Gigamon®
The Smart Route To Visibility™

ForeScout
Access ability.

Automating Network Visibility and Security Control

- **Optimize visibility and security controls:** Dynamically identify network assets, eliminate or dramatically reduce rogue systems, WAP and unwanted apps, enforce network access and configuration policy, and address endpoint security gaps.
- **Minimize core network switch load:** Reduce switch/router SPAN port and port density limitations and manage mirrored network data transmission to the ForeScout CounterACT™ platform.
- **Cost Savings:** Centrally mirror and manage content-rich network communications to reduce security incidents and help desk reaction, readily pinpoint violations, address threats without IT intervention, and enhance return on endpoint protection investments.

ForeScout + Gigamon

ForeScout and Gigamon have partnered to enable the availability and efficient use of mirrored network traffic to deliver real-time visibility and automated control over users, devices, systems, applications, and VMs accessing network resources and sensitive data.

By employing a Gigamon® Traffic Visibility Fabric™ solution, users can reduce SPAN port and port density limitations and filter traffic to enable CounterACT to provide enterprise-class network access control, flexible mobile security, automated endpoint compliance and advanced threat protection. The combined solution can increase situational awareness, security intelligence and operational responsiveness.

Problem: Infrastructure Visibility

Paramount to enable information security and meet compliance requirements is the ability to have an immediate and rich understanding of activity on your network. To accomplish this, network security solutions require the means to tap into your core switch infrastructure. This requirement can be challenging.

- **Port Density.** Often, the available ports on production switches and routers are being used and upgrading core switches to increase port count (density) is expensive.
- **Monitoring Cost.** Depending on the switch and router layer traffic being monitored, it can be unwieldy and expensive to monitor multiple ports and VLANS to support each type of network security tool.
- **Traffic Analysis.** In some cases, the sheer or peak volume of traffic being streamed from the switch to the security tool overwhelms the processing capacity of the network security device. Some environments, such as in shared facilities or networks with different classes of traffic, will want to filter traffic being sent to a network security device.

Problem: Access Control and End Compliance

Do you have visibility, control and intelligence over the users and endpoints accessing your enterprise? Can you enforce policy for employees and guests using mobile devices? Can you enforce endpoint compliance on virtual machines? How are you preempting access threats and enforcing endpoint compliance policy? Do you have the necessary information to easily assess, validate and support control effectiveness?

- **Centralized Intelligence.** The multitude of access points, user types and devices introduces security gaps and a variety of threats ranging from data leakage and malware propagation to targeted attacks and compliance violations. Identifying and assessing the security posture of the assets on your network is critical to close security gaps and expedite incident response.

- **Dynamic Control.** Security teams not only require complete situational awareness, but also need to effectuate controls in real-time in order to enforce policy, preempt endpoint vulnerabilities and security issues, and maintain compliance requisites.

Automating Network Visibility and Control

The Gigamon Traffic Visibility Fabric provides intelligent traffic mirroring to enable CounterACT to ensure that:

- Access to network resources and sensitive data is trusted and appropriate
- Endpoints are accounted for and meet security standards
- Volations and threats can be managed faster and with reduced IT intervention

ForeScout CounterACT automated security platform lets you see and control what is connected to your network no matter the user or device. ForeScout's real-time endpoint classification, policy assessment and threat remediation capabilities offer the means for organizations to apply strong access control policies, as well as find and fix endpoint security issues with little to no IT intervention. CounterACT can identify thousands of known and new endpoint devices, such as business critical servers, virtual machines, VoIP phones, unusual devices, and even rogue systems and wireless access points as they connect to the network. CounterACT's multi-factor application fingerprinting identifies installed software and patches, running services and processes, open ports, active Host Based Security Systems (HBSS) and other important criteria that can impact defenses and compliance. Since ForeScout leverages directory services, specific policies with regards to employees, contracts and guests and their devices can be effectively managed. Furthermore, CounterACT can identify and stop endpoint policy violations, propagating threats and malicious activity even after network connections have been granted.

By leveraging Gigamon's Traffic Visibility Fabric, users are able to pass data streams of all network traffic to the ForeScout CounterACT platform for device discovery and analysis, network admission, mobile security, endpoint compliance and threat prevention. This provides IT real-time inventory and security posture intelligence for active remediation while allowing users to seamlessly connect to the network without disruptions or changes in end-user experience unless necessary. In addition, the Gigamon G-TAP functionality reduces switch SPAN port and port density constraints to allow enhanced network visibility. The GigaVUE TAP functionality also allows "pruning" of traffic data sent to CounterACT to reduce the processing load of the CounterACT packet engine or to only send specific traffic for CounterACT to process.

Security Empowerment – Use Case

A large enterprise with a highly redundant core network was looking to deploy ForeScout CounterACT to enforce network access policy and enable endpoint compliance. Their two high availbility core switches had a limitation on the number of available SPAN ports. The customer had already deployed an Intrusion Protection System (IPS) and web proxies that maxed out the SPAN capability of these core switches. Deployment of CounterACT to the distribution layer was a physical impossibility and relatively cost prohibitive based on the number of switches. The aggregate bandwidth of the client network is roughly 5G of throughput supporting 6000 devices. This would require two ForeScout CounterACT 4000 appliances deployed in a high availability configuration. As such, this configuration required at least four SPAN ports with 10G interfaces.

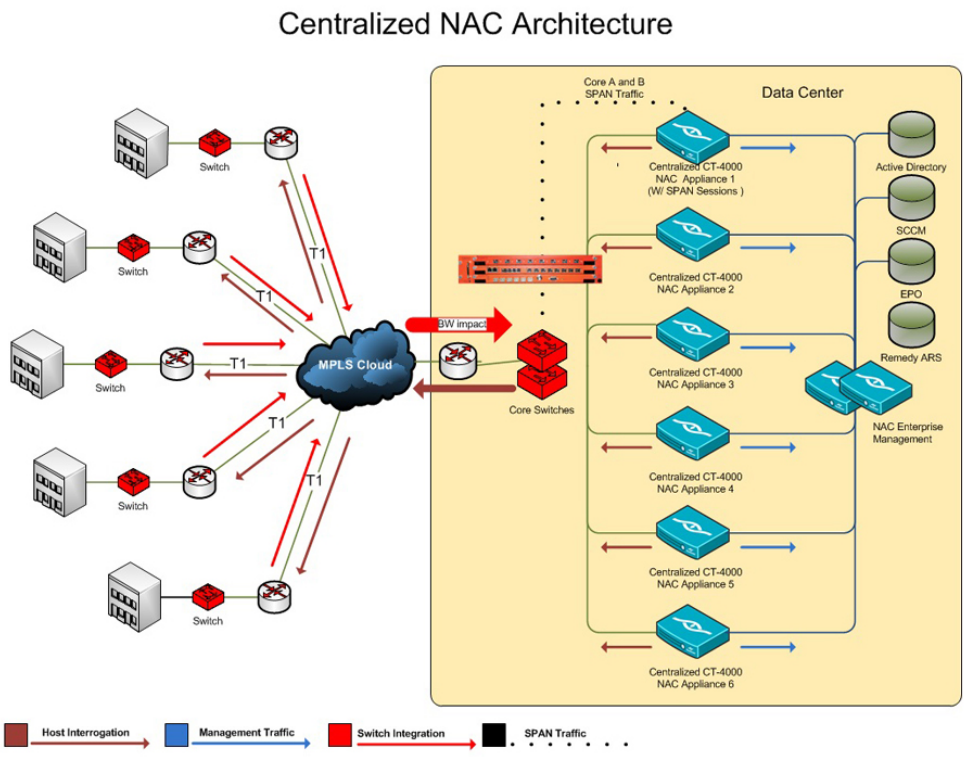
The customer placed a single GigeVUE-2404 Traffic Visibility Fabric Node with two 10G interfaces for SPAN connectivity and the required four ports for CounterACT. This configuration also provided additional port density for the customer's current IPS and web proxy configurations, as well as allowed for plenty of port capacity to support other tools in the future without the need for a redesign of the core switch infrastructure. The result was a scalable and more affordable, flexible and manageable solution that reduced the actual equipment cost for purchase and provided added capability for monitoring and network management.

Joint Solution Benefits

- Dynamically identify network assets, eliminate or dramatically reduce rogue systems, WAP and unwanted apps, enforce network access and configuration policy, and address endpoint security gaps.

- Reduce switch/router SPAN port and port density limitations and manage mirrored network data transmission to the ForeScout CounterACT platform.

- Centrally mirror and manage content-rich network communications to reduce security incidents and help desk reaction, readily pinpoint violations, address threats without IT intervention, and enhance return on endpoint protection investments.


Centralized NAC Architecture
Switch
Switch
Switch
Switch
Switch
T1
T1
T1
T1
T1
MPLS Cloud
BW impact
Core Switches
Core A and B SPAN Traffic
Data Center
Centralized CT-4000 NAC Appliance 1 (W/ SPAN Sessions)
Centralized CT-4000 NAC Appliance 2
Centralized CT-4000 NAC Appliance 3
Centralized CT-4000 NAC Appliance 4
Centralized CT-4000 NAC Appliance 5
Centralized CT-4000 NAC Appliance 6
Active Directory
SCCM
EPO
Remedy ARS
NAC Enterprise Management
Host Interrogation
Management Traffic
Switch Integration
SPAN Traffic

ForeScout CounterACT enterprise deployment with Gigamon GigaVUE Traffic Visibility Fabric Node

To learn more about the ForeScout/Gigamon Solution, please contact:

ForeScout Technologies, Inc.
10001 North De Anza Blvd.
Suite 220
Cupertino, CA 95014 USA
www.forescout.com
sales@forescout.com

Gigamon
598 Gibraltar Drive
Milpitas, CA 95035
Phone: 408-263-2022
www.gigamon.com