SOLUTION BRIEF

Visibility, Inventory, and Control

Identify and Mitigate Risk through the CDM Program

FORESCOUT

Visibility, Inventory, and Control

Identify and Mitigate Risk through the CDM Program

Federal Departments and Agencies (DAs) can continuously **identify** risk within federal network environments, **prioritize** risk based on potential impact and **mitigate** the most severe risks first through the Continuous Diagnostics and Mitigation (CDM) program. CDM provides capabilities and tools to DAs in a phased approach to meet these goals. As agencies increasingly align with Zero Trust architectures, this phased approach also supports foundational Zero Trust principles, such as continuous visibility and risk-based control. The first of these phases focuses on the foundational ability to know what's on the network, otherwise known as asset management. Forescout currently delivers this capability for nearly all federal agencies as the preferred solution for CDM hardware asset management (HWAM).

Notably, in the CDM framework, data collection, asset management and risk management processes happen continually, not periodically, across the environment. As new data about the IT environment becomes available, the CDM system ingests endpoint and contextual data, responds by elevating security thresholds and adapting network policies and controls access actions in a perpetual feedback loop. This iterative process is critical when mitigating vulnerabilities or responding to cyber incidents. In dynamic network environments where connected endpoints, running applications and configurations constantly change, mitigating risk is most successful when cybersecurity tools work collaboratively with "one source of truth." Forescout provides that "truth" – complete asset visibility in real- or near-real time.

Improve Risk Detection and Response Capabilities with Forescout

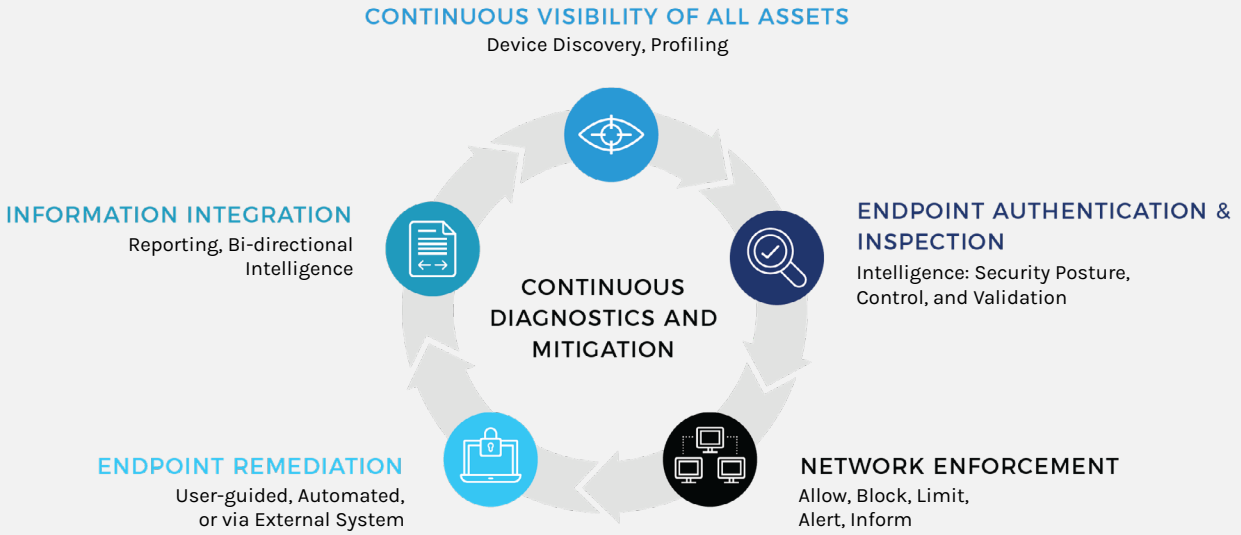
To achieve CDM goals, organizations must invest in real-time asset discovery and vulnerability management; automated, intelligence-driven response mechanisms; and continuous feedback of data into an enterprise management system. Furthermore, the system needs to be easily deployed within your existing IT framework and integrate with chosen tools.

Forescout Solves For:

- **Real-Time Visibility.** Gain automated, real-time visibility of endpoints as they connect to your network, including sniffer devices that do not utilize an IP address.
- **Active Asset Management.** Establish a real-time inventory of devices, hardware, operating systems, applications, patch levels, open ports, peripheral devices, users and more.
- **Policy-Based Access Control.** Limit network access to authorized users and devices with or without 802.1X.
- **Continuous Monitoring.** Assess the security and compliance posture of endpoints in real time, both pre- and post- connection.
- **Automated Remediation.** Automate remediation of noncompliant endpoints by auto-updating endpoint configurations, patches and updates, and install, activate, or disabling applications or peripherals.
- **Compliance Reporting.** Produce real- time compliance reports and shorten Detection Interval Latency by initiating compliance scans as hosts connect, rather than waiting for time-based scans.

Required Capabilities for CDM

The Forescout 4D Platform™ provides real-time visibility and automated control of all networked assets.



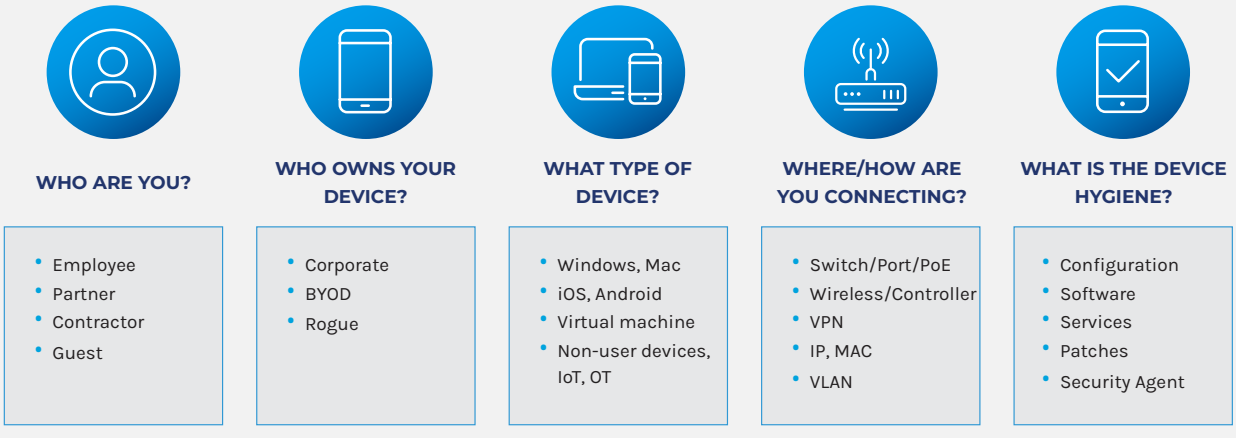
Visibility

Forescout's real-time asset discovery and vulnerability management system uses a combination of passive and active discovery and monitoring techniques to detect and profile systems on the network, independent of operating system or form factor. Active discovery techniques probe the network to track down idle devices. Passive discovery techniques monitor traffic to see which devices are active. Together, these methods allow full and constant visibility of IT assets. As soon as someone installs or reconfigures a device on the network, the Forescout 4D Platform™ detects the change and assesses the device. Visibility is especially important for unmanaged endpoints because existing endpoint management systems are typically blind to this class of devices.

The Forescout 4D Platform™ provides complete and continuous visibility of all endpoints, and through this discovery, it provides users with rich data about the device, users, configurations and more (see figure on next page). This information can be used to drive and inform data-driven security policies and actions.

Continuous Asset Discovery and Profiling

The Forescout 4D Platform™ yields rich data about a variety of endpoints (IT, IoT and OT) without requiring software agents or previous device knowledge.



Automation

The Forescout 4D Platform™ enforces and automates policy-based network and host controls through integrations with heterogeneous physical and virtual network infrastructure. These enforcement actions align closely with Zero Trust strategies, where continuous evaluation of trust based on device posture, identity, and risk context, are essential to governing access. Actions can be automated or administrator-initiated and gradually increased to minimize disruption while reducing the manual effort to enforce network access, improve device compliance, implement network segmentation and accelerate incident response. The automated response mechanism can take inputs from the asset discovery and vulnerability management system. Based on this information, plus an awareness of endpoint behavior, it generates a set of intelligent responses designed to reduce enterprise risk.

The Forescout solution can direct the antivirus server to automatically update a noncompliant host and prompt the patch management system to update the device's operating system. It can also disable unauthorized software (See next page). Support for leading SIEM systems can provide endpoint configuration details, correlate access and compliance violations and expedite incident response. And built-in reports help you monitor policy compliance, support regulatory audit requirements and produce real-time inventory reports.

As federal agencies contemplate implementing Zero Trust principles, their needs are evolving beyond network access control toward the concept of a policy decision point which considers authentication, authorization and device posture in real time as access requests to enterprise resources are made; a CDM system can provide this information.1 The rich data that CDM provides allows agencies to control access to enterprise resources based on user profile (guest, employee, contractor), device properties, classification and security posture, thus moving DAs toward a Zero Trust future.

Customize Control Actions Based Upon the Severity Level

The Forescout 4D Platform™ includes a wide range of endpoint remediation actions based on the endpoint's security posture.

Orchestration

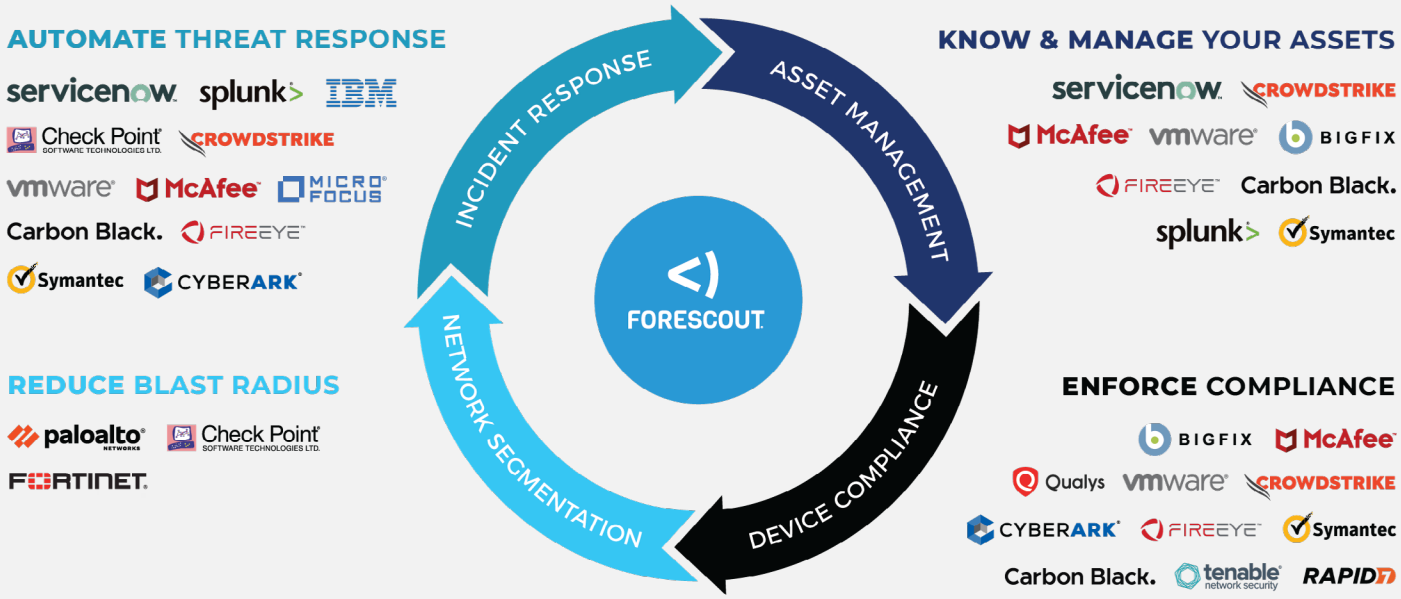
Forescout enables bi-directional integrations with other common CDM tools such as antivirus, patch management and security incident and event management (SIEM) systems to unify system-wide security management. Asset data and automated control actions can feed into other aspects of the CDM system to optimize the overall system's efficiency and effectiveness. This unique set of network, security, and management interoperability technologies extends the platform's power to more than 70 third-party solutions, allowing the combined system to accelerate response, achieve major operational

efficiencies and provide superior security. For example, the Forescout Extended Module for Splunk® enables Forescout and Splunk to share information and enable the Forescout 4D Platform™ to take action if a security control is degraded or no longer in place (e.g., if a device is missing a security software patch, has a newly reported flaw or is suspected of contributing to a malware outbreak).

Furthermore, Forescout helps IT managers achieve acceptable Detection Interval Latency (DIL) metrics by integrating with compliance scanners to add event-based scanning functionality. Through this integration, the Forescout 4D Platform™ triggers the compliance scanner when a host connects to the network. The addition of event-based scanning will significantly improve your DIL metric. Integrations exist with leading vulnerability assessment (VA) scanners such as Tenable® Nessus, BeyondTrust® Retina and Qualys®, with more under development. These integrations enhance the agency's ability to implement Zero Trust controls by ensuring decisions about access and segmentation reflect the most current risk intelligence.

Plug-and-Play Integrations Orchestrate Response

The Forescout 4D Platform™ integrates with a wide range of technology partners. According to policy, it shares real-time visibility and compliance data with third-party solutions and can enforce network access or segmentation controls.



Ease of Deployment

The Forescout 4D Platform™ is available as either a virtual or physical appliance that deploys seamlessly within your existing network, without typically requiring infrastructure changes. The Forescout appliance installs out-of-band, avoiding latency or potential for network failure, and can be centrally administered to dynamically manage tens or hundreds of thousands of endpoints from one console.

CDM Capabilities and Program Criteria[2]

Continuous Diagnostics & Mitigation Criteria		Forescout
Asset Discovery & Classification	Discover unauthorized or unmanaged hardware on a network, discover unauthorized or unmanaged software configuration in IT assets on a network.	Forescout discovers network devices in real time and maintains a comprehensive database of hardware and software assets. You can search and organize the inventory by various hardware and software attributes and generate inventory reports.
Assessment	Assess the security posture of endpoints resulting in an accurate and timely software inventory. This is essential to support awareness and effective control of software vulnerabilities and security configuration settings.	The Forescout 4D Platform™ assesses the security posture of IT, IoT and OT endpoints in your environment. This is especially important for unmanaged devices because existing management systems are typically blind to these devices. It performs a wide range of compliance checks, including monitoring for required software, software/patch versions, device configuration and endpoint vulnerabilities. It integrates with other host-based agents/tools and VA scanners to obtain additional compliance info.
Authentication & Access Control	Prevent, remove and limit unauthorized network connections/access to prevent attackers from exploiting internal and external network boundaries and then pivoting to gain deeper network access and/or capture network resident data in motion or at rest. Manage account access, security-related behavior, credentials and authentication.	The Forescout 4D Platform™ can block or restrict access to unauthorized devices as well as devices that become noncompliant while connected to the network. It is event-driven and reassesses an endpoint when a configuration changes in its operating system.
Automated Mitigation & Remediation	Prevent exploitation of the system by consciously designing it to minimize weaknesses and building the system to meet that standard to reduce the attack surface and increase the effort required to reach the parts of the system that remain vulnerable.	Upon detecting compliance violations, the Forescout 4D Platform™ can respond based on the severity of the violation by simply alerting or notifying the IT staff or auto-remediating, quarantining or blocking noncompliant endpoints. It can also interface with a third-party system such as patch management.
Situational Awareness	An accurate and timely endpoint status is essential to support awareness, effective control and reporting of any organizational security issues in the network.	The Forescout 4D Platform™ provides comprehensive situational awareness by identifying endpoints on the network and integrating with other security management systems such as endpoint lifecycle management products, asset management systems, databases, SIEM, VA and antivirus products, resulting in real-time endpoint intelligence and security posture awareness. It supports SIEM systems to provide endpoint configuration details, correlate access and detect compliance violations.

[1] Scott Rose et al., NIST Special Publication 800-207: Zero Trust Architecture, page 7, 10, 34-35, August 2020.

[2] U.S. Department of Homeland Security (DHS), Continuous Diagnostics and Mitigation (CDM) Resources, Last accessed January 2021.

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

©2025 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.
01_02