Open Integration Module

Highlights

See

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

Control

- Allow, deny or limit network access based on device posture and security policies
- Reduce attack surface by ensuring endpoints have up-to-date security defenses
- Initiate remediation and risk mitigation actions on malicious or infected endpoints

Orchestrate

- Build integration between 3rd party products and ForeScout CounterACT to collapse existing silos of information
- Share real-time information with existing security products and automate responses to mitigate threats and data breaches
- Improve overall security posture by automating routine activities and making better use of existing tools

The Challenges

Visibility. According to industry experts, a vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints. Most organizations are unaware of a significant percentage of the endpoints on their network because they are either not managed (personal devices, guest, and Internet of Things (IoT)), have disabled or broken agents, or aren't detected by periodic scans (transient devices). As such, you are unaware of the attack surface on these devices.

Threat Detection. Today's cyberthreats are more sophisticated than ever and can easily evade traditional security defenses. Multi-vectored, stealthy, and targeted, these attacks are focused on acquiring sensitive personal information, intellectual property, or insider information. Compromised endpoints and data breaches can often remain undetected for weeks or months. To detect these advanced threats, zero-day attacks and infected endpoints, you need new security controls that do not rely on signatures.

Response Automation. The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, are creating the perfect storm for IT security teams. Without an automated system to continuously monitor and mitigate endpoint security gaps, valuable time is lost performing these tasks manually. And without the ability to automatically and quickly respond to attacks and security breaches, you are leaving the window open for cyberthreats to propagate within your network and exfiltrate data.

How it Works

ForeScout CounterACT™ is a network security appliance that provides IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. CounterACT provides policy-based control of these devices and works with ForeScout ControlFabric™ Architecture to orchestrate information sharing and automate operation among disparate security and IT management tools.

The Open Integration Module allows customers, systems integrators, and third party product vendors to integrate third party products with ForeScout CounterACT. These bi-directional integrations enable third party systems to:

- Consume information generated by CounterACT such as device type, compliance status, user information, operating system information, application information, peripheral information, physical layer information, and more.
- Provide information to CounterACT such as host related property or event that can be used within a ControlFabric platform policy.
- Receive or send action triggers to CounterACT.

The Open Integration Module installs on the CounterACT appliance and allows it to send and receive information via the following open standards:

- **Web services.** The Open Integration Module can be configured to send and receive XML (Extensible Markup Language) formatted messages to a designated web service based on HTTP interaction. The communication uses REST (Representational State Transfer) web service requests and a simple XML format. The format of the messages is customizable and may contain CounterACT host property. For example:
  - CounterACT can update a firewall with up-to-date information about logged-in users and their current IP address. This allows the firewall to provide more accurate access rules.

- CounterACT can identify hosts that need remediation, based on company policies, and automatically open a new service ticket at the corporate help desk system.

- **SQL.** CounterACT is able to push and pull information into and out of a standard SQL (Structured Query Language) database. This type of integration is common for interfacing with home-grown applications and with third party products that are able to interface through an external or internal database. You can query external databases for information, and you can create CounterACT host properties to store the data which CounterACT retrieves. These host properties can be used in CounterACT policies, and viewed in NAC and Inventory views. You can update external databases based on the information that CounterACT has, typically for some third party product to act upon.

- **LDAP.** CounterACT is able to generate custom queries to pull and push information into and out of a standard LDAP server. You can query the LDAP server for information, and create CounterACT host properties to store the data which has been retrieved. These host properties can be used in CounterACT policies, and viewed in NAC and Inventory views.

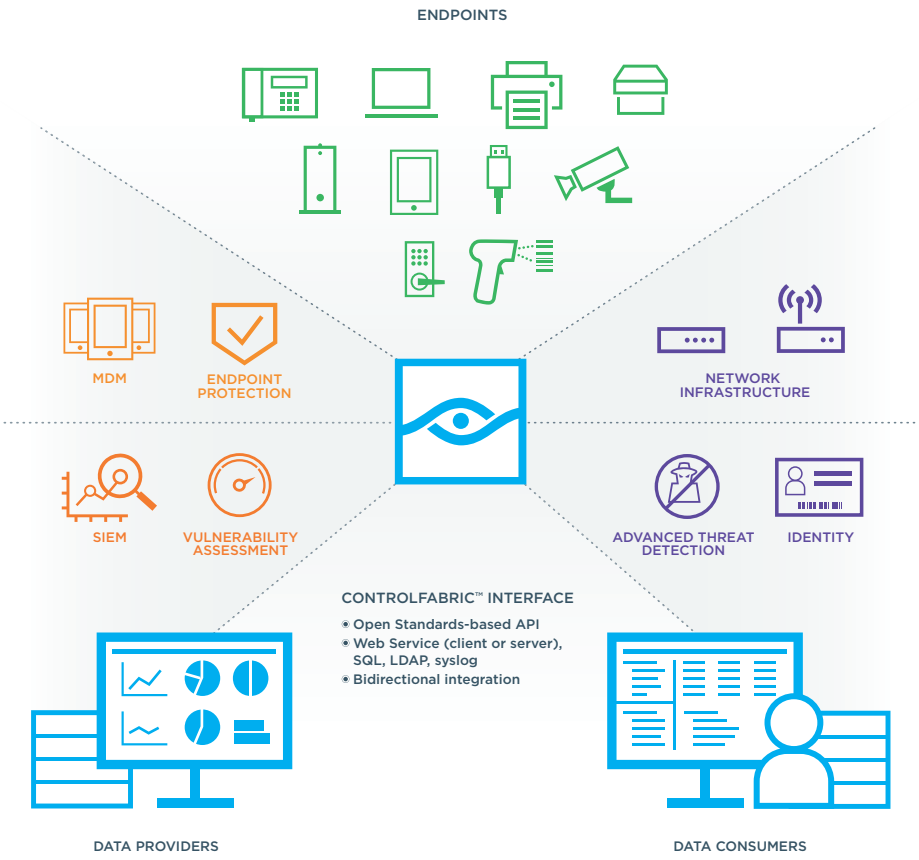

Figure 1: ForeScout ControlFabric Interface

Additionally, the following interface is included with ForeScout CounterACT (the Open Integration Module is not required):

- **Syslog.** CounterACT can be configured to send and receive information via syslog 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 security information and event management - SIEM, or with other solutions that can send and receive alerts in this manner. The message format is customizable.

ForeScout ControlFabric

The integration between ForeScout CounterACT and existing IT systems is just one way that leverages the ForeScout ControlFabric architecture. ControlFabric is an open technology enabling ForeScout CounterACT and other solutions to exchange information and more efficiently mitigate a wide variety of security issues. Learn more at www.forescout.com/controlfabric.

Learn more at
www.ForeScout.com

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