FORESCOUT

Device Compliance

Continuously assess, monitor and enforce policies to reduce risks

> "In addition to being vendor-agnostic, the Forescout solution is quick and easy to implement and provides outstanding visibility, compliance and classification capabilities in real time. Plus, it integrates easily with other systems in our organization, making them more effective and efficient."
>
> **— Phil Bates, Chief Information Security Officer, State of Utah**

Measuring compliance against policies and enforcing security controls can ensure continuous internal and external compliance. The Forescout platform identifies devices, their users and locations, whether they have up-to-date security agents, software and patches—and can automatically remediate issues.

The Challenge

Point-in-time scans, agent-only solutions and other traditional methods for maintaining device compliance are mostly ineffective. Bring Your Own Device (BYOD), IoT, and OT systems (whether on-site or off-site), as well as virtual machines and cloud instances, are dramatically expanding the volume and diversity of devices constantly accessing corporate networks. IT teams are dealing with security challenges like never before—including a rapidly growing remote workforce.

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

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

- When a data breach occurs, compliance failure is a top cost amplifier[1]
- In 2019, 56 percent of breaches took months or longer to discover[2]
- 2019 total cost of a data breach, global average: $3.92M (U.S.: $8.19M)[3]

Organizational Challenges

- Ensure the device hygiene and compliance of remote and BYOD systems
- Bring devices into compliance and ensure patches and appropriate software versions are current and running on managed and unmanaged devices
- Continuously discover and assess agentless devices without disrupting business operations
- Achieve continuous monitoring and mitigation capabilities using existing infrastructure investments
- Keep both internal and external auditors satisfied that your network is secure

Technical Challenges

- Detect and act upon 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 standard software platforms that complicate device compliance validation
- Measure the effectiveness of security controls and demonstrate compliance

The Forescout Solution

The Forescout platform delivers agentless visibility and continuous monitoring of connected devices to help you tackle these challenges. It's simple to deploy and lets you detect and identify all IP-connected endpoints in real time—even VPN-connected devices.

This device visibility and control platform is the ideal solution for keeping noncompliant or unsanctioned devices off your network. And 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. Upon identifying a noncompliant device, the platform can notify users or IT staff and take immediate remediation actions, including orchestrating workflows across many of your existing security and infrastructure tools.

Compliance Validation and Enforcement

Regardless of device location, the Forescout platform can enforce network access control based on your policies. It continuously checks and controls device system configurations to make sure managed devices have fully functional security agents on board, all patches are current and all applications are authorized. It also manages weak or default passwords—even on IoT and OT devices. As for BYOD and other unknown or unmanaged devices, such as those that aren't capable of onboarding security (e.g., IoT, OT, VMs, ICS, etc.), the solution can passively and actively ensure that they meet policy-based criteria at all times or face access restrictions, including blocking, limiting or quarantining.

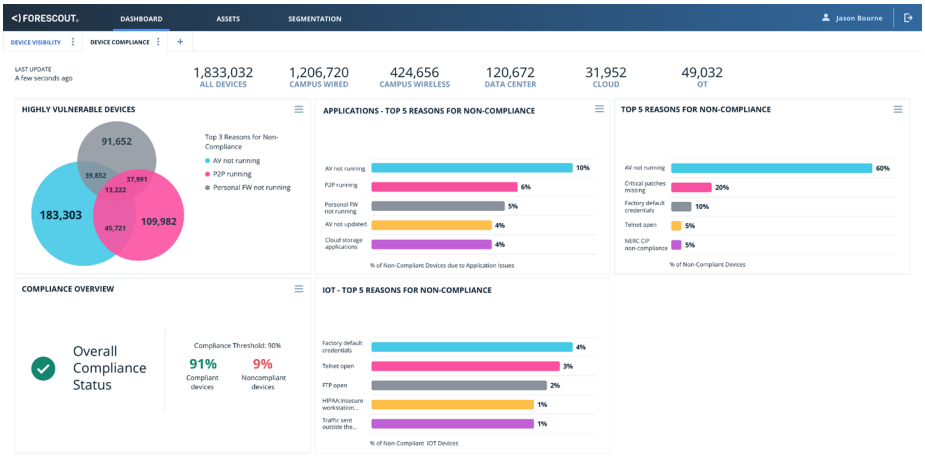

Figure 1 – Forescout's Device Compliance Dashboard provides a real-time view of compliance status for security/IT teams, compliance personnel and senior management.

Automate Threat Containment

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

Accelerate Remediation

Automate policy-based actions to restrict or quarantine noncompliant devices. Actions include notifications, user-based remediations, restricted access and automated remediation. The Forescout solution discovers unmanaged/unsecured devices as they connect, helping you proactively target remediation activities such as updating/activating antimalware and applying patches.

Increase Efficiency, Reduce Costs and Improve Audits

Automate previously manual hygiene tasks and free up IT 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.

Continuous Traffic Monitoring and Control Assurance

Through continuous monitoring, the Forescout platform keeps noncompliant or compromised devices from introducing risk to your network. It identifies anomalous behavior of both users and devices and restricts unauthorized traffic flows. What's more, the platform can trigger leading vulnerability assessment tools to scan and update devices missed by scheduled scans. It can also automate noncompliant device remediation, including installing or repairing broken agents. In fact, control actions can be automated or administrator-initiated. They can be gradually ramped up to minimize disruption while reducing manual effort when it comes to enforcing network access, implementing network segmentation, accelerating incident response and improving device compliance.

The Importance of Compliance

There are many reasons to establish and maintain device compliance—protecting your corporate assets and business reputation, avoiding regulatory fines and penalties, and the satisfaction of running a tight ship, just for starters. But soon there will be billions of more reasons. According to a recent estimate by IDC, 41.6 billion connected IoT devices will be in use worldwide by 2025.[4] And that extraordinary number doesn't include conventional IT devices, OT devices, industrial controls and cloud instances.

That said, you can make sure that all devices of all kinds connecting to your network are compliant with your organization's policies and those of your industry.

Forescout Technologies is the leader in device visibility and control. For more than 3,700 customers in over 90 countries,* Forescout provides agentless, scalable and cost-effective solutions that meet the highest standards for security and regulatory device compliance. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk.

*As of December 31, 2019

1 Cost of a Data Breach Report 2019, IBM Security/Ponemon Institute
2 2019 Data Breach Investigations Report, Verizon
3 Cost of a Data Breach Report 2019, IBM Security/Ponemon Institute
4 "41.6 Billion IoT Devices Will Be Generating 79.4 Zettabytes of Data in 2025," June 2019, https://www.helpnetsecurity.com/2019/06/21/connected-iot-devices-forecast/

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

Learn more at Forescout.com