FORESCOUT

Improving NIST CSF Maturity with the Forescout Platform

NIST

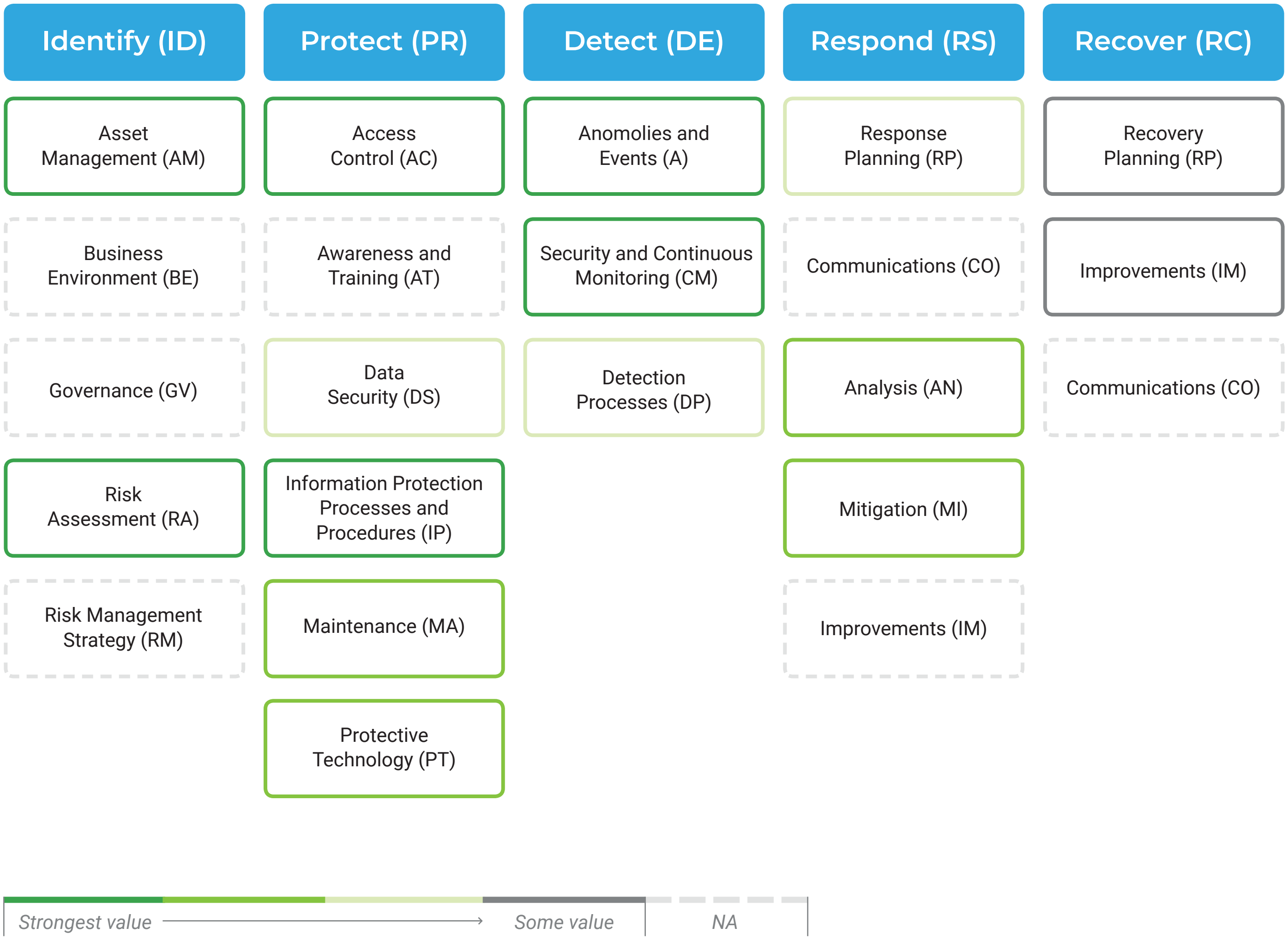
Maintaining NIST[1] Cybersecurity Framework (CSF) compliance can help organizations optimize operational function and reduce cyber risk. As part of the Forescout platform, SilentDefense and eyeSight work together to help simplify compliance with NIST CSF by continuously monitoring OT/ICS networks to provide in-depth visibility and risk-based alerts for both cyber and operational threats in real time.

How Forescout Platform Helps Compliance with NIST CSF 1.1

This NIST CSF consists of 22 requirements spread among five separate categories. While not all requirements apply to ICS cybersecurity or anomalous activity recognition, this document details how Forescout's platform address all core cybersecurity functions of NIST. By reducing the effort involved with compliance, we help operators and security teams maintain their focus on the reliability of critical infrastructure systems. According to a 2019 SANS Institute Survey, almost 40% of respondents use NIST CSF as the basis for cybersecurity standards within their organization.

Cybersecurity Framework Version 1.1

Below is the breakdown of NIST CSF requirements and how the Forescout Platform helps improve NIST CSF Maturity.



Identify (ID)	Protect (PR)	Detect (DE)	Respond (RS)	Recover (RC)
Asset Management (AM)	Access Control (AC)	Anomolies and Events (A)	Response Planning (RP)	Recovery Planning (RP)
Business Environment (BE)	Awareness and Training (AT)	Security and Continuous Monitoring (CM)	Communications (CO)	Improvements (IM)
Governance (GV)	Data Security (DS)	Detection Processes (DP)	Analysis (AN)	Communications (CO)
Risk Assessment (RA)	Information Protection Processes and Procedures (IP)		Mitigation (MI)	
Risk Management Strategy (RM)	Maintenance (MA)		Improvements (IM)	
	Protective Technology (PT)			

Strongest value → *Some value* *NA*

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

	Complete Platform	
Category	**SilentDefense**	**SilentDefense + Forescout Platform**
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	SilentDefense automatically determines the control system role for each device on the network/s, along with providing asset inventory information - such as model number, firmware version, serial number if available within the network protocols. All SilentDefense asset inventory data is available via our API to be consumed by asset repositories, compliance reporting systems or other systems.	Real-time agentless asset discovery, profiling, classification/prioritization and HW/ SW inventory allows our customers to have a seamless view across both IT and OT environments.
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	NA	NA
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	NA	NA
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	SilentDefense is used to optimize OT cyber and operational risk assessment processes by focusing on business impact risks using the Asset Risk Framework – which identifies and scores both cyber and operational risks for individual hosts. Combined with the Industrial Threat Library (ITL) and reporting functions, SilentDefense provides complete and timely status updates for stakeholders managing ICS networks.	Information-sharing integration & device control capabilities of the Forescout Platform support endpoint/ device compliance, configuration and vulnerability management and GRC/ SIEM tools. SilentDefense with the Forescout Platform extends threat and risk identification capabilities deep into OT and IoT device endpoints, maximizing threat identification coverage beyond typical IT/Enterprise tools.
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	NA	NA

Strongest value → *Some value* | *NA*

Develop and implement the appropriate preventative actions to ensure delivery of critical infrastructure services.

	Complete Platform	
Category	SilentDefense	SilentDefense + Forescout Platform
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	SilentDefense provides real-time visibility into network communications, supporting the creation of informed network access controls for OT/IoT device endpoints. In addition, SilentDefense automates the logging of successful and failed authentication attempts for complete historical records ideal for continuous process improvement. A detailed history of host activities including firmware changes, new protocols, new roles, etc., are always available.	Combining the threat detection and risk management capabilities of SilentDefense with the comprehensive IT policy enforcement, device compliance/control and intelligent segmentation capabilities of Forescout makes integration with network infrastructure vendors allowing for control and policy enforcement over switches, wireless controllers, firewalls, etc.
Awareness and Training (PR.AT): 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.	NA	NA
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	SilentDefense stores the information in a secure and continuously pentested environment helping to ensure data protection (at rest & in transit) for OT and IoT networks.	Together, SilentDefense and the Forescout Platform work in concert to store more information in a secure and continuously pentested environment, ensuring data protection (at rest & in transit) for IT and OT/IoT networks.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	SilentDefense can play an important role in defining communication baselines for all assets and applications in ICS environments. Also, SilentDefense logs and alerts if firmware / hardware versions are changed. Detailed ICS-specific threat indicators are critical for cybersecurity stakeholders to create and manage protective measures.	Information-sharing integration between SilentDefense and the Forescout Platform only extend what cybersecurity analysts can do. With a full suite of IT, OT and IoT endpoint information, analysts can automate, and better inform protective policies and regulatory best practices across enterprise environments.
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	SilentDefense enables field device access monitoring, alerting, and reporting on authorized or unauthorized engineering, contractor, or integrator activities, helping to ensure operational and business policies are adhered to. All of this information is stored, in detail and with associated risk ratings, in the asset inventory.	Information-sharing between the detail-rich asset inventory of SilentDefense, combined with Forescout's integration with configuration management/ CMDB solutions, SIEMs, data analytics and compliance reporting tools arms preventative and predictive maintenance endeavors with tons of operational and risk-related information down to the device level.

Strongest value → *Some value* | *NA*

	Complete Platform	
Category	SilentDefense	SilentDefense + Forescout Platform
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	SilentDefense helps ensure control system connections are reliable and provides all user activity logs and role-based access controls for the SilentDefense application itself.	All user event logs can be sent to SIEMs, log management, and correlation engines. Role based access controls can be defined based on Active Directory security groups.

Strongest value → *Some value* | *NA*

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The detect function enables timely discovery of cybersecurity events.

	Complete Platform	
Category	SilentDefense	SilentDefense + Forescout Platform
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	SilentDefense's Industrial Threat Library (ITL) features 2,400+ ICS-specific threat indicators. These indicators aren't only security related, but also include networking and operational indicators, providing additional value to those business areas and the ability to correlate events across all three key ICS domains. SilentDefense also creates both network and protocol baselines host ICS environments. These baselines help ensure all communications are approved and are working in the manner they have been designed. If a communication or protocol message is outside of our customers' approved baselines, then an alert and PCAP are immediately created to enable quick detection, response, recovery and reporting.	SilentDefense truly extends the threat detection capabilities of the Forescout Platform. Together, SilentDefense and the Forescout Platform provide the ability to evolve time-based vulnerability assessment to an event-based vulnerability assessment. The Active Response methodology detects and blocks the activity that precedes an attack (e.g. reconnaissance). All SilentDefense alerts can be sent to SIEMs, protective technologies, correlation engines, data analytics tools, and reporting/dashboard applications to bring additional use cases and value to our customers. Additionally, the Forescout Platform (eyeSight) can pull events from SilentDefense and correlate with other information and make them actionable.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	SilentDefense is a continuous network security monitoring technology designed specifically to detect security events in ICS and OT / IoT networks. SilentDefense also supports building automation and control protocols and security event detection and prioritization using a medley of hybrid techniques based on custom threat profiling, anomaly detection, queries and rules-based analysis.	The Forescout Platform (eyeSight) checks devices as they are admitted to the network to keep assets / details, continuously keeping inventories up-to-date. Combined with SilentDefense, data on defined intervals is extended with additional OT asset information. Also, a joint solution allows for integration with any malware detection and/or detonation technology for all files being sent over clear text protocols within the monitored network.
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	With the industry's most extensive library of known threat profiles and custom checks, SilentDefense can outline cyber and operational threats, combined with the recommended risk rating and remediation steps with specificity. Custom queries give the user the ability to draw from the rich analytics of SilentDefense to automate their own detection processes and respective responses as well. Use SilentDefense to inform your internal policy with detailed threat and risk information.	The policy-based threat detection and remediation capabilities of SilentDefense build upon the flexible response procedure of the Forescout Platform. Together, customers can setup control policies to check the efficiency of the system and assess / continuously monitor devices for policy compliance.

Strongest value → *Some value* *NA*

Develop and implement the appropriate activities to mitigate a detected cybersecurity event. The respond function supports the ability to contain the impact of a potential cybersecurity event.

	Complete Platform	
Category	**SilentDefense**	**SilentDefense + Forescout Platform**
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	NA	The Forescout Platform's effectiveness here is very strong. In some cases, we may be able to automate the entire response process.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	NA	NA
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	SilentDefense alerts provide rich contextual information about the source, nature and target of the threat, along with key input for its analysis (including packet capture related to the threat). Together with the ability to visually locate the threat and its spread on the interactive network map, the information contained in alerts is fundamental to initiate an effective incident response process. Dedicated visual network analytics allow incident responders to perform forensic analysis on real-time and historical network activity. Furthermore, responders can benefit from dedicated tools and API to perform threat hunting and quickly search the network for advanced threat indicators.	SilentDefense and the Forescout Platform can be integrated with automation and orchestration, or virtual security analyst technologies to automate response plans and reduce the mean time-to-resolution (MTTR). Together, the complete platform provides leading endpoint compliance, configuration management, vulnerability management, advanced threat detection (ATD) and GRC/SIEM tools to fully understand the threat, risk and vulnerability landscape.
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	SilentDefense provides contextual alert information to higher level SIEMs, automation and orchestration, and/or correlation engines to initiate appropriate response plans or actions.	SilentDefense can be integrated with 3rd party automation and orchestration or virtual security analyst technologies to automate response plans and analyst decisions. OS vendor and infrastructure agnostic to control the "who, what, when and where" across wired, wireless or VPN. Effective with or without 802.1X: Employing VLAN steering, port-based ACL, vFirewall capabilities. Continuous Intelligence Monitoring & Control. Ability to invoke configuration remediation techniques.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	NA	NA

Strongest value → *Some value* *NA*

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

	Complete Platform	
Category	SilentDefense	SilentDefense + Forescout Platform
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	SilentDefense's network and protocol baselines can be used in recovery situations to automate remediation actions and help ensure devices and applications are operating as expected.	In addition to SilentDefense's real-time agentless asset discovery, profiling, classification/prioritization - HW/SW inventory allows our customers to have a seamless view across both environments facilitating recovery and restoration.
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	NA	The policy-based architecture helps guarantee the flexible adjustment of procedures and the setup of improved control policies after postmortem analysis.
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	NA	NA

Strongest value → *Some value* | *NA*

Conclusion

The NIST CSF is the premier guideline for almost 40% of all ICS/OT cybersecurity stakeholders in nearly every industry sector [2]. Using this framework is ideal for and designing, implementing and managing any cybersecurity strategy where critical infrastructure and services are involved. With the Forescout Platform, users can directly address and track the key requirements and best practices defined by the NIST CSF.

[1] The National Institute of Standards and Technology's (NIST) Cyber Security Framework (CSF)

[2] https://www.forescout.com/platform/operational-technology/2019-sans-state-of-ot-ics-cybersecurity-survey/

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com