FORESCOUT

Datasheet

Forescout eyeExtend for Microsoft Defender for Endpoint & Vulnerability Management®

Strengthen endpoint defenses and accelerate threat response

Enterprise IT and security teams are managing increasingly complex environments with exponential growth in the volume and diversity of devices connecting to the network. The rise in network-connected devices increases the attack surface and allows threat actors to capitalize on the weakest link to gain a foothold on your network. To combat cyber threats, Microsoft's Defender family of solutions offers comprehensive threat prevention, detection, and response capabilities. However, unmanaged devices that connect to the network unnoticed pose a risk that must still be addressed. If compromised devices are left undetected, they can be used as launch pads to target higher-value assets, gain access to sensitive information, and cause significant business impact.

Forescout eyeExtend for Microsoft Defender for Endpoint (MDE) provides a comprehensive approach to security that spans complete device visibility, supplementing the Microsoft view with additional insights on all unmanaged devices throughout the environment. This helps increase MDE managed endpoint coverage and security hygiene, extends threat hunting to unmanaged devices and accelerates threat response in real time.

Challenges

- Understanding the entire attack surface to plan and execute protection against advanced threats
- Minimizing IT and security staff's manual workload of managing device compliance
- Reducing lengthy response times and manual processes to address threats to avoid lateral threat propagation

The Solution

Forescout eyeExtend for Microsoft Defender for Endpoint orchestrates information sharing and security workflows between the Forescout platform and Microsoft to improve device compliance, proactively detect threats across the entire network, and automate threat response.

eyeExtend for Microsoft Defender for Endpoint leverages the comprehensive device discovery, classification, assessment, and context provided by Forescout eyeSight. With complete device visibility, Forescout eyeExtend makes Microsoft aware of every single network-attached device—whether managed, unmanaged, xIoT, or transient - the instant it connects. This enables Microsoft to bring more devices under its endpoint protection management and detect threats across the entire enterprise attack surface. The Forescout platform continuously validates the integrity of Defender agents and helps enforce device compliance at all times by initiating remediation of the nonconforming devices. Forescout also strengthens threat detection and enforcement by extending Microsoft endpoint threat intelligence to automatically hunt for, mitigate, and remediate threats across device types and network tiers.

eyeExtend

Benefits

- Reduce security risk by extending Microsoft's threat intelligence to automatically hunt for, mitigate and remediate threats across all devices— managed and unmanaged
- Increase operational efficiency by assessing devices in real time and bringing all devices under Microsoft Defender endpoint protection
- Automate threat remediation and response for noncompliant or compromised devices via Forescout policy controls

Highlights

- Get complete visibility across managed, unmanaged and transient devices-on and off-premises
- Validate that all devices have Defender agents installed, operational, updated and communicating properly with the Microsoft cloud
- Prevent noncompliant Microsoft-managed devices from gaining access to corporate resources without appropriate remediation
- Dynamically control network access by isolating, restricting or blocking compromised devices in real time

Use Cases

Improve device security coverage and compliance

Forescout continuously verifies that the Defender Endpoint agent is installed and running on supported devices and communicating properly with the Microsoft cloud. After determining if a device is new, unmanaged or has a broken agent, Forescout notifies the administrators and facilitates remediation by redirecting users to a self-help page for agent installation. Devices that leave the network are verified when they reconnect to enforce compliance.

Improve insight into corporate devices on-site or off-premises

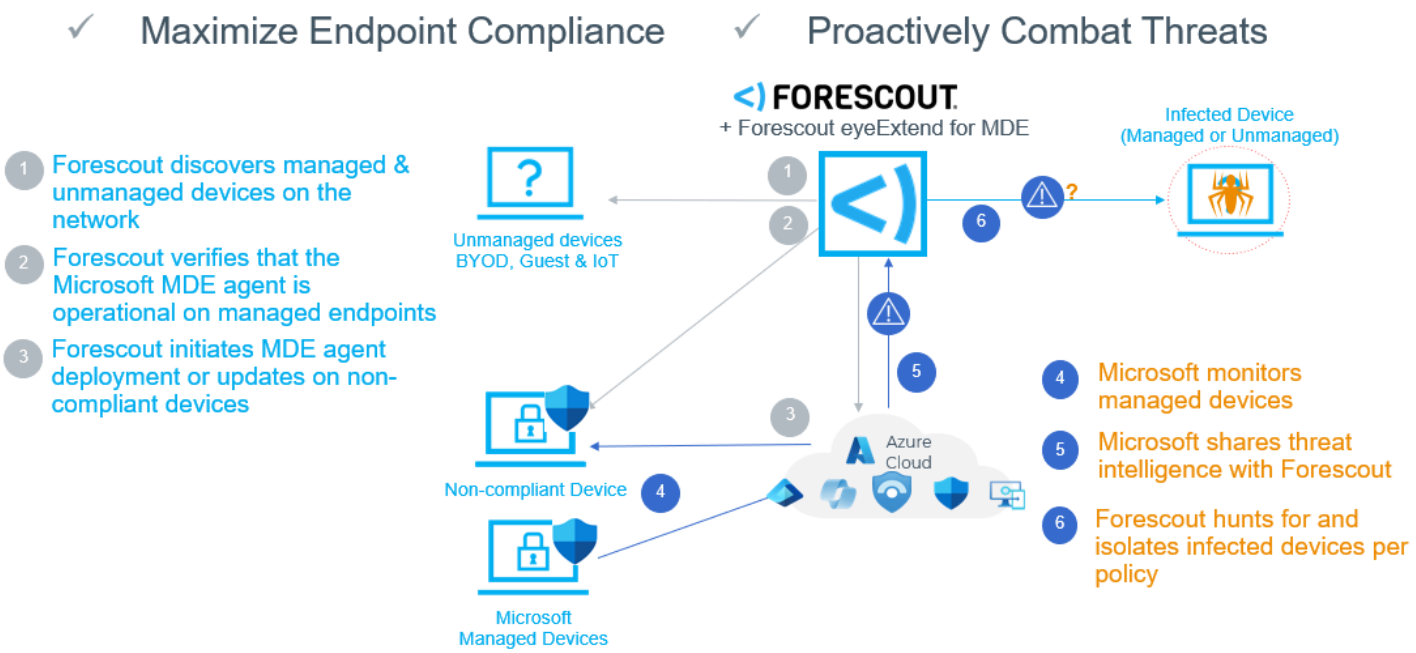
Forescout eyeExtend powered by Forescout eyeSight provides comprehensive visibility across all networked attached devices agentlessly. The Forescout platform also pulls device information on Defender-managed devices while those devices are on-site or off the enterprise network, providing you with a more comprehensive device inventory.

Leverage shared threat intelligence to maximize joint threat hunting and detection

Microsoft Vulnerability Management provides vulnerabilities & CVEs, incidents, and alerts on managed devices and notifies Forescout eyeExtend upon detection. Forescout leverages this additional threat intelligence to monitor across unmanaged devices such as BYOD, guest and IoT, as well as network infrastructure. Based on your policy, the Forescout platform can dynamically limit network access for compromised devices.

Accelerate and automate policy-driven threat response

Upon detection of malware or malicious behavior, Microsoft immediately informs Forescout eyeExtend. Based on threat type and your policies, the Forescout platform automatically takes appropriate network control actions, such as restricting or blocking compromised devices in real time. If an endpoint is infected, Microsoft can trigger the Forescout platform to isolate the device dynamically and contain the threat by cutting off all network access except for its access to the Microsoft cloud for remediation. Forescout's network control actions reduce your mean time to respond (MTTR) and limit the impact of threats.



FORESCOUT

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