Forcepoint

Solution Brief

Forcepoint Solutions to Meet NIST 2.0 Standards

Challenge

- **Evolving Risks & Regulations –** Organizations struggle to manage increasing cyber risks and changing regulatory requirements.
- **Inconsistent Security Policies –** Fragmented security controls across access channels create compliance gaps.
- **Limited Visibility & Control –** Lack of centralized management and alerts makes detecting security risks and policy violations difficult.

Solution

- **Zero Trust Security –** Continuous monitoring that protects data across endpoints, network, cloud, web and email.
- **AI-Powered Classification –** Intelligent continuous learning data classification engine enhances accuracy for effective policy enforcement.
- **Flexible Deployment –** Cloud, on-prem and hybrid options to align with business needs.

Outcome

- **Streamlined Compliance –** Centralized and adaptive protection reduces data loss risks before compliance violations occur.
- **Reduced Operational Burden –** Unified management and automated enforcement minimize manual effort.
- **Enables Business Growth –** Secure collaboration to support business innovation.

> The National Institute of Standards and Technology (NIST) cybersecurity framework is a cornerstone for many organizations aiming to bolster their security across many different domains in safeguarding critical assets and data while improving the management and response to risks and threats.

With the past introduction of NIST 2.0 CSF (Cybersecurity Framework) back in February 2024, the new guideline helps organizations improve their cybersecurity posture with a more simplified approach.

Forcepoint recognizes the significant role NIST plays in guiding organizations toward better security practices. We are committed to supporting these efforts by providing solutions that help identify, classify and protect sensitive data while enabling detection and response to potential exfiltration incidents. By aligning with NIST principles, Forcepoint enables organizations to meet compliance standards, enhance data protection and defend against risks in today's increasingly digital landscape.

What is NIST?

The National Institute of Standards and Technology is an agency within the U.S. Department of Commerce that provides guidance on compliance, privacy and security. Within the realm of cybersecurity, NIST Cybersecurity Framework (NIST CSF) gives information on core functions to allow organizations to strategize and build a successful cybersecurity program. The framework outlines the functions of Identify, Protect, Detect, Respond and Recover with the overarching function, Govern, which enables the business to determine which decisions best fit their strategy. Being a voluntary framework, NIST CSF is designed to offer high-level guidance while other standards such as NIST SP 800-53, 800-221, 800-171 and others provide specific guidelines.

Safeguarding Data Against Emerging Threats

The NIST Cybersecurity Framework by design allows organizations to be flexible in their cybersecurity posture. CSF describes the desired outcomes of different security controls at a high level while providing the tools and resources for a more granular outline on process, people and technology.

With the ever-increasing adoption of new technologies such as generative AI, many organizations face the challenge of protecting their sensitive data while using these tools. Abuse of these tools, whether intended or not, can lead to serious consequences for organizations. Confidential or sensitive information can be leaked over these tools, or the training of an AI model can be poisoned due to malicious content. Forcepoint is dedicated to helping organizations gain visibility over their data, protecting it and preventing its misuse.

The CSF continues to provide guidance and best practices for organizations in building, implementing and maintaining their cybersecurity programs. With new technology, organizations will need to think about how these tools can be used so they can communicate, measure and monitor risks.

Protection with Zero Trust

Incorporating Zero Trust is the practice and understanding that every request can be a potential threat. Applications, systems and people are not trusted unless they can be authenticated, whether they're in or out of the network.

The NIST 2.0 framework has embraced principles of Zero Trust architecture, in which core functions focus on Identity and Access Management and Privileged Access Management. These guidelines and architecture help organizations mitigate their risk while protecting their data.

Forcepoint offers data-first security solutions with Zero Trust in mind. This allows organizations to mitigate their risk by preventing sensitive data exfiltration to allow them to remain within compliance no matter where their employees or data are located.

Navigating Evolving Security Risks and Compliance Requirements

The NIST Cybersecurity Framework (CSF) 2.0 provides organizations with a flexible, high-level approach to managing cybersecurity risks. However, effectively implementing its core functions and prioritizing controls remains a challenge. Organizations must determine which security measures best align with their business needs while ensuring long-term adaptability.

Because NIST CSF is a voluntary guideline, some organizations risk adopting a "check-the-box" approach, focusing only on compliance rather than building a dynamic, resilient security strategy. To maximize effectiveness, businesses must continuously assess risks, refine security policies and align resources to keep pace with evolving threats.

Key Compliance Challenges Organizations Face:

→ **Staying Ahead of Evolving Threats and Regulations –** Businesses struggle to keep up with increasingly sophisticated cyber risks and shifting regulatory requirements.

→ **Inconsistent Policy Enforcement –** Many organizations lack a unified security strategy across endpoints, SaaS apps, web traffic and email, leading to security gaps and compliance risks.

→ **Gaps in Visibility and Control –** Without centralized data security management and real-time enforcement, identifying security gaps, policy violations and insider threats becomes significantly more difficult.

To successfully adhere to NIST 2.0 and strengthen security resilience, organizations need a proactive, risk-based approach that ensures unified policy enforcement, real-time threat detection and continuous monitoring across all digital environments.

A Unified, Adaptive Approach to Data Security

Organizations adopting NIST CSF 2.0 need a structured approach to risk management, policy enforcement and data protection that aligns with the framework's core functions. Forcepoint provides solutions designed to help organizations meet these requirements while improving security operations, reducing compliance complexity and addressing security risks before they become compliance violations.

Zero Trust Security Framework

Forcepoint's data security architecture is based on Zero Trust principles, ensuring that data usage is continuously monitored and verified, least-privilege policies are enforced and potential risks – both external and internal – are mitigated in real time. This approach aligns with NIST's recommendations for proactive risk management and access control.

Unified Policy and Compliance Management

→ **Unified Security Policies –** A single policy framework applies consistent security controls across endpoints, SaaS apps, web and email, addressing NIST's need for integrated security management.

→ **Automated Compliance Controls –** Pre-built and customizable policies for data protection, access control and incident response align with NIST CSF 2.0 recommendations.

→ **AI-Powered Data Classification –** Accurately identifies and categorizes sensitive data at rest, in motion and in use, reducing compliance blind spots.

Behavior-Based Detection and Enforcement

→ **Risk-Adaptive Protection –** Uses behavioral analytics to automatically adjust policy enforcement based on real-time risk levels.

→ **Forensics and Incident Investigation –** Provides detailed logging and analysis of security events and policy violations, helping organizations strengthen their incident response processes.

Deployment Flexibility and Scalability

→ **Cloud, On-Prem and Hybrid Options –** Organizations can deploy Forcepoint's solutions based on their security infrastructure needs while maintaining policy consistency.

→ **Scalable Security Management –** As security and compliance needs evolve, Forcepoint enables organizations to expand their protection without operational disruption.

Forcepoint's solutions are designed to help organizations operationalize NIST 2.0 guidelines, enforce security policies at scale and strengthen their overall cybersecurity posture.

Simplifying Compliance to Enable Innovation and Growth

Aligning with NIST CSF 2.0 provides a structured, risk-based approach to cybersecurity, helping organizations strengthen data protection while streamlining compliance. Continuous monitoring and adaptive controls reduce the risk of data loss and breaches by proactively identifying vulnerabilities before they become regulation violations.

By integrating modern data security with business operations, organizations can enable secure collaboration, support digital transformation and drive innovation without compromising compliance. A structured, risk-based approach strengthens security, optimizes operations and allows businesses to focus on growth.

Data Protection

The Forcepoint Data Security Everywhere approach protects sensitive information across all key access channels, unifying security enforcement and simplifying management.

FORCEPOINT DATA SECURITY SOLUTIONS
Forcepoint Data Loss Prevention (On-Premises / Hybrid / Cloud) – Endpoint, Network, Discovery, Email, SaaS apps, Web
Forcepoint DSPM (Data Security Posture Management, On-Premises / Cloud)
Forcepoint Risk-Adaptive Protection (On-Premises / Cloud)

Network Protection

Forcepoint security solutions deliver comprehensive protection across networks, cloud applications, email and web to prevent data loss, control access and ensure compliance.

FORCEPOINT NETWORK SOLUTIONS
Forcepoint (CASB and ZTNA)
Forcepoint Web Security (On-Premises / Hybrid / Cloud)
Forcepoint Email Security (On-Premises / Cloud)
Forcepoint NGFW and Secure SD-WAN
Forcepoint RBI (Remote Browser Isolation) with CDR (Content Disarm and Reconstruction)

Forcepoint Solutions Mapped to NIST CSF 2.0

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
IDENTIFY			
ID.AM-02	Inventories of software, services and systems managed by the organization are maintained	Forcepoint Network Solutions	Forcepoint solutions can provide logs and reports which can assist organizations in understanding web traffic, cloud application and data usage. Policy controls also allow organizations to determine which websites and cloud apps are appropriate for use while identifying or blocking categories and cloud apps that are inappropriate or unsafe.
ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained	Forcepoint Network Solutions	Forcepoint solutions can monitor network, web, cloud and private application usage for managed and unmanaged network/devices. With policy controls, Forcepoint solutions can identify or block access to these destinations based on risk, compliance or even productivity loss.
ID.AM-04	Inventories of services provided by suppliers are maintained	Forcepoint Network Solutions	Forcepoint CASB, Web Security and NGFW can also detect, manage and block traffic as well as access, to external sites and both managed and unmanaged SaaS applications. Additionally, Forcepoint NGFW can monitor the health of services.
ID.AM-05	Assets are prioritized based on classification, criticality, resources and impact on the mission	Forcepoint Data Security Solutions	Forcepoint helps in classifying, identifying and prioritizing data for protection through Forcepoint DSPM, Forcepoint Classification, Data Detection and Response (DDR), Enterprise DLP and Risk-Adaptive Protection (RAP). Forcepoint network solutions can also apply QoS rules and health monitoring.
ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	Forcepoint Data Security Solutions	Forcepoint allows organizations to discover, inventory and tag data within the environment, including the ability to maintain data registry of the data and responsible parties.
ID.AM-08	Systems, hardware, software, services and data are managed throughout their life cycles	Forcepoint Data Security	Forcepoint DSPM + DDR continually monitors data throughout its lifecycle to classify and re-classify data as it changes, tracking the lineage and even flagging for ROT data at the end of the lifecycle.

Forcepoint Solutions Mapped to NIST CSF 2.0

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
IDENTIFY			
ID.RA-01	Vulnerabilities in assets are identified, validated and recorded	Forcepoint Network Solutions	Forcepoint solutions can identify risks with websites in real time as well as address risk scores with cloud applications. Forcepoint offers insight into why such cloud resources are risky, with on-screen prompts or in-console messaging. Additionally, Forcepoint NGFW IPS/Inspection capabilities assess vulnerabilities outside of standard web channels.
ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	Forcepoint Network Solutions	Forcepoint solutions pull in threat feeds from various sources as well as our own dedicated teams that research and analyze cyber threats. This information is fed into our ACE (Advanced Classification Engine) and in conjunction our ThreatSeeker intelligence network, which is used to help identify and block cyber threats with our solutions. With this information, organizations can also create custom categories for Forcepoint Web Security solutions.
ID.RA-03	Internal and external threats to the organization are identified and recorded	Forcepoint Data Security Solutions Forcepoint Network Solutions	Any threat detected or blocked by Forcepoint solutions is logged and recorded. Organizations can use this information to identify the source, destination and other details associated with the event.
ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	Forcepoint Network Solutions	Any cyber threat that Forcepoint identifies and blocks is logged and recorded. Additionally, Forcepoint updates its threat detection engines daily. Other Forcepoint solutions such as Remote Browser Isolation, Content Disarm and Reconstruction and Advanced Malware Detection are designed to identify and stop zero-day threats.
ID.RA-05	Threats, vulnerabilities, likelihoods and impacts are used to understand inherent risk and inform risk response prioritization	Forcepoint Network Solutions	For any detected/blocked cyber threat by Forcepoint, logs are available for organizations to understand the source and type of threat. Additionally, threats are categorized by severity level depending on the type of threat.
ID.RA-06	Risk responses are chosen, prioritized, planned, tracked and communicated	Forcepoint Network Solutions	Forcepoint assists with this by providing information and tracking based on what threat was detected or blocked by providing information such as source, destination, threat type, etc.
ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded and tracked		Any configuration change within Forcepoint solutions is logged so organizations can review and re-implement policies based on their assessment. Additionally, Forcepoint supports a workflow framework and bi-direction API for integration with third-party ticket management solutions.
ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use		Forcepoint provides hashes for all released software downloadable files.
ID.RA-10	Critical suppliers are assessed prior to acquisition	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint can share any information involved about the products we offer, like how to administer them as well as any details involving the contract.

Forcepoint Solutions Mapped to NIST CSF 2.0

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
IDENTIFY			
ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties		Forcepoint solutions provide details involving cyber threats or data security events. Reports generated from this information can assist organizations in determining what areas need improvement.
ID.IM-03	Improvements are identified from execution of operational processes, procedures and activities		Forcepoint solutions provide details involving cyber threats or data security events. Reports generated from this information can assist organizations in determining what areas need improvement.

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
PROTECT			
PR.AA-01	Identities and credentials are managed for authorized devices and users	Forcepoint Data Security Solutions	Indirectly involved, Forcepoint helps limit interactions with sensitive data leaving the environment with Enterprise DLP and DLP for Email. Additionally, Forcepoint CASB can offer conditional access for SaaS apps based on SAML SSO authentication.
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions provide detailed logs of activity which can help organizations identify users or systems that are performing actions. With Risk-Adaptive Protection, credentials are bound to the context of local users, systems and data actions.
PR.AA-03	Users, services and hardware are authenticated	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions implement Zero Trust methods for authenticating users. Additionally, connections to Active Directory, Single Sign-On and Multi-Factor Authentication services are utilized.
PR.AA-04	Identity assertions are protected, conveyed and verified	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions that use any SAML 2.0 SSO or authentication through federated systems follow industry standards.
PR.AA-05	Access permissions, entitlements and authorizations are defined in a policy, managed, enforced and reviewed, and incorporate the principles of least privilege and separation of duties	Forcepoint Data Security Solutions Forcepoint Network Solutions	Organizations can utilize Forcepoint to restrict access to web resources, private applications, data and networks. Additionally, Forcepoint solutions offer role-based access controls which can prohibit access to areas within the solutions. Based on the role, users can have access to create/modify policy controls, run reports and manage the infrastructure or platform configuration.

Forcepoint Solutions Mapped to NIST CSF 2.0

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
PROTECT			
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions can provide tailored messaging for training. This form of user coaching can enable organizations to be more aware of potential cybersecurity threats.
PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint requires our partners and encourages users of our solutions to undergo our product training. Forcepoint also provides many knowledge articles, how-to videos and documentation to provide skills and knowledge to users of our solutions.
PR.DS-01	The confidentiality, integrity and availability of data-at-rest are protected	Forcepoint Data Security Solutions	Forcepoint can discover and classify data-at-rest with Forcepoint DSPM. The solutions are capable of providing this capability across on-prem and cloud resources while being a hybrid deployed solution.
PR.DS-02	The confidentiality, integrity and availability of data-in-transit are protected	Forcepoint Data Security Solutions	Forcepoint DLP can protect sensitive data-in-transit over web resources such as websites, cloud and custom applications, email and endpoint channels. The solutions are capable of providing this capability across on-prem and cloud resources while being a hybrid deployed solution.
PR.DS-10	The confidentiality, integrity and availability of data-in-use are protected	Forcepoint Data Security Solutions	Forcepoint DLP protects sensitive data by preventing unauthorized exfiltration of data that is being cut/copied/pasted, applications accessing files, printing, removable media and email. DLP enforcement controls are active regardless of where the user's machine is located. Controls are active on-site and remotely. The solutions are capable of providing this capability across on-prem and cloud resources while being a hybrid deployed solution.
PR.PS-01	Configuration management practices are established and applied	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions have pre-defined controls that can enable organizations to apply best practices in regard to network controls and data security needs. These pre-defined policies allow organizations to quickly deploy security controls for the environment.
PR.PS-04	Log records are generated and made available for continuous monitoring	Forcepoint Data Security Solutions Forcepoint Network Solutions	Organizations can use Forcepoint solutions to monitor user activity across different channels to make sure they comply with company policy. This includes both network channels and channels for data exfiltration. Forcepoint DLP retains forensic data records for future audits.
PR.PS-05	Installation and execution of unauthorized software are prevented	Forcepoint Network Solutions	Forcepoint can prevent download of potentially malicious payloads proactively preventing execution on the user machine.

Forcepoint Solutions Mapped to NIST CSF 2.0

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
PROTECT			
PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	Forcepoint Network Solutions	Forcepoint network solutions can prevent users from accessing specific categories of the web and cloud applications, and can detect and prevent incoming/outbound traffic to networks in addition to east-west traffic via SD-WAN/NGFW.
PR.IR-02	The organization's technology assets are protected from environmental threats	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions can be deployed in high-availability configurations to comply with disaster recovery plans.
PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint cloud solutions have mechanisms in place to maintain uptime. For any on-premises deployment, Forcepoint recommends high-availability and hybrid deployments.

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
DETECT			
DE.CM-01	Networks and network services are monitored to find potentially adverse events	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint monitors web and network traffic for potential data loss, general, malicious network traffic and the monitoring of insider threats via Risk-Adaptive Protection and Forcepoint Insider Threat.
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions can monitor user activity with real-time risk calculation to monitor network and data events. Additionally, Forcepoint Risk-Adaptive Protection can monitor user activity with real-time risk calculations across 130+ indicators of behavior.
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	Forcepoint Network Solutions	Forcepoint solutions can monitor user activity and solution applications with real-time risk calculation to monitor network and data events. Additionally, Forcepoint controls such as ZTNA can help monitor external connections to internal applications to identify and block for potentially adverse events.
DE.CM-09	Computing hardware and software, runtime environments and their data are monitored to find potentially adverse events	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions can monitor user activity and solution applications with real-time risk calculation to monitor network and data events. Forcepoint solutions monitor/block data exfiltration and network traffic to determine if events are adverse based on established policy controls.

Forcepoint Solutions Mapped to NIST CSF 2.0

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
DETECT			
DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint can provide incident details that can help determine if an event is adverse or not by enabling SOC teams with in-depth log details and forensics.
DE.AE-03	Information is correlated from multiple sources	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions can provide centralized reporting to help consolidate incidents to help organizations respond appropriately. Additionally, the ThreatSeeker network correlates from all Forcepoint deployments to help identify threats.
DE.AE-04	The estimated impact and scope of adverse events are understood	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions can provide rich incident details along with severity and risk rankings to help organizations understand impact.
DE.AE-06	Information on adverse events is provided to authorized staff and tools	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions provide detailed information on events which can be controlled for viewing by RBAC. When Forcepoint detects an incident, alerts can be generated to be sent to appropriate teams via dashboard alerts, email and integration with third-party tools (e.g., SIEM, ticketing systems)
DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint policies utilize contextual analysis and integrations with other feeds (e.g., SIEM, third-party intelligence feeds) to identify risk events and/or identify and block data exfiltration actions.
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint provides incident details based on violated established policy controls to assist organizations in the declaration process.

Forcepoint Solutions Mapped to NIST CSF 2.0

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
RESPOND			
RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint policies offer proactive and reactive actions that align with the organization's incident response plans. Bi-directional API also aids in incident response workflows with third-party solutions.
RS.MA-02	Incident reports are triaged and validated	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions provide centralized management and reporting to help triage and investigate threats.
RS.MA-03	Incidents are categorized and prioritized	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint incidents can be sorted based on source, severity, policy, etc. Prioritization can be based on the most recent, highest severity, highest risk score, etc.
RS.MA-04	Incidents are escalated or elevated as needed	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint provides detailed information on incidents with severity levels / risk scores which can help prioritize incidents/cases for escalation.
RS.MA-05	The criteria for initiating incident recovery are applied	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint can provide detailed information about an incident which can contribute to incident recovery processes.
RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint can provide detailed information about an incident to include source, destination, channel and rules violated along with forensics information for detected data security events.
RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint keeps an audit trail of admin activities along with forensic incident details, which can be preserved within an encrypted location.

Forcepoint Solutions Mapped to NIST CSF 2.0

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
RESPOND			
RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint solutions collect and store forensic incident information which is stored in an encrypted repository.
RS.AN-08	An incident's magnitude is estimated and validated	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint provides detailed information on incidents with severity levels / risk scores which can help prioritize incidents/cases for escalation.
RS.CO-02	Internal and external stakeholders are notified of incidents	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint can provide incident information and send alerts to designated parties. With Forcepoint DSPM, asset registry can notify various data owners of detections and changes in classification or risk of data within their charge.
RS.CO-03	Information is shared with designated internal and external stakeholders	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint policies utilize contextual analysis and integrations with other feeds (e.g., SIEM, third-party intelligence feeds) to identify risk events and/or identify and block data exfiltration actions.
RS.MI-01	Incidents are contained	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint policies offer proactive and reactive actions that align with the organization's incident response plans. Forcepoint DLP can automatically block/quarantine data to prevent exfiltration.
RS.MI-02	Incidents are eradicated	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint policies offer proactive and reactive actions that align with the organization's incident response plans.

Forcepoint Solutions Mapped to NIST CSF 2.0

FUNCTION AND SUB-CATEGORY	DESCRIPTION	FORCEPOINT PRODUCTS	VALUE
RECOVER			
RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process	Forcepoint Data Security Solutions Forcepoint Network Solutions	Review of Forcepoint DLP incidents and responses can be integrated into the organization's recovery and improvement plans.
RC.RP-06	The end of incident recovery is declared based on criteria, and incident-related documentation is completed	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint can help organizations in the process by providing incident details.
RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging	Forcepoint Data Security Solutions Forcepoint Network Solutions	Forcepoint can help organizations by providing incident details on a breach that is detected by Forcepoint solutions so that an update and message can be made.

forcepoint.com/contact