FORESCOUT

Organizational Challenges

- Develop effective device compliance strategies that detect issues promptly and minimize threats and costs
- Apply appropriate policy controls across a mix of network and security infrastructure technologies
- Bring devices into compliance and ensure patches and appropriate software versions are installed, running and current on managed and unmanaged devices
- Continuously discover and assess agentless devices without disrupting 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
- Obtain real-time endpoint compliance capabilities without the costs and delays of security personnel interventions

Technical Challenges

- Detect and take action against suspicious or rogue endpoints the instant they access the network
- Achieve device compliance without the administrative burden or end user inconvenience of software agents
- Control endpoint configurations according to organizational best-practice policies and regulatory mandates
- Eliminate vulnerabilities on common software platforms that leave you exposed to breaches and make it difficult to validate device compliance
- Put a system in place that can measure effectiveness of security controls and demonstrate compliance to internal auditors and executive staff

Device Compliance

Automate device and endpoint security to reduce your attack surface and improve compliance

Noncompliance equals business risk. ForeScout solutions measure compliance against endpoint security policies and enforce the appropriate controls to help you comply with internal mandates and industry regulations. Quickly. Automatically. Continuously. ForeScout can find and secure devices—including 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

Point-in-time scans, agent-based solutions and other traditional methods for maintaining device compliance are largely ineffective. Especially now, with BYOD, IoT, and OT systems as well as virtual machines dramatically expanding the numbers of managed and unmanaged devices accessing networks every day, IT professionals are dealing with endpoint security challenges like never before.

Fortunately, there is nothing traditional about the ForeScout platform. The ForeScout platform offers a unique combination of agentless visibility and continuous monitoring of connected devices, as well as orchestration with popular security and infrastructure tools. When it discovers devices that are noncompliant with policies and regulations, this visibility and control platform can either take immediate remediation actions itself or can alert IT staff and other security systems.

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

- In 2017, 68 percent of breaches took months or longer to discover[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

The ForeScout platform 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

Automate Threat Containment

The ForeScout platform lets you automate host and network controls to quickly and effectively contain device-based threats. In addition, the platform can block attacks from travelling laterally, and can reduce your attack surface and the number of threats that require mitigation.

Accelerate Remediation

Automate policy-based actions to restrict or quarantine noncompliant devices, achieving a higher level of compliance and security. Actions include notifications, user-based remediations, restricted access and automated remediation. Also, by revealing unmanaged/unsecured devices connecting to your network, the ForeScout platform helps you proactively target remediation activities such as updating or activating antimalware and applying patches.

Increase Efficiency, Reduce Costs and Improve Audits

Automate previously manual network hygiene tasks and free up IT management and security staff to focus on more strategic projects. By reaching a higher level of device hygiene through automation, your security teams have fewer tasks that require their attention, and auditors can point to far fewer issues.

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

access your network as well as those already connected. Unlike systems that simply flag violations and send alerts to IT and security staff, ForeScout lets you automate and enforce policy-based network access control.

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

See The ForeScout platform offers the unique ability to discover devices the instant they connect to your network and monitor them continuously after connection, without requiring software agents or previous device knowledge. It gathers rich contextual insights regarding the device, 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, the ForeScout platform can identify devices with out-of-date security software and operating systems, as well as those with noncompliant configuration settings, and those that exhibit aberrant behavior.

Control The ForeScout platform enables you to allow, deny or limit network access based on device posture and security policies. For example, it can notify a user of noncompliance and redirect them to a self-service portal for an antivirus or other endpoint software updates, prior to granting network admission. Upon recognizing devices without software agents (BYOD, IoT and OT systems), the ForeScout platform can place them on an appropriate network segment by automatically assigning them to the proper access control list (ACL) or VLAN. 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—ForeScout streamlines your ability to demonstrate compliance with industry mandates and regulations.

Orchestrate The ForeScout platform orchestrates information sharing and operation with more than 70 network, security, mobility and IT management products.* With an assist from ForeScout Modules, the platform exchanges real-time endpoint compliance data and automates workflows with leading security solutions of all kinds to automate antivirus enforcement, patch management and continuous vulnerability assessment. This lets you take rapid, coordinated action against noncompliant or risky devices and allows you to enforce a unified network security policy to reduce vulnerability windows and automate system-wide threat response. Should you prefer to enforce segmentation using next-generation firewalls, the ForeScout platform works with leading firewall vendors to provide dynamic, policy-based segmentation based on real-time device context.

For more than 2,900 customers in over 80 countries,* ForeScout is providing the agentless, scalable and cost-effective solution that meets the highest standards for device compliance.

*As of June 30, 2018
[1] 2018 Data Breach Investigations Report, Verizon
[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
[4] IDC: The Business Value of Pervasive Device and Network Visibility and Control with ForeScout, https://www.forescout.com/idc-business-value/