SOLUTION BRIEF

Fortinet and ForeScout IoT Security Solution

Comprehensive Protection for IoT

The Internet-of-Things (IoT) revolution is underway, with billons of new IP-enabled IoT devices being deployed worldwide. IoT poses significant challenges for organizations from a security standpoint.

IoT devices are expected to generate unprecedented amounts of traffic and data, taxing already saturated access points, networks, and data centers, not to mention overburdened IT staff. Most IoT devices are headless and not designed with security in mind—it's almost impossible to install a security client on these devices, or in many cases, even push bulk security updates to their firmware. These devices are vulnerable to attacks and can be weaponized to deliver distributed denial-of-service (DDoS) attacks.

Organizations are looking for IoT security solutions that provide visibility into all devices on the network, coupled with constant monitoring, unified management, and automated response to threats.

Solution Description

Fortinet and ForeScout have collaborated to address the above challenges and deliver the Fortinet-ForeScout integrated security solution that provides security without compromise for IoT deployments.

The joint ForeScout-Fortinet solution leverages Fortinet's award-winning FortiGate network security platform for end-to-end protection and combines the agentless classification, assessment, and control capabilities of ForeScout CounterACT® to provide automated, policy-based capabilities to control network access.

ForeScout CounterACT gives IT organizations the unique ability to see new devices the instant they connect to the network, as well as allowing IT to continuously monitor, control, and remediate these devices as they repeatedly join and leave the network. ForeScout CounterACT identifies devices based on their IP addresses, including network infrastructure, bring-your-own-device (BYOD) systems, nontraditional IoT devices (handhelds, sensors, and machines), and rogue endpoints (unauthorized switches, routers, and wireless access points)—no management agents or previous device awareness is required.

The Fortinet FortiGate network security platform provides high-performance, layered security services and granular visibility for end-to-end protection across the entire enterprise network. Innovative security processor (SPU) technology delivers high-performance application layer security services (next-generation firewall, secure sockets layer [SSL] inspection, and threat protection), coupled with the industry's fastest SSL inspection engine to help protect against malware hiding in SSL/transport layer security (TLS) encrypted traffic. The platform also leverages global threat intelligence to protect individual customers, by using Fortinet FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

The Fortinet-ForeScout solution integration provides end-to-end visibility of the organization's entire deployment, including IoT devices, delivering unparalleled protection and security without compromise.

Joint Solution Components

- Fortinet FortiGate
- ForeScout CounterACT

Joint Solution Benefits

- Comprehensive, end-to-end visibility across the entire deployment, including wired, wireless, and IoT devices
- Continuous monitoring and remediation as devices come and go from the network
- Easy to configure, deploy, and maintain without requiring endpoint agents
- Leverage the industry's best validated security protection offered by Fortinet's award-winning FortiGate network security platform to protect against sophisticated cyber threats

FORTINET FABRIC-READY

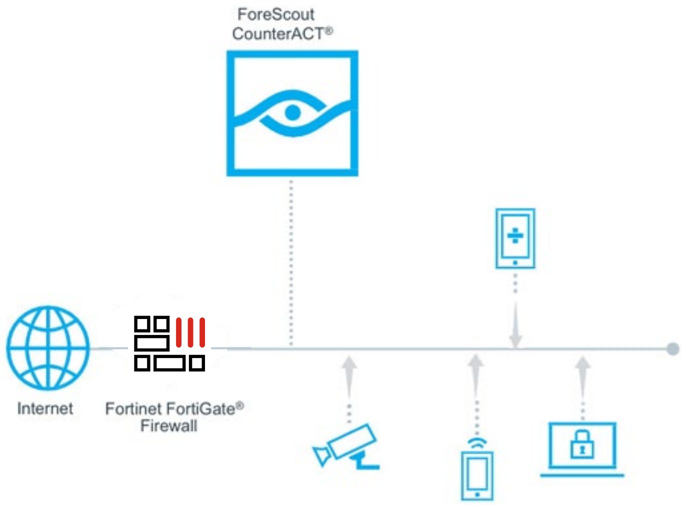

Figure 1: Fortinet-ForeScout integrated security solution.

Learn

With complete network visibility, authenticate and classify IoT devices to build a risk profile and assign them to IoT device groups. Obtain total IT awareness with instant visibility into every security element and key networking components.

Segment

Segment IoT devices into policy-driven groups based on their risk profiles, leveraging the Fortinet Security Fabric, and block threats from spreading through your network.

Protect

Monitor, inspect, and enforce policies and deliver fast and synchronized responses to IoT threats. Protect IoT communications with advanced anti-malware and other security controls in the FortiGate enterprise firewall. Quarantine and remediate compromised IoT devices, ensuring malicious traffic does not reach critical systems or data.

About ForeScout

ForeScout Technologies 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. As of June 30, 2017, more than 2,500 customers in over 70 countries improve their network security and compliance posture with ForeScout solutions. Learn more at www.forescout.com.

www.fortinet.com

September 27, 2021 3:42 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 4:sb-fortinet-forescout-092021:sb-fortinet-forescout-092021

131298-A-0-EN