

HOW PROOFPOINT HELPS ORGANIZATIONS MEET NIST CYBERSECURITY GUIDELINES

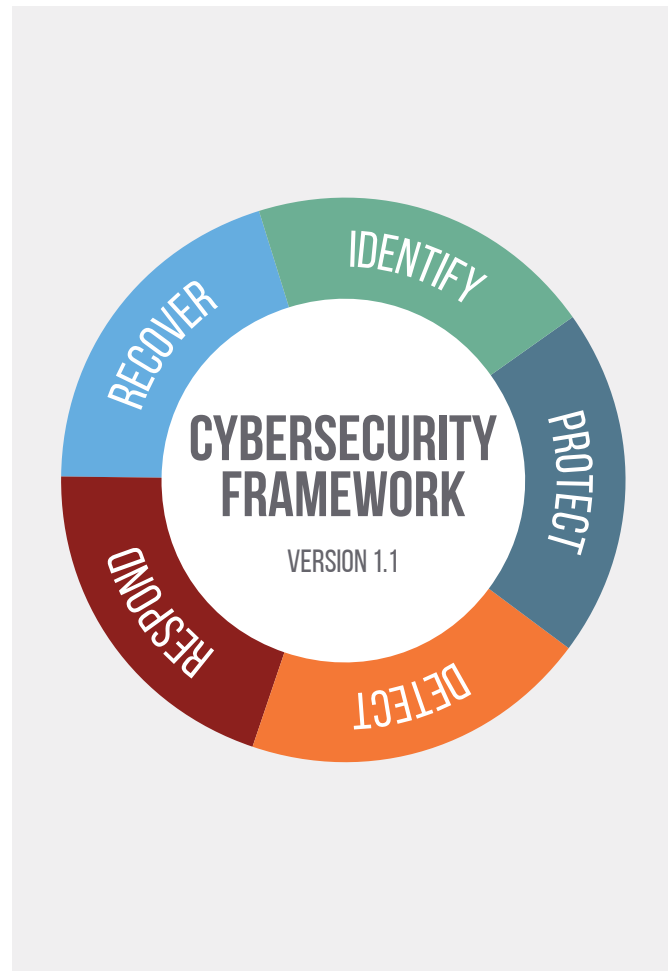
INTRODUCTION

In the face of today's security threats, it's important to build a strong defense. The National Institute of Standards and Technology (NIST) Cybersecurity Framework 1.1 is designed to help. It provides you with critical guidance when developing your security programs. You can use it to assess your entire cybersecurity posture, or tailor it to measure against the specific requirements of your organization.

Proofpoint solutions fit easily into this framework and provide NIST compliance across the following key areas:

- Risk assessment
- Awareness and training
- Data security
- Anomalies and events
- Security continuous monitoring
- Detection processes
- Analysis
- Mitigation

This document explains how Proofpoint can help you meet NIST guidelines and achieve your security goals.



HOW PROOFPOINT CAN HELP

<p>Proofpoint Targeted Attack Protection (TAP) provides risk assessment with deep visibility into threats entering your organization.</p>	<p>Proofpoint Email Protection identifies email fraud at the gateway, and prevents it from reaching recipients.</p>	<p>Proofpoint Premium Threat Intelligence Service (PTIS) offers detailed threat reports, analyst observations, and access to our threat experts.</p>
<p>Proofpoint Phishing Simulation and Security Awareness Training helps your people understand and protect against threats.</p>	<p>Proofpoint Threat Response Auto-Pull automatically removes malicious emails from the recipient's inbox.</p>	<p>Proofpoint Email Data Loss Prevention (DLP) prevents data loss stemming from negligence or email fraud.</p>
<p>Proofpoint Data Discover identifies private information improperly secured on the network, so you can enforce policy.</p>	<p>Proofpoint Mobile Defense provides protection for iOS and Android devices, apps and networks.</p>	<p>Proofpoint Email Encryption lets you communicate securely with policy-based encryption of messages and attachments.</p>

RISK ASSESSMENT (ID.RA)

Overall goal: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

REQUIREMENT ID.RA-2

Threat and vulnerability information is received from information sharing forums and sources.

References:

- **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** PM-15, PM-16, SI-5

Products that help meet the requirement:

- TAP
- PTIS

The Nexus platform analyzes 20 billion emails per day, and over 5 million malware samples collected from the Emerging Threats Malware Exchange.

REQUIREMENT ID.RA-3

Threats, both internal and external, are identified and documented.

References:

- COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04

Products that help meet the requirement:

- TAP
- PTIS

The TAP Threat Dashboard can be accessed through a web browser. You get deep visibility into the threats entering your organization. See who is attacking, which users are under attack, how they're attacking, and what they're after.

It shows you data at the organization, threat, and user levels. This detail helps you prioritize alerts and act on them.

PTIS offers detailed threat reports, analyst observations and access to our threat experts.

REQUIREMENT ID.RA-4

Potential business impacts and likelihoods are identified.

References:

- **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12
- **COBIT 5** DSS04.02
- **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12
- **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14

Products that help meet the requirement:

- TAP
- PTIS

Using the TAP Threat Dashboard, users have visibility into potentially infected users, including high-value users. With this insight, you can understand the potential impact and prioritize remediation efforts.

REQUIREMENT ID.RA-5

Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

References:

- **COBIT 5** APO12.02
- **ISO/IEC 27001:2013** A.12.6.1
- **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16

Products that help meet the requirement:

- TAP
- PTIS

TAP provides insight into how widespread or targeted a threat is, helping you determine your risk.

REQUIREMENT ID.RA-6

Risk responses are identified and prioritized.

References:

- **COBIT 5** APO12.05, APO13.02
- **NIST SP 800-53 Rev. 4** PM-4, PM-9

Products that help meet the requirement:

- TAP
- PTIS

Through TAP, you can see infected users and high-value targets to prioritize your response and manage risk.

AWARENESS AND TRAINING (PR.AT)

Overall goal: The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

REQUIREMENT PR.AT-1

All users are informed and trained.

References:

- **CCS CSC** 9
- **COBIT 5** APO07.03, BAI05.07
- **ISA 62443-2-1:2009** 4.3.2.4.2
- **ISO/IEC 27001:2013** A.7.2.2
- **NIST SP 800-53 Rev. 4** AT-2, PM-13

Products that help meet the requirement:

- Phishing Simulation and Security Awareness Training

We offer comprehensive end-user security awareness training across a wide range of security topics.

REQUIREMENT PR.AT-2

Privileged users understand roles & responsibilities.

References:

- **CCS CSC** 9
- **COBIT 5** APO07.02, DSS06.03
- **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3

- **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
- **NIST SP 800-53 Rev. 4** AT-3, PM-13

Products that help meet the requirement:

- Phishing Simulation and Security Awareness Training

We offer training modules tailored to privileged users and other high-value targets.

REQUIREMENT PR.AT-3

Third-party stakeholders (such as suppliers, customers, partners) understand roles and responsibilities.

References:

- **CCS CSC 9**
- **COBIT 5** APO07.03, APO10.04, APO10.05
- **ISA 62443-2-1:2009** 4.3.2.4.2
- **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
- **NIST SP 800-53 Rev. 4** PS-7, SA-9

Products that help meet the requirement:

- Phishing Simulation and Security Awareness Training

We can help outside vendors and partners understand and protect against threats.

REQUIREMENT PR.AT-4

Senior executives understand roles and responsibilities.

References:

- **CCS CSC 9**
- **COBIT 5** APO07.03
- **ISA 62443-2-1:2009** 4.3.2.4.2
- **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
- **NIST SP 800-53 Rev. 4** AT-3, PM-13

Products that help meet the requirement:

- Phishing Simulation and Security Awareness Training

We train executives to recognize threats that might affect them and to understand that they are highly targeted.

REQUIREMENT PR.AT-5

Physical and information security personnel understand roles and responsibilities.

References:

- **CCS CSC 9**
- **COBIT 5** APO07.03
- **ISA 62443-2-1:2009** 4.3.2.4.2
- **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
- **NIST SP 800-53 Rev. 4** AT-3, PM-13

Products that help meet the requirement:

- Proofpoint Phishing Simulation and Security Awareness Training

We offer training modules tailored to security personnel.

DATA SECURITY (PR.DS)

Overall goal: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

REQUIREMENT PR.DS-1

Data-at-rest is protected.

References:

- **CCS CSC 17**
- **COBIT 5** APO01.06, BAI02.01, BAI06.01, 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** SC-28

Products that help meet the requirement:

- Data Discover

Data Discover identifies private information that is improperly secured on the network, enabling administrators to enforce policy.

REQUIREMENT PR.DS-2

Data-in-transit is protected.

References:

- **CCS CSC 17**
- **COBIT 5** APO01.06, 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

Products that help meet the requirement:

- Email Data Loss Prevention
- Email Encryption

Policy-based encryption can enforce DLP and Encryption rules automatically without administrator or end-user involvement.

REQUIREMENT PR.DS-5

Protections against data leaks are implemented.

References:

- **CCS CSC 17**
- **COBIT 5** APO01.06
- **ISA 62443-3-3:2013** SR 5.2
- **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
- **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

Products that help meet the requirement:

- Email Data Loss Prevention
- Email Encryption

Guards against leaks of private and confidential information in email and web protocols with highly accurate detection using smart identifiers and managed dictionaries. If sensitive data is detected, encryption policies can be enforced on the data to prevent it from being usable except by intended recipients.

ANOMALIES AND EVENTS (DE.AE)

Overall goal: Anomalous activity is detected in a timely manner and the potential impact of events is understood.

REQUIREMENT DE.AE-2

Detected events are analyzed to understand attack targets and methods.

References:

- **COBIT 5** DSS03.01
- **ISA 62443-2-1:2009** 4.4.3.3
- **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4

Products that help meet the requirement:

- Email Protection
- TAP
- PTIS

We sandbox all URLs and attachments, identifying malware and preventing it from getting into the environment. Proofpoint Email Protection identifies email fraud at the gateway and prevents it from reaching the intended recipient. TAP allows for inspection of threats to determine exactly how the attack was carried out. PTIS provides even deeper individualized context from security analysts about specific targeted attacks.

REQUIREMENT DE.AE-3

Event data are aggregated and correlated from multiple sources and sensors.

References:

- **ISA 62443-3-3:2013** SR 6.1
- **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4

Products that help meet the requirement:

- TAP
- PTIS

We sandbox all URLs and attachments, identifying malware and preventing it from getting into the environment. TAP allows for inspection of threats to determine exactly how the attack was carried out. PTIS provides even deeper individualized context from security analysts about specific targeted attacks.

REQUIREMENT DE.AE-4

Impact of events is determined.

References:

- **COBIT 5** APO12.06
- **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4

Products that help meet the requirement:

- TAP
- PTIS

We sandbox all URLs and attachments, identifying malware and preventing it from getting into the environment. TAP allows for inspection of threats to determine exactly how the attack was carried out. PTIS provides even deeper individualized context from security analysts about specific targeted attacks.

REQUIREMENT DE.AE-5

Incident alert thresholds are established.

References:

- **COBIT 5** APO12.06
- **ISA 62443-2-1:2009** 4.2.3.10
- **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8

Products that help meet the requirement:

- TAP

TAP alerts administrators when it discovers a potential threat.

SECURITY CONTINUOUS MONITORING (DE.CM)

Overall goal: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

REQUIREMENT DE.CM-3

Personnel activity is monitored to detect potential cybersecurity events.

References:

- **ISA 62443-3-3:2013** SR 6.2
- **ISO/IEC 27001:2013** A.12.4.1
- **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11

Products that help meet the requirement:

- Email Protection
- TAP
- Mobile Defense

We can monitor user activity across email, social and mobile to detect potential cybersecurity events.

REQUIREMENT DE.CM-4

Malicious code is detected.

References:

- **CCS CSC** 5
- **COBIT 5** DSS05.01
- **ISA 62443-2-1:2009** 4.3.4.3.8
- **ISA 62443-3-3:2013** SR 3.2
- **ISO/IEC 27001:2013** A.12.2.1
- **NIST SP 800-53 Rev. 4** SI-3

Products that help meet the requirement:

- TAP
- Mobile Defense

We identify malicious code located in email or mobile applications that are designed to infect a user or steal data.

REQUIREMENT DE.CM-5

Unauthorized mobile code is detected.

Products that help meet the requirement:

- Mobile Defense

Mobile Defense protects devices against malicious code (such as xCodeGhost and iBackDoor) embedded in apps.

DETECTION PROCESSES (DE.DP)

Overall goal: Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

REQUIREMENT DE.DP-4

Event detection information is communicated to appropriate parties.

References:

- **COBIT 5** APO12.06
- **ISA 62443-2-1:2009** 4.3.4.5.9
- **ISA 62443-3-3:2013** SR 6.1
- **ISO/IEC 27001:2013** A.16.1.2
- **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4

Products that help meet the requirement:

- TAP
- PTIS

We alert administrators to a threat, and can also integrate into a SIEM to aggregate threat data.

ANALYSIS (RS.AN)

Overall goal: Analysis is conducted to ensure adequate response and support recovery activities.

REQUIREMENT RS.AN-2

The impact of the incident is understood.

References:

- **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
- **ISO/IEC 27001:2013** A.16.1.6
- **NIST SP 800-53 Rev. 4** CP-2, IR-4

Products that help meet the requirement:

- TAP

The TAP Threat Dashboard can be accessed through a web browser. You get visibility into the threats entering your organization. See who is attacking, how they're attacking, and what they're after.

We provide data at organization, threat and user level. This detail helps you prioritize alerts and act on them.

REQUIREMENT RS.AN-3

Forensics are performed.

References:

- **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
- **ISO/IEC 27001:2013** A.16.1.7
- **NIST SP 800-53 Rev. 4** AU-7, IR-4

Products that help meet the requirement:

- TAP
- PTIS

The TAP Threat Dashboard provides detailed forensic information on threats and campaigns in real time. You get downloadable reports and can integrate with other tools through APIs. The dashboard offers forensics screenshots, detailed sandbox results, indicators of compromise, and targeted nature of attack. It also provides threat campaign data and information about the threat actor when available.

MITIGATION (RS.MI)

Overall goal: Activities are performed to prevent expansion of an event, mitigate its effects and eradicate the incident.

REQUIREMENT RS.MI-1

Incidents are contained.

References:

- **ISA 62443-2-1:2009** 4.3.4.5.6
- **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4
- **ISO/IEC 27001:2013** A.16.1.5
- **NIST SP 800-53 Rev. 4** IR-4

Products that help meet the requirement:

- Email Protection
- TAP

Email threats are identified and blocked at the gateway. Malicious emails are sent to quarantine for analysis by security administrators.

REQUIREMENT RS.MI-2

Incidents are mitigated.

References:

- **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10
- **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5
- **NIST SP 800-53 Rev. 4** IR-4

Products that help meet the requirement:

- Email Protection
- TAP
- TRAP
- Email Encryption

If email threats are detected, malicious emails are automatically removed from the inbox of the victims.

Emails leaving the organization that contain sensitive data can be automatically encrypted using policy-based encryption.

To learn more about how Proofpoint can help you comply
with the NIST cybersecurity framework, visit

proofpoint.com

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint.

www.proofpoint.com

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.

0518-022