FORESCOUT

Highlights

See

- Discover devices as they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Assess device hygiene and continuously monitor security posture

Control

- Notify end-users, administrators or IT systems about security issues
- Conform with policies, industry mandates and best practices
- Restrict, block or quarantine non-compliant or compromised devices

Orchestrate

- Verify Symantec Endpoint Protection agent and its threat protection components are functioning properly
- Trigger real-time malware scans based on third-party threat intelligence
- Isolate non-compliant or infected devices to minimize malware propagation

ForeScout Extended Module for Symantec™ Endpoint Protection

Any connected device on the 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 network breaches. To reduce your security risk and stop these sophisticated attacks, you need a comprehensive approach that spans endpoint detection, prevention and response.

The Challenges

Visibility. Serious attempts to manage security risk must start with knowing who and what is on your network, including visibility into whether networked devices comply with your security standards. Most organizations are unaware of a significant percentage of endpoints on their network because they are:

- Unmanaged guest or Bring-Your-Own-Device (BYOD)
- Internet of Things (IoT) devices
- Devices with disabled or broken agents
- Transient devices, undetected by periodic scans

As a result, organizations are often unaware of the additional attack surface and elevated risk from these devices.

Threat Landscape. According to industry reports[1] corporate-owned devices and servers are among the top enterprise assets targeted and breached by external attackers. These breaches—caused by inadequate security or use of security point products—can cause organizations to lose their competitive edge, reputation and revenue. To protect your organization from these advanced threats and infected devices, you need next-generation security controls that do not rely solely on signatures.

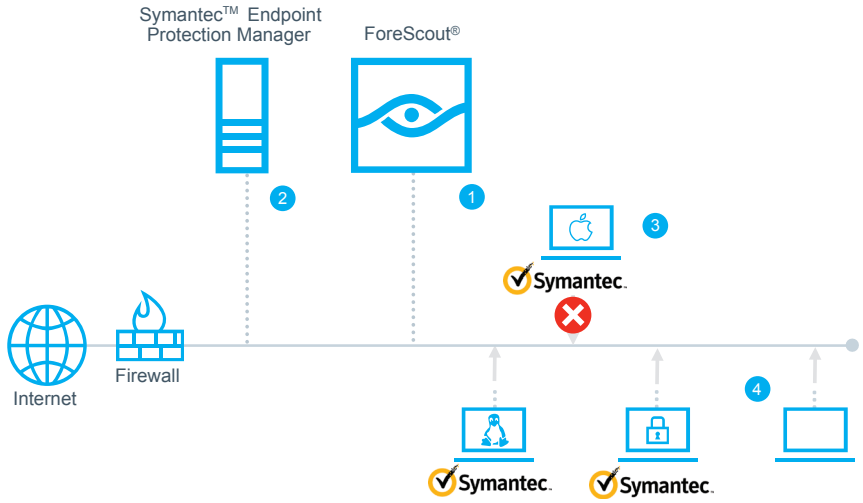
Response Automation. Traditional response techniques rely on manual measures and IT staff to correlate heaps of information, identify high-priority incidents and act on potential threats. The velocity and evasiveness of today's targeted threats, coupled with increasing network complexity, mobility and BYOD, can easily overwhelm this response chain and render it ineffective. For combating today's cyberthreats, it is essential for IT teams to devise a cohesive, automated response strategy to limit threat propagation, security breaches and data exfiltration.

How it Works

ForeScout CounterACT® is a network security solution that gives you the unique ability to see devices, including non-traditional devices, as they connect to the network. CounterACT provides policy-based assessment, monitoring and precise automated control of these devices.

The Extended Module for Symantec™ Endpoint Protection leverages CounterACT's real-time visibility and control capabilities to validate Symantec Endpoint Protection agent integrity, trigger real-time malware scans and help enforce compliance at device connection time. It also provides automated response options to isolate or restrict network access of non-compliant or infected devices and facilitate remediation actions. As a result, you can reduce your attack surface, minimize malware propagation and limit the impact of data breaches.

1. Different devices attempt to connect to the network and ForeScout CounterACT discovers and classifies them
2. The ForeScout Extended Module 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 Extended Modules

The ForeScout Extended Module for Symantec Endpoint Protection is an add-on module for ForeScout CounterACT that is sold and licensed separately. It is one of many ForeScout Modules that enables CounterACT to exchange information, automate multivendor workflows and accelerate system-wide response. For details on our licensing policy, see www.forescout.com/licensing

When devices connect to the network, the ForeScout Extended Module checks the device status with Symantec Endpoint Protection Manager to identify missing agents and initiate their enrollment process. It can also perform granular checks to verify that the Symantec Endpoint Protection agent is running and up-to-date, real-time protection is enabled, and components such as IPS, firewall and SONAR are configured and running. If the 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 agent.

When Symantec Endpoint Protection detects malware on a managed device, it notifies ForeScout to quarantine the device on the network or restrict its access to network resources. In addition, the Extended Module can facilitate malware detection on connected devices by leveraging indicators of compromise (IOCs) from other third-party products that participate in threat intelligence sharing with ForeScout. For Symantec-managed devices, ForeScout can trigger real-time scans by Symantec Endpoint Protection which can then provide granular corrective actions, including notifying the logged-in user or an administrator, performing a full hard disk scan or deleting the offending file. For non-Symantec managed devices, ForeScout can directly scan for IOCs to detect the presence of malware. In either case, ForeScout can quarantine infected devices or restrict their network access, and facilitate remediation actions to limit lateral spread of malware.

Learn more at
www.ForeScout.com

FORESCOUT

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134, USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

[1] The Forrester Wave™: Endpoint Security Suites, Q4 2016