Forescout eyeExtend

for Symantec™ Endpoint Protection 14

Strengthen endpoint defenses, improve device compliance and automate threat response

Any connected device on a corporate network can be a launchpad for cyberattacks. With the threat environment evolving quickly and the exponential growth and proliferation of connected devices, weak endpoint defenses can lead to security breaches. To combat cyberthreats, organizations use endpoint security solutions such as Symantec Endpoint Protection (SEP) to help protect endpoints from attack vectors. However, unmanaged and transient 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 Symantec Endpoint Protection 14 provides a comprehensive approach to security that spans complete endpoint visibility without requiring agents. In addition, it automates response workflows for device compliance and threat remediation in real time.

Challenges

- Understanding the entire attack surface to plan protection from cyberthreats
- Ensuring all devices get safeguarded by Symantec Endpoint Protection
- Minimizing IT and security staffs' manual workload of managing device hygiene and compliance
- Reducing lengthy response times and manual processes to address security threats posed by noncompliant or compromised devices

The Solution

Forescout eyeExtend for Symantec Endpoint Protection 14 strengthens Symantec Endpoint Protection by bringing unmanaged devices under Symantec's security management and by providing policy-based assessment, monitoring and precise automated control of these devices to reduce the impact of security breaches.

eyeExtend for Symantec Endpoint Protection 14 leverages the complete device visibility and assessment provided by Forescout eyeSight to make Symantec Endpoint Protection aware of every single network-attached device—whether managed, unmanaged or transient—the instant it connects. This gives you an accurate picture of the potential attack surface. With Forescout, customers have discovered approximately 30% more devices connected to their networks than they were previously aware of.

eyeExtend

Benefits

- Enhance the power of Symantec Endpoint Protection 14 with complete device visibility across managed, unmanaged and transient devices
- Increase operational efficiency through real-time device assessment and SEP agent deployment
- Reduce security risk by continuously enforcing proper device configuration and security policies
- Automate remediation and response for noncompliant or compromised devices

Highlights

- Validate Symantec Endpoint Protection agent and its threat protection components are functioning properly at all times
- Facilitate enrollement of unmanaged devices to Symantec Endpoint Protection in real time
- Enforce device compliance at the time of connect and thereafter
- Initiate immediate malware scans on managed and unmanaged devices based on SEP or third-party threat intelligence
- Isolate, block or quarantine noncompliant or infected devices from accessing the network

Forescout eyeExtend also ensures that devices maintain the correct security posture and are compliant with enterprise security policies from the time they connect to your network and for the entire duration they remain connected. It continuously validates the integrity of Symantec Endpoint Protection agents, triggers real-time malware scans across managed and unmanaged devices and helps enforce device compliance at all times. Forescout provides automated response actions to isolate or restrict network access of noncompliant or infected devices and also facilitates remediation workflows. As a result, you can reduce your attack surface, minimize malware propagation and limit the impact of security breaches.

Use Cases

Expand endpoint security coverage and improve device compliance

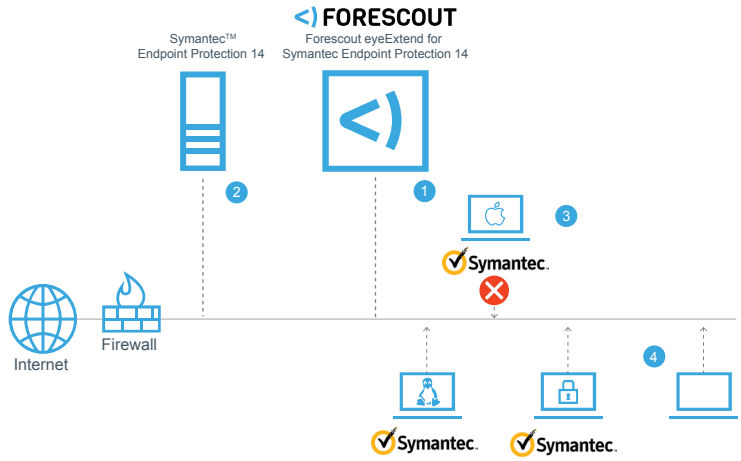
eyeExtend for Symantec Endpoint Protection 14 verifies that the Symantec agent and related components such as Intrusion Prevention System (IPS), firewall and Symantec Online Network for Advanced Response (SONAR) are installed, configured and properly running on all devices at all times. If a connecting device does not comply with your security policy, Forescout can isolate the device from the network and facilitate remediation, such as redirecting the user to a self-remediation page or enabling real-time protection features on the device.

Leverage shared threat intelligence to maximize joint threat hunting and detection

Symantec Endpoint Protection identifies malware and notifies Forescout upon detection. Forescout leverages this threat intelligence to scan the network for malware across Symantec-managed devices and non-Symantec-managed devices, including Bring Your Own Devices, guest and Internet of Things devices, as well as network infrastructure. In addition, Forescout can facilitate malware detection on connected devices by leveraging indicators of compromise from other third-party products that share threat intelligence with Forescout directly or via Symantec Endpoint Protection.

Accelerate and automate policy-driven threat response

Forescout can automatically take policy-driven actions such as restricting, isolating or blocking the compromised device from accessing the network and initiating remediation workflows. The combination of Symantec host actions such as deleting the offending file and Forescout network-based dynamic access control actions reduces your mean time to respond and limits the lateral spread of malware.



1. Different devices attempt to connect to the network and Forescout eyeSight discovers and classifies them
2. Forescout eyeExtend checks if the Symantec Endpoint Protection agent is installed and advanced components (SONAR, real-time protection etc.) are functional
3. If a device doesn't comply with your security policies or Symantec Endpoint Protection detects malware, Forescout isolates the device on the network to facilitate remediation actions
4. Additionally, Forescout can directly scan unmanaged devices or trigger Symantec to scan managed devices for any IOCs from third-party sources, and isolate infected devices

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