Solution Brief

ForeScout CounterACT Integration with Brocade Network Infrastructure

Highlights

Improved Visibility | Expand your network visibility to include real-time information about 100% of the endpoints on your network, including unauthorized devices and BYOD endpoints owned by employees, guests and contractors.

Enhanced Security | Assess the security and compliance posture of all devices in real-time before and after they connect to the network. Auto-remediate non-compliant endpoints and block unauthorized or infected devices.

Increased Productivity | Keep employees and guests productive on your network while protecting critical resources and sensitive data. Grant the appropriate level of network access to each user and device without intrusive intervention or software installation.

Cost Savings | Eliminate manual processes associated with opening or closing network ports for guest access, and restricting, remediating or quarantining risky devices on the network. Reduce troubleshooting and downtime caused by rogue network devices and infected endpoints.

ForeScout
Access ability.

BROCADE

Improve Network Security and Operational Efficiency

ForeScout has integrated its automated security control platform for network access control (NAC), mobile security and endpoint compliance with Brocade's switch infrastructure to provide network security managers with superior visibility and control of both managed and unmanaged devices on the network.

With this joint solution, organizations can deploy ForeScout CounterACT in their Brocade environment to prevent unauthorized device access and create a secure guest and "bring your own device" (BYOD) environment. CounterACT deploys out-of-band without relying on endpoint agents, thus eliminating network latency issues and costly software roll-outs.

The Challenges

Visibility. Today, most security threats and breaches come from inside your firewall. Thus, any serious attempt to manage security must start with complete knowledge of who and what is on your network, and whether those devices are secure.

Traditional network management software is unable to provide information about the security posture of endpoint devices. Agent-based security solutions are blind to unmanaged devices (devices without agents) such as guest/BYOD endpoints and rogue wireless access points. Vulnerability scanners are useful, but they do not provide real-time information. For completely visibility of 100% of the devices on your network, including their security posture, you need a real-time network security solution such as ForeScout CounterACT.

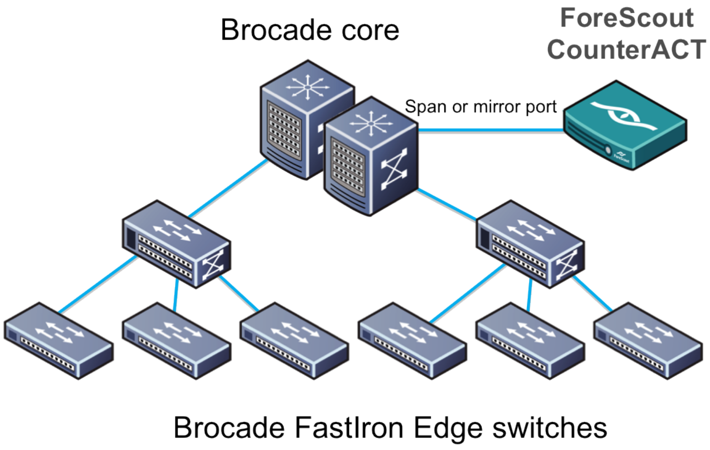
Network access control. Your guests and contractors bring their own personal laptops and devices with them. To remain productive, they need internet access, and may also need access to corporate data and applications. Increasingly, your employees are looking to use their personal smartphones and tablets on your network. If you provide unlimited access to your enterprise network, you can expose your environment to malware and possible data loss.

Endpoint security. Mobile devices that connect to corporate and public networks can become infected or non-compliant over time. Endpoints can become misconfigured. Security agents can be disabled. Antivirus software can fall out-of-date. Unauthorized software can be installed by employees.

To control risk, IT managers need to know the security posture of all devices before they're allowed to connect to the network. Once connected, IT security managers need an automated system that continuously monitors endpoint devices to detect malicious activity, risky user behavior, or failure of one or more of the onboard security agents.

The ForeScout-Brocade Joint Solution

ForeScout CounterACT integrates with Brocade switches to solve all of the challenges listed above. The CounterACT network appliance (or virtual appliance) installs out-of-band, thus adding no latency or potential for network failure. While there are several flexible deployment scenarios, CounterACT is usually attached to the span or mirror port of a Brocade switch at the network core, thereby allowing it to monitor network traffic. It communicates with distribution and access layer switches via SNMP, CLI and SSH. Multiple CounterACT appliances within the enterprise network can be centrally managed by the CounterACT Enterprise Manager.



CounterACT delivers unique capabilities to a Brocade network environment:

» **Visibility.** ForeScout CounterACT gives you real-time visibility into everything on your network—all devices, all operating systems, all users, all applications. CounterACT incorporates the most granular host interrogation engine in the industry and can determine almost every configuration detail on every endpoint. Administrators can access this information using a Google-like search interface that displays a detailed catalog of all connected users and devices.

» **Guest registration.** ForeScout CounterACT's automated process allows guests to access your network without compromising your internal network security. ForeScout CounterACT includes several guest registration options allowing you tailor the guest admission process to your organization's needs.

» **Role-based network access control.** ForeScout CounterACT ensures that only the right people with the right devices gain access to your important network resources. ForeScout leverages your existing directory where you assign roles to user identities.

» **Flexible enforcement options.** Unlike early generation NAC products that employed heavy-handed controls and disrupted users, ForeScout CounterACT provides a full spectrum of enforcement options that let you tailor the response to the situation. Low-risk violations can be dealt with by sending the end-user a notice and/or automatically remediating his security problem; this allows the user to continue to remain productive while remediation takes place. High-risk violations can be quarantined or blocked.

» **802.1x or not.** ForeScout CounterACT lets you choose 802.1X or other authentication technologies such as LDAP, Active Directory, Oracle and Sun. WIth hybrid mode, you can use multiple authentication technologies concurrently, which speeds NAC deployment in large, diverse environments.

- **Automated exception handling.** ForeScout CounterACT automates the handling of printers, phones, and other equipment that cannot authenticate via 802.1X. CounterACT continuously monitors endpoint behavior to eliminate the security risk of MAC address spoofing.

- **BYOD friendly.** Flexible policies allow full or limited network access based on user name, device type, and security posture. Control access based on VLANs, ACLs, or built-in virtual firewall. Hybrid mode lets you use either 802.1X certificates or LDAP user credentials to authenticate.

- **Endpoint compliance automation.** ForeScout CounterACT can ensure that every endpoint on your network is compliant with your security policy. CounterACT can automatically fix most endpoint security problems, such as updating the antivirus, or prompting the patch management system to update the device's operating system, or disabling unauthorized software.

- **Deep integration.** ForeScout CounterACT deeply integrates with Brocade switches for easy deployment. Auto-discovery allows the administrator to add a single Brocade switch to the CounterACT system, and CounterACT automatically discovers the other switches. CounterACT listens to SNMP traps sent by Brocade switches to automatically detect new devices trying to connect to the network. CounterACT can automatically manage ACLs on Brocade switches to open or close network zones, services or protocols for specific hosts connected to a switch port; this is particularly useful on flat networks without VLANs.

Joint Solution Benefits

- Enhanced network security based on complete visibility of all endpoints on the network, including BYOD

- Increased productivity by enabling guest and BYOD provisioning and on-boarding

- Cost savings based on automated remediation, reduced troubleshooting and downtime