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

Orchestrate

- Share user and device insight with next-generation firewalls 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 controls

ForeScout Extended Modules for Next-Generation Firewalls

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

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

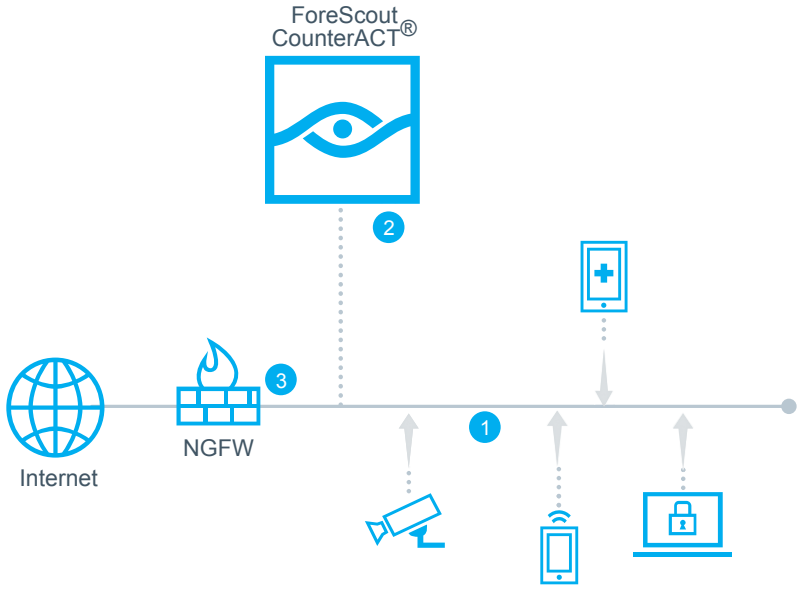
As a result, organizations are often unaware of the additional attack surface and elevated risks from these devices.

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 network controls, such as dynamic segmentation, to help ensure 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 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 sends user, device and security context information to the next-generation firewall
3. The next-generation firewall leverages user, device and security context from ForeScout to enforce security policy and network access

The joint solution between ForeScout and next-generation firewalls allows you to gain unique endpoint visibility, assign access to resources on the move and enforce granular context-aware security policies. This helps to reduce your attack surface, prevent unauthorized access to sensitive resources, and minimize malware proliferation and data breaches.



Supported Next-Generation Firewalls

Check Point®

Palo Alto Networks®

How ForeScout Extended Modules for Next-Generation Firewall Work

ForeScout CounterACT® works with next-generation firewalls 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 context-aware security policies within their next-generation firewalls based on endpoint context from the Extended Module.

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 next-generation firewalls.

Next-generation firewalls provide network control based on user, device, application and traffic classification. They leverage 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 next-generation firewalls for corporate, BYOD, guest, IoT and other IP-connected devices. This enables next-generation firewalls to segment resources on a need-to-know basis and assign appropriate access to resources, regardless of location.

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