Forescout Extended Modules for Federal Civilian Agencies

The Forescout platform enables granular visibility into all connected assets in a federal agency's network. Integrations with leading cybersecurity and IT solutions enhance security and operational efficiency through additional device visibility, automation and asset management capabilities.

Forescout eyeExtend for ServiceNow

Leverage real-time device visibility and provide up-to-date properties, classification, configuration, and network context to the ServiceNow platform. This can ensure a current view of networked assets, track asset movement and identify assets to remediate or retire. As a result, agencies can:

- Make informed decisions based on an accurate single-source-of-truth asset repository
- Avoid time-consuming and error-prone manual processes
- Optimize IT governance and service operations.

With eyeExtend for ServiceNow, the CMDB is updated in real time. Agencies can verify that software updates delivered to managed devices have been properly installed. When updates are not applied, the Forescout platform can quarantine the device and initiate policy-based remediation, reducing exposure to potential cyber threats. Read more or watch video about eyeExtend for ServiceNow.

Leverage an accurate single-source-of-truth CMDB to optimize IT governance and service operations.

Forescout eyeExtend for Tenable Vulnerability Assessment

Use bi-directional communications to trigger a real-time vulnerability scan when a connecting device joins the network. This significantly enhances security by detecting transient endpoints when they are on the network and helps produce up-to-date and complete vulnerability reports. A connecting device can be isolated in an inspection VLAN to confirm its risk posture while Tenable performs a scan. If the endpoint's risk rating is acceptable, the Forescout platform can admit the endpoint to the production network. Read more or watch video about eyeExtend for Tenable.

Increase detection of transient endpoints and produce up-to-date and complete vulnerability reports.

Forescout eyeExtend for CyberArk

Enhance visibility into privileged accounts on the network and protect against threats from undetected devices with privileged credentials. Improve visibility and actionable intelligence about privileged accounts, especially those residing across devices, to help disrupt privileged account compromise and reduce the risk of data breaches. Agencies can fortify credential management by centrally storing and managing privileged credentials, supporting a comprehensive audit trail for regulatory requirements. Read more or watch video about eyeExtend for CyberArk.

Forescout eyeExtend for HCL BigFix

Integrate to deliver an automated, simplified security patching process to all endpoints from a single console. This improves security, compliance, and control of all devices on and off the enterprise network. Continuously validate systems for compliance with the agency's security and patching policies, to ensure all systems have the right software, security patches and posture the entire time they are connected. Further, the Forescout platform inspects endpoints at the time of connection to verify that the BigFix agent is installed, enabled and fully operational on supported corporate systems. If the agent is absent, broken or disabled, the Forescout platform can either enroll the device itself or trigger the automated BigFix deployment process. Read more or watch video about eyeExtend for HCSL BigFIx.

Automate patching from a single console to all endpoints on and off the enterprise network.

Forescout eyeExtend for Splunk

Combine agentless device visibility, control and automated response capabilities with powerful data correlation, rich analytics, incident management and search features. Improve understanding of overall security risk posture and create incident response workflows that leverage the Splunk Adaptive Response framework. With Forescout eyeExtend for Splunk, agencies can:

- Store Forescout data in Splunk Enterprise for long-term trend analysis, visualization, and incident investigation
- Correlate high-value device context from the Forescout platform with other data sources to better identify and prioritize anomalous behavior and events
- Accelerate incident response by initiating Forescout network and/or endpoint actions from Splunk through the Adaptive Response framework
- Increase valuable user and location context by resolving overlapping IT addresses and layering tenant ID with IP address in meta data

Read more or watch video about eyeExtend for Splunk.

Correlate high-value device context to better identify and prioritize anomalous behavior and events.

Forescout eyeExtend Connect

Quickly build, consume and share integrations that connect the Forescout platform to many other technologies. Build apps that learn and share endpoint context, take network control actions and enforce system-wide policies. eyeExtend Connect provides an easy-to-use JSON schema to define parameters, tags and user-controlled configurations to make eyeExtend Apps portable (migrating from Test to Production, Region A to B, IT to OT environments, etc.). In addition, third-party API interactions are defined with popular Python scripts which provide significant flexibility by expanding the types of integrations that can be built. Essential use cases and enforcements, such as threat mitigation, incident response and compliance management can be automated with policy templates that can be built into apps. Read more or watch video about eyeExtend Connect.

Build apps that leverage the Forescout platform’s device visibility, control and automation capabilities.

Get more information on all Forescout eyeExtend Modules.

FORESCOUT
Active Defense for the Enterprise of Things™

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

Intl. + 1.408.213.3191
Support +1.708.237.6591