Forescout eyeExtend Connect

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

Forescout customers have invested in a wide variety of IT and cyber security technologies and want to leverage the Forescout platform as they orchestrate security workflows. While Forescout provides out of the box integrations with selected products in nine popular cyber security categories, customers want a quick and easy way to integrate with additional technologies. eyeExtend Connect, a new product offering from Forescout now empowers our customer and partner community to quickly build, consume and share eyeExtend apps connecting the Forescout platform to other technologies. This enables the community to unlock the value in 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 enables integrations to be created as apps that are easy to consume and deploy. Through Forescout eyeExtend apps, you can now easily orchestrate security workflows across assorted cyber security technologies.

eyeExtend Connect allows your current security technology leverage deep device context of the Forescout eyeSight's data that includes the properties of devices, their security posture, consequent 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 help accelerate threat response by letting you automate systemwide 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

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 an 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

Challenges

- Reliance on pre-built integration offerings from Forescout or technology partners excludes workflow orchestration with other in-house security technologies
- Long lead times 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 in responding to the security incidents resulting in increased cyber risk and loss of productivity

Benefits

- Maximize return on current technology investments by integrating with all types of 3rd party tools
- Get faster time to value by easily and quickly integrating with the Forescout platform via 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

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 (Test to Production, Region A to B, from an IT environment to an OT environment etc.). Additionally, third party API interactions are defined with popular Python scripts which provide significant flexibility expanding the types of integrations that can be built. Essential use-cases and enforcements for the App, 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 Apps
- New device and property discovery
- External third-party control actions
- Custom policy templates
- Scriptable API interactions
- Customize 3rdy 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 plugin enables bi-directional communication between the Forescout platform and third-party REST API to share real-time device context.

SQL

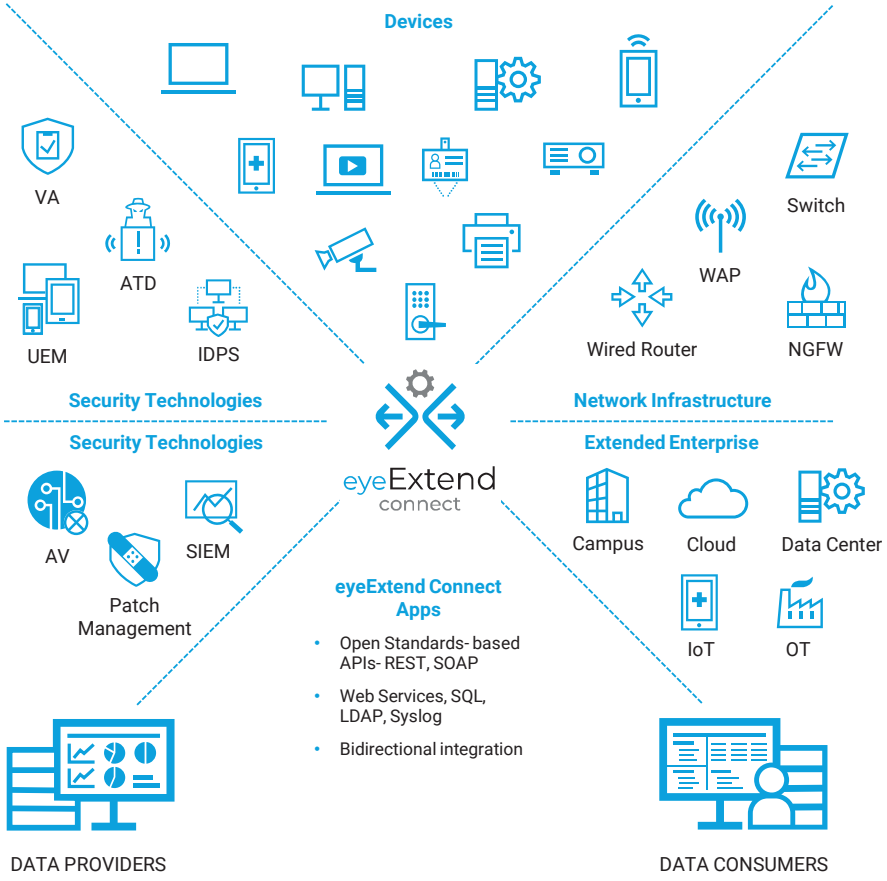
DataExchange (DEX) plugin is able to push and pull information into and out of a standard SQL (Structured Query Language) database. This type of integration is common for interfacing with homegrown applications and with third-party products that are able to interface through an external or internal database.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

LDAP

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

Syslog

A 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 products, or with other solutions that can send and receive alerts in this manner. The message format is customizable.



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

The Solution: Orchestrating workflows across many kinds of devices across many environments and other security technologies

General Use Cases

While we have twenty-five out of the box solutions to solve for a specific set of use cases, eyeExtend Apps can be used to solve customer's custom use cases. The following use cases represent a sample of how some of our customers are using or can use eyeExtend Apps running on eyeExtend Connect.

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, datacenter, OT and cloud. For example, the eyeExtend app for Ubiquiti helps customers increase visibility into their wi-fi connected devices and use those attributes 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 ITSM or asset management product to true-up their CMDB. Another 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. Security operators, leveraging the integration with the Forescout platform can determine if 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 EMM 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 the Chromebook device context. This data helps with refining the 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 Forescout platform to take a specific action or direct another integrated product to take a specific action. These triggers are based upon policy-driven automation, rather than playbook-based decision making which requires a human operator. This translates into faster response times, a more secure network and more valuable resources saved.

Leverage in-depth, contextual device data for correlation analysis to accelerate incident response

eyeExtend Connect can feed in-depth device data into a SIEM (Security Information Event Management) system where it is analyzed for correlations. The comprehensive and rich contextual device data provides a complete picture of your entire enterprise attack surface, helps reduce time to insight and facilitates investigations. Forescout also helps with streamlining security operations by automating policy-based actions limiting access of the device to the network based on incident severity feed from SIEM in real time.

To sum up, you get higher-security ROI by taking security tools out of silos and plugging them in to a highly intelligent Forescout platform that can automate threat mitigation and policy compliance to a large extent. This enables you to get much more value out of your security tools and a rapid return on your current investments.

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