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

The 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.

ForeScout Base and Extended Modules leverage the capabilities of the ForeScout ControlFabric™ Architecture to provide ForeScout CounterACT™ with unprecedented interoperability, integration and multivendor security orchestration capabilities.

Base Modules are included with ForeScout CounterACT to provide open integration with a broad range of network and security infrastructure.

Extended Modules are co-developed by ForeScout and ForeScout Technology Partners to orchestrate information sharing and policy-based security enforcement operations between CounterACT and leading IT and security management products. These separately licensed software modules are available for a free, 30-day, evaluation.

Advanced Threat Defense (ATD)

Our ATD modules provide true security orchestration between CounterACT and your ATD system. The combined solution can automatically detect indicators of compromise (IOCs) on your network and quarantine infected devices, thereby limiting malware propagation and breaking the cyber kill chain.

How they work:

1. The ATD system detects malware then 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)

Our VA modules share comprehensive vulnerability assessment data between CounterACT and leading VA systems to initiate VA scanning of devices and automate policy-based enforcement actions as necessary.

How they work:

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 the 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

The 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**

Enterprise Mobility Management (EMM)

Our EMM modules facilitate policy-based orchestration between CounterACT and leading EMM systems to provide unified security policy management for mobile devices on your network.

How they work:

1. CounterACT instantly profiles managed and agentless mobile devices connected to the enterprise network.
2. CounterACT provides comprehensive information about devices to EMM systems.
3. When CounterACT discovers a device without a functional EMM agent, CounterACT redirects it to the EMM app store for installation according to policy.
4. CounterACT enforces network security policies, monitors and reports on policy compliance and sees network information such as where and how devices connect to your network.

Security Information and Event Management (SIEM)

Our SIEM modules facilitate information sharing and policy management between CounterACT and leading SIEM systems to improve situational awareness and mitigate risks using advanced analytics.

How they work:

1. CounterACT discovers infected endpoints then sends the information to the SIEM.
2. CounterACT receives instructions from the SIEM and automatically takes policy-based mitigation actions to contain and respond to the threat.
3. 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

Endpoint Protection Platform (EPP)

Our EPP modules provide bi-directional integration between CounterACT and leading endpoint protection platforms to facilitate compliance with antivirus, patch management, encryption and other endpoint management policies.

How they work:

1. CounterACT detects and profiles endpoint systems as they connect to the network and shares this information with the EPP.
2. If the system's endpoint agent is working, the EPP tells CounterACT what it knows about the device's compliance status.
3. CounterACT allows access to compliant devices and authorized users.

4. If the device has a missing/broken agent, CounterACT informs the EPP to install/repair the agent. CounterACT can also capture the endpoint's browser and send the user to a self-remediation page. CounterACT continues to monitor systems for compliance and threatening behavior.
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.

Open Integration Module

Custom integrations can be developed via the Open Integration Module, which allows customers, systems integrators and technology vendors to integrate security and management systems with CounterACT. This module supports the following open, standards-based integration mechanisms:

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

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.

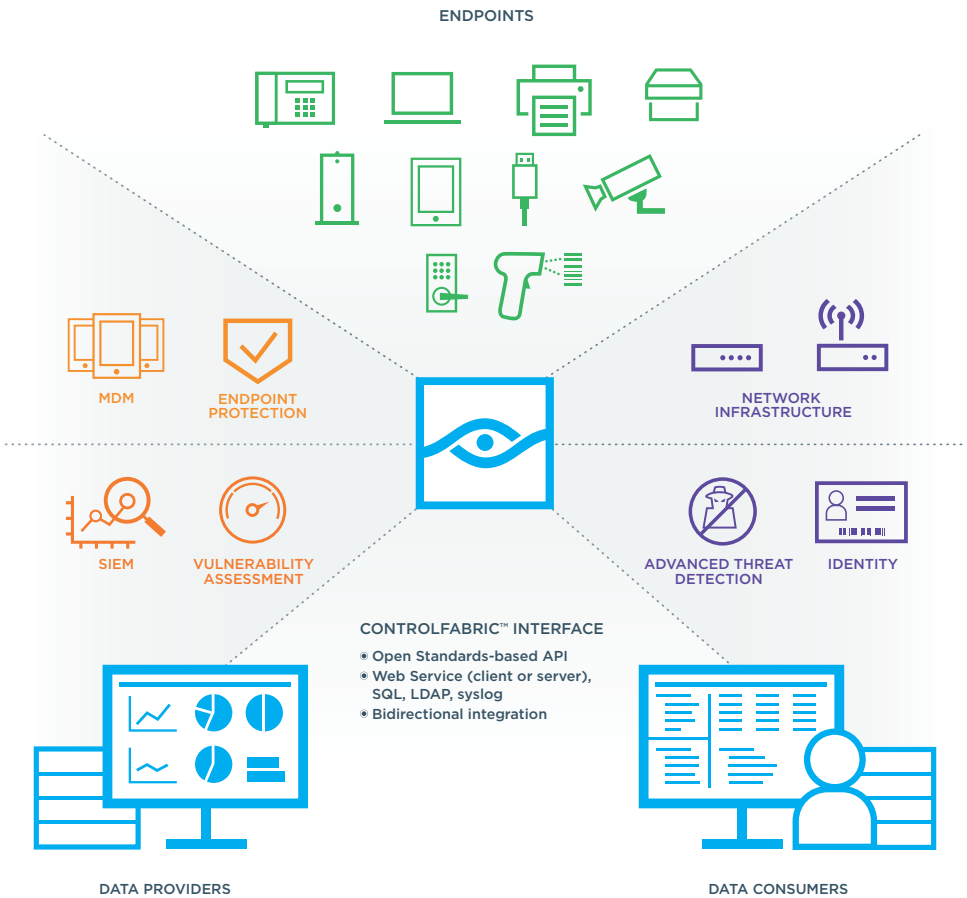

Figure 1: ControlFabric Ecosystem
ControlFabric Architecture lets CounterACT share contextual insights and automate workflows with third-party security tools over your existing network infrastructure to improve and unify system-wide security. ForeScout currently integrates with more than 70 network,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

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 January 2016