattern**, select the name of the **Pattern** you just created.
- 9. For **Threshold**, enter the number of matches of this pattern needed to consider the file sensitive.

🧝 SIFT   Secure Integrated File Tagg 🗙	S Archive - Discovery X +	~ <b>— — </b> X
← → C ▲ Not secure   H	tes://pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Discovery	☞ ☆ 🛛 😩 :
<b>PKWARE</b> "	Actions System Basics Advanced Dashboard Archive Events <sup>990</sup> Policies Discovery Remediations Classification Communities Assignments Lockers Accounts Deployments Devices Support	Help Log out Change Password
Discovery Smart Filter Bur	dle	
Filter Na	me Word Dictionary	
Pattern	Threshold	
Custom: Custom Dictionary Names	· 1	
Add		
Exclusions		
Patt	ms	
Inclusions	Ŀş.	
Patt	rns	
Save Cancel		
	PKNARE Enterprise Manager 18.3.203 - <u>About</u> - ploaerem 1/25/23 54634 PM	

- 10. Click Save.
- 11. Navigate to **Archive** > **Lockers**.
- 12. Ensure that a PKWARE client is installed on the device which will be monitored for encryption. The device should show up in the list. If it doesn't you can search for the device and select it from the list.

	ntegrated File Tag		hive - Lockers	× +					~		
→ C ( vices	Not secure	https://pkwa	arevm.dc.ipdrr/mds/Su	uperUser/Archive/	Lockers				€ ☆	u	
earch											
		Device Platform	Windows								
		Owner	windows								
		Owner UPN wner Email									
		Last IP									
			Search								
Show 10	✓ entries						last				
Show 10 Device	entries     Enabled	Platform	Application	Owner 🕴	Owner UPN	Owner Email	Last Accessed	Last IP	URN		
		<b>Platform</b> Windows Desktop	Application Smartcrypt 16.40.0010	Owner	Owner UPN	Owner Email		Last IP	URN 376002ef- 7035-4cad- 90ac- 03508625d5d1	k} Add	

- 13. Click **Add** on the device you wish to add a locker for.
- 14. Enter a **Name** for the locker.
- 15. Enter the **path** to the protected folder.
- 16. Select AES 256 for the Algorithm.

- 17. Select the PKWARE Smartkey to use.
- 18. Check all the boxes next to **Encryption Events**.

SIFT   Secure Integrated File Tagg 🗙 🔘 A	rchive - Lockers × +		~	_		X
← → C ▲ Not secure   https://pkv	warevm.dc.ipdrr/mds/SuperUser/Archive/Lockers	Ê	☆			÷
Name	ENCRYPT-STORAGE					-
Path	C./Share/SECRET				٦	
Algorithm	AES (256-bit)				_	
Smartkey	Community: Domain Users Commnity Key					
Whitelist						
Blacklist						
	Enable Scan-Only Mode					
	Scan-only mode disables the local file system watcher in the Locker Service.					
	Instead of reacting to real-time file system events, the Locker Service will perform traditional folder scans.					
Sweep Interval (seconds)	86400					
	Report Compliance and Status					
	Report Advanced File Attributes					
	Z Exclude Hidden Files					
	Z Exclude System Files					
Encryption Events	Report Successful Encryptions					
	Report Encryption Failures					
Discovery	Enable Discovery Mode					
Re-Encryption	Enable Re-Encryption					
Save Cancel						

- 19. Check the box next to **Enable Discovery Mode**.
- 20. Add the relevant rules to the **Smart Filter Bundles** box.
- 21. Select Report and Encrypt for Remediation Action.

🧝 SIFT   Secure Integrated Fil	Tagg X 🕲 Archive - Lockers X +		~	-	-	X
← → C ▲ Not se	zure   https://pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Lockers	Ē	☆			÷
	<ul> <li>Report Advanced File Attributes</li> <li>Exclude Hidden Files</li> <li>Exclude System Files</li> </ul>					
Discovery	C Enable Discovery Mode					
Remediation Actio	ns					
▲ Sr	nart Filter Bundles Remediation Action					
= PC	PAA - Diagnosis Lexicon and Social Security Numbers     Physical Security Numbers       PDS5 - Credit Cards and Social Security Numbers     Physical Security Numbers       Sconally Identifiable Information     SSN Discovery       World Dictionary     World Dictionary	<u>Dele</u>	<u>ete</u>			
Showing 1 to 1 of 1 e						
Re-Encryption	Enable Re-Encryption					
	PONIARE Enterprise Manager 18.5203 - <u>Abput</u> - pixoareum 1/25/23 54808 PM					

- 22. Click Save.
- 23. Now the folder on the device you selected will be monitored, and files which match the selected rules will be encrypted automatically.

# 2.15 Integration: Dispel and Cisco Duo

In this build, Dispel acts as an intermediary between the user and enterprise systems, by providing temporary remote desktops with access to enterprise systems. In this integration, we primarily installed Cisco Duo on the enterprise systems, to require multifactor authentication over RDP between Dispel's temporary remote desktops and the enterprise systems.

In this particular integration, no extra work was required other than installing Cisco Duo (see <u>Section</u> 2.7) on systems to control remote desktop access between Dispel machines and the other machines. However, it is important for organizations to check that this integration works and is present, to ensure that multifactor authentication is being applied to users who are logging in remotely.

# Appendix A List of Acronyms

Provide a list of alphabetized acronyms and abbreviations and spell out each one. Use Word Style: Glossary. Bold each acronym to enhance readability.

SIEM	Security Information and Event Management
RDP	Remote Desktop Protocol
IP	Internet Protocol
ТСР	Transmission Control Protocol
SFTP	Secure File Transfer Protocol
DNS	Domain Name Service
NTP	Network Time Protocol
2FA	Two Factor Authentication
UDP	User Datagram Protocol
WSS	Web Security Service
TLS	Transport Layer Security
SSL	Secure Sockets Layer
GPO	Group Policy Object
PAC	Proxy Auto Configuration
AES	Advanced Encryption Standard
REST	Representational State Transfer
ΑΡΙ	Application Programming Interface
WFS	Write-protected File System