Forescout eyeExtend

for Check Point® Threat Prevention

Strengthen advanced threat detection and accelerate threat response

Organizations deploy advanced threat detection (ATD) solutions such as Check Point Threat Prevention to detect and eliminate known and advanced cyberthreats via multiple methods of security analysis. However, the speed and evasiveness of today's targeted attacks and increasing network complexity from a proliferation of network-attached devices—traditional campus , data center devices, cloud instances, unmanaged bring your own device (BYOD), Internet of Things (IoT), and transient—can overwhelm security defenses and render them ineffective. IT and security teams must have a complete picture of the entire enterprise attack surface and a comprehensive, automated response strategy to combat today's cyberthreats, limit threat propagation and prevent security breaches and data exfiltration.

Forescout eyeExtend for Check Point Threat Prevention enhances the power of Check Point's solution by helping organizations identify their entire attack surface, extend threat hunting to managed and unmanaged devices, and accelerate threat response.

Challenges

- Reducing the time to detect and evaluate potential threats across managed and unmanaged devices
- Responding quickly and effectively to the most advanced threats before they can propagate across the network and inflict damage

The Solution

Forescout eyeExtend for Check Point Threat Prevention orchestrates workflows between the Forescout platform and Check Point Threat Prevention to provide real-time device discovery and assessment for all network-connected devices, scan for indicators of compromise (IOCs) across all devices and accelerate threat response by isolating compromised devices in real time to prevent lateral threat propagation.

Check Point Threat Prevention fortifies network security by examining ingress and egress traffic and detecting and stopping bot command and control communications, unknown malware, viruses and file transfers. However, preventing unmanaged devices and devices infected on outside networks or via non-network pathways—such as USB devices—from connecting to the corporate network remains a challenge. Organizations must also find ways to determine the full extent of network infection and contain threats to prevent further internal propagation. It is often up to the IT or security staff to analyze threat information and determine the best way to stop attacks from spreading, resulting in unnecessary delays and errors that enable damaging data breaches.

This is where Forescout eyeExtend for Check Point Threat Prevention steps in. Forescout eyeExtend powered by Forescout eyeSight enables organizations to

eyeExtend

Benefits

- Reduce security risk by extending Check Point's threat detection to all network-connected devices, including known and unknown devices
- Increase operational efficiency by automating threat response and remediation of infected devices the moment they connect or upon detection of a new threat

Highlights

- Scan all network devices for IOCs discovered by Check Point Threat Prevention
- Contain threats by limiting or blocking access of infected devices to the network in real time
- Eliminate threats from infected devices by killing suspicious processes
- Notify stakeholders such as security teams via emails detailing specific threats and their affected devices
- Get out-of-the-box integration with Check Point Anti-Bot Software Blade, Anti-Virus Software Blade and SandBlast Threat Emulation for easy deployment and a quick ROI

discover, classify and assess all network connected devices, including campus, data center, IoT, BYOD devices and cloud instances. The integration then orchestrates information sharing and automates workflows for policy-based control of these devices. Check Point Threat Prevention alerts Forescout eyeExtend when it discovers new threats, including their indicators of compromise. The Forescout platform quickly applies its rich device knowledge and automates response actions such as notifying security teams, initiating scans of all network-attached devices for new IOC's, blocking infected endpoints from accessing the network, and activating remediation processes to stop threats from spreading.

In summary. Forescout eyeExtend for Check Point Threat Prevention helps organizations reduce their attack surface and helps to prevent threats from spreading and breaching sensitive data.

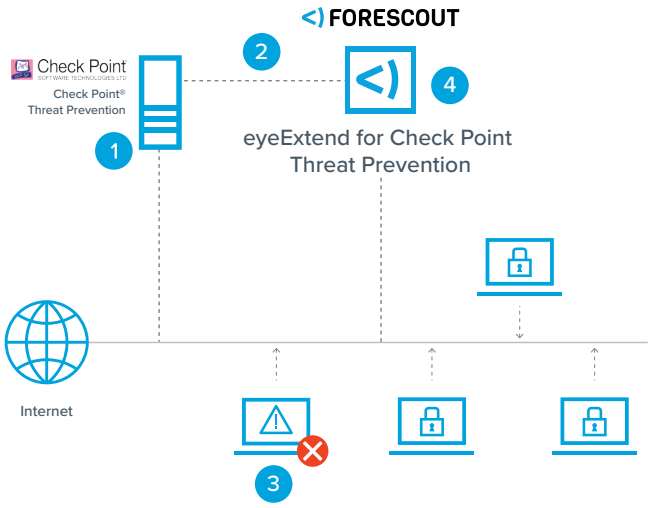
Use Cases

Leverage shared threat intelligence to maximize joint threat hunting and detection

When Checkpoint Threat Prevention identifies malicious files and IOCs on managed devices, it immediately notifies Forescout eyeExtend for Check Point Threat Prevention. Forescout eyeExtend then extends this threat intelligence to the entire network using Forescout platform, monitoring all network-connected devices—including unmanaged BYOD, guest and IoT devices—for IOCs. The Forescout platform also uses the threat information provided by Check Point Threat Prevention to scan newer or transiently connected devices for threat IOC's the moment they connect. It then initiates device isolation and remediation, preventing the spread of threats from any connected device across the network.

Accelerate and automate policy-driven threat response

Forescout eyeExtend helps organizations react in real time to threats based on predefined security policies using Forescout platform. IT and security teams can create Forescout policies for handling antibot, antivirus and threat emulation detections. Based on policy and threat severity, the Forescout platform automatically takes appropriate actions such as restricting, isolating or blocking compromised devices and initiating remediation workflows. These actions reduce mean time to respond and limit the impact of threats.



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

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