FORESCOUT

Highlights

See

- 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 non-compliant, vulnerable or compromised endpoints
- Improve compliance with industry and government mandates and regulations

Orchestrate

- Share user identity with Check Point Next Generation Firewall® to enforce context-aware security policies
- Implement dynamic network segmentation based on real-time device intelligence
- Exchange contextual information to accelerate threat response and more rapidly mitigate risks

ForeScout Extended Module for Check Point® Next Generation Firewall

Improve defenses with identity-aware access policies and granular network segmentation

Today, many cyberattacks attempt to bypass traditional security defenses to exploit the weakest link or device on your network. Once they gain a foothold, they're 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 enforcing access policies based on user, device and security context, you can reduce your attack surface 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 connected devices are compliant with your security standards. Most organizations are unaware of a significant percentage of endpoints on their network because they are:

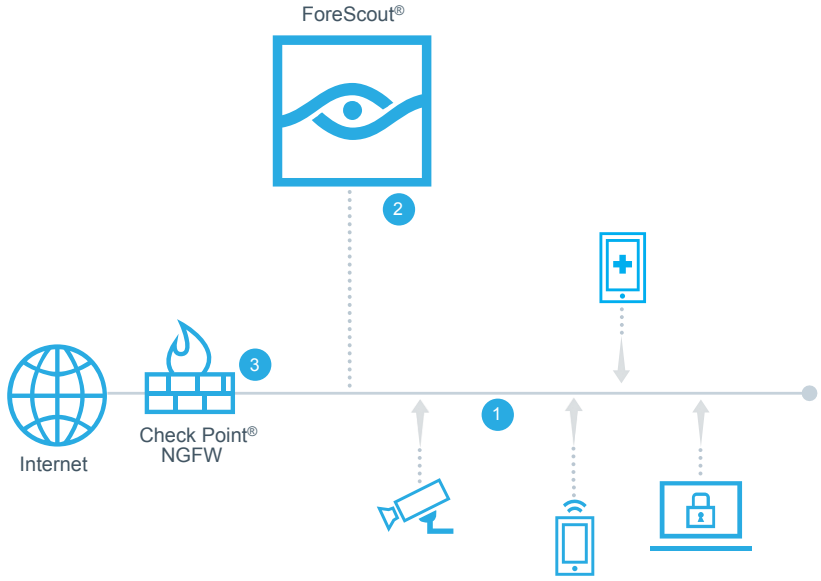
- Unmanaged guests—or Bring-Your-Own-Devices (BYODs)
- Internet of Things (IoT) devices
- Devices with disabled or broken agents
- Transient devices, undetected by periodic scans

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

Threat Landscape. A vast majority of successful attacks exploit well-known vulnerabilities and security gaps on devices 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, to provide appropriate access to resources 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 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. CounterACT discovers, classifies and assesses devices as they connect to the network.
2. The ForeScout Extended Module shares user, device classification and identity information with the NGFW.
3. The Check Point NGFW leverages this information from ForeScout to enforce security and access policies.



ForeScout Extended Modules

The ForeScout Extended Module for Check Point Next Generation Firewall is an add-on module for ForeScout CounterACT that is sold and licensed separately. It is one of many ForeScout Extended Modules that enables ForeScout CounterACT to exchange information, 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.

ForeScout Extended Module for Check Point Next Generation Firewall

The Extended Module for Check Point Next Generation Firewall enables sharing of contextual information between ForeScout CounterACT® and Check Point Next Generation Firewall (NGFW). The joint solution leverages complementary capabilities to provide real-time visibility and precise, automated controls for secure access to critical applications and resources. This enables IT organizations to implement dynamic network segmentation and create identity-aware security policies within their NGFW based on device context from ForeScout.

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 Extended Modules to orchestrate information sharing and automate workflows among disparate security and IT management tools, including Check Point NGFW.

Check Point Next Generation Firewall is a security gateway which scans network traffic content and allows creation of granular security policies based on user identity and device context. The Extended Module for Check Point NGFW provides this identity information and real-time device context to the NGFW for various IP-connected devices, including corporate, BYOD, guest and IoT devices.

The joint solution leverages CounterACT's profiling, classification and assessment capabilities to accurately classify endpoints and dynamically register them in the predefined groups within the NGFW. This enables the NGFW to segment resources on a need-to-know basis and assign access to resources on the move. Additionally, by providing user identity information to the Check Point NGFW with Identity Awareness blade, the Extended Module enables you to create granular identity-aware security policies.

With the Extended Module for Check Point NGFW, you can gain unique endpoint visibility, assign access to resources on the move and create granular, identity-aware security policies. This helps to reduce your attack surface, prevent unauthorized access to sensitive resources and minimize malware proliferation and data breaches.

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

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. **Version 12_18**