FORESCOUT

Mergers and Acquisitions

Minimize cybersecurity risks while enabling rapid change

> "The Forescout platform provides visibility into our acquired companies and affiliates, including device hygiene levels. It checks the OS, patching and antivirus status of any device that attempts to connect to the corporate network and blocks those that don't meet our criteria, allowing us to take quick action."
>
> **Joseph Cardamone, Senior Information Security Analyst and NA Privacy Officer, Haworth**

Merger and acquisition (M&A) activity can add risk. It requires integrating people, processes and disparate technologies, all of which can lead to cyber vulnerabilities. The Forescout platform streamlines and secures the M&A process by providing absolute device visibility and automated control to effectively manage cyber, operational and compliance risks while building interoperability into security infrastructure.

The Challenge

Consolidation is the norm. In many industries today, it's not a question of if mergers and acquisitions will occur, but when. And while M&A activity may be prudent, it can present significant challenges, including:

Acquired risk: The Marriott-Starwood breach that was first reported in late 2018 made one thing abundantly clear: You don't just acquire a company, you also acquire its risks. It's essential to see every device—including its security posture—on acquired network segments prior to merging networks.

Endpoint invisibility. Large numbers of endpoints go undetected on most networks. Many are unmanaged and unseen, such as BYOD, IoT, operational technology (OT), guest and rogue devices. Others are managed but have disabled or broken agents or are transient devices that aren't detected by periodic scans. What's out there? Who owns them? Who knows?

Business Challenges

- Protect sensitive systems and data during transition
- Rapidly secure new network segments
- Securely embrace BYOD, IoT, OT and guest devices
- Preserve investment in legacy infrastructure
- Leverage existing network security investments
- Ensure interoperability with current and future systems
- Maintain resiliency and availability for critical services
- Comply with regulatory mandates

Technical Challenges

- Discover unknown (unmanaged) devices that do not have security software (agents) on board
- Classify devices and determine their owners regardless of location on complex heterogeneous networks
- Ensure security software is up to date on devices
- Scale to address rapid growth and distributed networks
- Assess and continuously monitor devices to detect anomalous behavior
- Prevent infected or noncompliant devices from spreading malware across the network
- Integrate disparate security solutions into a unified, enterprise-wide system

Vendor lock-in. It happens when infrastructure includes proprietary components that aren't built for interoperability. Constant bug fixes and upgrades are often the result, not to mention getting stuck in a costly relationship where divorce is not an option.

Integration complexity. Merging networks is complicated, especially when security solutions are siloed and incapable of sharing intelligence or automating network access control and endpoint remediation. This isn't news to the criminal element, and once a deal goes public, they know exactly whose "work-in-progress" infrastructure is ripe for targeting.

Deployment issues. Too many security solutions are inflexible and may cause incompatibility problems with systems already in place, as well as network performance issues. Lack of scalability is also a common problem, especially when merging infrastructures.

The Forescout Solution

The Forescout platform provides absolute device visibility and automated control to effectively manage cyber, operational and compliance risks while increasing security operations productivity.

Device Visibility: Agentless discovery and classification in real time plus continuous posture assessment equals accurate situational awareness.

- **Discover** every IP-connected physical and virtual device across campus, data center, cloud and industrial environments
- **Classify** diverse IT, IoT and OT/ICS devices in real time
- **Assess** and continuously monitor device compliance without requiring agents or active interrogation

Automated Control: Use accurate situational awareness to automate policy-based controls and orchestrate actions.

- **Conform** with policies, industry mandates and best practices such as network segmentation
- **Restrict**, block or quarantine noncompliant or compromised devices
- **Automate** endpoint, network and third-party control actions

> The fact that we don't need an agent to identify everything on the network makes all the difference in the world. Integrations and the additional functionality that came with our Forescout solution were incredibly important, too. A lot of people around here were saying, 'I can't believe you guys can do all this.
>
> **— CISO, pharmacy benefit management company**

> Due to growth from numerous acquisitions, we needed a solution that would help us manage our devices, integrate our IT teams and meet changing compliance requirements. The Forescout platform and Forescout Professional Services were exactly what we were looking for. We not only gained endpoint visibility, control and compliance, we gained interoperability with our existing security management systems.
>
> **— CISO, leading online travel company**

How Forescout Addresses Key M&A Security Issues

Infrastructure agnostic approach

The Forescout platform works with popular switches, routers, VPNs and firewalls—without infrastructure changes or upgrades. It rapidly integrates with directories, asset management systems, patch management systems, antivirus systems, and ticketing systems. In fact, Forescout eyeExtend products and Base modules provide unprecedented interoperability, integration and multivendor security orchestration capabilities. eyeExtend integration solutions currently support more than 70 third-party solutions,* with more on the way.

Knowing what's on your networks

Before you merge networks and consolidate infrastructure, you need the ability to discover managed and unmanaged devices on both companies' networks. The Forescout platform provides a real-time inventory of what's on your networks—without requiring agents. From day one, you can discover, auto-classify and assess traditional systems, BYOD, IoT, OT and other types of endpoints—even virtual machines and cloud instances—as they access the network. The Forescout platform can share these up-to-the-minute insights with security operations, help desk staff and tools such as ServiceNow®, providing an accurate configuration management database.

Visibility from campus to data center to cloud

The Forescout platform can scale and deploy in the largest and most complex heterogeneous networks—extending security with single-pane manageability of two million devices per deployment. It offers insight into increasingly prevalent devices on enterprise networks, including devices managed by cloud network controllers such as Cisco® Meraki. It can provide cloud-based intelligence to auto-classify new devices as well as real-time and continuous visibility into Microsoft® Azure, Amazon® Web Services (AWS) and VMware® deployments. Integration with Cisco ACI also provides visibility into SDN environments for data centers.

Rapid deployment and phased integration

The Forescout platform supports both 802.1X and non-802.1X implementations as well as hybrid mode. This flexibility helps speed deployment and accelerate time to value. Forescout gives you the flexibility to determine if, when and how networks will merge and devices connect. You may choose to standardize on a single antivirus solution during a compliance period to ensure that all endpoints are patched and running up-to-date operating systems. The same is true for advanced threat protection tools. The Forescout platform and eyeExtend products allow for a rapid integration and standardization of security management systems and tools, with the ability to monitor the environment over time prior to allowing new devices onto your network.

Granular access controls

Not all companies opt for bilateral access polices as employees from one company begin accessing the network resources of the other. Forescout lets you define and enforce granular access policies, monitor user and device behavior and modify policies over time. For example, companies may have different criteria for BYOD, guest or contractor access. Strategic contractors may require elevated access privileges whereas others may be limited to specific network segments. Forescout allows you match the proper access controls to the specific people, devices, applications and business situations.

Enterprise-wide segmentation

M&A activity presents an excellent opportunity to re-evaluate network segmentation. Segmentation is a cost-effective way to reduce the attack surface of converging networks and prove regulatory compliance. It's also an effective way to protect assets that can't load agents. The Forescout platform helps you agentlessly visualize asset dependencies and flow data to refine segmentation policies. It can dynamically assign assets to network segments based on business policies, real-time device context and compliance status.

The Forescout platform lets you restrict the access of a noncompliant device, limit access to internet-only, quarantine devices within a secure VLAN, or grant access to appropriate corporate VLAN segments. Equally important, Forescout lets you automate segmentation controls across all infrastructures, including switches, next-generation firewalls (Palo Alto Networks®, Check Point® and Fortinet®), SDN networks (Cisco DNA-C/Trustsec, VMware NSX), cloud (Azure), and hypervisors (VMware)—without requiring upgrades to maximize your M&A investments.

Consulting services

Forescout Consulting Services is available to assist in the design, installation and configuration of your network security infrastructure. Our consultants offer industry-specific expertise and are well-versed in the issues surrounding mergers and acquisitions.

* As of December 31, 2018

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

© 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 04_19