FORESCOUT

Organizational Challenges

- Protect the security of intellectual property and other sensitive data
- Enhance network security without impeding employees' ability to improve their productivity
- Comply with regulatory mandates pertaining to your company or industry
- Facilitate streamlined network access and information sharing for trusted contractors and customers
- Gain continuous monitoring and mitigation capabilities that leverage existing investments

Technical Challenges

- Discover personally owned and rogue devices as well as other endpoints connected to your network in addition to corporate-owned devices
- Control access to confidential data
- Prevent infected or non-compliant devices from spreading malware across the network
- Keep targeted attacks from stealing data or forcing network downtime
- Measure effectiveness of security controls and demonstrate compliance with regulations

Mobile and BYOD

Automatically detect, profile, assess and control mobile devices for secure network access

Today's employees work everywhere and don't go anywhere without their notebooks, smartphones or tablets. Most employees use multiple devices per day for both business and personal functions. The same is true for contractors and visitors. Of course, every device that accesses your network is a potential hacking or data leakage point. ForeScout offers an automated, policy-based approach to secure your networks and the devices trying to access them.

The Challenge

Here are a few facts about mobile devices that reinforce the need for comprehensive mobile security solutions:

- Hackers breached more than one million Google accounts in Q2 2016 using malware that infects Android-based mobile devices and steals information from Gmail, Google Docs and other Google apps.[1]
- 67 percent of nearly 600 IT security professionals surveyed in a 2016 Ponemon Institute study said it is certain or likely that their organization had a data breach as a result of employees using their mobile devices to access sensitive company information.[2]
- Using cheap, readily available equipment, hackers can access a nearby mobile device in less than 30 seconds and either see everything on it instantly or install malware that siphons data for later viewing.[3]

Traditional Enterprsie Mobile Management (EMM) systems provide some help in securing Bring Your Own Device (BYOD) systems. However, EMM systems alone aren't capable of deterring today's sophisticated and relentless attacks on networks. For example, most EMM systems:

- Only see and manage enrolled devices, leaving IT managers blind to personal and unmanaged devices on the network.
- Control access to applications, but access to the network is wide open. Compromised devices are therefore free to attack the network and move laterally, thus rendering sensitive data completely vulnerable.
- Use polling-based profiling, so a device is only as benign and compliant as it was during the last check.

As mobile devices proliferate, additional intelligence must be applied in order to eliminate intrusions, protect sensitive information and mitigate exposure to mobile threats. IT security managers need the ability to control where mobile devices are allowed on the network, based on the device type, operating system, owner of the device and user login credentials. Also, they need to be able to secure devices upon network resource request and based on policy, and limit many devices to Internet-only access. Lastly, they need EMM systems—and network access control monitoring and mechanisms—to work together on a continuous, 24x7 basis.

> ForeScout CounterACT is BYOD-ready technology, which is important. Quite simply, I cannot imagine being without CounterACT—our IT support team has benefited extensively since its deployment, and will continue to do so for a long time to come."
>
> **— Ronald D'sa**
> **IT Manager**
> **Orbit Showtime Networks**

> We are a commuter college, so everyone brings their own device. With CounterACT, the first time a new worm broke out, the three computers that became infected were immediately isolated, the infection was contained and users were automatically notified."
>
> **— Morris Altman**
> **Director of Network Services**
> **Queens College**

The ForeScout Solution

So, how do you manage mobility and BYOD trends in ways that are secure and reliable without impeding the productivity of employees, partners and customers?

ForeScout CounterACT® can help you manage myriad devices, not to mention mobility and BYOD trends. It continuously scans the network and monitors the activity of the wide range of devices attempting to gain access, as well as those already logged on. That includes unknown devices such as unmanaged, personally owned devices as well as the new waves of wearables and IoT devices seeking network access.

And unlike systems that simply flag violations and send alerts to IT and security staff, CounterACT lets you automate device onboarding and enforce policy-based network access control, endpoint compliance and mobile device security.

The foundation of CounterACT intelligence and functionality can be summed up in three words:

See Know what's on your network and its security posture—including employee-owned, contractor-owned and IoT devices.

- Discover devices the instant they connect to your network without requiring agents
- Classify and profile devices, users, applications and operating systems
- Assess device hygiene and continuously monitor security posture

Control Enforce the appropriate level of access control—from modest to stringent—using policy-based automation.

- Notify end users, administrators or IT systems about security issues.
- Conform with your policies, industry mandates and best practices such as network segmentation. Visitors may only receive Internet access and contractors can be restricted to resources on appropriate network segments.
- Restrict, block or quarantine non-compliant or compromised devices

Orchestrate Tear down security silos by orchestrating policy-based actions between third-party security systems and the ForeScout platform.

- Share contextual insights with EMM, Endpoint Protection Platform (EPP) and other IT and security management systems
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

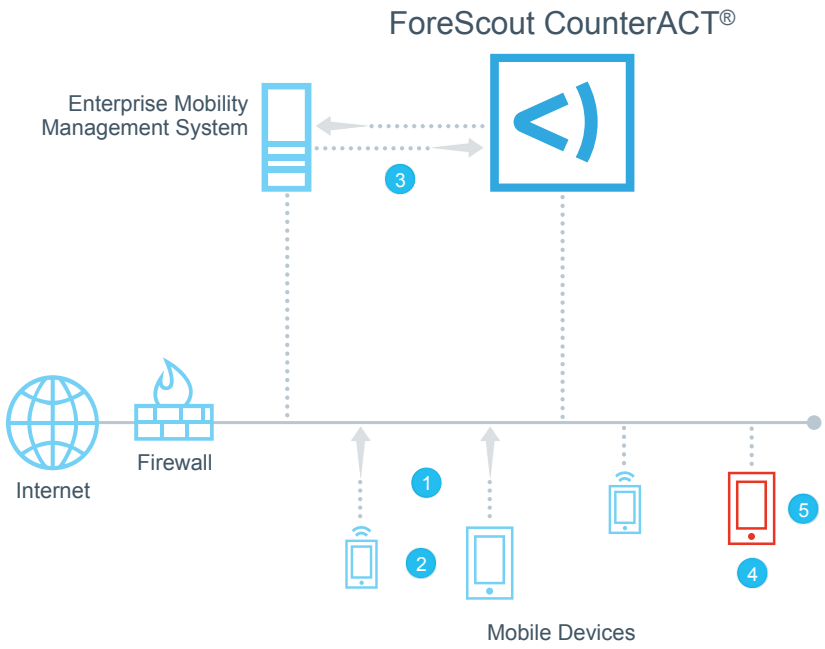
Making CounterACT, EMM and EPP Tools Work Smarter Together

ForeScout Extended Modules provide in-depth endpoint insight, improve situational awareness and accelerate incident response by automating security workflows among third-party security tools. For example, if a device is missing required security software or has a broken Endpoint Protection Platform or Enterprise Mobility Management agent, CounterACT can notify the user and send them to a self-help portal to resolve the issue. CounterACT can also automate notification and agreement of acceptable use policies for visitors.

In addition, Extended Modules allow CounterACT to exchange information with leading EMM tools to validate the device hygiene of tablets and smartphones, monitor security posture and automate enforcement and remediation processes.

Here's how:

1. ForeScout discovers endpoints as they connect to the network—managed or unmanaged.
2. ForeScout validates the EMM agent is installed, fully functional and up to date.
3. ForeScout checks with EMM server to confirm agent is communicating correctly; if needed, ForeScout restarts/reinstalls EMM agent, or triggers EMM server to reinstall it.
4. If EMM agent is missing, ForeScout queries EMM server for compliance and, if required, isolates endpoint and initiates EMM agent installation.
5. Once the endpoint is considered compliant, ForeScout allows the endpoint on to the network.



Learn more at
www.ForeScout.com

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

[1] http://www.cnbc.com/2016/12/01/android-malware-breaches-security-of-more-than-1-million-google-accounts.html
[2] http://www.darkreading.com/endpoint/new-study-shows-mobile-devices-the-cause-of-some-data-breaches/d/d-id/1324415
[3] http://focus.forsythe.com/articles/55/Mobile-Device-Security-in-the-Workplace-5-Key-Risks-and-a-Surprising-Challenge

© 2019 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 01_19**