ESG

Enterprise Strategy Group | **Getting to the bigger truth.™**

SOLUTION SHOWCASE

Case Study: ForeScout CounterACT

Date: October 2015 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: As part of its ongoing coverage of the network security market, ESG interviewed a senior security manager working at a large global financial services company with over 100,000 employees. This organization is a ForeScout customer and is well into a global implementation of the company's CounterACT platform.

The origins of the project described in this paper go back as far as 2008. At that time, the organization was interested in enforcing network access control policies. More specifically, the initial goal was to deny network access to rogue devices and move vulnerable endpoints to a quarantine VLAN for remediation. Unfortunately, the security team determined that deploying a NAC solution created numerous interoperability challenges as it couldn't find a product that worked using the 802.1X protocol in a large multi-vendor environment.

> "When we realized how inflexible 802.1X was and how much extra work was required, we knew we had to rethink the whole project." – Information Security Manager

Network Security Project Redux

In 2013, the project was resurrected with its new focus on continuous monitoring of all users and devices requesting access to the network. More specifically, the organization wanted to implement a solution that could identify rogue, unknown, out-of-compliance, or malicious wired and wireless devices and also have the tools to correlate devices to specific users (i.e., employees, guests, contractors, etc.).

The ForeScout Decision

After testing and eliminating multiple solutions, the security team decided to move forward with ForeScout CounterACT because:

- CounterACT is a vendor-agnostic network security solution designed for integration with most popular networking and security technologies.
- ForeScout CounterACT provides endpoint visibility immediately, even if no agents are installed by employing 802.1X and alternate authentication mechanisms.

ForeScout CounterACT's capabilities to enforce policy use various methods, and are based on endpoint and user profiles. This can enable continuous monitoring and response for security and compliance.

> "We really had to weigh the cost versus the benefit after our earlier NAC experience. The 'eureka' moment was when we decided to start our project with continuous monitoring. This simple decision was really the key to getting tremendous value in a relatively short timeframe." – Information Security Manager

2013: The Project Rollout Begins

The logistics of installing equipment in a wide range of network environments spanning the globe presented numerous challenges in terms of coordinating local teams for physical installation of equipment and addressing all local compliance and governance requirements.

CounterACT identified and assessed each device against corporate security policies, device classification, and inspection techniques.

By the end of 2013, the program went into production in North America and Europe, providing visibility into more than 493,000 endpoints. Since then, the organization has increased its scope with visibility into over 900k devices worldwide. As this phase concluded, the organization was able to:

1. Centrally manage multiple CounterACT appliances.
2. Discover, classify, and assess all devices on the network.
3. Provide endpoint profiling data for cybersecurity investigations.
4. Use ForeScout data to start enforcing network access policies.

Phase 2: Integration

With the endpoint visibility phase completed, the organization moved on to integrating CounterACT endpoint discovery and profiling data with other systems that make up its security infrastructure in order to use the ForeScout ControlFabric with other network and security systems and create more actionable security intelligence. To accomplish this, the security team integrated CounterACT with McAfee (Intel Security) ePO, HP ArcSight (SIEM), and Microsoft Active Directory. The organization plans to integrate CounterACT with additional security tools over time.

Phase 3 Plan: Automation

Once CounterACT data is tightly integrated into other security management tools, the security team plans to add value to the organization's security processes by:

- **Coordinating with advanced threat defenses**. CounterACT can share endpoint profiling data with the advanced malware analysis to accelerate incident detection and response processes.
- **Blocking "kill chain" tactics emanating from compromised systems.** ForeScout network access controls may prevent access to specific network segments or applications containing sensitive data. If a device attempts to conduct network reconnaissance or use ports outside normal use, ForeScout can alert IT or take action.
- **Taking remediation actions to limit the scope of an attack.** When an attack is discovered, ForeScout can coordinate with ATD systems to isolate a breached endpoint, receive indications of compromise (IOC) data from the ATD system, and scan for that IOC when a system requests access to network resources—both pre- and post-network admission.

> "ForeScout integration helps us highlight the issues detected by other security systems. This is especially important for incident detection and response."
> – Information Security Manager

When an actual cyber-attack is identified, the organization plans to use ForeScout further to:

- **Investigate and fix vulnerable endpoints.** Information from the CounterACT and VA data can be shared to discover and take action on vulnerable or compromised systems. This reduces transient device and poll-based vulnerability scanning risks. In addition, VA data can trigger ForeScout to take network enforcement and endpoint remediation actions such as activating a host control.
- **Remediate compromised systems.** As part of this interoperability, ForeScout can participate in the process to automate fixes in a timely manner. CounterACT can identify a missing patch and trigger the endpoint to request an update from Microsoft System Security Manager (SCCM).
- **Fine-tune access policies and security controls.** ForeScout will further interoperate with networking and security equipment to segment application/network traffic, create firewall rules, or trigger other controls.