CHECK POINT + FORESCOUT

BOLSTER DEFENSES WITH CONTEXT-AWARE ACCESS POLICIES AND GRANULAR NETWORK SEGMENTATION

BENEFITS

Realize

- Discover devices as they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Assess and continuously monitor corporate, BYOD, guest and IoT devices

Control

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

Orchestrate

- Share user and device insight with Check Point's Next-Generation Threat Prevention Platform to enable context aware security policies
- Implement dynamic network segmentation based on real-time device intelligence
- Enforce identity and host-aware network and application access control

INSIGHTS

Many cyber-attacks today rely on stealth and persistence to bypass traditional security defenses. Once they gain a foothold, attackers are able to move laterally across flat networks to gain access to important applications and sensitive information. By implementing best practices – such as dynamic network segmentation and enforcement of access based on user, device and security context – users can reduce attack surfaces and limit the impact of data breaches.

THE CHALLENGES

VISIBILITY

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

- Unmanaged guests 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 surfaces and elevated risks from these devices.

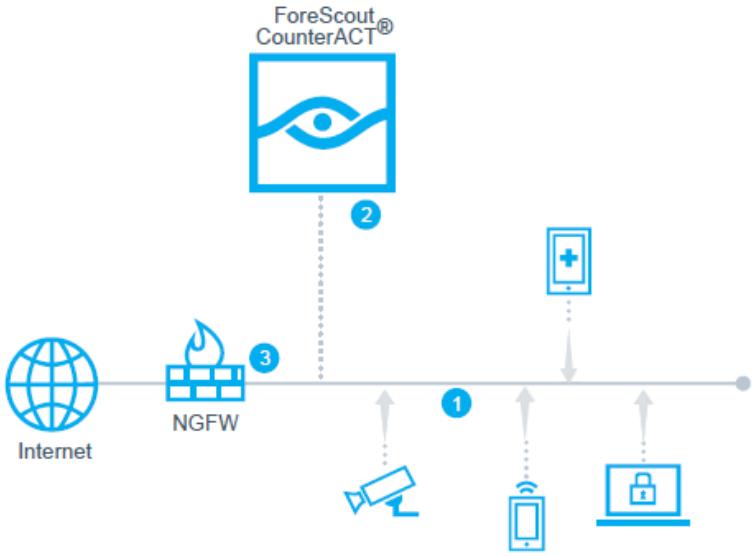
THREAT LANDSCAPE

According to industry experts, a vast majority of successful attacks exploits 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 network controls such as dynamic segmentation. This ensures limited resource access on a need-to-know basis.

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 these targeted threats, coupled with increasing network complexity, mobility and BYOD, can easily overwhelm the response chain and render it ineffective. To combat today's cyber threats, IT teams need to devise a cohesive and automated response strategy to limit threat propagation, security breaches and data exfiltration.

1. CounterACT discovers, classifies and assesses devices as they connect to the network
2. The ForeScout Extended Module sends user, device and security context information to Check Point's Next-Generation Threat Prevention Platform
3. Check Point's Next-Generation Threat Prevention Platform leverages user, device and security context from ForeScout to enforce security policy and network access



The joint solution between ForeScout and Check Point allows users to gain unique endpoint visibility, assign access to resources on the move and enforce granular context-aware security policies. This reduces attack surfaces, prevents unauthorized access to sensitive resources, and minimizes malware proliferation and data breaches.

HOW FORESCOUT EXTENDED MODULES FOR CHECK POINT WORK

ForeScout CounterACT® works with Check Point's Next-Generation Threat Prevention Platform to provide real-time visibility and automated controls for secure access to critical applications and resources. This enables IT organizations to implement dynamic network segmentation and create context-aware security policies within their Check Point gateways based on endpoint context from the Extended Modules.

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. CounterACT works with the ForeScout Modules to orchestrate information sharing and automate workflows from disparate security and IT management tools, including Check Point's Next-Generation Threat Prevention Platform.

Check Point's Next-Generation Threat Prevention Platform provides network control based on user, device, application and traffic classification. Check Point leverages user and device context from a variety of sources to enforce granular access policies with precise and flexible control over resources. ForeScout Extended Modules provide real-time user and device context to Check Point for corporate, BYOD, guest, IoT and other IP-connected devices. This enables Check Point to segment resources on a need-to-know basis and assign appropriate access to resources, regardless of location.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest pure-play security vendor globally, providing industry-leading solutions and protecting customers from cyber-attacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

ABOUT FORESCOUT

ForeScout Technologies (www.forescout.com) is transforming security through visibility. ForeScout has pioneered an agentless approach to network security to address the explosive growth of mobile computing, IoT and cloud computing. We offer a highly scalable, heterogeneous platform that provides Global 2000 enterprises and government agencies with agentless visibility and control of traditional and non-traditional devices, including physical and virtual infrastructure, PCs, laptops, tablets, smartphones and the latest IoT devices, the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments.

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com