eyeControl Datasheet

Enforce and automate control actions for the Enterprise of Things across heterogeneous networks

Thank you for downloading this Forescout datasheet. Carahsoft is the dealer and distributor for Forescout cybersecurity solutions available via GSA Schedule 70, NASA SEWP V, ITES-SW, and other contract vehicles.

To learn how to take the next step toward acquiring Forescout's solutions, please check out the following resources and information:

For additional resources:
carah.io/ForescoutResources

For upcoming events:
carah.io/ForescoutEvents

For additional Forescout solutions:
carah.io/ForescoutProducts

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Forescout@carahsoft.com
833-FSCT-GOV

To purchase, check out the contract vehicles available for procurement:
carah.io/ForescoutContracts

For more information, contact Carahsoft or our reseller partners:
Forescout@carahsoft.com | 833-FSCT-GOV

FORESCOUT
Active Defense for the Enterprise of Things.

eyeControl

Policy-Based Control Enforcement

NON-DISRUPTIVE

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

AGENTLESS

Assess device hygiene and auto-remediate devices to enforce compliance without agents.

EFFECTIVE

Unified policy engine to implement Zero Trust secure access.

NO UPGRADES REQUIRED

Works with existing infrastructure without the need for software or hardware upgrades.

LOWER TCO

Flexible, non-disruptive, agentless and multivendor support – lower deployment, maintenance and operational costs. Faster ROI.

Enforce and automate control actions for the Enterprise of Things across heterogeneous networks

Forescout eyeControl provides the most flexible and frictionless network access control for heterogeneous enterprise networks. It enforces and automates Zero Trust policies for least-privilege access for all managed and unmanaged devices across the Enterprise of Things (EoT). Policy-based controls can be applied to enforce device compliance, proactively reduce your attack surface and rapidly respond to incidents.

SECURE NETWORK ACCESS

Enforce network access based on user, device identity and posture

Deploy with or without 802.1X in heterogeneous networks

ENFORCE DEVICE COMPLIANCE

Comply with security policies, standards and regulations

Initiate remediation and risk mitigation workflows

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

At the core of eyeControl is an intuitive and flexible policy engine that enables you to apply granular and targeted control actions. This Zero Trust policy engine provides:

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

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

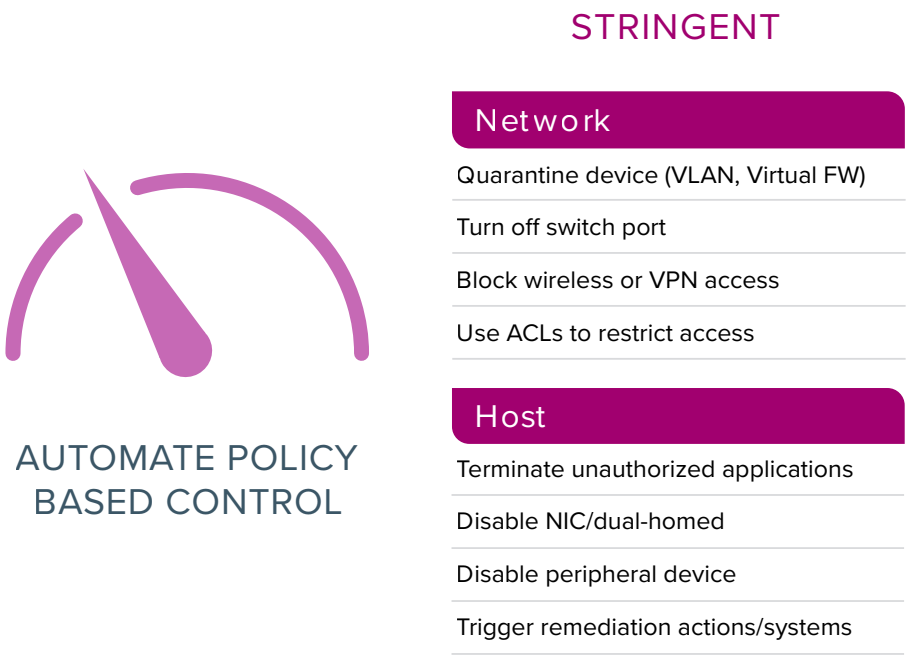

Figure 1. Enforce policies at the network and on endpoints, increasing automation over time.

CONTROL

Secure network access

eyeControl provides the most flexible, heterogeneous and non-disruptive network access control solution for organizations. With eyeControl, you can enforce secure access across wired and wireless networks for all managed and unmanaged EoT systems, 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, shadow IT and spoofing devices
- Quarantine or isolate noncompliant and high-risk devices until 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/hardware upgrades
- Directly integrate with 30+ network infrastructure vendors across hundreds of product models

COMPLY

Enforce device compliance

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

- Validate endpoints are properly configured and initiate remediation for critical configuration violations
- Identify and remediate managed devices with broken or missing security agents

eyeControl SOLVES FOR:

Unauthorized, rogue or spoofing devices 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 devices, missing critical patches & unauthorized applications.

Lateral propagation of threats due to the inability to quickly contain compromised or malicious devices.

Noncompliance due to inability to continuously monitor and enforce device posture for connected devices.

NAC implementation challenges in heterogeneous, multivendor environments and wired networks.

- Detect and disable unauthorized applications that introduce risk, impact network bandwidth or impede productivity
- Identify devices with high-risk vulnerabilities and missing critical patches and initiate remediation actions
- Enforce remediation and risk mitigation actions agentlessly on Windows, Mac, Linux, IoT and OT devices
- Implement policies and automate controls for configuration compliance in cloud deployments, including AWS, Azure and VMware

AUTOMATE

Accelerate incident response

- Quickly and effectively contain threats and respond to security incidents to minimize disruption to operations and impact to the business. Automate basic, repetitive incident response tasks and free up skilled staff to focus on higher-impact issues and priorities.
- Identify indicators of compromise and risks on devices at connect time 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 devices
- Reduce MTTR by providing valuable device context (device connection, location, classification and security posture) to cross-functional incident response teams and siloed technologies

Don't just see it. Secure it.

Contact us today to actively defend your Enterprise of Things.

forescout.com/platform/eyeControl salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things.

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