FORESCOUT

Highlights

See

- Discover devices as they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor endpoints on the network, including corporate, BYOD, guest and IoT

Control

- Allow, deny, change or limit network access based on user, network segment, application, device profile and security posture
- Initiate threat mitigation actions on non-compliant, vulnerable and compromised endpoints
- Improve compliance with industry and government mandates and regulations

Orchestrate

- Scan endpoints connecting to your network for IOCs identified by Check Point Threat Prevention
- Quarantine or remediate infected endpoints to help prevent lateral malware propagation
- Automate system-wide responses to quickly mitigate threats and data breaches

ForeScout Extended Module for Check Point® Threat Prevention

Improve defenses against advanced threats and automate threat response to combat modern threats

ForeScout Extended Module for Check Point Threat Prevention allows you to reduce your attack surface, identify advanced threats, scan for indicators of compromise (IOCs), and automate threat response. As a result, you can disrupt the cyber kill chain, limit malware propagation, minimize data breaches and avoid costly investigation and reputation risk.

The Challenges

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

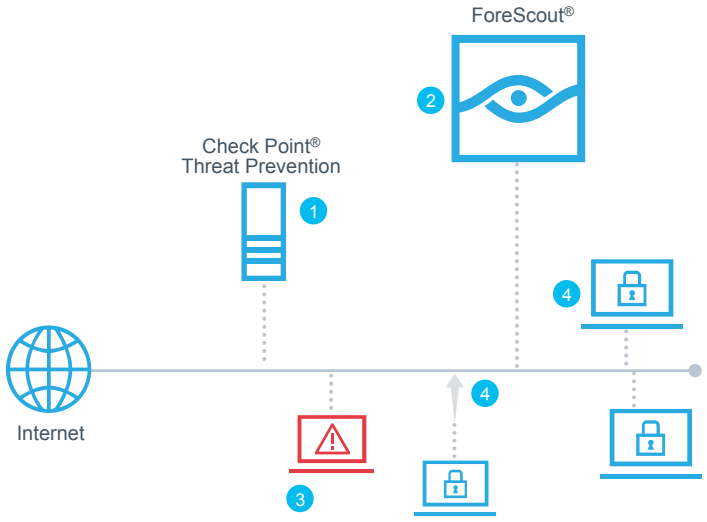
- Unmanaged guest or Bring-Your-Own-Devices (BYODs)
- Internet of Things (IoT) devices
- Devices with disabled or broken agents
- Transient devices, undetected by periodic scans

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

Threat Landscape. According to industry experts, a vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints connected to your network. These threats can easily evade traditional security defenses and move laterally across flat networks to gain access to sensitive applications and information. To reduce your attack surface and confine threat propagation, you need rapidly identify threats, isolate compromised endpoints to prevent lateral propagation and create automated threat responses for mitigation.

Response Automation. Traditional response techniques rely on manual measures and IT staff to correlate heaps of information, identify high-priority incidents and act on the potential threats. The velocity and evasiveness of these 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.

1. Check Point Threat Prevention detects malware and IOCs.
2. Threat Prevention system notifies ForeScout Extended Module about infected endpoints and IOCs.
3. Based on the policy, ForeScout CounterACT isolates the infected endpoint and takes remediation actions.
4. CounterACT also scans connecting and other endpoints on the network for IOCs and initiates mitigation actions.



ForeScout Extended Modules

The ForeScout Extended Module for Check Point Threat Prevention is an add-on module for ForeScout CounterACT that is sold and licensed separately. It is one of many ForeScout Extended Modules that enable ForeScout CounterACT to exchange information bi-directionally, automate threat response and remediation, and more efficiently mitigate a wide variety of security issues.

For details on our licensing policy, see www.forescout.com/licensing.

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

ForeScout Extended Module for Check Point Threat Prevention

The ForeScout Extended Module for Check Point Threat Prevention enables ForeScout CounterACT® and Check Point Threat Prevention to work together. They leverage complementary capabilities of each solution to quickly detect advanced threats and IOCs, contain infected endpoints and break the cyber kill chain. This joint solution provides real-time visibility, compliance management of endpoints on your network and effective response to Advanced Persistent Threats (APTs) including automated remediation.

The CounterACT network security appliance provides IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. CounterACT provides policy-based control of these devices. It works with the ForeScout Modules to orchestrate information sharing and automate workflows among disparate security and IT management tools, including Check Point Threat Prevention.

Check Point Threat Prevention consists of Check Point Software Blade Architecture™, which includes SandBlast™ inspection engine to detect today's advanced threats that may bypass traditional security defenses. It leverages the sandboxing engine to examine a broad range of file types, including executable files, before they enter your network.

When Check Point Threat Prevention detects an endpoint connection to a command and control server, it blocks outbound callbacks and informs ForeScout Extended Module about the infected system, the threat severity and the IOCs. Based on your policy, ForeScout CounterACT then leverages this IOC information from Check Point Threat Prevention to block the specific endpoint, trigger an IOC scan and take pre-defined remediation actions. CounterACT also enables you to scan for IOCs across the network on existing or the new endpoints that are attempting to connect for presence of infection and take necessary actions. This disrupts the cyber kill chain and helps to prevent further lateral threat propagation and data exfiltration.

With the ForeScout Extended Module for Check Point Threat Prevention, your organization can realize improved visibility and real-time intelligence, detect advanced threats and zero-day malware, provide a rapid response to compromised endpoints and have policy-based automated responses to identified threats. As a result, customers can limit malware propagation, minimize data breaches, avoid costly investigations and protect their reputation.