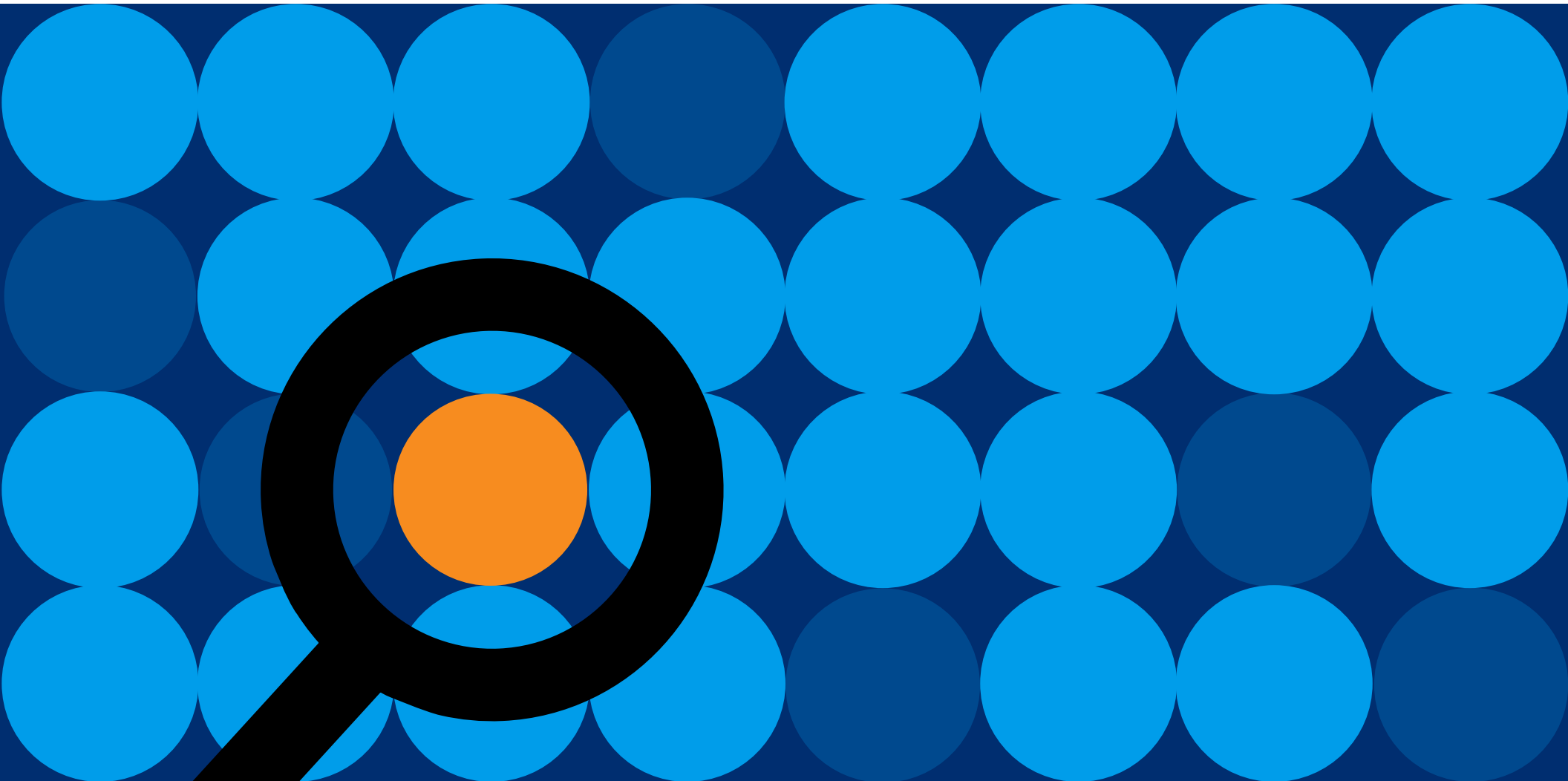
eBOOK

FORESCOUT

How to Reduce Risk by Aligning with the NIST Cybersecurity Framework



CONTENTS

3 Executive Summary

4 NIST Cybersecurity Framework (CSF)

4 Advantages of the NIST CSF

5 Identify (ID)

6 Protect (PR)

8 Detect (DE)

10 Respond (RS)

11 Recover (RC)



EXECUTIVE SUMMARY

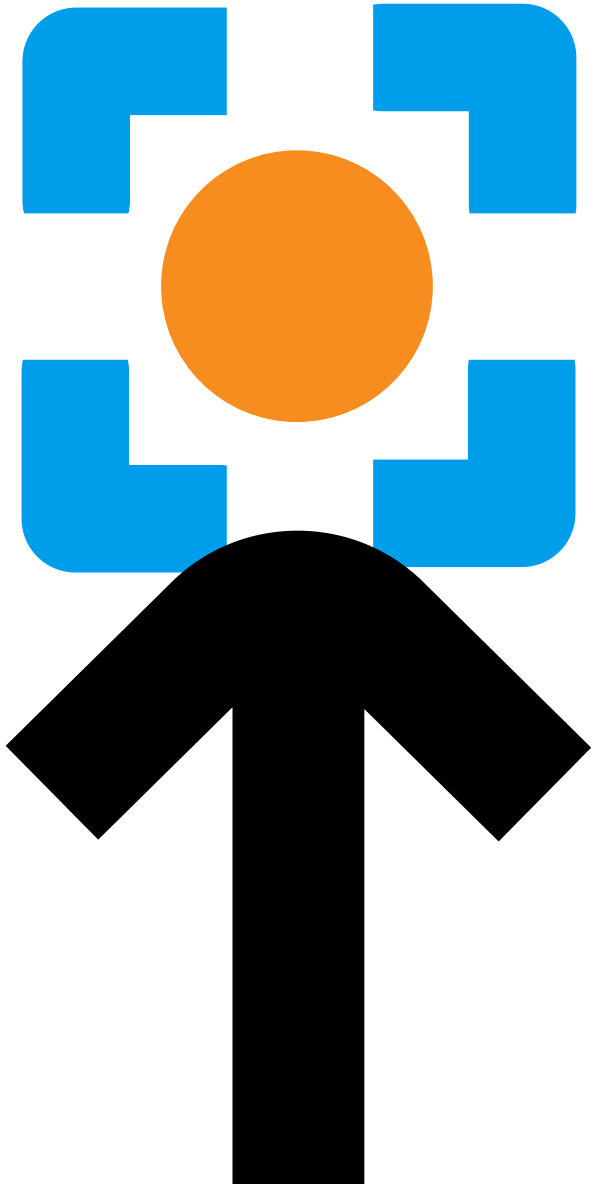
Forescout supports the NIST CSF with comprehensive IT/OT visibility and automated mitigation across the enterprise of connected things.

A converged IT-OT platform can simplify adoption of the NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) in the following ways:

Device visibility. NIST CSF can only be accomplished with comprehensive visibility. Forescout continuously identifies, classifies and assesses every IP-connected device – managed and unmanaged – that touches your extended enterprise network, allowing you to visualize the security posture of each device and have a complete picture of the network. Forescout also improves asset inventory by detecting serial-attached ICS devices by monitoring communications between the programmable logic controller (PLC) and its management devices.

Zero Trust. Network access control and network segmentation techniques can deliver Zero Trust across the enterprise IT infrastructure. With Forescout's network segmentation capabilities, you can logically separate your network into secure zones to contain any damage.

Compliance. Forescout's comprehensive and continuous monitoring helps ensure device and regulatory compliance to reduce cyber and operational risk and adhere to industry regulations and standards.



CYBERSECURITY FRAMEWORK (CSF)

NIST CSF is the primary framework utilized by industrial control system (ICS) and operational technology (OT) security practitioners.[1] By aligning with the NIST CSF, your organization can benefit from clear, actionable and prioritized standards, guidelines and best practices to help you protect your critical infrastructure and increase cyber resiliency.



For more information:

Read about how to implement the FAIR Model.

Advantages of the NIST CSF

The framework provides a number of advantages:

1

Reduce cyber risk.
Improve how you understand, manage and reduce cyber risk.

2

Optimize operations.
Prioritize activities that are most important to maintain critical operations and service delivery.

3

Quantify risk.
Lay the foundation for accurate risk assessment by defining a structure that can be used in conjunction with a risk assessment methodology such as the FAIR Institute's framework.[2] This helps you determine the potential impact from failure of a specific control, allowing you to evaluate investments to mitigate cyber risk.



IDENTIFY (ID)

Asset Management (ID.AM)

Forescout increases situational awareness with real-time forensic analysis of network flows and events to accurately identify the devices connected in your IT/OT network.

The Forescout Continuum Platform generates a complete asset inventory without impacting your industrial network or process. It helps you visualize, classify and prioritize control systems and IT hardware and software. This gives you a "full picture" view across both IT and OT environments. The asset inventory can also be accessed by third-party reporting tools and systems.

Risk Assessment (ID.RA)

Full device visibility is key to an accurate risk assessment as it provides the basis for continuous analysis and reporting of the active devices and services on the network. The Continuum Platform leverages bi-directional information sharing with leading endpoint compliance, configuration management, vulnerability management, advanced threat detection and governance, risk and control (GRC)/ security information and event management (SIEM) vendors to provide a complete view of your threat, risk and vulnerability landscape. With an expansive industrial threat library, Forescout simplifies and accelerates a robust risk assessment by helping you quickly identify OT/ICS device and protocol vulnerabilities.

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



PROTECT (PR)

Access control (PR.AC)

The Continuum Platform provides real-time visibility into network devices and communications. It tracks and logs all successful and failed authentication attempts to network resources and supports the concept of least privilege through role-based access control (RBAC). Integration with our partners allows you to leverage the Continuum Platform to control the who, what, where and when across wired, wireless and VPN access – with or without 802.1X. The platform detects and controls access to external devices, as well as tracks changes to host activities such as firmware changes, new protocols, changes to roles and other critical system changes.

Data security (PR.DS)

Forescout helps to protect the confidentiality, integrity and availability of device, network and security status data by storing information generated by the Continuum Platform in a secure, encrypted and continuously pen-tested environment. Our platform can report any undesired network communication and activity, helping ensure that network integrity and segregation are preserved.

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



PROTECT (PR) — cont.

Information protection processes and procedures (PR.IP)

Forescout streamlines the complex process of defining communication baselines for devices and assets both in IT and OT environments. The Continuum Platform automatically generates a full network behavioral blueprint – an accurate and detailed view into OT/ICS network communications – that can be used to maintain a baseline of running network design and configuration. Through bi-directional information sharing, as well as our proprietary detection capabilities, our platform can report any change in network configuration and invoke configuration remediation techniques that are safe in any industrial environment.

Maintenance (PR.MA) & Protective Technology (PR.PT)

The Continuum Platform helps ensure that control systems' connections are reliable and provides access to all user activity logs and role-based controls. It enables device access monitoring, alerting and reporting on authorized or unauthorized access. Whether these activities are initiated by users, engineers, contractors, integrators or threat actors, Forescout helps to protect access and ensure adherence to operational and business policies.



DETECT (DE)

Anomalies and Events (DE.AE)

Forescout's patented ActiveResponse™ methodology detects and blocks activities that precede an attack. Alerts can be sent to SIEMs, protective technologies and other tools. Our industrial threat library features thousands of ICS-specific threat indicators that are not only security-related, but also include networking and operational indicators, allowing the business to correlate events across all levels of industrial control – process-level, plant-wide and across an enterprise.

Forescout helps you save time and investment cost with unified policies for automating security controls across IT and OT networks. If a threat is detected, the Continuum Platform provides the intelligence needed to analyze and understand the cause and scope of a cybersecurity event, including assets involved and copies of the suspicious network packets for faster and more effective mitigation workflows.

Develop & implement the appropriate activities to discover a cybersecurity event in a timely manner.

DETECT (DE) — cont.

Security Continuous Monitoring (DE.CM)

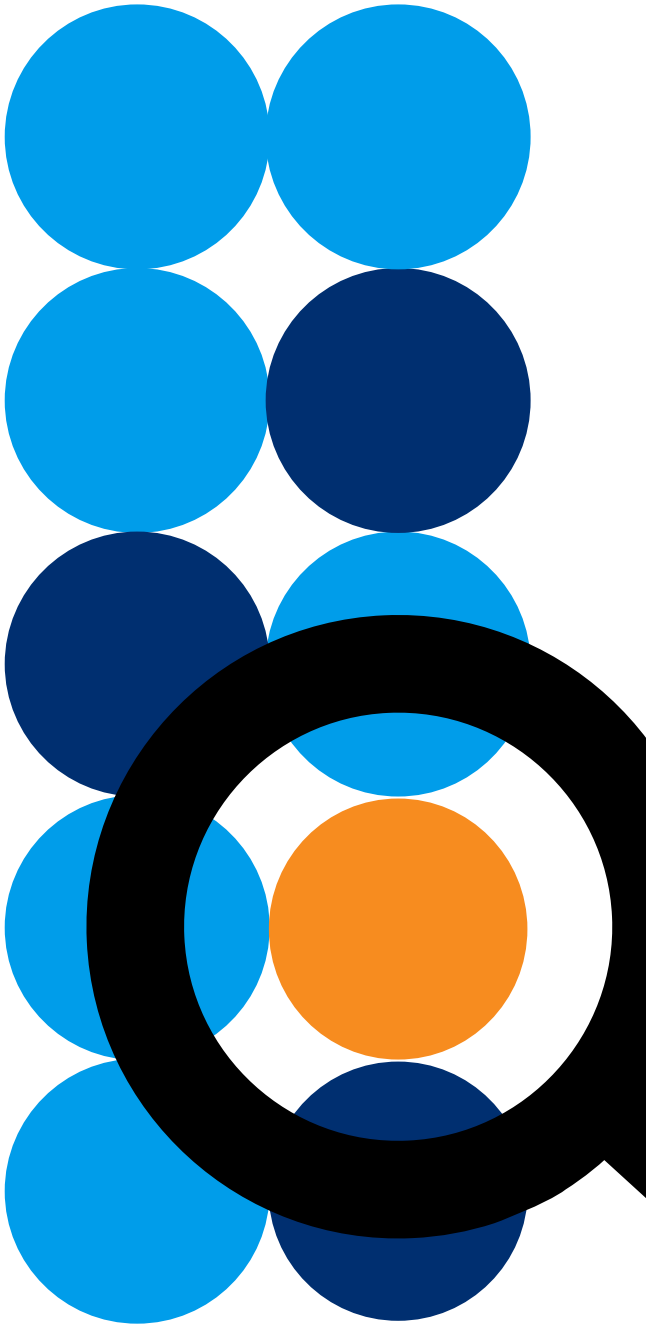
The Continuum Platform not only helps you identify cybersecurity events, it helps you verify whether your current protective measures are effective. Through continuous monitoring of devices for policy compliance and analysis of network communications, down to the values exchanged by network devices, greater detection is achieved for a broad range of cybersecurity events, including:

- Unauthorized connections, commands and operations
- Unauthorized values sent/received
- Malware detection and detonation

Because of our experience in identifying security events in operational technology and industrial control systems, Forescout parlays this experience to be a powerful solution to protect building automation systems as well, providing you with a comprehensive security and operational support platform.

Detection processes (DE.DP)

The Continuum Platform tracks more than 1,000 different event types and integrates with leading SIEM solutions, including Splunk and their OT add-on. Together, the technologies work to help you focus on the relevant anomalies and threats that are unique to your environment.





RESPOND (RS)

Response Planning (RS.RP)

A response plan begins with a flexible, policy-based architecture that helps you set up control policies and track the effectiveness of the plan.

Analysis (RS.AN)

Forescout alerts provide rich contextual information about the source, nature and target of the threat, including packet capture related to the threat, to increase situational awareness. Together with the ability to visually locate the threat and its spread on the interactive network map, the information contained in alerts helps incident responders quickly prioritize remediation and limit the blast radius of an incident.

Integration with market-leading endpoint compliance, configuration management, vulnerability management, advanced threat detection and GRC/SIEM tools helps automate the response.

Mitigation (RS.MI)

The Continuum Platform can send deep contextual information to leading SIEMs, allowing you to quickly initiate appropriate actions.

Develop & implement the appropriate activities to contain & mitigate a detected cybersecurity event.



RECOVER (RC)

Recovery Planning (RC.RP)

In order to recover from a cybersecurity event, incident responders need to have accurate, prioritized information at hand.

Forescout's device, network and protocol baselines provide incident responders with a prioritized list of action points, which can be used to reestablish normal business operations in a timely manner. Our solution also ensures that after the recovery processes are complete, all devices and applications are operating in the desired state.

Communications (RC.CO)

The Continuum Platform can provide evidence of a cybersecurity event or produce evidence of its successful resolution and recovery to be used for internal and external communications.

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

FORESCOUT — YOUR NIST CSF PARTNER

Why Forescout

Forescout actively defends the enterprise network by identifying, segmenting and enforcing compliance of every connected thing. The Continuum Platform deploys quickly on your existing infrastructure without requiring agents, upgrades or 802.1X authentication to help you:

- **Continuously discover, classify, assess risk and monitor** compliance of all OT/ICS devices
- **Gain in-depth visibility of all IP-connected devices** across campus, data center and cloud networks
- **Enforce and automate policy-based controls** to proactively reduce the attack surface and rapidly respond to incidents
- **Accelerate the design, planning and deployment** of dynamic network segmentation across the extended enterprise
- **Share device context** between the Continuum Platform and other IT and security products to automate system-wide policy enforcement and incident response

Get a Demo

References:

[1] SANS 2019 ICS/OT Survey
[2] www.fairinstitute.org

forescout.com/solutions/operational-technology salesdev@forescout.com toll free 1-866-377-8771

Forescout Technologies, Inc.
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

© 2022 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 04_01