FORESCOUT

Device Visibility: The Key to Reducing Risk and Improving Your Security Posture

Six Ways to Enhance Security with 100 Percent Device Visibility

Securing network infrastructure continues to grow more complex by the day. This complexity is driven by the phenomenal growth of IoT devices, platform diversity, cloud adoption and IT and OT convergence. The vast majority of new devices joining your networks aren't designed to support management agents—creating a serious visibility and risk gap. And this gap further widens as cloud computing extends to the furthest corners of the distributed network.

Of course, what you can't see can kill you. You need a way to discover devices whether they have agents on board or not, whether they're physical or virtual—regardless of where they're located. You also need continuous, real-time monitoring and the ability to profile and classify devices the second they attach to your network.

Closing this visibility gap is the most effective way to achieve a positive impact on your network security and risk mitigation efforts. Here are six opportunities to do just that using absolute visibility:

1 Get agentless visibility into all systems, including BYOD, IoT devices and OT

You can't secure what you can't see. So, it's a no-brainer: for a solution to be viable, it must provide an accurate, real-time view into all endpoints on your network.

Conventional network access control (NAC) security solutions are only capable of detecting devices that have been equipped with agents. But you can't load agents onto all the BYOD and non-traditional devices that are hitting your network—the employee-owned smartphones, tablets, and wearables as well as IoT devices, OT and contractors' laptops, not to mention rogue devices from who knows where. And they all put you at risk.

You need agentless visibility the minute any device connects to your network. It's not enough to simply discover an IP or MAC address—you need detailed insights into every device to determine its purpose, owner and security posture.

2 Unify visibility and control across data center, campus and cloud environments

Not so long ago, all you had to do was protect your data center. But as you know all too well, the world has gotten a lot more complex. In many cases, single data centers have morphed into multiple ones on distributed campuses that can span the globe. And then there's the cloud.

You need to do more than simply control the perimeter—whatever constitutes a perimeter these days. What's required is instant, real-time access to all endpoints, whether in the data center, campus or cloud. It's no longer feasible to attempt to manage and secure devices and workloads using disparate one-off tools and interfaces. **A viable solution must provide a consolidated view of traditional systems, mobile and IoT devices as well as virtual machines and cloud instances—regardless of where they are located.** Not only that, the solution you put into place must scale as never before to handle your growing network requirements.

This new technology- and location-independent paradigm requires a new way of thinking about solution interoperability (and less tolerance for vendor lock-in). Today, technology value is amplified as systems share visibility through common dashboards and control mechanisms. The new paradigm requires the flexibility to deploy both centralized and distributed architecture based upon changing business requirements.

3 Meet device and regulatory compliance mandates

Abject failure. It's pretty common these days when it comes to penetration tests or regulatory compliance audits because of undetected IoT devices or other threats that were improperly segmented. Successful security strategies start with continuous device visibility and complete device inventories. Otherwise, you put yourself at risk—legally and financially.

Inaccurate IT asset management (ITAM) data can result in noncompliance with regulatory mandates such as GDPR, HIPAA, PCI, FISMA and others. This can cause heavy fines to be levied against your company.

No matter what kinds of assets you are securing—financial, medical, industrial or "other"—the first step to successful risk and compliance is absolute visibility. You need to be able to *see and classify, then automate control of devices and limit access* to areas of the network based on authorization levels, corporate security policies and regulatory mandates.

Given that many of the current regulations, whether state, federal or international, require breach disclosure within hours of an incident, it is critical that security platforms work together to remediate and respond quickly and effectively.

4 Automate device inventory and management

To effectively manage and secure business assets, you need an accurate inventory that includes every device on your network. Remember, it only takes one device missing from your inventory or one with outdated or inaccurate configuration details for hackers to seize an opportunity to breach your network. Discovering devices using traditional approaches can be challenging. According to Gartner, "Through 2020, 30 percent of enterprise assets will remain undetected without active discovery."

Manual asset discovery can result in an incomplete and inaccurate configuration management database (CMDB), undermining your security management initiatives. Tracking inventory through Excel spreadsheets and other manual methods results in errors, and inventory data quickly becomes outdated. An up-to-date device inventory can accelerate response by help desk teams. In addition, *immediate access to accurate device details is critical to security operations teams that are tasked with responding to targeted attacks on specific endpoint operating systems or IoT device types*.

Also, unless you accurately track software, you can risk overutilization and noncompliance with license agreements, which can result in severe penalties.

By automating inventory and management, you can share contextual data with ITAM tools such as ServiceNow® for a real-time, up-to-date CMDB. Your up-to-date inventory can also efficiently manage the lifecycle of devices, helping you with asset capital budgeting.

5 Do context-aware network segmentation

Network professionals and security experts generally concur that network segmentation should be your top priority when securing your network. By assessing and segmenting devices, you can automate policy-based assignment and enforcement of access control lists and VLANs as well as dynamically assign devices to segments to effectively enforce access control and limit access to authorized resources with those segments. It's an effective strategy to prevent employees from wandering into areas of the network where they don't belong and limiting the spread of a malware outbreak.

Adding real-time device context to segmentation assignment dramatically improves security in several ways. For example, a solution with this capability can validate a device's compliance posture prior to segmentation assignment. In addition, it can continuously monitor security posture and device behavior and quickly reassign an unauthorized or noncompliant device to an appropriate segment or restricted VLAN as necessary (for example, if a printer tries to access an HR database or a surveillance camera attempts to access anything other than a digital video recorder). *This new intelligent and dynamic method of segmentation also dramatically simplifies network modifications and allows greater architectural flexibility by allowing context sharing and orchestration with next-generation firewalls.*

To achieve this, you need a NAC solution that integrates easily with switches, virtual private networks (VPNs), cloud-based management systems, and next-generation firewalls.

6 Reduce your window of exposure with orchestrated incident response

Network security teams manage up to 15 tools on average, meaning companies are spending a lot of money—and a lot of time—purchasing, learning and coordinating the use of all these tools. In addition, most of these security solutions are great at sending alerts, yet incapable of enforcing actions. As a result, security teams are overwhelmed with the volume of alerts that must be manually evaluated and resolved.

To accelerate incident response, tools must act upon alerts in a highly automated fashion, respond automatically to known situations, and provide security analysts with prioritized insights when new threats emerge.

To get the most out of these tools, you need out-of-the-box workflow interoperability as well as the ability to perform automated discovery and classification. Also, the solutions you choose should be plug and play with your existing network tools to orchestrate real-time data sharing, alerts, and responses with other ITAM and security tools.

Any new tools should also support multivendor networks regardless of whether assets are physical or virtual across campus, data center and cloud environments.

The ForeScout Solution

The ForeScout device visibility and control platform helps you complete all of these six steps, and more. It continuously discovers all IP-connected devices—without requiring agents—the instant they connect to your network. It provides in-depth visibility into those devices using a combination of active and passive discovery, profiling, and classification techniques. It also provides industry-leading scalability—supporting up to two million devices in a single CounterACT® Enterprise Manager appliance.

Our unique, agentless approach makes a comprehensive range of devices visible—managed and unmanaged, corporate and personal, wired and wireless—even personally owned BYOD systems, servers, switches, rogue hardware and IoT devices.

ForeScout is raising the bar on device visibility and control to mitigate risk, reduce the attack surface and automate incident response across the extended enterprise network—***your*** network.

Now is the time to experience the difference of the ForeScout Visibility Platform. Download ForeScout's Solutions Guide to learn how 100 percent visibility can help solve your security and IT management use cases.

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