Forescout eyeExtend

for Micro Focus® ArcSight ESM

Improve situational awareness, prioritize incidents and accelerate threat response

Organizations use the data analytics provided by ArcSight Enterprise Security Manager (ESM) by Micro Focus for threat detection, analysis and compliance management. But in the absence of complete device visibility across managed and unmanaged devices—including bring your own device (BYOD), transient devices and Internet of Things (IoT)—the data analysis is unable to produce an accurate security snapshot of the network. By combining the Forescout platform's complete device visibility and insight with ArcSight ESM's data mining expertise, Forescout eyeExtend for Micro Focus ArcSight ESM allows security managers to achieve a broader understanding of their security posture and helps automate response to mitigate a range of security issues. Your organization benefits by optimizing time to insight, achieving quicker incident response and realizing strengthened network security.

Challenges

- Gaining real-time device visibility and context across managed and unmanaged devices for better situational awareness
- Improving identification and prioritization of incidents across all devices
- Compressing incident response time to curb lateral attacks

The Solution

Forescout eyeExtend for Micro Focus ArcSight ESM enables bi-directional communication and workflow orchestration between the Forescout platform and ArcSight ESM. Forescout eyeExtend for Micro Focus ArcSight ESM combines complete device visibility, broad array of controls and automated response capabilities from Forescout platform with ArcSight ESM's data correlation, analytics and incident management.

With complete device discovery, classification and assessment, Forescout eyeExtend makes ArcSight ESM aware of every single network-attached device—whether managed, unmanaged or transient—the instant it connects. This enables ArcSight ESM to keep its asset repository up to date, and improve correlation and prioritization of events by triaging the additional device information from Forescout platform with other security products and applications. Forescout platform can also proactively take network access control actions based on ArcSight ESM's correlation rules, such as limiting device access to the network based on threat severity in real time.

Forescout eyeExtend for Micro Focus ArcSight ESM helps improve situational awareness, prioritize incidents and automate remediation to enhance overall IT and security operations efficiency and minimize security and business risk to an organization.

eyeExtend

Benefits

- Reduce risk and refine security policies by collecting real-time device and network insight across all network connected devices
- Improve operational efficiency by enhancing incident categorization of ArcSight ESM with Forescout's rich contextual device data
- Minimize security risk by automating incident response to rapidly mitigate threats

Highlights

- Get complete device discovery, classification and assessment of all IP-connected virtual and physical devices, including unmanaged BYOD, guest, transient, IoT and OT devices
- Share device status, compliance posture and state changes with ArcSight ESM
- Maintain ArcSight asset repository up to date in real time
- Validate ArcSight's SmartConnector agents' health to help ensure they are fully functional and current at all times
- Dynamically isolate or block noncompliant or infected devices for threat containment

Use Cases

Enhanced incident correlation and prioritization

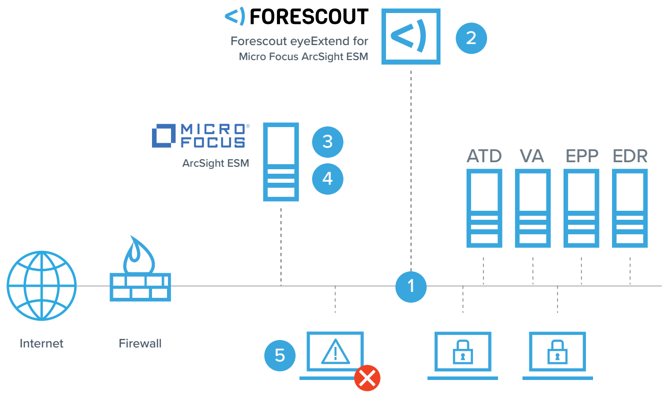
eyeExtend for Micro Focus ArcSight ESM continuously sends device property and status information on devices— managed and unmanaged—to ArcSight ESM and helps update ArcSight assets dynamically. ArcSight ESM correlates this real-time device information from the Forescout platform with other security products. ArcSight ESM leverages the additional device insight to determine if a suspicious event is actually malicious or violates policy. ArcSight ESM then escalates or reduces the severity of the event based on the device and user context.

Continuous ArcSight ESM's SmartConnector agent health and compliance assessment

eyeExtend for Micro Focus ArcSight ESM verifies that ArcSight ESM's SmartConnector agents, which collect event logs on Windows devices, are installed, configured and properly running on Windows devices at all times. If a connecting Windows device does not comply with security policy, the Forescout platform can facilitate remediation.

Automated incident response

ArcSight ESM shares threat information, including severity level with Forescout platform via eyeExtend. The Forescout platform can dynamically trigger policy-based mitigation and response actions such as isolating or quarantining potentially compromised or noncompliant devices, depending on the severity of the violation. For example, when ArcSight ESM detects, via firewall log correlation, a targeted denial of service (DOS) attack, it can direct the Forescout platform to have the firewall automatically block the source of the attack to prevent further disruption of service to the application(s) on the network.



1. Forescout platform discovers, classifies and assesses devices as they connect to the network
2. Forescout eyeExtend sends up-to-date device context, classification and compliance information to ArcSight ESM
3. ArcSight ESM enriches events from other data sources with device context from Forescout platform to help identify and prioritize security incidents
4. For incidents related to vulnerable, non-compliant or infected devices, ArcSight ESM sends a trigger to Forescout platform to initiate policy based action on the device
5. Forescout platform initiates threat mitigation actions on the device based on the severity of the incident e.g. isolate the endpoint, trigger remediation actions, or notify the user of the issue

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