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. 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.
Required capabilities for CDM

The Forescout platform provides real-time visibility and automated control of all networked assets.

CONTINUOUS VISIBILITY OF ALL ASSETS
Device Discovery, Profiling

INFORMATION INTEGRATION
Reporting, Bi-directional Intelligence

CONTINUOUS DIAGNOSTICS AND MITIGATION

ENDPOINT AUTHENTICATION & INSPECTION
Security Posture, Control Validation

ENDPOINT REMEDIATION
User-guided, Automated, or via External System

NETWORK ENFORCEMENT
Allow, Block, Limit, Alert, Inform

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 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 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 platform yields rich data about a variety of endpoints (IT, IoT and OT) without requiring software agents or previous device knowledge.

**WHO ARE YOU?**
- Employee
- Partner
- Contractor
- Guest

**WHO OWNS YOUR DEVICE?**
- Corporate
- BYOD
- Rogue

**WHAT TYPE OF DEVICE?**
- Windows, Mac
- iOS, Android
- Virtual machine
- Non-user devices, IoT, OT

**WHERE/HOW ARE YOU CONNECTING?**
- Switch/Port/PoE
- Wireless/Controller
- VPN
- IP, MAC
- VLAN

**WHAT IS THE DEVICE HYGIENE?**
- Configuration
- Software
- Services
- Patches
- Security Agent

**AUTOMATION**

The Forescout platform enforces and automates policy-based network and host controls through integrations with heterogeneous physical and virtual network infrastructure. 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 platform includes a wide range of endpoint remediation actions based on the endpoint’s security posture.

### Automate Policy Based Control

#### Network
- Move to guest network
- Change wireless user role
- Assign to self-remediation VLAN
- Restrict rogue devices/infrastructure

#### Host
- Start mandatory applications/process
- Update antivirus/security agents
- Apply OS updates/patches
- External drive compliance

---

#### 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 (See next page). 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 Forescout 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 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).

Further, 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 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.
Plug-and-play integrations orchestrate response

The Forescout 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 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

<table>
<thead>
<tr>
<th>CONTINUOUS DIAGNOSTICS &amp; MITIGATION CRITERIA</th>
<th>FORESCOUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Discovery &amp; Classification</td>
<td>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.</td>
</tr>
<tr>
<td>Discover unauthorized or unmanaged hardware on a network, discover unauthorized or unmanaged software configuration in IT assets on a network.</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Assessment</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Authentication &amp; Access Control</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Automated Mitigation &amp; Remediation</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Situational Awareness</strong></td>
<td>An accurate and timely endpoint status is essential to support awareness, effective control and reporting of any organizational security issues in the network.</td>
</tr>
</tbody>
</table>