FORESCOUT

eyeControl

Policy-Based Control Enforcement

Enforce and automate control actions across heterogeneous networks

Non-Disruptive
Flexible deployment and access control options – with or without 802.1X.

Agentless
Continuously assess asset hygiene and automatically remediate assets to enforce compliance without installing agents.

Effective
A flexible and unified policy engine to implement zero trust network access.

No Upgrades Required
Seamlessly integrates with existing infrastructure without the need for software or hardware upgrades.

Lower Cost of Ownership
Lower deployment, maintenance, and operational costs leads to a faster ROI.

Forescout eyeControl provides flexible and frictionless network access control for heterogeneous enterprise networks. It enforces and automates Zero Trust security policies for least-privilege access on all managed and unmanaged assets across your digital terrain. Policy-based controls can continuously enforce asset compliance, proactively reduce your attack surface, and rapidly respond to incidents.

Secure Network Access

- Enforce network access based on user, device identity and security posture
- Deploy with or without 802.1X in heterogeneous networks

Enforce Asset Compliance

- Automate compliance with security policies, industry standards and government regulations
- Initiate remediation and risk mitigation workflows in real-time

Automate Incident Response

- Automate response to security incidents
- Contain threats to minimize propagation and disruption

Automate Controls with Confidence

Zero trust policies can only be enforced when grounded in complete asset visibility and context. This includes real-time knowledge of user identity, device identity, security posture and risk profile for all connecting assets. Controls implemented without full visibility can be disruptive and put operations at risk. eyeControl uses the rich asset context from eyeSight to enforce and automate Zero Trust security controls with confidence.

At the core of eyeControl is a unified and flexible policy engine that enables you to apply granular and targeted control actions. This unified policy engine provides:

- Dynamic grouping and scoping of assets by business logic and context
- Compound conditions and actions using Boolean logic and waterfall policies to implement sophisticated control workflows
- Policy graphs for accurate policy creation, policy flow analysis and fine-tuning of policies before turning on enforcement actions
- Start with manually initiated control actions and slowly dial up automated enforcement to increase security operations efficiency

Policies are triggered and evaluated in real time by events and changes that occur to a specific asset or on the network itself. Figure 1 below illustrates the range of control actions available in eyeControl when a policy is triggered.

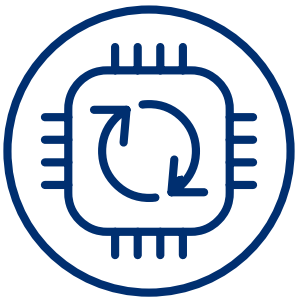
Moderate

Network

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

Host

- Start mandatory applications/process
- Update antivirus/security agents
- Apply OS updates/patches
- Ensure external drive compliance



Automate Policy Based on Control

Stringent

Network

- Quarantine assets (VLAN, Virtual FW)
- Turn off switch port
- Block wireless or VPN access
- Use ACLs to restrict access

Host

- Terminate unauthorized applications
- Disable NIC/dual-homed
- Disable peripheral devices
- Trigger remediation actions/systems

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

eyeControl Solves for:

- **Unauthorized, rogue or spoofed** assets on the network that pose risk and compliance issues.
- **Security gaps** when agent-based tools are not up to date or functioning properly.
- **Flat, under-segmented networks** that leave organizations susceptible to threats and increase the blast radius.
- **Business disruption risks** due to vulnerable assets, missing critical patches and unauthorized applications.
- **Lateral propagation** of threats caused by inability to quickly contain compromised or malicious assets.
- **Noncompliance** due to inability to continuously monitor and enforce policy for connected assets.
- **NAC implementation challenges** in heterogeneous, multivendor environments and wired networks.

Control

Secure Network Access

eyeControl provides the most flexible and non-disruptive network access control solution for organizations with heterogenous networks. Enforce secure access across wired and wireless networks for all managed and unmanaged assets, comply with audit requirements, reduce your attack surface and quickly mitigate threats. Capabilities include:

- Provision zero trust network access for employee, guest, contractor and BYOD devices
- Identify and block rogue, unauthorized or spoofed assets including shadow IT
- Quarantine or isolate noncompliant and high-risk assets until properly remediated
- Leverage a wide range of access control methods – with or without 802.1X authentication
- Incorporate agentless posture assessment and enforce both network and endpoint actions via a unified zero trust policy engine
- Interoperate with existing infrastructure without software or hardware upgrades
- Directly integrate with 30+ network infrastructure vendors across hundreds of product models

Comply

Enforce Asset Compliance

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

- Validate that endpoints are properly configured and initiate remediation for critical configuration violations
- Identify and remediate managed assets with broken or missing security agents
- Detect and disable unauthorized applications that introduce risk, impact network bandwidth or impede productivity
- Identify assets with high-risk vulnerabilities or missing critical patches and automatically initiate remediation actions
- Enforce remediation and risk mitigation actions agentlessly on Windows, Mac, Linux, IoT, IoMT and OT assets
- Implement policies and automate controls for configuration compliance in cloud deployments including Amazon Web Services, Microsoft Azure and VMware

Automate

Accelerate incident response

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

- Automate basic, repetitive incident response tasks and free up your limited resources to focus on higher-impact issues and priorities.
- Identify indicators of compromise (IOCs) and risks to assets in real time to reduce mean time to respond (MTTR)
- Automatically isolate and contain compromised or malicious assets to limit the potential blast radius by avoiding lateral propagation of malware
- Automate incident response and initiate remediation workflows on assets in real time
- Reduce MTTR by providing valuable asset context (device connection, location, classification and security posture) to cross-functional incident response teams and siloed technologies

Discover, Assess, Govern

Forescout Continuum Platform extends the value of eyeControl by providing 100% asset visibility, continuous compliance, network segmentation and a strong foundation for zero trust.

Visit www.forescout.com/products to learn more.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com