FORESCOUT

THE NIST CYBERSECURITY FRAMEWORK 2.0

THE NIST CYBERSECURITY FRAMEWORK 2.0

is essential for organizations looking to strengthen their defenses in today's dynamic digital threat landscape. This journey demands a holistic cybersecurity approach that spans the entire lifecycle of security operations from prevention to recovery. A critical element of this comprehensive strategy is identifying a robust cybersecurity technology that supports the implementation of the core areas outlined in the NIST CSF 2.0 and helps organizations turn risk into resilience.

The Forescout Vistaro™ platform is a key enabler in this context, as it provides advanced capabilities to accelerate the adoption of the framework and ensure its successful integration into an organization's cybersecurity practices.

NIST CSF 2.0 REQUIRED CAPABILITIES

To effectively use the NIST Cybersecurity Framework 2.0, organizations must develop a broad range of security capabilities that are essential to address the wide scope of the framework and serve as a roadmap to effectively manage and mitigate risks. To maximize the adaptability of the NIST framework across industries and sizes of operations, it is important to align these core capabilities with the organization's specific threat landscape, risk profile and business requirements. Essentially, these capabilities form the backbone of a successful implementation of the NIST Cybersecurity Framework 2.0 and allow organizations to navigate the complex cybersecurity landscape with confidence and agility.

FORESCOUT DELIVERS 9 REQUIRED CAPABILITIES FOR EFFECTIVE NIST CSF 2.0 IMPLEMENTATION

Cybersecurity maturity assessment

A cornerstone to improving security maturity is the use of visibility solutions that uncover systems, assets and configurations, security vulnerabilities and exposures. Best of breed solutions also map roles, show communication flows and display dependencies to help assess an organization's current cybersecurity posture against the framework's best practices. These solutions will identify gaps and areas for improvement — and define a clear path to maturity.

Adaptable risk management

In today's dynamic risk landscape, organizations need solutions that not only cover advanced threats, but are flexible enough to adapt to their specific context, including industry, technology, operational or process-related risk factors. These tools should seamlessly integrate cybersecurity risks into the organization's broader Enterprise Risk Management (ERM) framework to ensure strategic alignment and informed decision making.

Industry-specific security profiles

Industry-specific threats require the development and implementation of industry-specific security use cases and risk indicators. These tailored profiles are developed for specific cybersecurity needs, challenges and objectives of different sectors, such as manufacturing, energy, healthcare or financial services. They enable organizations to take a more targeted cybersecurity approach, improve security measures, support regulatory compliance and increase operational efficiency.

Collaborative threat intelligence

Collaborative threat intelligence emphasizes the importance of community and shared knowledge in cyber security. By bringing together threat data from a variety of sources, organizations gain access to a more comprehensive view of the threat landscape, including emerging ones, adversarial TTPs and campaigns that relate to their environment to stay steps ahead of attackers.

Policy management

For governance, policy management platforms are proving essential to streamline the creation, management, enforcement and review of cybersecurity policies. These platforms ensure that policies are consistent throughout the organization — and that up-to-date, compliant and effective cybersecurity protocols are maintained with minimal effort. The key is to use solutions that enforce compliance and not only monitor policies.

Assets and systems lifecycle

Solutions that support the full lifecycle of NIST's 'Govern, Identify, Protect, Detect, Respond and Recover' approach ensure a comprehensive approach to cybersecurity. Managing configurations, vulnerabilities, compliance and risks throughout the asset lifecycle for all asset types – from initial installation to decommissioning – is critical to maintaining a robust security posture.

Advanced threat detection and response

Advanced threat detection and response systems are at the heart of a proactive cybersecurity strategy. They analyze patterns and anomalies across extensive data sets while correlating information from multiple sources to detect threats with greater accuracy and speed to avoid false positives — which is essential for defending against sophisticated cyberattacks.

Automated security operations centers (SOCs)

The automation of Security Operations Centers (SOCs) is a testament to the power of innovative technology that improves cybersecurity efforts. Being able to rapidly triage events via orchestration within an organization's security tools limits the spread of an attack, enhances compliance, minimizes business disruption and creates more efficient response protocols.

Recovery and resilience plans

Managing recovery and resilience plans is essential for ensuring business continuity after a cybersecurity incident. The creation and testing of plans must include system baseline information and historical data on assets. They serve as the foundation for preparing for potential incidents and restoring systems to an operational state following an incident.

TABLE OF CONTENTS

NIST CSF 2.0 COMPLIANCE GUIDE

The NIST CSF provides a structured approach to governing, identifying, protecting, detecting, responding, and recovering from cybersecurity threats. However, the path to full compliance can be complex and requires a nuanced understanding of the framework's components and how they apply to an organization's unique technology landscape.

This compliance mapping guide was developed to bridge the gap between the theoretical underpinnings of the NIST CSF 2.0 with practical, actionable steps for compliance. See how our Forescout Vistaro™ platform capabilities directly align with the core requirements of the NIST framework and provide a clear, navigable path to successfully use and adopt the NIST CSF to manage risk exposure. Whether you're at the beginning of your compliance journey or looking to improve your cybersecurity, this guide is your compass pointing the way to a secure, compliant future.

GOVERN (GV)

Establish and monitor the organization's cybersecurity risk management strategy, expectations and policies.

ORGANIZATIONAL CONTEXT (GV.OC):

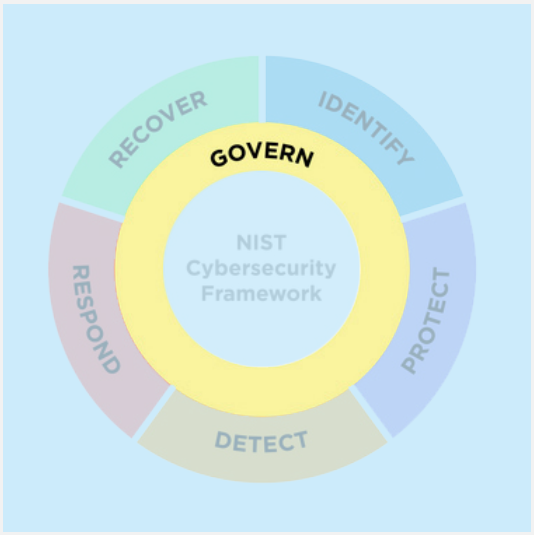
The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE).

The Forescout Vistaro™ platform improves organizational insight. It enables companies to better understand their complete cyber context. Identify key assets, systems and services that are critical to the operation — and specify dependencies posing risk of failure. The unique visibility Forescout provides allows asset owners to clearly understand critical subsystems and external services that are relied on to execute industrial processes, achieve business objectives and deliver vital services. The Platform allows organizations to automatically discover, identify and monitor critical assets, systems, services and users across the business environment (IT, IoT, OT, IoMT and BAS). With this greater visibility of components, functions and critical cross-system communications, security teams can perform impact analysis using real-time and historical data, develop contingency plans — and share risk information and performance with internal and external stakeholders.

RISK MANAGEMENT STRATEGY (GV.RM):

The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM).

Forescout enables organizations to monitor cybersecurity objectives, measure and manage risk and performance. The Platform provides an overall view of cybersecurity risks along with compliance and regulatory requirements helping to implement a risk management strategy, monitor objectives and refine them based on actual security exposure. Forescout improves the risk management process by automatically



discovering, assessing and classifying all connected assets, ensuring the organization's digital environment is reliably protected. The Platform calculates a comprehensive risk score for each asset based on vulnerabilities, misconfigurations and asset criticality to optimize risk and performance management. This process provides a transparent evaluation of the organization's risk level and helps refine business objectives and risk appetite based on current risk exposure. Forescout's data visualization and reporting capabilities enhance the organization's ability to regularly inform its stakeholders about its cybersecurity posture, promoting transparent communication about cyber risks.

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (GV.SC):

Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC).

Forescout assists organizations integrate supply chain security practices into cybersecurity risk management strategies and measure performance throughout the lifecycle of devices and systems. The Platform plays a vital role in several areas of supply chain risk management, such as enforcing and monitoring supplier access policies, tracking critical asset updates for unauthorized changes — and supporting end-of-life, obsolescence and recall of equipment.

ROLES, RESPONSIBILITIES, AND AUTHORITIES (GV.RR):

Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID. GV-02).

Forescout enhances the performance review process by providing deep insights into cyber risks and key performance indicators (KPIs), promoting a culture of accountability, thorough performance evaluation and continuous improvement measures. The Platform provides accurate assessments of an organization's cybersecurity posture, identifies opportunities for improvement and facilitates preventative risk management. By leveraging historical risk and compliance data, Forescout creates the foundation for benchmarking and strategic decision-making, leading to more informed decisions and a stronger, more efficient risk management framework.

POLICIES, PROCESSES, AND PROCEDURES (GV.PO):

Organizational cybersecurity policies, processes and procedures are established, communicated, and enforced (formerly ID.GV-01).

Forescout provides organizations with a comprehensive view of cybersecurity risk and facilitates the continuous monitoring and evaluation of risk metrics and policy effectiveness to align with strategic risk management objectives. The Platform streamlines the implementation and monitoring of security policies tailored to specific asset profiles, roles, responsibilities and regulatory requirements to manage access to critical resources, segment the industrial environment and detect non-compliant issues. Forescout's automation capabilities allow organizations to autonomously take appropriate remediation actions in response to different scenarios, enhancing policy

compliance without the need for manual intervention. In addition, Forescout efficiently detects policy violations and maintains detailed historical logs that enable thorough documentation and analysis of compliance.

OVERSIGHT (GV.OV):

Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.

Forescout helps monitor risk management strategy and measure results by identifying the risks the organization is exposed to, including likelihood and potential impact — providing insights and performance indicators for cyber risks. Especially in converged IT/OT environments, this increased visibility of threats and risk exposures enables organizations to address technology issues that hinder operations or innovation, reassess strategy after security events, and effectively report and communicate cybersecurity risk management metrics to senior leadership. Forescout ensures adherence to compliance standards, facilitates re-evaluation of strategies following security incidents and supports the effective communication of cyber security metrics to senior leadership. This comprehensive visibility into cyber risks empowers organizations to proactively manage their cybersecurity policies, processes and procedures.

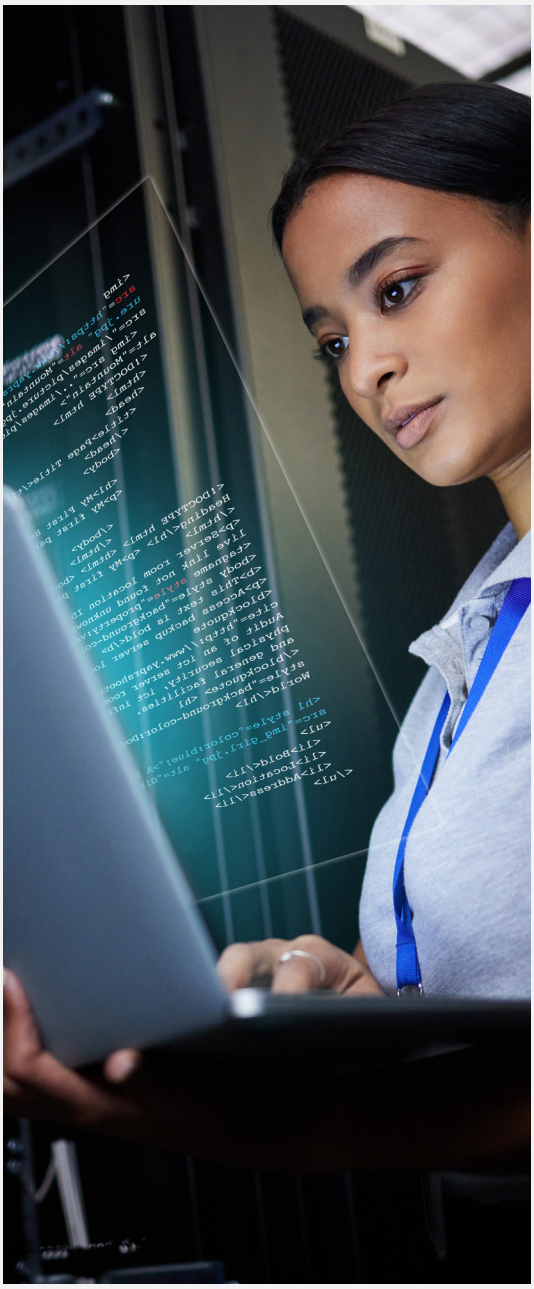
IDENTIFY (ID)

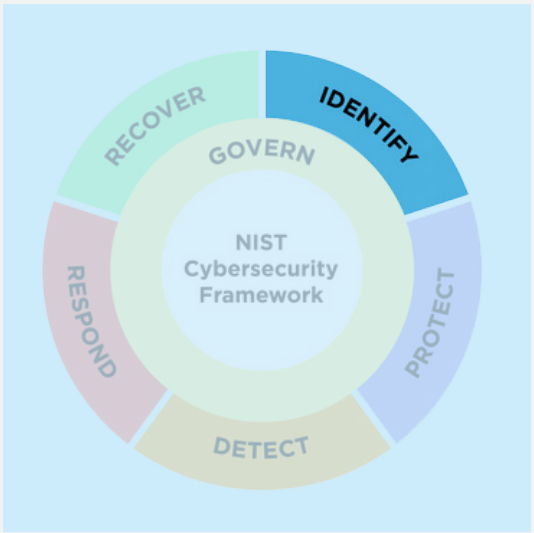
Help determine the current cybersecurity risk to the organization.

ASSET MANAGEMENT (ID.AM):

Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Forescout automatically generates and updates inventories of assets, systems and services, as well as detailed mappings of the organization's network communications and data flows internally and externally. It ensures these inventories are kept up to date throughout the equipment's lifecycle. It considers historical data, such as change and configuration management and risk timelines. Assets are systematically prioritized according to their classification, criticality, exploitability and potential impact on the business. This comprehensive approach leads to improved decision making, enhanced compliance and asset utilization — and proactive risk management. The Platform revolutionizes asset discovery and vulnerability management by combining passive and active techniques to continuously monitor and profile networked systems, regardless of their operating system or form factor. This approach ensures a comprehensive inventory of the organization assets that is automatically updated to reflect new installations or configurations. Forescout provides detailed visualizations of the devices connected to the network and their interactions and helps identify security boundaries and associated device groups through a dynamic traffic flow matrix. This provides deep insight into communication patterns, including protocols, ports and traffic volumes. The Platform extends its monitoring to external systems and services, ensuring that they comply with the organization's security standards and facilitating access management based on roles or security status. By automatically categorizing resources by role, classification and criticality, Forescout empowers organizations to





effectively manage their entire digital ecosystem and improve security and operational efficiency across IT, OT, IoT, BAS and IoMT domains.

RISK ASSESSMENT (ID.RA):

The organization understands the cybersecurity risk to the organization, assets, and individuals.

Forescout improves risk management by automating the identification of threats, assessing their potential impact and likelihood — and enabling the prioritization of risks. The platform equips security teams with comprehensive tools for vulnerability lifecycle management, threat monitoring, analyzing network and system designs for cybersecurity weaknesses, and documenting changes and exceptions for risk assessment. Forescout provides organizations with complete visibility into the converged attack surface, identifying, quantifying, and controlling cyber threats across the entire extended IT/OT environment, from endpoints (managed and unmanaged) to ICS, embedded, virtual and cloud systems, external services, CCTV, access control, HVAC and building management automation systems (BMS/BAS). Each connected asset and system receive a risk score based on its configuration, function and behavior, enabling immediate action or automated remediation by Forescout's policy engine. The multi-factor risk score prioritizes risks based on a continuous assessment that incorporates vulnerability assessment data, asset criticality, misconfigurations, exposure to the internet, exploitability, compliance and environmental context to optimize orchestration and patching processes. The Forescout Vistaro™ platform supports organizational risk management decisions, enabling security teams to identify and prioritize threat response and initiate fully automated remediation and mitigation workflows in real time. Leveraging open-source technologies, such as NVD and MITRE, and proprietary intelligence from Forescout's Vedere Labs, Forescout contextualizes organization-specific threats to increase operational efficiency and reduce response times.

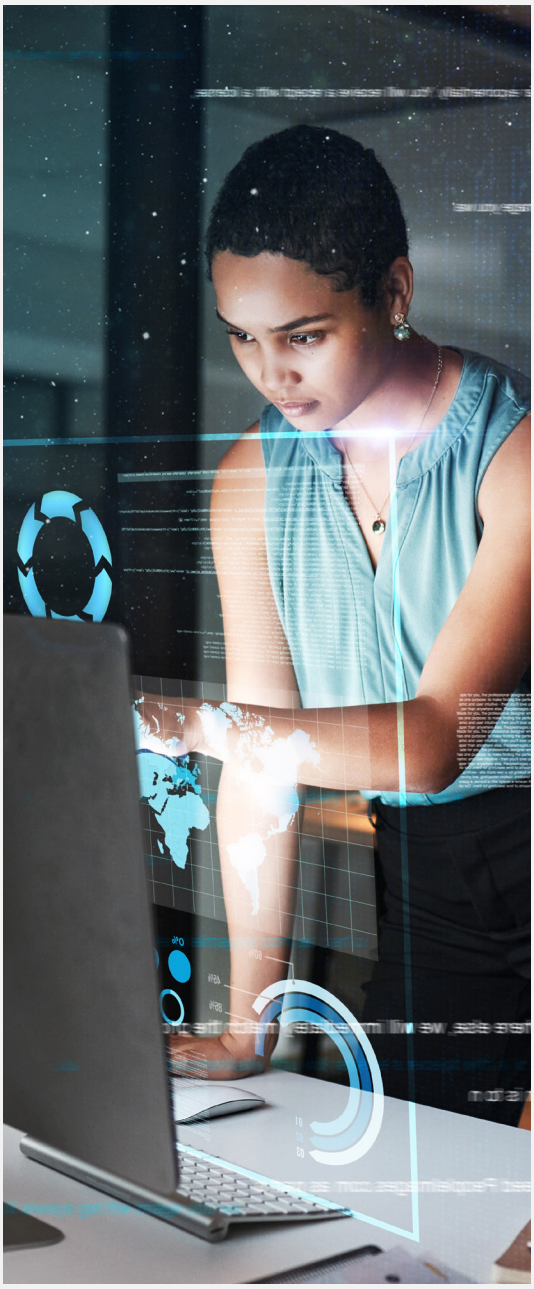
IMPROVEMENT (ID.IM):

Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all Framework Functions.

The Forescout Vistaro™ platform provides security insights, risk and performance indicators that enable organizations to improve their cybersecurity risk management processes with data-driven evidence for decision making across all functions. Key metrics include: The number of compliant assets, vulnerability distribution, change and configuration management efficiency, likelihood of threats, their impact, incident response times, etc. This helps to better understand the current exposure and effectiveness of existing security measures and to prioritize risk mitigation actions. Using these metrics improves the risk management process and leads to a more robust cybersecurity posture, optimized resource allocation and improved regulatory compliance. Forescout automates the incident response process and helps with system recovery and rebuilding after a crisis. The platform enables a continuous monitoring strategy that utilizes ICS-specific threat indicators for real-time control assessments and security effectiveness against advanced threats. In addition, Forescout enables the creation of customized analytics and dashboards as well as reporting to communicate key security metrics and KPIs to ensure a comprehensive assessment of cyber and physical security controls. The Platform supports (and automates) the incident response process and provides critical information for testing the recovery and rebuilding of the system to a known state after a catastrophic event.

PROTECT (PR)

Use safeguards to prevent or reduce cybersecurity risk



IDENTITY MANAGEMENT, AUTHENTICATION AND ACCESS CONTROL (PR.AA):

Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC).

Forescout orchestrates information sharing and automates workflows between many security tools to actively reduce the risk of cyberattacks behind the misuse or compromise of identities and credentials. The Platform enables the implementation of granular access policies and dynamic segmentation rules based on the device's risk score and the principles of least privilege and separation of duties. Forescout streamlines the development, management, enforcement and review of an organization's policies and procedures and continuously validates the identity and integrity of each connected device to detect modifications or changes that could alter the risk posture. The Platform continuously detects, profiles and monitors devices and users accessing the organization's digital environment to quickly identify and automatically respond to threats and prevent unmanaged privileged accounts. In addition, Forescout provides audit trails, details and logs for all user activity, along with usernames, user privileges, type of event, severity, date, and time. Forescout integrates with third-party solutions (e.g. IDM systems) to proactively manage the entire identity authentication lifecycle and uniquely identify and authenticate organizational and non-organizational users.

AWARENESS AND TRAINING (PR.AT):

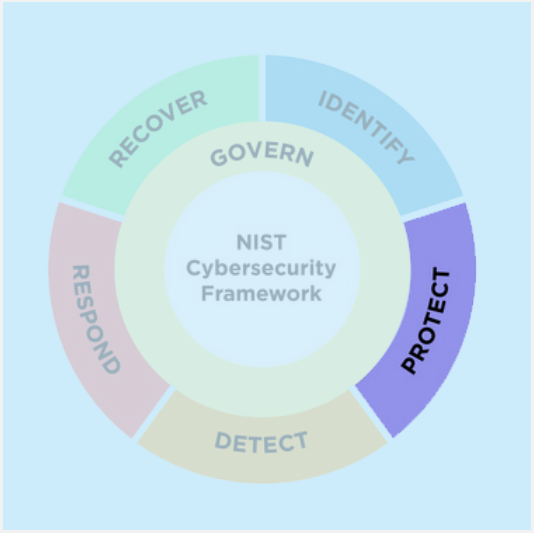
The organization's personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks.

Our Professional Services offer end-user training aimed at assisting customers design, plan, deploy and optimize a comprehensive information security program through the Forescout Vistaro™ platform. In addition, Forescout's analytics and insights facilitate the regular evaluation of security issues, such as common security breaches, threat scenarios or historical incidents. This enables the creation of tailored awareness training for different roles and responsibilities based on real security events and use cases, improving security awareness and readiness of the organization.

DATA SECURITY (PR.DS):

Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Forescout helps customers monitor and manage access to sensitive or confidential data when it is stored or transmitted. With complete visibility of network access and data flow, customers can easily detect unauthorized connections, insecure communication channels, unauthorized changes and attempts to exfiltrate data. The combined use of NAC and segmentation with a Zerto Trust approach provides multiple layers of defense against unauthorized access and data breaches, significantly



improving the overall protection of sensitive data. This also ensures a more resilient network architecture capable of surviving and recovering from cyber incidents while maintaining data confidentiality, integrity and availability. With complete visibility into network access and data flow, customers can easily detect unauthorized connections, unauthorized changes and attempts at data exfiltration. This is particularly useful in ICS environments where data protection mechanisms are often not in place.

PLATFORM SECURITY (PR.PS):

The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity and availability.

Forescout provides comprehensive device lifecycle management that includes robust configuration, change and risk management measures. The Platform automatically discovers devices and maps communication and data flows with users, roles and responsibilities for organizational and external entities. Based on this inventory, Forescout creates and maintains a baseline configuration for assets and systems and enables real-time monitoring and updating of changes. This comprehensive strategy ensures that software and hardware are appropriately maintained, updated or decommissioned depending on the associated risk. Moreover, Forescout blocks unauthorized software installations and executions. In addition, it works with its correlation engine, to automatically report on alerts on events related to change control, authentication activities, user privileges, access provisioning and malware executions. The platform's user-friendly interface allows security analysts to easily navigate through device information timeline, detect non-compliant devices, deviations from baseline configurations — and identify security issues with minimal effort to improve the overall security posture.

TECHNOLOGY INFRASTRUCTURE RESILIENCE (PR.IR):

Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.

Forescout enables organizations to increase the resilience of their infrastructure through visibility and control over every system, component and service spanning IT, OT, IoT, IoMT networks and physical systems, including CCTV, building management, HVAC and controls for water, power, temperature and humidity, and more. This provides granular control over device risk and compliance, network access and communication patterns. It helps implement robust segmentation policies to effectively minimize and restrict access to what is absolutely necessary. Forescout accelerates Zero Trust segmentation across different digital landscapes, users, services and device types by performing real-time assessments of the security posture of endpoints before granting access to resources. This increased visibility of the network and data flow also helps identify single points of failure or bottlenecks in traffic within systems and infrastructures, increasing operational resilience, supporting incident containment and improving network performance.

DETECT (DE)

Find and analyze possible cybersecurity attacks and compromises.

CONTINUOUS MONITORING (DE.CM):

Assets are monitored to find anomalies, indicators of compromise and other potentially adverse events.

Forescout automatically discovers and monitors users, assets and systems, including access control, CCTV, HVAC and building automation to detect anomalies, indicators of compromise and other potentially adverse events. The Platform combines various protection mechanisms, including: Network traffic and behavior analysis, automatic or on-demand device scanning, code and configuration integrity checking, monitoring of local and remote maintenance activities, and file exchange to detect potentially dangerous scenarios. This capability extends across the network, operations and industrial process to detect not only security events but also operational issues that could pose a potential threat to the delivery of the industrial process or the security of information. To provide even more effective protection, threat and risk detection is constantly being improved with IoC and IoA derived from research conducted by Vedere Labs, Forescout's threat intelligence research center. The monitoring capabilities extend to hardware and software components with an asset inventory that includes details about the device's operating system, firmware inventory, registry keys, shared and encrypted folders for software or network adapters, asset IDs, X.509 certificates, physical drives, motherboards, CPUs, monitors and display devices for the hardware. In addition, Forescout helps organizations establish a baseline of acceptable system behavior and set precise thresholds for event detection. This allows security professionals to customize alert settings and automate incident response to optimize the overall security posture.

ADVERSE EVENT ANALYSIS (DE.AE):

Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)

Forescout uncovers known and unknown cyber threats using several techniques and deploying thousands of specific, proprietary checks and Indicators of Compromise (IOCs) to detect cyber and operational events and prioritize them according to urgency and potential business impact. The platform is characterized by precise detection, drastic minimization of false positives, and advanced event classification. Events are automatically categorized into groups (security, networking, operational, anomalies) and several subcategories (including data breaches, DoS attacks, IOC matches, malware activity, etc.), enabling quick identification of events and accelerating analysis and remediation workflows. Additional event information with full details and actionable data, including underlying events and historical context, triggers, causes, impacts, TTP's MITRE ATT&CK mapping and playbooks, are available to security teams to facilitate cross-team and cross-role communication and improve alert triage and incident response. The Platform implements role-based access so that the groups that are allowed to access incident information or handle alarms can be precisely defined. It is also possible to forward or export detection data to other tools such as SIEM or ticketing and service solutions. The detection and classification of events is enhanced by threat intelligence from Vedere Labs. This enhancement not only improves threat detection capabilities, but also provides key insights to contextualize events that detail attackers' behaviors, strategies and tactics in executing cyberattacks.

RESPOND (RS)

Take action regarding a detected cybersecurity incident.

INCIDENT MANAGEMENT (RS.MA):

Responses to detected cybersecurity incidents are managed (formerly RS.RP).

Forescout enhances incident response by offering an integrated capability that includes detection, analysis, containment, eradication and recovery. The Platform uniquely combines advanced threat identification with effective incident classification and prioritization leveraging Tactics, Techniques and Procedures (TTPs). This enables security analysts to manage events more efficiently through data correlation, automated incident categorization and attacker behavior monitoring. By integrating essential SOC technologies into a unified, cloud-native platform, Forescout simplifies management from a single console and enables automated response and orchestration via NAC, segmentation, SIEM and TDR. This approach enhances detection, streamlines analysis, and supports faster recovery. By prioritizing incidents based on scope, impact and urgency, Forescout facilitates comprehensive investigations, tracks the status of incidents and produces detailed, evidence-based reports for broader security collaboration.

INCIDENT ANALYSIS (RS.AN):

Investigation is conducted to ensure effective response and support forensics and recovery activities.

Forescout helps security analysts respond to incidents by giving them the tools they need to analyze alerts and uncover systemic root causes within a single user interface. The Platform enables a detailed investigation into the timeline of the incident showing which assets and resources were involved in each event. Analysts can also identify the vulnerabilities, threats and TTPs that were directly or indirectly involved, providing a full view of the incident's dynamics. Forescout also facilitates the collection and retention of all relevant data and metadata related to an incident from multiple sources, enabling responders to preserve the integrity of evidence and automatically scan other potential targets of the incident to look for indicators of compromise and signs of persistence.

INCIDENT RESPONSE REPORTING AND COMMUNICATION (RS.CO):

Response activities are coordinated with internal and external stakeholders as required by laws, regulations or policies.

Forescout contributes significantly to improving incident reporting and communication strategies. The platform collects detailed incident data and provides in-depth analysis, forensic details and key insights into what happens during and after cybersecurity incidents. Forescout's ability to deliver this information in a consistent language and reporting format is essential for analyzing the details and nuances of each incident. This promotes a consistent understanding of the impact of the incident and subsequent actions by all parties involved and supports legal, regulatory or policy requirements for coordinated response activities with internal and external stakeholders.

INCIDENT MITIGATION (RS.MI):

Activities are performed to prevent expansion of an event and mitigate its effects.

Forescout's robust integration with various IT and security systems enables security teams to streamline and accelerate cybersecurity incident response across third-party solutions. The Platform provides end users with the flexibility to either automate or manually initiate a range of containment and eradication actions to effectively isolate or remediate compromised endpoints. From detection to remediation, enhanced incident management enables organizations to quickly and deftly manage security incidents, reduce their impact with limited resources and strengthen resilience against future attacks. The Platform enables shorter system recovery times and increases cyber security. This approach not only mitigates the immediate impact of incidents but also strengthens defenses against future threats and ensures a more resilient infrastructure.

RECOVER (RC)

Restore assets and operations that were impacted by a cybersecurity incident.

INCIDENT RECOVERY PLAN EXECUTION (RC.RP):

Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.

The Forescout Vistaro™ platform significantly improves the execution of incident recovery plans, a critical component to the resilience and reliability of an organization's cybersecurity infrastructure. Forescout provides security teams with comprehensive access to historical data, including device configurations, communication patterns and process behavior. The Platform allows thorough review of the integrity and normal operation of assets, systems and services post-recovery. This comprehensive insight is instrumental for restoring operations and for ensuring that the restored environments are free of vulnerabilities or threats that could lead to future security breaches.

INCIDENT RECOVERY COMMUNICATION (RC.CO):

Restoration activities are coordinated with internal and external parties.

Forescout equips asset owners with a range of features that streamline the recovery process and facilitate coordination and communication between internal and external stakeholders. The platform highlights incidents by providing actionable insights and evidence that are essential for documentation and reporting purposes. Each step of the operational recovery process can be closely tracked, allowing a detailed comparison between the previously established baseline and the status to monitor progress. In addition, Forescout uses standardized language and terminology (e.g. MITRE ATT@CK event mapping) to effectively articulate and share details of attacker tactics and incident specifics across all organizational levels. This approach ensures that threat information is communicated clearly and comprehensively, improving the organization's incident response and communication strategies.

EXPERIENCE

Take a personalized tour of Forescout to learn how to continuously discover, assess and govern all your assets in one platform.

https://www.forescout.com/demo/

FORESCOUT

Experience the Forescout Vistaro™ platform today.

GET STARTED

About Forescout

As AI-driven vulnerability discovery and exploitation accelerate attack velocity to machine speed, Forescout is a foundational cyber defense layer that allows organizations to segment and isolate compromised systems, block lateral movement, and automate response across IT, OT, IoT, and IoMT environments. The Forescout Vistaro™ platform, powered by agentic AI and enhanced with Vedere Labs threat intelligence, delivers a Universal Zero Trust Network Access (UZTNA) architecture that integrates seamlessly with 180+ security and IT products. With Forescout Vistaro, organizations get comprehensive inventory and classification of both managed and unmanaged assets, continuous exposure management, and real-time protection including dynamic network segmentation and automated threat response.

FORESCOUT

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com