Juniper-ForeScout Joint Solution for Endpoint Visibility and Control

Agentless solution ensures that wired and wireless devices comply with corporate security policies

Challenge

With the proliferation of BYOD, IoT, and unmanaged devices, corporate networks are exposed to increased risks and cyberattacks from unsecured, noncompliant devices. Lack of complete visibility into all of these devices, wired or wireless, can lead to unexpected downtime, loss of productivity, and spiraling operational costs.

Solution

ForeScout CounterACT, working with Juniper's network infrastructure, offers complete visibility into, control over, and remediation of wired and wireless devices the moment they connect to the network, making sure they comply with corporate security policies and risk mitigation.

Benefits

Organizations benefit from:

- Corporate policy-compliant network
- Reduced security vulnerabilities and risks
- Increased productivity
- Reduced downtime and operational costs

Market research suggests the number of Internet of Things (IoT) connected devices to triple over the next three years. Gartner predicts that number to grow from 6.4 billion in 2016 to 20.4 billion by 2020, with 5.5 million new devices being connected every day[1]. This massive proliferation of connected devices demands new, less intrusive ways for IT to maintain continuous visibility, monitoring, and compliance.

ForeScout CounterACT gives IT organizations the unique ability to see new devices the instant they connect to the network, as well as allowing IT to continuously monitor, control, and remediate these devices as they repeatedly join and leave the network. Juniper Networks, working in conjunction with ForeScout CounterACT, creates an end-to-end multilayer secure network by defining risk mitigation policies and implementing them at the access, aggregation, core, and network perimeter, greatly enhancing the security profile of the network.

The Challenge

Organizations are facing a number of security challenges when it comes to protecting their internal network.

Visibility

According to industry experts, a vast majority of successful attacks exploit well-known vulnerabilities and security gaps on network endpoints. Unfortunately, organizations are unaware of most of these endpoints because they are unmanaged, BYOD, guest, or IoT devices not under their direct control. These endpoints may have disabled or broken agents, or they may be transient devices that aren't detected by periodic scans, making them invisible to most security tools.

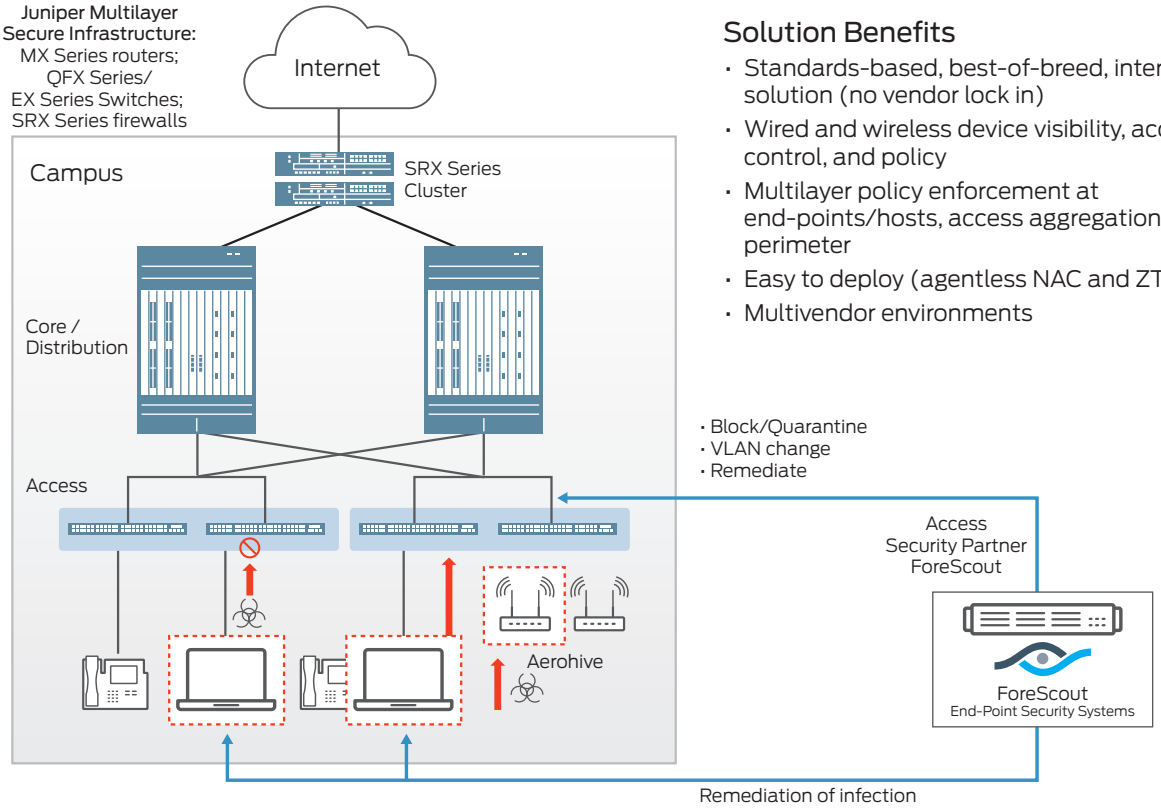
Threat Detection

Today's cyberthreats are more sophisticated than ever and can easily evade traditional security defenses. Multivectored, 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 even months, providing ample time for these attacks to find what they are looking for. Detecting these advanced threats, zero-day attacks, and infected endpoints requires next-generation 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 permissive BYOD policies, are creating a perfect storm for IT security teams. Without an automated system for continuously monitoring and mitigating 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.

[1] Source: http://www.gartner.com/newsroom/id/3165317



Solution Benefits

- Standards-based, best-of-breed, interoperable solution (no vendor lock in)
- Wired and wireless device visibility, access control, and policy
- Multilayer policy enforcement at end-points/hosts, access aggregation, core, perimeter
- Easy to deploy (agentless NAC and ZTP)
- Multivendor environments

Figure 1. Juniper-ForeScout Joint Solution

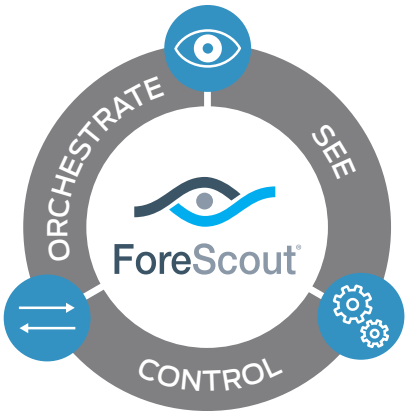
The Juniper Networks-ForeScout Joint Solution

ForeScout CounterACT occupies a unique space among network security solutions due to its agentless approach. Available as both a physical and virtual solution, ForeScout CounterACT identifies devices based on their IP addresses, including network infrastructure, BYOD systems, nontraditional IoT devices (handhelds, sensors, and machines), and rogue endpoints (unauthorized switches, routers, and wireless access points)—no management agents or previous device awareness is required. ForeScout CounterACT detects and profiles endpoints as they get deployed and, based on the device posture, coordinates an instant response through its integration with Juniper Networks® EX Series Ethernet Switches.

Working in concert with ForeScout CounterACT, Juniper offers layered security policy enforcement and control at the access, aggregation, core, and perimeter, implemented on EX Series Ethernet Switches and Juniper Networks SRX Series Services Gateways. This multilayer approach mitigates risk and noncompliance at multiple levels while increasing the security profile of the network. Using standard protocols such as 802.1X, RADIUS, SNMP, and Dynamic Host Configuration Protocol (DHCP), CounterACT discovers endpoint posture and authentication status, as well as appropriate security policies. Agreed upon actions are then applied at the Juniper EX Series switches.

Features and Benefits

- **Multilayer security:** The joint ForeScout-Juniper solution provides layered security, policy enforcement, and control at the access, aggregation, core, and perimeter, greatly increasing the network security profile and reducing noncompliance risks and unauthorized access.
- **Agentless:** No endpoint agents are required for authentication and network access control (NAC), allowing CounterACT to see and control managed, unmanaged, and IoT devices, simplifying deployments.
- **Open interoperability:** The Juniper-ForeScout integration is based on industry-standard protocols, enabling it to interoperate with other third-party solutions. CounterACT works with popular switches, routers, VPNs, firewalls, and endpoint operating systems without requiring any infrastructure changes or upgrades.
- **Multiple authentication options:** You can choose 802.1X or other authentication technologies such as Lightweight Directory Access Protocol (LDAP), Active Directory, RADIUS, Oracle, and Sun. Hybrid mode supports multiple technologies concurrently.
- **Comprehensive endpoint visibility and assessment:** CounterACT sees the network in incredible detail, identifying and evaluating network devices and applications as well as determining the device's operating



- Agentless and 802.1X solution
- Offers real-time visibility into wired and wireless end points
- Supports broad range of responses across:
  - User
  - Network
  - End point
- Supports multivendor network devices, firewalls, third-party SIEMs
- Integrates with existing IT systems

Figure 2. ForeScout CounterACT features and benefits

system, configuration, software, services, patch state, and the presence of security agents. CounterACT automatically classifies a growing number of IoT endpoints as it quickly clarifies and assesses the status and security posture of devices on the network. And it makes all of this possible with or without 802.1X infrastructure.

Equally important, CounterACT gains this in-depth visibility very quickly. In a recent evaluation by testing and research firm Miercom, CounterACT discovered and classified 100 percent of endpoints in all network environments tested. In addition, CounterACT discovered and classified 500 endpoints in less than five seconds.[2] This is in stark contrast to traditional NAC solutions that typically offer few discovery and classification capabilities and are often limited to displaying only a device's IP address.

Juniper Solution Components

EX Series Ethernet Switches are designed to meet the demands of today's high-performance businesses, enabling companies to grow their networks at their own pace while minimizing large up-front investments. Based on open standards, EX Series switches provide the carrier-class reliability, security risk management, virtualization, application control, and lower total cost of ownership (TCO) that businesses demand.

SRX Series Services Gateways are next-generation intelligent security platforms that deliver outstanding protection, market-leading performance, six nines reliability and availability, scalability, and services integration. SRX Series devices are ideally suited for service provider, large enterprise, and public sector networks, delivering the highest level of protection from Layer 3 to Layer 7. The SRX Series platforms also feature a carrier-grade next-generation firewall with advanced services such as application security, Unified Threat Management (UTM), intrusion prevention system (IPS), and integrated threat intelligence services.

ForeScout Solution Components

ForeScout CounterACT is a physical and virtual security solution that dynamically identifies and evaluates network devices and applications the instant they connect to a network. ForeScout CounterACT is an agentless solution, and it works with both known and unknown managed and unmanaged endpoints—PCs, mobile, embedded, and virtual. CounterACT quickly determines the user, owner, operating system, device configuration, software, services, patch state, and the presence of security agents. It provides remediation, control, and continuous monitoring of these devices as they come and go from the network.

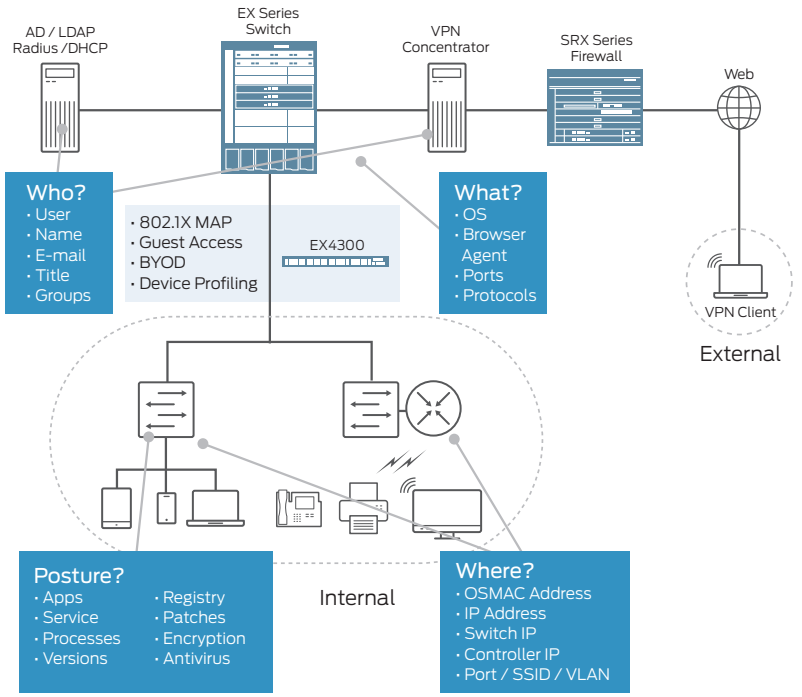
Every ForeScout CounterACT appliance, physical or virtual, ships with a built-in integration module that interoperates with EX Series switches. CounterACT works seamlessly with Juniper Networks devices, requiring no infrastructure changes, upgrades, endpoint agents, or endpoint reconfiguration. Working with the Juniper switching infrastructure, it discovers and assesses connected endpoints, identifies risks and threats, automatically restricts the access of compromised or noncompliant devices, and alerts administrators to initiate remediation.

How ForeScout CounterACT Detects and Profiles Juniper Networks Endpoints

While CounterACT includes and fully integrates 802.1X authentication, its methods for device detection and assessment are far more extensive, allowing it to see and thoroughly profile devices that do not have or will not support 802.1X agents.

When a device connects to a Juniper-based network, CounterACT collects the device's media access control (MAC) and IP addresses, switch port, service set identifier (SSID), and other details from EX Series switches as well as wireless controllers, allowing it to determine where the device is connecting. It acquires user identity context from directories, DHCP servers, VPN concentrators, and other sources to determine who is connecting. Additional device context such as operating system, ports, and protocols comes from network monitoring

[2] "An Independent Assessment of ForeScout CounterACT," Miercom, June 2016



ForeScout CounterACT does the following:

- Continuous device discovery
- Continuous device monitoring
- Device posture assessment
- Remediation

CounterACT agentless mechanism includes:

- SNMP poll of devices on the network
  - (Switched, VPN concentrators, AP controllers)
- Monitor HTTP, DHCP requests; Netflow
- Import external MAC or LDAP data

CounterACT can optionally use 802.1X

Based on device posture, CounterACT pushes NETCONF configs to EX Series switch to:

- Block the port
- Assign endpoint to a different VLAN
- Quarantine, upgrade/downgrade privilege

Figure 3. Juniper and ForeScout endpoint visibility and access control

via Switched Port Analyzer (SPAN) or mirror ports. CounterACT inventories the applications, services, and processes running on the device, checks the OS version and registry settings, and verifies the presence of security agents. The result: a complete profile of the device and its security status.

ForeScout CounterACT-Juniper Joint Solution Response to Threats

When CounterACT detects a device that is either noncompliant or potentially compromised, it coordinates an instant response through its integration with the EX Series switching infrastructure. By sending new configuration files to the switches using the IETF Network Configuration (NETCONF) protocol, CounterACT can affect different types of changes in how a device accesses network resources. These include:

- Blocking the switch port and denying all network access
- Assigning the device to a quarantine VLAN with restricted resource access
- Applying a firewall policy to the interface to restrict access
- Downgrading the device or user privileges via change of authorization (CoA)

Device Type Profiling:

- Identifies the type of device connected (e.g., printer, IP phone, Windows, or iOS device, etc.)
- Assigns network access based on the user identity/role, device type, location, ownership, and security compliance status
- Eliminates the need for enterprises to manually maintain a list of known device MAC addresses and device-type mapping
- Mitigates threats from malicious endpoints that spoof MAC addresses (note: MAC address is not used for device profiling)
- Enables dynamic provisioning of ports based on type of connected device

MAC Authentication Bypass:

- Devices like printers and IP phones can use MAC RADIUS to bypass 802.1X authentication
- CounterACT can look for known MAC addresses and place them in an appropriate VLAN or restrict them
- If the device is unknown, CounterACT can send a reject notice or place that device in a restricted VLAN

Guest Access or BYOD:

- All personally owned devices get a consistent wired and wireless experience
- Users can be redirected to a webpage via a captive portal to provide instructions on how to authenticate/register
- Users need to agree to an acceptable use policy (AUP) to get a restricted guest access
- Guest users can log in using pre-allocated guest access credentials or can easily self-enroll

- Employees with noncorporate devices can be required to register their devices and autoconfigure their endpoints
- Devices are continuously monitored to ensure security policy compliance (i.e., antivirus, OS version, firewall enabled)

CounterACT can also alert administrators to initiate a remediation process and restore all authorized resource access when repairs are complete.

Summary: ForeScout and Juniper Deliver Advanced Protection

The Juniper-ForeScout integrated solution offers enterprises an end-to-end monitoring, control, and remediation solution that provides unparalleled visibility into wired and wireless devices. The agentless CounterACT solution is easy to manage and deploy. Complementing ForeScout's endpoint visibility, Juniper's multilayer security architecture greatly enhances the security posture of the network and mitigates vulnerabilities and risks. With the proliferation of BYOD and IoT devices, the enterprise-grade unified access solution from Juniper Networks and ForeScout could be key for maintaining the organization's productivity and security.

Next Steps

To learn more about comprehensive device visibility and policy-based security automation in Juniper switching environments, visit www.ForeScout.com.

To learn more about Juniper Networks products and solutions, including EX Series Ethernet Switches, QFX Series Switches, MX Series 3D Universal Edge Routers, and SRX Series Services Gateways, please visit www.juniper.net.

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. As of January 2016, more than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions. Learn more at www.forescout.com.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

3510598-001-EN Nov 2016