FORESCOUT

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 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 non-compliant devices from spreading malware across the network
- Integrate disparate security solutions into a unified, enterprise-wide system

Mergers and Acquisitions

Minimize cybersecurity risks while enabling rapid change

Any merger or acquisition poses daunting challenges to IT leaders. Not only are they tasked with integrating people, processes and technology in the shortest possible time frame, they must also remain vigilant about addressing the added cybersecurity risks. ForeScout offers solutions and expertise to help safeguard your business-critical networks, build interoperability into your security systems and help demonstrate regulatory compliance.

The Challenge

Consolidation is now the norm in many industries. It's not a question of if mergers and acquisitions will occur, but when. In these highly competitive businesses, information technology is considered a strategic differentiator that yields competitive advantage. As such, technology diversity is commonplace. Here are some of the top challenges created by merger and acquisition (M&A) activity:

Endpoint Invisibility. Large numbers of endpoints go undetected on most networks for a lot of reasons. 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?

Vendor Lock-in. It's what happens when infrastructure is built using proprietary components that don't embrace interoperability. Constant bug fixes and upgrades are often the result, not to mention getting stuck in a relationship where divorce is not an option.

Integration Complexity. Once a deal goes public, the criminal element knows exactly whose "work-in-progress" infrastructure is ripe for targeting.

Infrastructure integrations take time and M&A restructuring expectations can be unrealistic, especially when you consider that most security solutions are siloed and incapable of sharing intelligence or automating network access control and endpoint remediation.

Deployment Issues. Too many security solutions are inflexible when it comes to implementation 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 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**

The ForeScout Solution

ForeScout serves as the common thread that binds security infrastructure together and unifies security management. ForeScout can mitigate M&A-related IT infrastructure issues in three distinct ways:

See The ForeScout platform offers the unique ability to see unmanaged devices—BYOD, guest, IoT, OT and rogue—the instant they connect to your network, without requiring software agents or previous device knowledge. In addition to discovering endpoints using agentless visibility, this visibility and control platform helps you quickly classify and assess their security postures, and continually monitors the devices as they drop on and off the network.

Control Once you understand each device on your network, its owner and purpose, the ForeScout platform enables a broad range of network access controls. You can restrict access to a non-compliant device, block Internet access, quarantine any device based upon anomalous behavior and/or notify its owner of a security concern. In addition, should you choose to isolate specific devices to a specific network segment or virtual local area network (VLAN), our platform simplifies this process.

Orchestrate ForeScout's ability to tear down security management silos through multivendor orchestration dramatically enhances network security. Orchestration begins with the ForeScout platform's broad interoperability with network infrastructure, third-party security and management systems and our commitment to share security insights with them. We extend the platform's agentless visibility and control capabilities to leading solutions for advanced threat defense, enterprise mobility management, vulnerability assessment, security information and event management and endpoint protection via a growing number of ForeScout Extended Modules.

How ForeScout Addresses Key M&A Security Issues

Open interoperability

The ForeScout platform works with popular switches, routers, VPNs, firewalls, endpoint operating systems (Windows®, Linux®, iOS®, OS X® and Android®), patch management systems, antivirus systems, directories and ticketing systems—without infrastructure changes or upgrades. ForeScout Base and Extended Modules provide unprecedented interoperability, integration and multivendor security orchestration capabilities. Modules currently support more than 70 third-party solutions,* with more on the way.

Knowing what's onyour 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 network—without requiring agents. From day one, you can discover, 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.

> Due to growth from numerous acquisitions in 2015, we needed a solution that would help us manage our devices, integrate our IT teams and meet changing compliance requirements. ForeScout CounterACT 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**

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. It offers insight into some of the fastest-growing devices on enterprise networks, including IPv6-addressable systems and 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 and control of Amazon Web Services (AWS) deployments. It can even allow, deny or segment virtual machines and cloud instances based on policy compliance.

Phased integration

ForeScout gives you the flexibility to determine if, when and how networks will be merged. For example, you may choose to migrate endpoints to the same antivirus vendor during a compliance period and ensure that all endpoints are patched and running up-to-date operating systems. The same is true for advanced threat protection tools. ForeScout Extended Modules 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 endpoints onto your network.

Granular access controls

Not all companies opt for fully merged networks with bilateral access polices as employees from one company begin accessing the network resources of the other. ForeScout allows you to define and enforce granular access policies, monitor user and device behavior and modify policies over time as needs and priorities change. For example, companies often may have different criteria for BYOD, guest or contractor access. In some companies, 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.

Flexible deployment, scalability and centralized management and control

The ForeScout platform offers proven scalability to two million endpoints. It can be deployed as physical or virtual management appliances that support both 802.1X and non-802.1X implementations or in hybrid mode, which speeds network access control deployment in large, diverse environments. Unlike solutions that limit you to a single switch vendor, ForeScout supports multiple switch architectures concurrently.

Dynamic network segmentation

The ForeScout platform provides real-time dynamic segmentation based on its rich visibility assessment insights. This allows you to restrict access to a non-compliant device, limit access to Internet-only, quarantine devices within a secure VLAN or grant access to appropriate corporate VLAN segments. IT staff can easily define policies within the ForeScout platform to control network access based on device types, user profiles, applications

or numerous role-based characteristics shared via Active Directory or a Lightweight Directory Access Protocol (LDAP)-based directory service.

Consulting services

ForeScout Consulting Services is available to assist in your 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. They are thoroughly trained, experienced and certified in product implementation, process and schedule integration, as well as network access and endpoint compliance best practices.

Learn More

ForeScout offers many ways to gain greater insight into the ForeScout device visibility and control platform, including:

- **Take a Test Drive:** Experience the before-and-after difference of the ForeScout platform with a hands-on test drive that takes you through five powerful use cases.
- **Request a Demo:** Visit the ForeScout demo page to request a personal demo and access a full complement of on-demand demos and video options.
- **Use the ForeScout Business Value ROI Tool:** Quantify the business value the ForeScout platform can provide to your organization (as calculated by IDC's Business Value Model) in just 10 minutes.

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

* as of March 31, 2018