FORESCOUT

Organizational Challenges

- Apply uniform policy controls across a mix of network and security infrastructure technologies
- Narrow the windows of endpoint non-compliance
- Defend intellectual property and other sensitive data against external threats without impeding business operations
- Achieve continuous monitoring and mitigation capabilities that leverage existing infrastructure investments
- Keep both internal and external auditors satisfied that your network is secure

Technical Challenges

- Obtain real-time endpoint compliance capabilities without security personnel interventions
- Detect and take action against suspicious or rogue endpoints the instant they access the network
- Achieve endpoint compliance without the administrative burden or end user inconvenience of software agents
- Control endpoint configurations according to organizational best-practice policies and regulatory mandates
- Put a system in place that can measure effectiveness of security controls and demonstrate compliance with regulations

Endpoint Compliance

Automate endpoint security to comply with policies and regulations

Without compliance, there's chaos. ForeScout Technology, Inc. solutions measure compliance against endpoint security policies and remediate issues when they occur. Quickly. Automatically. Continuously. ForeScout can find and secure endpoints—regardless of who owns them, their form factors or whether or not they have security agents installed. The result is vastly improved situational awareness, rapid incident response and strict compliance with security policies and regulations.

The Challenge

PCs, tablets, smartphones and other devices pose serious threats to all networks. Each one is a potential point of entry for hackers to exploit. And now, with BYOD* and IoT* dramatically expanding the numbers of managed and unmanaged devices accessing networks every day, IT professionals are tasked with greater endpoint security challenges than ever before. ForeScout CounterACT™ discovers a wide-range of devices—with or without security agents—the instant they connect to your network, allowing CounterACT, IT staff and other security systems to take immediate action.

Here are a few facts that reinforce the need for comprehensive endpoint compliance:

- 98.7 percent of records compromised were the result of external hacking in 2014.[1]
- 75 percent of mobile applications will fail basic security tests.[2]
- The average enterprise has more than 2,000 unsafe or malicious apps installed on users' BYOD devices.[3]

As an IT manager, you have to be able to separate the up-to-date, properly managed endpoints from the unmanaged, unpatched and potentially infected or rogue devices that populate the planet in growing numbers. In other words, you must be able to automate and enforce endpoint compliance.

The ForeScout Solution

ForeScout CounterACT can help you maintain endpoint compliance with relative ease. Placed out-of-band on the network as a dedicated security appliance, it's simple to deploy and provides real-time visibility into endpoints attempting to access your network as well as those already logged on. Unlike systems that simply flag violations and send alerts to IT and security staff, CounterACT lets you automate and enforce policy-based network access control.

Gain Proactive Remediation

By revealing unmanaged systems and insecure endpoints connecting to your network, CounterACT helps you proactively target remediation activities such as updating or activating anti-malware and applying patches.

CounterACT can discover the properties of virtually any endpoint and uses those properties to enforce security within any policy or regulation that you, your organization, your industry or a government agency can define.

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

See CounterACT offers the unique ability to discover devices the instant they connect to your network, without requiring software agents or previous device knowledge. It gathers rich contextual insights regarding the endpoint, its location, who owns it and what's on it. It profiles and classifies devices, users, applications and operating systems while continuously monitoring managed devices, personally owned devices and other endpoints. During this process, CounterACT can identify devices with out-of-date security software and operating systems, as well as those with non-compliant configuration settings.

Control CounterACT can assess and remediate malicious or high-risk endpoints, mitigating the threat of data breaches and malware attacks that would otherwise put your organization at risk. It enables you to allow, deny or limit network access based on device posture and security policies. For example, CounterACT can redirect your antivirus server to auto-update a non-compliant endpoint. In addition, by continuously monitoring devices on your network and controlling them in accordance with your security policies—or any policy or regulation that your organization, industry or a government agency can define—CounterACT streamlines your ability to demonstrate compliance with industry mandates and regulations.

Orchestrate CounterACT leverages the ForeScout ControlFabric™ Architecture to orchestrate information sharing and operation with more than 70 network, security, mobility and IT management products.** It exchanges real-time endpoint compliance data and automates workflows with leading antivirus, patch management and vulnerability assessment products, allowing you to enforce a unified network security policy to reduce vulnerability windows and automate system-wide threat response.

For more than 2,000 enterprises in over 60 countries**, ForeScout is providing the agentless, scalable and cost-effective solution that meets the highest standards for endpoint compliance.

Seeing Is Believing

ForeScout CounterACT is sold as either a virtual or physical appliance that deploys within your existing network, typically requiring no changes to your network configuration. The CounterACT appliance physically installs out-of-band, avoiding latency or issues related to the potential for network failure. It can be centrally administered to dynamically manage tens or hundreds of thousands of endpoints from one console.

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

1 Privacy Rights Clearinghouse research, http://www.securityweek.com/data-breaches-numbers
2 Gartner Research, Sept 2014 http://www.scmagazine.com/gartner-75-percent-of-mobile-apps-will-fail-security-tests-through-end-of-2015/article/372424/
3 https://www.veracode.com/average-large-enterprise-has-more-2000-unsafe-mobile-apps-installed-employee-devices

*Bring Your Own Device (BYOD), Internet of Things (IoT)
**As of October 2015