
# eyeExtend Datasheet

Automate EoT security processes and response across your third-party solutions

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™

# eyeExtend
Orchestrated EoT security

**INTEROPERABLE**
Integrate with all types of IT and security tools using open APIs.

**VERSATILE**
Address advanced use cases that are refined and expanded regularly.

**HIGHLY EXTENSIBLE**
Choose from our vast ecosystem of integrations with more than 70 technology vendors.

**PRE BUILT**
Quickly deploy Forescout-built, tested and supported integrations across many popular technology areas.

**CROWDSOURCED**
Build your own or leverage community-built apps and customize them per your need.

**PARTNER-BUILT**
Leverage integrations built and supported by our partners.

**FASTER ROI**
Easily deploy and consume Forescout /community/partner-built apps and integrations.

## Automate EoT security processes and response across your third-party solutions

Forescout eyeExtend products automate Enterprise of Things (EoT) security processes between the Forescout platform and other IT and security solutions to improve operational efficiency and your overall security posture. Integrate Forescout device intelligence and enforcement capabilities across your current IT and security investments to:

- Eliminate device visibility blind spots
- Automate cross-product workflows
- Accelerate response to risks, incidents and compliance gaps

### SHARE DEVICE CONTEXT

Enrich your security tools' visibility of managed and unmanaged devices

True up CMDB and synchronize device properties bi-directionally

Provide real-time device context to SOC for incident correlation and prioritization

### AUTOMATE WORKFLOWS

Digitize security processes and on-connect workflows across multiple tools

Trigger real-time vulnerability scans, initiate patching and security updates

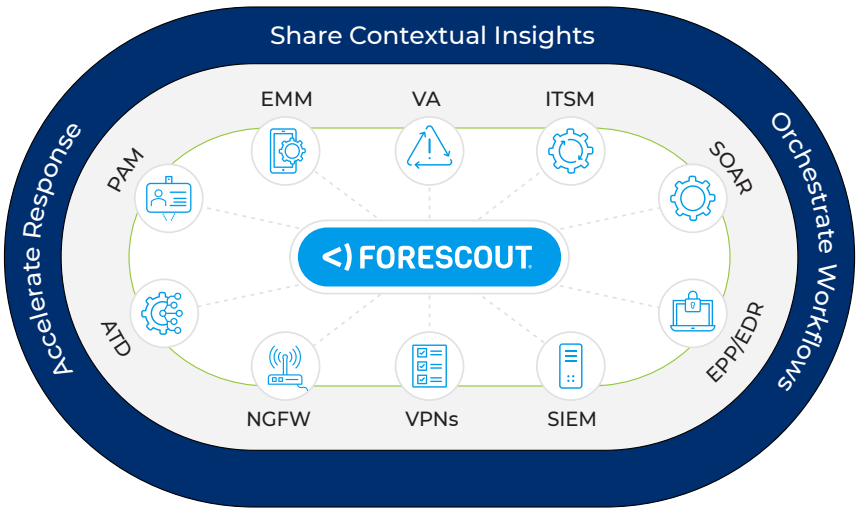
Verify endpoint agents are functional, aggregate threat information and hunt for risks

### ACCELERATE RESPONSE

Speed up system-wide mitigation and remediation for incident response

Enforce policy-driven network access, based on user, device and posture

Contain, quarantine or block vulnerable, compromised and high-risk devices




Integrate with any security solution with an open API

## SHARE DEVICE CONTEXT

Share device information and context bi-directionally across all types of third-party solutions for better policy decisions.

- Leverage Forescout's contextual device insight on device type, configuration, user information, device location and authentication patterns as well as agentless posture assessment for all EoT including IT, IoT and OT devices
- Keep asset inventory databases up to date in real time
- Use data from the Forescout platform and other sources to detect anomalies and identify and prioritize incidents

## AUTOMATE WORKFLOWS

Automate cross-product workflows for security posture assessment and remediation to maintain continuous compliance with internal security policies, external standards and industry regulations.

- Trigger real-time vulnerability scans for new and transient devices at connection time per policy
- Initiate patching and security updates to reduce attack surface
- Verify endpoint agents are functional and automate remediation in case of noncompliance
- Automatically and continuously discover unmanaged privileged accounts and enforce compliance
- Get threat information from other tools, share indicators of compromise and policy violations bi-directionally and extend threat hunting to unmanaged devices

## ACCELERATE REPONSE

Enforce Zero Trust security across Enterprise of Things and accelerate system-wide response to alerts from third-party solutions to decrease mean time to resolution of incidents and threats.

- Initiate network access control actions automatically or manually based on security policies
- Limit or block network access for compromised or malicious devices
- Quarantine or isolate noncompliant devices until compliance deviations have been addressed

### EYEEXTEND SOLVES FOR:

**Noncompliance with security, regulatory and software licenses mandates** caused by visibility blind spots in security technology solutions.

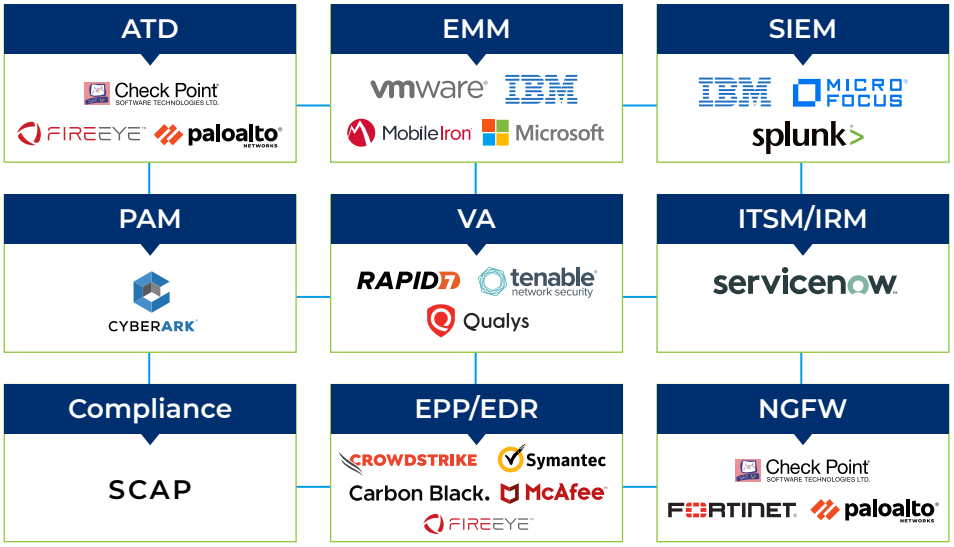
**High operational costs and diminished productivity** due to multiple security tools working in silos, requiring manual coordination for remediation of issues.

**Risk of threat propagation** caused by third-party solutions' limited ability to quickly and effectively respond to system-wide security threats and incidents.

# THE MOST EXTENSIBLE PLATFORM WITH A WIDE RANGE OF INTEGRATIONS

## eyeExtend Modules: Forescout-Built | Supported

Forescout offers pre-built, fully supported eyeExtend modules covering eight security technology areas. The customer use cases are updated and refined on a regular basis.




## eyeExtend Connect Apps: Community-Built | Shared

eyeExtend Connect apps are easy to build, consume and share. They are portable across environments and fully customizable. See the complete catalogue of apps here.


**"We wanted something that would 'play nice.' In addition to being vendor- agnostic, the Forescout solution is quick and easy to implement and provides outstanding visibility, compliance and classification capabilities in real time. Plus, it integrates easily with other systems in our organization, making them more effective and efficient."**

**PHIL BATES**
**CHIEF INFORMATION SECURITY OFFICER, STATE OF UTAH**
Read the case study here

# Partner Integrations
# Partner-Built | Supported

Partner integrations are developed and supported by Forescout technology partners and certified by Forescout.

## Advanced Threat Detection (ATD)
Infoblox, Infocyte®

## ICS/OT Security
tripwire, Indegy, OTORIO

## Network Services/Next-Gen Packet Brokers
Gigamon, ixia, UNISYS, Infoblox

## Compliance Automation
qmulos

## IoT & IoMT Security
MEDIGATE, 802secure, PWNIE EXPRESS, Phosphorus

## Privileged Access Management (PAM)/Identity Management
BeyondTrust, tdi technologies, thycotic

## Data Center and Cloud Security
apstra, netskope

## IT Service Management (ITSM)
nuvolo

## SIEM/Business Intelligence (BI)
exabeam, LogRhythm, Yellowfin, SECURONIX, seceon

## Deception
Attivo NETWORKS, TRAPX SECURITY

## Machine Identity Protection
VENAFI

## Security Orchestration Automation & Response (SOAR)
DEMISTO, SWIMLANE, D3 SECURITY, VULCAN

## Encryption/Data Security
RHEINMETALL, VARONIS, stealthbits

## Network Infrastructure
IS5

## Vulnerability Assessment (VA)
tripwire, SAINT, joval, KENNA Security, DIGITAL DEFENSE, SKYBOX SECURITY, network perception

## Endpoint Protection, Detection & Response (EPP/EDR)
Malwarebytes, SentinelOne, TREND MICRO

## Network Modeling/Risk Scoring
REDSEAL

## Don't just see it. Secure it.™

Contact us today to actively defend your Enterprise of Things.

forescout.com/platform/eyeExtend/ 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