ForeScout

ForeScout ControlFabric™ Architecture

IMPROVE MULTI-VENDOR SOLUTION EFFECTIVENESS, RESPONSE AND WORKFLOW AUTOMATION THROUGH COLLABORATION WITH INDUSTRY-LEADING TECHNOLOGY PARTNERS.

The Challenge

Why are the bad guys still penetrating heavily defended networks? In large part it's because traditional IT security architectures are not built to handle today's threat landscape and IT environment. They suffer from four weaknesses:

"50% of respondents surveyed indicated they own 13 or more security systems, yet only one in three systems share information with each other and automatically mitigate risk."

—SC Magazine/ForeScout Research, September 2015

1. IT security systems operate independently, creating security management silos

If your IT security organization is like most others, you've probably purchased a variety of security and management systems. You likely have antivirus, encryption, intrusion prevention, vulnerability assessment, firewalls, data leak prevention, security information and event management (SIEM), and mobile device management (MDM). Each of these systems serves a valuable function, but each typically operates as an independent silo. This robs you of critical synergies such as the ability to share contextual information and automate security management workflows. Without information sharing, you can't optimize the effectiveness of your IT security investments.

2. Security alerts aren't the same as enforcement

Many IT security systems issue alerts, but they can't take immediate action to mitigate a risk or control a breach. This burdens your IT staff who have to manually sift through the alerts and follow up on them, and it gives hackers more time to compromise your systems. Vulnerability assessment, advanced threat detection and SIEM systems commonly suffer from this weakness. Manual intervention simply cannot address today's relentless pace of cyberattacks.

3. Too many IT security processes are periodic, not continuous

Many network access control systems examine the security posture of an endpoint at the time of admission, then ignore the endpoint after it's on the network. Vulnerability assessment systems are typically configured to scan networks on a periodic basis, such as monthly or quarterly, so they fail to scan many transient devices. And patching processes are typically done on a periodic basis (often monthly), not continuously.

4. Security agents only work when they are installed and up to date

Agents serve a valuable function, but their scope is limited to known devices, such as corporate-owned computers. Increasingly, enterprise networks contain devices that are not corporate-owned, as employees and contractors bring their own devices (BYOD), or endpoints that can't accommodate management agents, such as industrial equipment or non-traditional Internet of Things (IoT) endpoints. Also, agents often fail or become misconfigured. These situations create security blind spots, leaving networks vulnerable to cyberattack.

The Solution

ForeScout ControlFabric™ Architecture extends the capabilities of ForeScout CounterACT™ to a wide variety of enterprise security and management systems, allowing the combined solution to exchange information and efficiently mitigate a wide variety of network, security and operational issues. As a result, you can squeeze higher utility from your existing security investments, efficiently preempt and contain exposures and enhance your overall security posture.

ControlFabric allows CounterACT to share security insights regarding network devices and vulnerabilities that were previously unknown to you, including BYOD endpoints, corporate-owned devices with broken management agents, servers, routers and access points and even IoT endpoints and rogue devices.

ControlFabric Integration Modules

The ControlFabric partner ecosystem includes popular network, security, IT management and mobile infrastructure vendors who have teamed with ForeScout to develop ControlFabric Extended Integrations. These integrations are available as separately licensed software modules that can be added to the CounterACT appliance. Current integration modules include:

Advanced Threat Detection (ATD)

Gain continuous monitoring and mitigation of sophisticated enterprise threats

ForeScout CounterACT integrates with your ATD system to detect indicators of compromise (IOCs) on your network and quarantine infected devices, thereby rooting out the sources of cyberattacks and limiting malware propagation. Here's how:

1. The ATD system detects malware and suspects that a device within your network has been compromised. It informs CounterACT about the affected system(s) and IOCs.
2. Based on your policy, CounterACT leverages its IOC repository to scan other endpoints that are attempting to connect or are already connected to your network for presence of infection.
3. CounterACT automatically takes policy-based mitigation actions to contain and respond to the threat. Various actions can be performed depending on the severity or priority of the threat.

Vulnerability Assessment (VA)

Improve vulnerability assessment and response across your enterprise

ForeScout's VA Integration Module provides comprehensive vulnerability assessment data to see devices and trigger VA scans the instant devices join your network. Here's how:

1. CounterACT triggers the VA system to perform a real-time scan of the connecting device when it joins the network.
2. CounterACT isolates the connecting device in an inspection VLAN while the VA system performs a scan.
3. CounterACT triggers VA scans on devices that meet certain policy conditions, such as endpoints with specific applications, or when endpoint configuration changes are detected.
4. After the VA system scans a device, CounterACT can obtain the scan results and initiate risk mitigation actions if vulnerabilities are detected.

Making Disjointed Security Products Work As One

The intelligence and functionality of CounterACT and ControlFabric Architecture can be summed up in three words: See, Control and Orchestrate.

See

- Discover devices the instant they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor managed devices, BYOD and IoT endpoints

Control

- Allow, deny or limit network access based on device posture and security policies
- Assess and remediate malicious or high-risk endpoints
- Improve compliance with industry mandates and regulations

Orchestrate

- Share contextual insight with IT security and management systems
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

ControlFabric Architecture extends the advanced visibility, control and remediation capabilities of ForeScout CounterACT to a wide variety of enterprise security products and management systems.

"ForeScout ControlFabric represents a flexible approach to gain the context and policies necessary to advance endpoint compliance, continuous monitoring and security analytics."

—Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group

Mobile Device Management (MDM)

Improve mobile security and unify mobile compliance management

ForeScout CounterACT works with leading MDM systems and our MDM Integration Module to provide unified security policy management for devices on your network. Here's how:

1. CounterAct instantly profiles managed and agentless (unmanaged) mobile devices connected to the enterprise network.
2. CounterACT provides comprehensive information about each device to MDM systems.
3. CounterACT enforces network security policies, monitors and reports on policy compliance and sees network information such as where and how each device is connected to your network.

Security Information and Event Management (SIEM)

Turn situational awareness into action

This module improves situational awareness and mitigates risks using advanced analytics. Here's how:

1. CounterACT discovers infected endpoints then receives instructions from the SIEM and automatically takes policy-based mitigation actions to contain and respond to the threat.
2. Various actions can be performed depending on the severity or priority of the threat, such as:
   - o Quarantine endpoints
   - o Initiate direct remediation
   - o Share real-time context with other incident response systems
   - o Initiate a scan by another third-party product
   - o Notify the end user via email or SMS

Intel® Security Integration

Automate threat response on managed and unmanaged devices

This module provides deep bi-directional integration between CounterACT, McAfee® ePolicy Orchestrator® (ePO™) and McAfee® Threat Intelligence Exchange (TIE), leveraging the best-of-breed capabilities of each product. Here's how CounterACT and McAfee TIE integration works:

1. CounterACT scans the system to identify all running processes and communicates this information to McAfee TIE via the McAfee Data Exchange Layer.
2. McAfee TIE responds with a threat score for each process.
3. Based on this information, CounterACT can either allow devices onto the network or terminate a process, remediate the endpoint or isolate the device until remediation is performed.

4. When McAfee TIE receives information about new malware, it broadcasts this information over the McAfee Data Exchange Layer to CounterACT. Once CounterACT receives this threat alert, it scans unmanaged Windows® devices on the network to see if they contain the malicious file or process.
5. Based upon your security policies, CounterACT can perform a wide range of control actions, including endpoint isolation, killing a malicious process or initiating other remediation actions and alerting the user.

Splunk® Integration

The joint ForeScout-Splunk solution allows CounterACT to automate security controls based on the attributes of the device, the user and data received from Splunk Enterprise. Here's how:

1. Splunk Enterprise determines that a set of endpoints has a material security issue.
2. CounterACT can automatically quarantine the endpoints and/or initiate remediation.
3. CounterACT actions can be defined based on the exact problem that Splunk identifies. As a result, Splunk Enterprise can leverage CounterACT to remediate endpoint security issues, isolate breached systems or trigger other policy-based controls.

Custom Integrations Using the ForeScout Open Integration Module

ForeScout's open ControlFabric Interface allows you or third parties to easily implement new integrations based on common, standards-based protocols. The ControlFabric Interface can be enabled on the CounterACT appliance by purchasing the Open Integration Module. This module supports the following open, standards-based integration mechanisms:

- **Web Services API** for sending and receiving XML messages
- **SQL**, allowing reading from and writing to databases, such as Oracle®, MySQL, and SQL Server
- **LDAP**, enabling reading from standard directories

CounterACT also natively supports the syslog interface, which can be used to send and receive information to a designated server. This interface is used for a variety of integrations with products that aggregate logs and enable log analysis, such as SIEM systems.

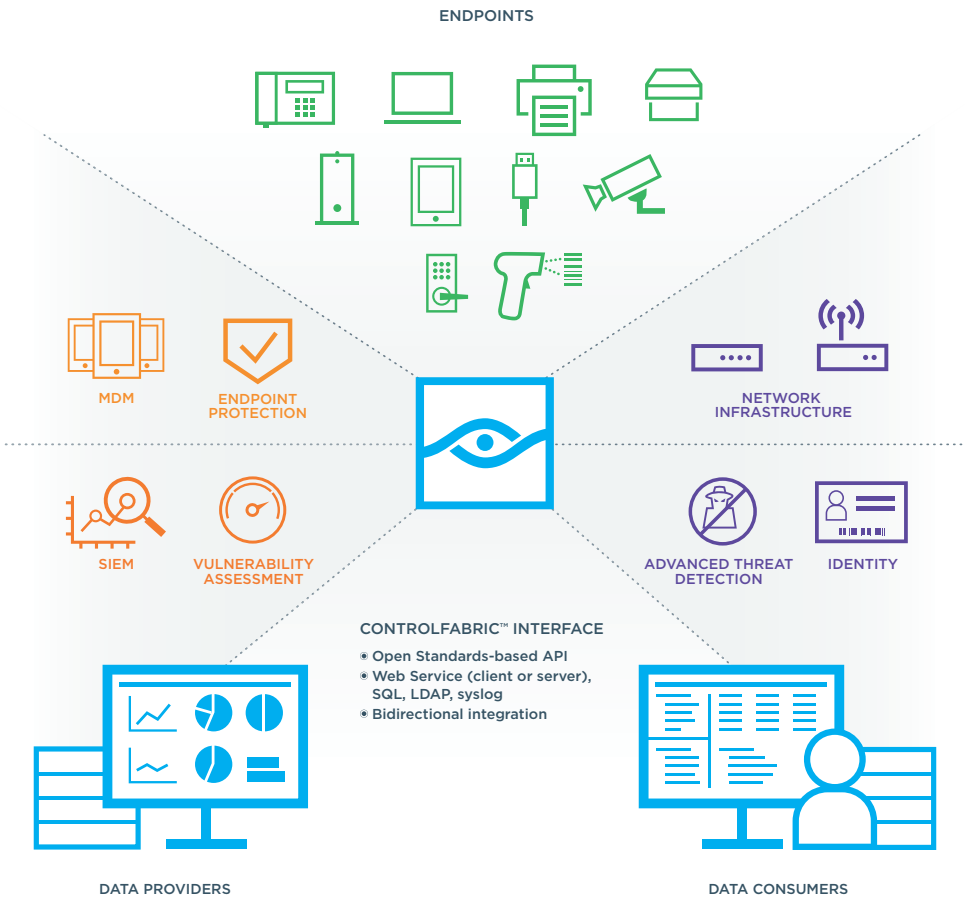

Figure 1: ControlFabric Ecosystem
ControlFabric Architecture lets CounterACT share contextual insights and automate workflows with your SIEM, MDM, ATD, VA, Intel Security solutions and more over your existing network infrastructure to improve and unify system-wide security. ForeScout currently integrates with more than 70 network, security, mobility and IT management products,* with additional integrations underway.

ForeScout ControlFabric Architecture currently integrates ForeScout CounterACT with more than 70 network, security, mobility and IT management products,* with additional integrations underway.

About ForeScout

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. More than 2,000 customers in over 60 countries* improve their network security and compliance posture with ForeScout solutions.

Put the Power of ControlFabric to Work for You

ForeScout ControlFabric offers a solution for everyone in the security value chain. Whether you are a technology vendor looking to leverage the capabilities of ForeScout CounterACT, an integrator seeking to automate system-wide security or an enterprise customer who needs to improve security effectiveness and maximize the return on investment of your existing security products, you owe it to yourself to check out ControlFabric. **Learn more at www.forescout.com/controlfabric today.**

To request a demo, visit www.forescout.com/request-demo.

ForeScout™

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 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 October 2015