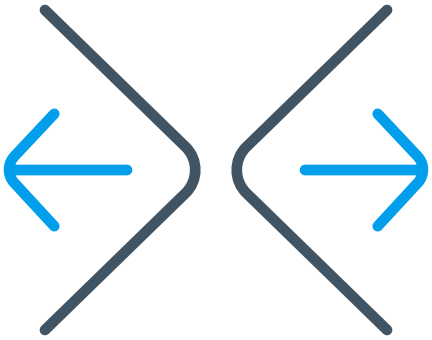
FORESCOUT



eyeExtend Ecosystem

Automate cybersecurity processes and response across your third-party solutions

Highly Extensible
Choose from our vast ecosystem of integrations with more than 70 technology vendors.

Prebuilt
Quickly deploy integrations built, tested, and supported by Forescout across many popular technology areas.

Faster ROI
Save time and money with readily available, proven apps and integrations.

Forescout eyeExtend Ecosystem integrations enable you to automate security processes between Forescout Continuum Platform and other IT and security solutions to improve operational efficiency and your overall security posture. Integrate Forescout asset intelligence and enforcement capabilities across your current IT and security investments to:

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

Share Device Context

- Enrich your security tools' visibility of managed and unmanaged devices
- Update 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 and initiate patching and security updates
- Verify endpoint agents are functional and updated, 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 security posture
- Contain, quarantine or block vulnerable, compromised and high-risk devices

eyeExtend Ecosystem Solves For:

- **Noncompliance with security, regulatory and software license mandates** caused by blind spots in existing 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 respond quickly and effectively to security threats and incidents.

Share Device Context

Share device information and context bi-directionally across third-party solutions for better policy workflows.

- Leverage Forescout Continuum's contextual asset insights on asset type, configuration, user information, asset location and authentication patterns, as well as agentless posture assessment across your digital terrain, including IT, IoT and OT devices
- Save your team valuable time by automatically keeping asset inventory databases up to date
- Detect anomalies and prioritize incidents by combining data from the Continuum platform with other sources of cyber intelligence

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
- Initiate patching and security updates to reduce the attack surface
- Verify endpoint agents are functional and automate remediation in the case of noncompliance
- Automatically discover unmanaged privileged accounts in real time and enforce compliance
- Extend threat hunting to unmanaged devices by leveraging threat information, indicators of compromise and policy violations from other tools

Accelerate Reponse

Decrease mean time to resolution for incidents and threats by accelerating responses to alerts from third-party solutions.

- 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 remediation has been addressed

"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

The Most Extensible Platform with a Wide Range of Integrations

eyeExtend Ecosystem Modules: Forescout-built and Supported

Forescout offers fully supported eyeExtend Ecosystem Modules covering eight security technology areas that are updated and refined on a regular basis.

ATD
Check Point SOFTWARE TECHNOLOGIES LTD.
FIREEYE
paloalto NETWORKS

EMM
vmware
IBM
MobileIron
Microsoft

SIEM
IBM
MICRO FOCUS
splunk>

PAM
CYBERARK

VA
RAPID7
tenable network security
Qualys.

ITSM IRM
servicenow

COMPLIANCE
SCAP

EPP/EDR
CROWDSTRIKE
Symantec
Carbon Black.
McAfee
FIREEYE

NGFW
Check Point SOFTWARE TECHNOLOGIES LTD.
FORTINET
paloalto NETWORKS

Included in Forescout eyeExtend Ecosystem

	INCLUDED
Advanced Compliance Module	✔
eyeExtend for Carbon Black	✔
eyeExtend for Check Point Next Generation Firewall	✔
eyeExtend for Check Point Threat Prevention	✔
eyeExtend for CrowdStrike	✔
eyeExtend for CyberArk	✔
eyeExtend for FireEye EX	✔
eyeExtend for FireEye HX	✔
eyeExtend for FireEye NX	✔
eyeExtend for Fortinet Next-Generation Firewall	✔
eyeExtend for HPE ArcSight	✔
eyeExtend for IBM BigFix	✔
eyeExtend for IBM Qradar	✔
eyeExtend for McAfee ePolicy Orchestrator	✔
eyeExtend for Palo Alto Networks Next-Generation Firewall	✔
eyeExtend for Palo Alto Networks WildFire	✔
eyeExtend for Qualys Vulnerability Management	✔
eyeExtend for Rapid7 Nexpose	✔
eyeExtend for ServiceNow	✔
eyeExtend for Splunk	✔
eyeExtend for Symantec Endpoint Protection Manager	✔
eyeExtend for Tenable Vulnerability Management	✔

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