



Forescout eyeExtend for Microsoft Sentinel®

Intelligent security analytics for your entire enterprise

**Manage risks.
Contain events.
Mitigate threats.**

The Forescout Platform continuously identifies, protects and helps ensure the compliance of all managed and unmanaged cyber assets – IT, IoT, IoMT and OT.



Forescout eyeExtend helps you improve your security posture, enforce compliance and increase security operations efficiency by automating security processes and response across products.

Improve situational awareness, prioritize incidents and automate threat response

Organizations use Microsoft Sentinel’s data analytics to gather, analyze and correlate security information and events for incident investigation and compliance reporting. But the challenges to get an accurate security snapshot of the network and ability to dynamically respond to any identified incident remain for organizations. By combining the Forescout® Platform’s complete device visibility and insight with Sentinel’s data mining expertise, Forescout® eyeExtend for Microsoft Sentinel allows security managers to achieve a broader understanding of their security posture, visualize key control metrics and respond more quickly to mitigate a range of security incidents. Organizations benefit by optimizing time to insight, achieving quicker incident response and strengthening network security.

Challenges

- ▶ Gaining real-time visibility across managed and unmanaged devices
- ▶ Improving the accuracy and reliability of Microsoft Sentinel’s trend analysis for incident investigation
- ▶ Rapidly detecting and prioritizing alerts and assessing criticality of incidents to focus resources on the most urgent security events
- ▶ Compressing incident response time to curb lateral attacks
- ▶ Unauthorized PLC logic and firmware changes

Joint Value Proposition



Sentinel: Correlates and analyzes Forescout data with other data. Analyzes complete incident lifecycle.



Sentinel: Incident detection reveals security incident exposure.



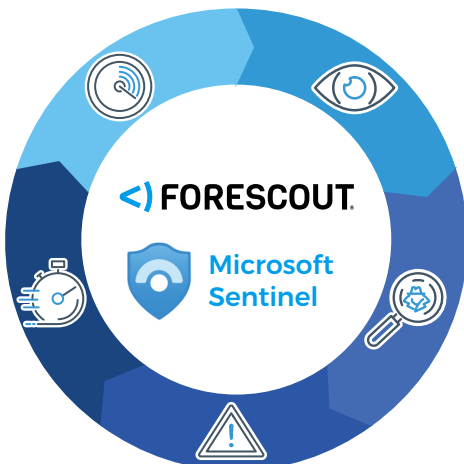
Sentinel: Automation workflow begins. Request for action sent to Forescout. Adaptive Response action triggered.




Forescout: Takes automated incident response actions to mitigate and remediate.




Forescout: Continuously discovers, classifies and assesses rich device data. Data sent to Sentinel, including results of any actions taken.




Highlights

 Complete device visibility including unmanaged BYOD, guest, IoT, IoMT and OT devices

 Rich contextual device data

 Enhanced incident correlation and prioritization

 Automated and closed-loop incident response workflows across entire incident lifecycle

Use Cases

Automated threat management

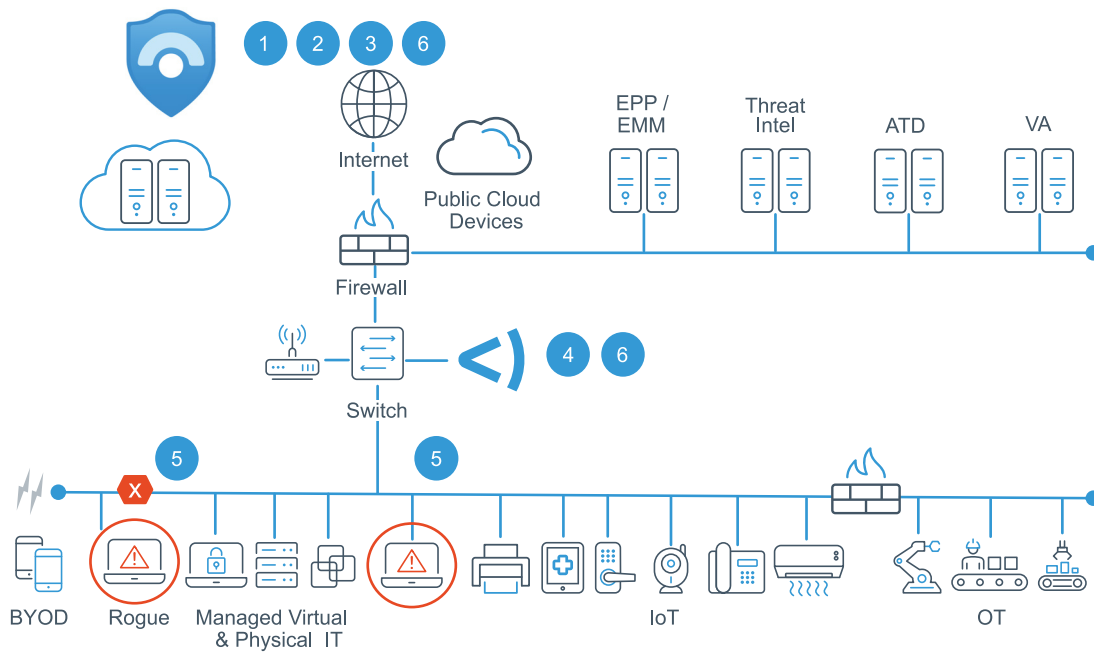
Reduce your mean time to respond to threats with Microsoft Sentinel's security incident workbook powered by Forescout's Logic App to automate network response.

Context enrichment for threats and detections

Enrich Microsoft Sentinel's threat with Forescout's complete visibility including physical and logical network location of threats, compromised users or endpoints, and real-time exposed risk surface.

Visibility and trend analysis

Gain real-time insights into risk and attack surface telemetry for all your IT, IoT, IoMT and OT devices by visualizing and analyzing data such as device properties, profiling and classification.



1. Sentinel built-in or customized detection rules detect a threat.

2. Threats are enriched and correlated into a security incident

3. Sentinel incidents trigger workflow notebook and responds by calling a LogicApp

4. LogicApp on Sentinel sends an action request to Forescout to remediate or restrict

5. Forescout executes the remediation or restriction action

6. Forescout records the action in Sentinel