



### Business Challenges

- Protect sensitive systems and data during transition
- Rapidly secure new network segments
- Securely embrace BYOD, IoT 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
- Ensure security software is up to date on devices
- Scale to address rapid growth and distributed networks
- Assess and 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

## Minimizing the Cybersecurity Risk Factor



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 because they are unmanaged, Bring Your Own Device (BYOD), Internet of Things (IoT), guest and rogue devices 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** ForeScout CounterACT® offers the unique ability to see unmanaged devices—BYOD, guest, IoT 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, CounterACT 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, CounterACT 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), CounterACT simplifies this process.



**Orchestrate** ForeScout's ability to tear down security management silos through multivendor orchestration dramatically enhances network security. Orchestration begins with CounterACT's broad interoperability with third-party network and management systems and ForeScout's commitment to share security insights with them. We extend CounterACT'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

CounterACT 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 leverage the capabilities of ForeScout ControlFabric® Architecture to provide CounterACT with 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 on Your Networks

Before you merge networks and consolidate infrastructure, you will need the ability to discover managed and unmanaged devices on both companies' networks. CounterACT gives you advanced device discovery capabilities from day one, letting you classify and assess BYOD, IoT and other types of endpoints as they access the network. In addition, it continuously monitors the network so that endpoints can be detected and controlled even if they are only intermittently on the network.

### 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



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

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.

### Custom Integration

Custom integrations of security and management systems with CounterACT can be accomplished via the ForeScout Open Integration Module. This module works with ForeScout ControlFabric Architecture to markedly accelerate integrations.

### Granular Access Controls

Not all companies opt for fully merged networks with bilateral access policies 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 whereby 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

Both CounterACT and ForeScout CounterACT Enterprise Manager (the centralized console that lets you manage distributed CounterACT appliances) offer proven scalability to one million endpoints. They can be deployed as physical or virtual management appliances that support both 802.1X and non-802.1X implementations. In addition, CounterACT’s 802.1X and non-802.1X hybrid mode lets you use multiple technologies concurrently, which speeds network access control deployment in large, diverse environments. Unlike solutions that limit you to a single switch vendor, ForeScout allows you to support multiple switch architectures concurrently.

### Consulting Services

ForeScout Consulting Services is available to assist in your deployment, including 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.

### The ForeScout Solution

Let us know which ForeScout solution is right for you, and we’ll arrange a free on-site evaluation.

**Learn more at [www.forescout.com](http://www.forescout.com).**

Learn more at  
[www.ForeScout.com](http://www.ForeScout.com)



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  
**Fax** 1-408-371-2284

\* as of January 2016

Copyright © 2016. All rights reserved. ForeScout Technologies, Inc. is a privately held Delaware corporation. ForeScout, the ForeScout logo, ControlFabric, CounterACT Edge, ActiveResponse and CounterACT are trademarks or registered trademarks of ForeScout. Other names mentioned may be trademarks of their respective owners.

**Version 6\_16**