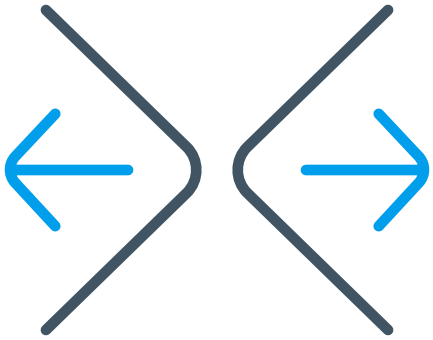
FORESCOUT



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.

The Forescout eyeExtend Ecosystem enables you to automate security processes between the Forescout Platform and the other IT and security investments 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 workflows across product
- 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's contextual asset insights on asset type, configuration, user information, asset location and authentication patterns, as well as agentless posture assessment across your extended enterprise, 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 Forescout 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

Included in Forescout eyeExtend Ecosystem

USE CASE	MODULE
Advanced Threat Detection (ATD)	eyeExtend for Check Point Threat Prevention
	eyeExtend for Trellix Network Security (NX Series)
	eyeExtend for Palo Alto Networks WildFire
Client Management Tools (CMT)	eyeExtend for HCL BigFix
	eyeExtend for Microsoft Intune
	eyeExtend for Jamf
Endpoint Protection (EPP/EDR)	eyeExtend for Carbon Black
	eyeExtend for CrowdStrike
	eyeExtend for Tanium
	eyeExtend for Trellix Email Security (EX)
	eyeExtend for Trellix Endpoint Security (HX)
	eyeExtend for Trellix ePolicy Orchestrator (ePO)
	eyeExtend for Symantec Endpoint Protection Manager
Secure Remote Access	Palo Alto Networks Global Protect VPN
IT Services Management (ITSM)	eyeExtend for ServiceNow
Next-Generation Firewall (NGFW)	eyeExtend for Palo Alto Networks NGFW
	eyeExtend for Fortinet NGFW
	eyeExtend for Check Point NGFW
Privileged Access Management (PAM)	eyeExtend for CyberArk
Security Information and Event Management (SIEM)	eyeExtend for IBM Qradar
	eyeExtend for HPE ArcSight
	eyeExtend for Splunk
	eyeExtend for Microsoft Sentinel
Vulnerability Assessment (VA)	eyeExtend for Qualys Vulnerability Management
	eyeExtend for Rapid7 Nexpose
	eyeExtend for Tenable Vulnerability Management
Compliance	Advanced Compliance Module

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