Brochure

ForeScout

ControlFabric™ Technologies

Continuous Monitoring

Information Sharing

Policy-based Control

Automated Mitigation

ForeScout

ForeScout ControlFabric Technologies

Benefits

- Increase situational awareness by sharing real-time security information among the IT security products that you already own
- Improve security posture by automating remediation and incident response
- Gain visibility and control over unmanaged devices
- Maximize investment in existing network and security products
- Save time and money by automating routine IT tasks and processes

"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 Principle Analyst,
Enterprise Strategy Group

What's Wrong with IT Security?

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

1. Too many IT security systems operate independently

If your IT security organization is like most others, you've probably purchased a variety of security and management systems. You probably 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 critically needed synergies such as the ability to share contextual information. Without information sharing, you can't optimize the effectiveness of your IT security investments.

2. Too many IT security systems just provide information

Many IT security systems provide information only. They 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 a hacker more time to compromise your systems. Vulnerability assessment , advanced threat detection (ATD), and SIEM commonly suffer from this weakness.

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

For example, some 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, and so they miss scanning transient devices. And patching processes are typically done on a periodic basis (e.g. monthly), not continuously.

4. Too much reliance on security agents

Agents serve a valuable function, but their scope is limited to corporate-owned computers. Increasingly, enterprise networks contain devices that are not corporate-owned or that can't accommodate management agents (e.g. industrial equipment). Also, agents often break or become misconfigured. When this happens, you have a blind spot, and finding and fixing these corporate-owned computers can be very challenging.

Fortunately, a solution is now available.

ControlFabric

The Solution

ForeScout ControlFabric™ is a set of technologies that enables ForeScout CounterACT™ and other IT solutions 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.

Because CounterACT is a network appliance, the scope of what it can see and control is far greater than an agent-based solution. And because it operates continuously, it provides more complete and more timely information than a periodic (e.g. monthly) solution. ControlFabric technologies allow CounterACT to see network devices and vulnerabilities that were previously unknown to you, including transient endpoints, personally-owned (BYOD) devices, and corporate-owned devices with broken management agents.

ControlFabric Base Integrations

ForeScout CounterACT includes a wide variety of integrations with network and IT infrastructure (switches, wireless controllers, VPN, routers, directories), endpoints (Windows, Mac, Linux, VMware), and endpoint software (antivirus, instant messaging, WMI, etc.). CounterACT currently supports over 60 integrations with IT infrastructure products and services. These base ControlFabric integrations give you tremendous power to discover and classify endpoints; track users and applications; assess security posture; control network access; enforce endpoint compliance policy; and fix security gaps such as broken endpoint security agents.

ControlFabric Extended Integrations

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

- **Security Information and Event Management (SIEM)** — CounterACT helps SIEM systems obtain visibility of devices on the network, not just managed devices (which the SIEM is typically aware of) but also unmanaged devices. This allows SIEM systems to more accurately assess enterprise risk. Additionally, some SIEM systems can trigger CounterACT to initiate automated remediation when a security exposure has been detected.

- **Mobile Device Management (MDM)** — CounterACT helps automate the enrollment of new mobile devices into your MDM system; this reduces helpdesk costs and boosts employee productivity. Additionally, CounterACT can trigger many leading MDM systems to re-assess the compliance of a mobile device the moment the device attempts to connect to your network, for improved security. Also, CounterACT can block unauthorized or non-compliant devices from your network.

- **Advanced Threat Detection (ATD)** — Your ATD products have the ability to detect advanced threats, but they might not have the ability to automatically remediate the problem. Integration with CounterACT allows these products to trigger rapid response by CounterACT such as quarantine of the infected system, scan of the entire network to assess the extent of infection, and automated remediation of the infected endpoint.

- **Vulnerability Assessment (VA)** — CounterACT can trigger your VA product to scan new devices the moment they join your network. This gives you more up-to-date risk information. Additionally, your VA product can trigger CounterACT to remediate, limit or block endpoints that are found to contain serious vulnerabilities.

- **McAfee ePO** — CounterACT augments your ePO deployment by bringing visibility and control over unmanaged devices, and detects and remediates missing or broken McAfee agents. ePO shares managed device compliance status with CounterACT which continually monitors the network and remediates or quarantines endpoints with security exposures.

ControlFabric Custom Integrations

ForeScout's open ControlFabric Interface allows you or any third party 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. The Open Integration Module supports the following open, standards-based integration mechanisms:

- **Web Services API** — for sending and receiving XML messages
- **SQL** — reading from and writing to databases, e.g. Oracle, My SQL, SQL Server, etc.
- **LDAP** — reading from standard directories

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

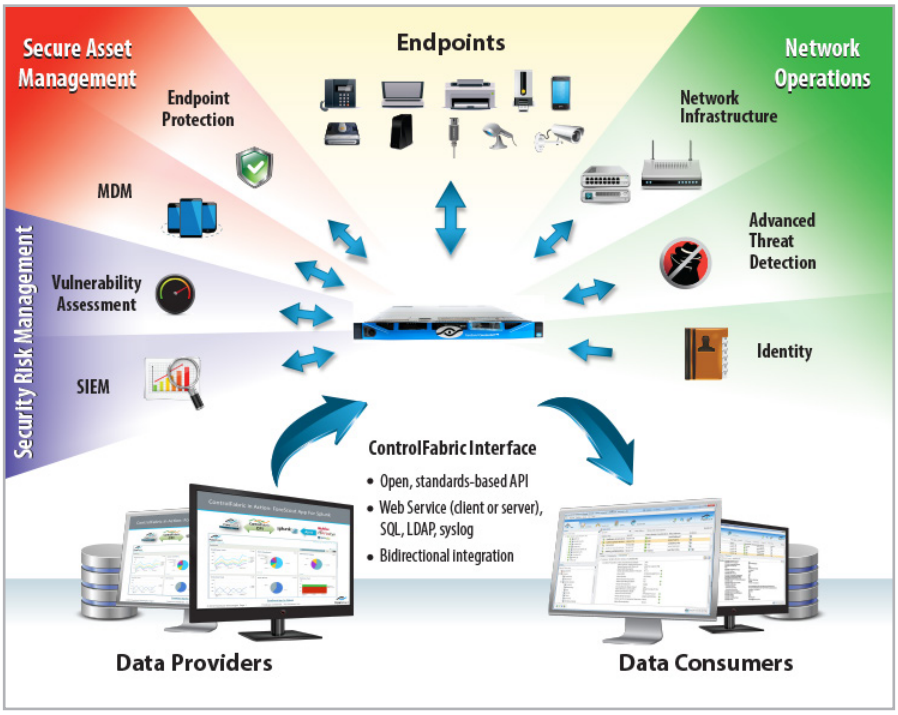

Figure 1: The ControlFabric Interface

About ForeScout

ForeScout enables organizations to continuously monitor and mitigate security exposures and cyber attacks. The company's CounterACT platform dynamically identifies and evaluates network users, endpoints and applications to provide visibility, intelligence and policy-based mitigation of security problems. ForeScout's open ControlFabric architecture allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, extensible and scalable, as of January 1, 2015, they have been chosen by more than 1,800 of the world's most secure enterprises and government agencies in over 62 countries. Headquartered in Campbell, California, ForeScout offers its solutions through its global network of authorized partners. **Learn more at www.forescout.com.**

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

ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Ave.,
Suite 300
Campbell, CA 95008
U.S.A.

Contact Us
T 1-866-377-8771 (US)
T + 1-408-213-3191 (Intl.)
F + 1-408-371-2284 (Intl.)
www.forescout.com

Doc: 2015.0071 REV. 4