Forescout eyeExtend Connect

Easily integrate with the Forescout platform to get contextual device insights and accelerate enterprise-wide threat response

To increase the value derived from investments in security and IT technologies, Forescout customers leverage out-of-the-box integrations with products in nine popular security technologies. These integrations drive tremendous efficiencies through the orchestration of security workflows. In addition to these pre-built offerings, Forescout now offers a faster, easier way for customers to integrate more of their existing technologies with the Forescout platform. eyeExtend Connect, a new product offering from Forescout, now empowers our customer and partner community to quickly build, consume and share eyeExtend Apps, that connect the Forescout platform to other technologies. This enables the community to unlock the value of existing security products with in-depth device context from Forescout, automate security workflows and policy enforcement across disparate solutions, and accelerate system-wide response to mitigate risks.

The Solution

Forescout eyeExtend Connect simplifies the creation of apps that are easy to consume and deploy. Through Forescout eyeExtend Apps, you can now easily integrate Forescout platform with your IT and security technologies and orchestrate security workflows across assorted cybersecurity technologies.

With eyeExtend Connect, your current security technologies can leverage the deep device context of Forescout eyeSight's data, including device properties, security posture, device compliance with company policies, location on the network, user context and more. This device data can be pulled automatically by other IT or security products or they can push their own data to the Forescout platform. eyeExtend Connect also helps accelerate threat response by letting you automate system-wide, policy-based actions to mitigate threats, incidents and compliance gaps.

eyeExtend Connect provides the following tools to enable workflow orchestration and device context sharing.

eyeExtend connect

Challenges

- Reliance on pre-built integration offerings from Forescout or technology partners excludes workflow orchestration with other in-house security technologies
- Long development cycles for custom-built integrations increase time to realize the value of current security investments
- Security tools working independently without sharing device and user context, require a lot of manual effort when responding to security incidents, resulting in increased cyber risk and loss of productivity

Benefits

- Maximize return on current technology investments by integrating with all types of third-party tools
- Get faster time to value by easily and quickly integrating with the Forescout platform via eyeExtend Apps
- Elevate your security posture by making your IT and security tools work better together, getting faster actionable device insights and automating resolution of risks and threats

Highlights

- Easily build and deploy eyeExtend Apps to integrate with the open Forescout platform
- Share your apps with the community to contribute and seek feedback
- Build portable apps with Python scripts and JSON configuration
- Integrate with a wide array of third-party web services
- Expand Forescout visibility and control capabilities with third-party device context and controls
- Enable bidirectional integrations with open, standards-based REST APIs
- Push and pull information into and out of a standard Structured Query Language (SQL)
- Generate custom queries to pull and push information into and out of a standard LDAP server
- Send and receive information via syslog to a designated server

eyeExtend Apps

Build apps that leverage key Forescout platform functions to 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 your 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.

Key Features of eyeExtend Apps:

- Plug-and-play
- New device and property discovery
- External third-party control actions
- Custom policy templates
- Scriptable API interactions
- Customizable third-party icons

WebAPI & DataExchange (DEX)

The Forescout platform provides a set of RESTful APIs that enable external applications to retrieve Forescout device properties and policy information. The DEX (Data Exchange) plugin enables bi-directional communication between the Forescout platform and third-party RESTful APIs to share real-time device context.

SQL

The DEX plugin is able to push and pull information into and out of a standard SQL database. This type of integration allows homegrown applications to share information with third-party products that are able to interface through an external or internal database. You can query external databases for information and create host properties to store the data that the Forescout platform retrieves. These host properties can be used in Forescout policies and viewed in network operating system (NAC) and Inventory views. You can also update external databases based on information gathered by the Forescout platform, typically for a third-party product to act upon.

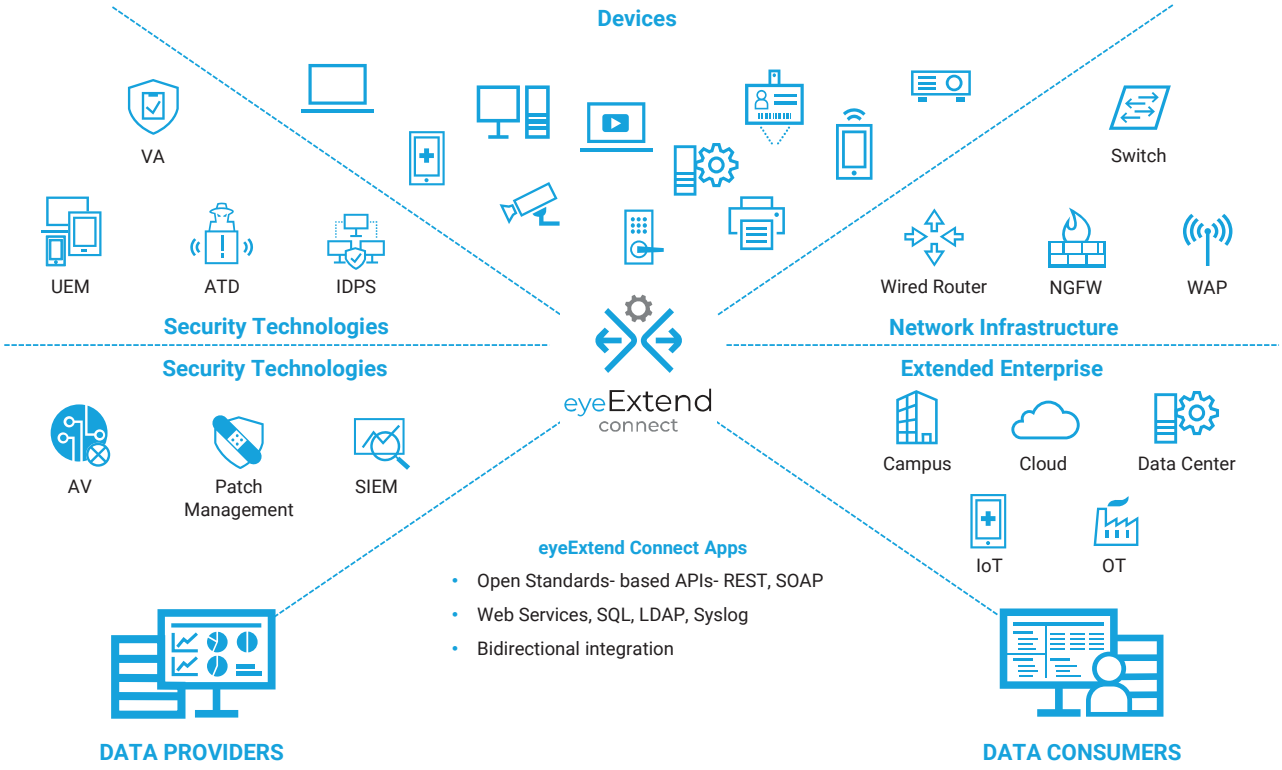
LDAP

Generate custom queries via the DEX plugin to push and pull information into and out of a standard LDAP server. For example, you can query the LDAP server for information and create Forescout host properties to store data that has been retrieved. These host properties can be used in Forescout platform policies and viewed in NAC and Inventory views.

Syslog

The DEX plugin can be configured to send and receive information via syslog to a designated server. This type of interface is used for a variety of integrations with products that aggregate logs and enable log analysis, such as security information and event management (SIEM) products, or with other solutions that can send and receive alerts in this manner. The message format is customizable.

Figure 1: Orchestrate workflows across diverse devices, environments and security technologies



VA: Vulnerability Assessment, **ATD:** Advanced Threat Protection, **IDPS:** Network Intrusion Prevention, **UEM:** Unified Endpoint Management, **AV:** Anti Virus, **SIEM:** Security Information and Event Management, **WAP:** Wireless Access Point, **NGFW:** Next Generation Firewall

General Use Cases

While Forescout offers 25 out-of-the-box solutions to solve for specific use cases, eyeExtend Apps can be used to solve customers' custom use cases. Here are a few examples:

Discover, classify and assess every network-attached device the instant it connects

Forescout eyeExtend Connect, powered by Forescout eyeSight, enables an integrated IT or security product to provide context to better identify devices across the enterprise, including campus, data center, OT and cloud environments. For example, the eyeExtend App for Ubiquiti helps customers increase visibility into their Wi-Fi connected devices and use the device attributes they discover to make better policy decisions in the Forescout platform. eyeExtend App for Ubiquiti can now feed the Ubiquiti Wi-Fi connected device information to another IT Service Management (ITSM) or asset management product to true-up their CMDB. Another important app, eyeExtend App for Google Cloud, helps customers gain real-time visibility into their evolving cloud compute instances by integrating with Google Cloud and pulling in Google Cloud inventory context.

Improve visibility and control into VPN-connected devices accessing the network
eyeExtend Connect identifies all devices connecting to the corporate network via VPN. By leveraging the integration with the Forescout platform, security operators can determine whether the asset connecting via VPN is a corporate asset and control access of devices connecting from unauthorized locations.

Orchestrate security or IT policy violation information workflow
Send real-time alerts of policy violations using different collaboration and messaging platforms. You can set up a policy to get device incident data from the Forescout platform either via email, messaging or collaboration platforms when making policy decisions to automate network control actions. For example, the eyeExtend App for Slack integrates with the collaboration platform to send real-time alerts of policy violations to a channel used by the IT or security team on Slack.

Automate mobile device enrollment, improve security management and enforce continuous compliance
eyeExtend Connect orchestrates device information sharing and control actions with UEM systems to provide unified security policy management for devices on your network regardless of the type (PC, Mac, Linux®, tablet, smartphone), the connection (wired, wireless, VPN), or ownership of the device (corporate or personal). This comprehensive device management allows for the automation of device enrollment, the enforcement of device compliance through policy-driven actions, the application of custom network access controls, and the acceleration of response actions and remediation. For example, with eyeExtend App for Google Mobile Management, customers now have visibility into Chromebook device context. This data helps with refining corporate BYOD security and access policies.

Automate actions and workflows within the IT and security product ecosystem to improve operations and strengthen security across the enterprise
eyeExtend Connect can send or receive action triggers that direct the Forescout platform or another integrated product to take a specific action. These triggers are based upon policy-driven automation, rather than playbook-based decision-making that requires a human operator. This translates into faster response times and more secure networks across the board.

Leverage in-depth, contextual device data for correlation analysis to accelerate incident response|
eyeExtend Connect enables the Forescout platform to feed in-depth device data into a SIEM system for correlation analysis. This provides a complete picture of your entire enterprise attack surface, helps reduce time to insight and facilitates investigations. The Forescout platform also helps streamline security operations by automating policy-based actions—limiting access of the device to the network based on incident severity fed from the SIEM in real time.

In summary, eyeExtend Connect helps you rapidly achieve higher security ROI by taking security tools out of silos and plugging them in to the highly intelligent Forescout platform to significantly automate threat mitigation and policy compliance.

Note: Certain capabilities of eyeExtend Connect were formerly part of the OIM Product. All previous OIM capabilities are now part of eyeExtend Connect.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
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