ForeScout

# Protecting the Connection Lifecycle

## Extending visibility, control and orchestration beyond cybersecurity environments

In theory, cybersecurity, IT security and IT systems management are highly symbiotic services that can benefit greatly from shared tools, insights and resources. In practice, however, this is rarely the case. Most enterprises use specialized point products and redundant processes to manage functional tasks. All of which raises an important question: Why?

### Protecting the Connection Lifecycle: Why We Do It

According to a research report from Hewlett-Packard, roughly 48 percent of recorded cyberattacks in 2015 were from known vulnerabilities that were five or more years old[1]. In 2016, AT&T's *Cybersecurities Insights* report stated that 90 percent of their reported cyberattacks were also from known vulnerabilities[2]. Both indicate that existing defense-in-depth cybersecurity methods are not performing efficiently and effectively by themselves. HP's report is significant, as it indicates vulnerabilities can lie dormant for years on a network without an organization knowing. Further digging into these metrics illustrates two common threads into how attackers consistently break through defenses. The first results from a combination of incomplete asset visibility and situational awareness. Simply put, you cannot protect or manage what you cannot see on your network. The second reason is many organizations' solutions operate in silos and do not adequately protect an endpoint's connection lifecycle.

All endpoints have connection lifecycles. ForeScout defines an endpoint's connection lifecycle as the initiation and granting of access onto the network, performing or consuming some level of work or services, and disconnection from the network. Endpoint examples include servers, laptops and mobile devices as well as Internet of Things (IoT) devices such as smart printers, Voice over Internet Protocol (VoIP) phones, climate control systems, networked machine tools and sensors. Each of these have varying connection duration, risk posture and mission criticality. At ForeScout, it's considered a given that access control is not a point-in-time transaction. Rather, access control is fluid, perpetual and sometimes random. As a result, effective security requires constant and complete monitoring and protection of the endpoint connection lifecycle.

Imagine two night clubs: A and B. Club A is managed by a security team with a bouncer at the entrance and his teammates inside. They all wear headphones to share information regarding clubgoers so they can react quickly to any incidents. The bouncer at the door makes sure only invited guests attend. Additionally, he checks their bags, takes notes and shares data with his team regarding any potential troublemakers. The security team in Nightclub B, however, attempts to shout at one another to communicate instead of using headsets. When Club B is busy, communication is difficult and security can become compromised. Another challenge with Club B is that it has two doors: one managed by their bouncer similar to Club A, and another with a list of names for people to self-verify. These patrons bypass the bouncer, and the Club B team has no idea how risky those patrons could be.

It's fair to assume that the team in Club B will have a significantly tougher time keeping the peace than their counterparts in Club A. Unfortunately, the Club B security set-up functions a lot like traditional defense-in-depth and systems-management solutions. Critical technologies, or "team members," do not communicate well with others. Also, like Club B, cybersecurity solutions that knowingly or otherwise allow endpoints to bypass security controls can leave themselves open to a great deal of risk.

ForeScout estimates that an average of 35 percent of devices are not detected or managed to customer expectations within organizations. This population of endpoints represents a potential beachhead for an attacker to exploit and is emblematic of our nightclub example, where Team B can't provide complete protection and management of its patrons given the team's limited communications and situational awareness. When a large percentage of patrons are never verified, the potential risk they pose to the club and other clubgoers can't be assessed. The same holds true for organizations that are not able to see and assess endpoints across the entire connection lifecycle.

The Club B analogy reflects the struggle existing solutions go through as they fail to measure up when it comes to meeting the needs of traditional computing devices throughout their connection lifecycle. And if that wasn't scary enough, the IoT juggernaut is making traditional access control and compliance management solutions struggle even harder. According to Gartner, this explosive technological trend will move the total number of connected devices to 30 billion or more by 2020, 20 billion of which will be IoT devices.

As we enter this incredibly disruptive new era, we must look at new ways of protecting and managing our endpoints throughout their entire connection lifecycle. ForeScout is a good place to start.

## How We Do It

Organizations require pre-connect and post-connect protection. ForeScout CounterACT® delivers this by authenticating both the user and the endpoint, then continuously assessing the compliance of the endpoint to help ensure the device is not posing risks to the environment. This continuous visibility improves situational awareness into an organization's endpoints without requiring agents. The ForeScout platform can also share information among third-party solutions, improving their visibility and scope of coverage. And it helps automate simple, repeatable tasks—increasing operational efficiency and capacity through task and process workflow automation.

As the diagram illustrates, CounterACT applies both pre-connect and post-connect support, helping to ensure endpoint protection throughout the connection lifecycle. It can help ensure that printers, VoIP phones, HVAC (heating, ventilation, and air conditioning) systems and other IoT devices are not making illegal network calls that may potentially trigger botnet attacks. CounterACT also improves the cyber hygiene of your environment by helping to ensure that third-party agents and patches are up to date, and that endpoints are compliant, accounted for and operational. Additionally, the ForeScout platform can share its wealth of information for long-term storage and use in configuration and asset management systems. CounterACT's data collection speed and accuracy is helping thousands of organizations with the clarity and accuracy required to protect and manage today's network services and resources.

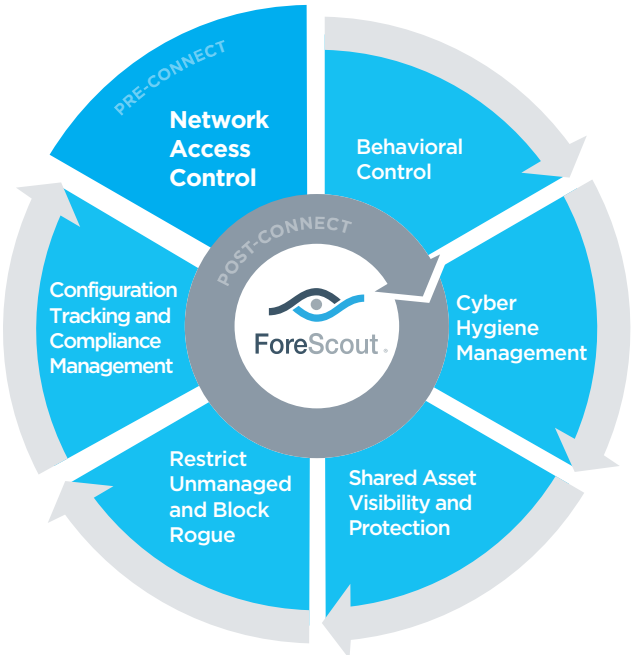


**Figure 1:** Continuous connection lifecycle protection.

## ForeScout SEE - Asset Visibility and Situational Awareness

Several challenges span IT security and asset management. First, you can't protect what you can't see. You cannot manage IT assets very well, or accurately amortize their value, while they are in production which, coincidentally, is when endpoints are exposed to their greatest risk. That's why most organizations have cyber defense systems to protect the various aspects of an endpoint's connection lifecycle.

Common examples include:

- Patch Management
- Incident and Event Monitoring
- Ongoing Cyber and Systems Management Hygiene (patches, updates and agents, etc.)
- Configuration/Asset Management
- Network Access Control/Compliance Management
- Network and Host-Based Security Solutions
- Behavioral Control/Advanced Persistent Threats

CounterACT can share the endpoint data with third-party solutions, helping to fill contextual gaps in coverage that exist with traditional solutions. This is accomplished through our more than 70 ForeScout Base and Extended Modules*. Consider ForeScout CounterACT as a flashlight illuminating the "dark places" in your network and feeding contextual endpoint data to other key security solutions—accelerating multivendor response and improving system-wide effectiveness. This results in better IT security and management services across your organization while automating active asset tracking and compliance activities.

## ForeScout CONTROL & ORCHESTRATE – Task and Process Workflow Automation

Through policy execution, ForeScout allows organizations to automate simple, repeatable security and systems management tasks. This allows higher-tiered engineers to move their repeatable tasks over to the ForeScout platform and have lower-tiered staff deliver the support. It's a key way organizations leverage ForeScout to improve the capacity of their operations and engineering staff.

CounterACT's policy-driven automation and control capabilities are key elements in moving from reactive to proactive IT security and operations. Other solutions such as Security Information and Event Management, Advanced Threat Protection, Configuration Management Databases, and Information Technology Access Management tend to be poorly suited to automate tasks (and thus require tasks to be performed manually). Each of these solutions traditionally has a very specific set of functions, which often conflict with and overlap other solutions in production. But with CounterACT, simple, repeatable tasks can be executed automatically. One example is adjusting the configuration on an endpoint to bring it back into compliance. The ForeScout platform can act as a second pair of hands on behalf of your monitoring tools for a quicker and more effective response.

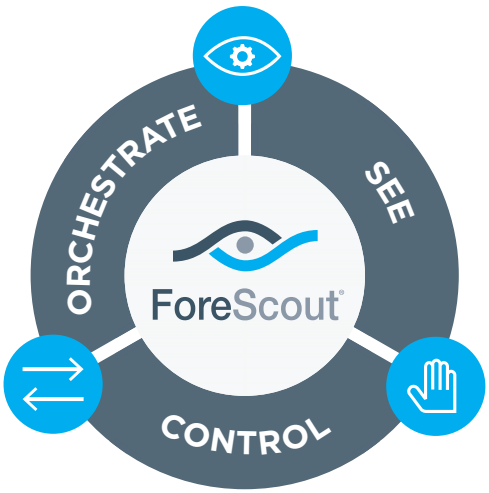


**Figure 2:** ForeScout's unique ability to see devices as they connect to the network, control them and orchestrate information sharing and response among disparate security tools can be extended across the connection lifecycle.

Through orchestration, ForeScout delivers effective dataflow exchange to third-party solutions, and to managed environments. The ForeScout platform drives process workflow automation by integrating two or more products in a safe, policy-controlled manner. This allows organizations to combine automated tasks into closed-loop processes, driving operational costs down while improving the overall efficiency and effectiveness of their IT security and systems management.

## Bringing It All Together

ForeScout's approach to network access control and compliance management provides a comprehensive security and management platform to empower your IT security and managed services. ForeScout starts by delivering visibility to understand what is on the network. This establishes an accurate asset baseline and allows organizations to prioritize levels and types of protection based on their business case. From there, the ForeScout platform shares that information with third-party tools through ForeScout Modules and allows extensive application customization, including orchestration with home-grown applications, through our Open Integration Module. This improves customers' scope of coverage and ability to maintain their appropriate level of protection across the organization. Once visibility and situational awareness have been restored, ForeScout CounterACT can then work to provide post-connection protection to all identified assets in efforts to eliminate the largest exposure of risk to the organization. Finally, the ForeScout platform delivers pre-connect support for an organization's environment that is capable of and appropriate for support. This approach reduces costs and project false starts due to poor asset intelligence while enhancing protection across the organization and mitigating risk of failure.

For more information, visit www.forescout.com and ask for a free demonstration.

Learn more at
**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

[1] HPE Security Research, Cyber Risk Report 2016

[2] AT&T Cybersecurity Insights: The CEO's Guide to Data Security, http://about.att.com/story/att_announces_cybersecurity_insights_report.html

*As of December 31, 2016