FORESCOUT

Forescout eyeControl

Enforce and automate policy-based controls to proactively reduce your attack surface and rapidly respond to incidents

IT security teams are inundated with increasing numbers of security and compliance issues reported by a vast collection of security tools that constantly generate alerts with no ability to take action. Unfortunately, these tools either lack sufficient device context for prioritization or automation capabilities to enforce controls for risk mitigation. As a result, highly skilled security teams waste time manually troubleshooting low-impact issues, unable to focus on proactive risk reduction or fast threat response.

Policy-Based Control Enforcement

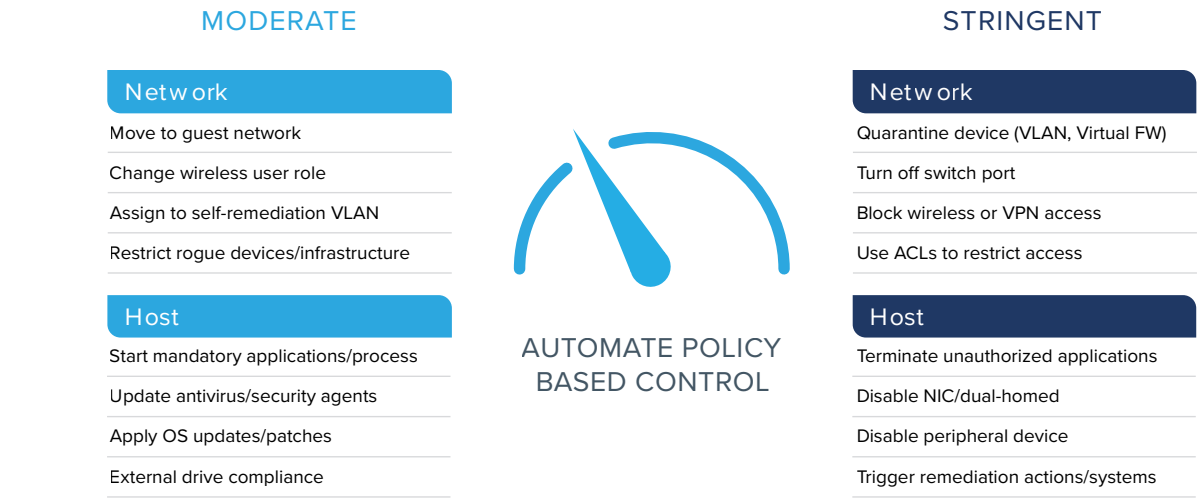
Forescout eyeControl, powered by rich device context from Forescout eyeSight, empowers security teams to prioritize, enforce and automate policy-based controls with confidence. Organizations are able to improve security hygiene, reduce their attack surface and accelerate response and remediation to quickly mitigate threats, security incidents and compliance gaps.

Depending on your security initiatives, you can enforce both network and endpoint actions using eyeControl. To orchestrate network actions, eyeControl directly integrates with heterogeneous physical and virtual networking infrastructure—switches, wireless, VPN, software-defined and cloud-based networking. Endpoint actions can be enforced agentlessly on Windows, Mac and Linux endpoints, or via the use of SecureConnector™.

Highlights

- Protect sensitive data against external threats
- Prevent infected, vulnerable or noncompliant devices from spreading malware
- Prevent targeted attacks from stealing data or forcing network downtime
- Help ensure network access and availability to employees, contractors and customers
- Enforce compliance with internal policies and external regulations
- Automate control actions to provide the right action(s) for each situation

Figure 1. Enforce policies at the network and on endpoints, increasing automation over time.



Automate controls with confidence

eyeControl leverages an intuitive and flexible Policy Engine that enables organizations to apply granular, targeted controls. Sophisticated workflows and compound actions can be implemented with easy-to-use dynamic scoping, Boolean logic and waterfall policies. The Policy Graph feature facilitates accurate policy creation, analysis of policy flows and fine-tuning of policies prior to turning on enforcement actions.

Control actions can be manually initiated by security teams or, to increase security operations efficiency, automation can be gradually introduced. Starting with basic, repetitive tasks and expanding over time to more complex controls, automation can free up skilled IT resources to focus on higher-impact issues. This approach helps ensure minimal business disruption while dramatically improving network access, device compliance, network segmentation and incident response initiatives.

> "Often we can automate action against an endpoint, but when manual intervention is needed, a simple right click is all it takes." – *Joseph Cardamone, Senior Information Security Analyst and North America Privacy Officer, Haworth*

Challenges

- Noncompliant or unauthorized devices on the network pose a large risk
- Flat, under-segmented networks leave organizations susceptible to lateral threats
- Inability to quickly and effectively respond to security threats and incidents
- Limited capacity to enforce continuous device posture through security tools
- Business-disruption risk limits security control automation

Enforce network access

Control access to enterprise resources based on user profile (guest, employee, contractor), device classification and security posture.

- Enable differentiated access for guest and BYOD devices
- Enforce network access policies with or without 802.1X authentication
- Take action against suspicious, rogue or shadow IT devices on the network
- Limit or block network access for compromised or malicious devices
- Quarantine or isolate noncompliant devices until compliance deviations have been addressed

"One of the reasons why we chose the Forescout platform was that this technology doesn't rely on the 802.1X protocol, which makes the deployment very easy. The idea of not installing agents provides high performance and simplicity as well."
—Juan Ignacio Gordon, Head of IT Security, ACCIONA

Improve device compliance

Automate compliance assessment and enforce remediation controls for continuous compliance with internal security policies, external standards and industry regulations.

- Help ensure endpoints are properly configured and initiate remediation for critical configuration violations, including weak or default passwords
- Help ensure required applications and security agents are installed, running and up-to-date
- Disable or block unauthorized applications that could introduce risk or put an unnecessary burden on network bandwidth or resource productivity
- Identify high-risk vulnerabilities and missing critical patches and initiate remediation actions
- Proactively target remediation actions such as installing required security software, updating agents or applying security patches
- Implement policies and automate controls for configuration compliance in cloud deployments, including AWS, Azure and VMware®

"With the Forescout solution, we expect to save millions from exponentially faster audits that produce fewer findings and require less remediation effort."
— Phil Bates, Chief Information Security Officer, State of Utah

Implement dynamic network segmentation

Apply dynamic network segmentation policies across disparate enforcement technologies in your extended enterprise through a common policy framework.

- Dynamically assign devices to segmentation groups based on device properties, classification and security posture
- Apply segmentation controls via VLANs, ACLs, WLAN controls and tagging in campus and OT networks
- Apply segmentation controls via security groups/tags in public and private cloud environments such as AWS and VMware NSX
- Segment noncompliant and vulnerable devices into separate zones—especially those that can only be patched or remediated within scheduled maintenance windows—to enable business continuity while reducing your attack surface
- Enforce segmentation policies to zone devices and critical data flows from the rest of the network, as required by regulations such as HIPAA, PCI and SWIFT CSP

"Not only can Forescout isolate devices and do network segmentation, it can also discover networks that haven't been seen previously." *–Deputy CISO, Large Healthcare Organization*

Accelerate incident response

Quickly and effectively contain threats and respond to security incidents to minimize disruption to operations and damage to the business.

- Identify high-risk devices that haven't been contained or remediated
- Identify indicators of compromise (IOCs) on devices at time of connect to reduce mean time to respond (MTTR)
- Quickly isolate and contain compromised or malicious devices to avoid lateral propagation of malware
- Automate incident response and initiate remediation workflows on compromised devices
- Reduce MTTR by providing valuable device context (device connection, location, classification and security posture) to cross-functional incident response teams and siloed technologies

"Forescout is like having an automatic threat hunter on the team that hunts for threats around the clock across our global network. We are now addressing issues that we couldn't tackle before. Tasks that would have taken hours now take just minutes." *— Nick Duda, Principal Security Engineer, HubSpot*

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