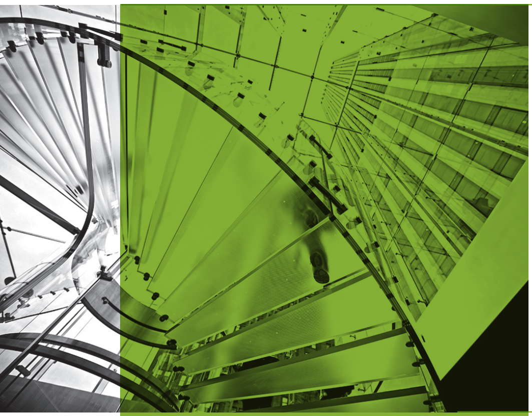

EXTEND SECURITY WITH JUNIPER CONNECTED SECURITY AND FORESCOUT

Leverage the entire network for lateral threat remediation

The increasingly sophisticated cyber attack landscape demands that businesses deploy a comprehensive security platform that not only unites and coordinates various threat analytics platforms, but provides a simpler policy mechanism as well. This requires leveraging the entire network as a threat detection and enforcement tool.

The Juniper Connected Security framework does just that, empowering all network devices—not just perimeter firewalls—to work together as a threat detection and security enforcement domain. Juniper Networks® Junos Space® Security Director Policy Enforcer management software orchestrates policies created by the Juniper Advanced Threat Prevention cloud-based malware detection solution, distributing them to Juniper Networks EX Series Ethernet Switches, QFX Series Switches, and third-party switches, as well as the physical and virtual Juniper Networks SRX Series Services Gateways. The Juniper solutions work in concert with ForeScout CounterACT®, giving IT organizations the unique ability to see new devices the instant they connect to, or leave, the network, allowing them to continuously monitor, control, and remediate these devices.

Working together, Juniper and ForeScout create a secure, end-to-end, multilayer network by defining risk mitigation policies and implementing them at the access, aggregation, core, and network perimeter, greatly enhancing the system's overall security profile.

The Challenge

Visibility

Most successful cyber attacks exploit well-known vulnerabilities and security gaps on network endpoints. Unfortunately, organizations aren't aware of all endpoints in their network because many are unmanaged transient BYOD, guest, or IoT devices that go undetected during periodic scans, making them invisible to most security tools.

Control

Perimeter security alone is not sufficient to secure networks; it merely protects the system from outside intruders. With the proliferation of internally launched attacks, it's now imperative to know about each and every device on your network, including

Challenge

The proliferation of BYOD, IoT, and unmanaged systems exposes corporate networks to cyber attacks from unsecured, noncompliant devices. Lack of visibility into and control over these devices—wired or wireless—can lead to downtime, lower productivity, and spiraling operational costs.

Solution

The joint Juniper-ForeScout solution offers complete visibility into, and control over, wired and wireless devices the moment they connect to the network. This prevents lateral threat propagation and ensures that these devices comply with corporate security and risk mitigation policies.

Benefits

- *Defends against unknown malware and advanced attacks*
- *Expands threat protection with vendor-agnostic mechanisms*
- *Ensures consistent policy enforcement on third-party devices such as switches and wireless access points*
- *Prevents lateral threat movement by moving infected hosts to quarantined or blocked states*
- *Minimizes threat exposure by extending security deeper into the network*

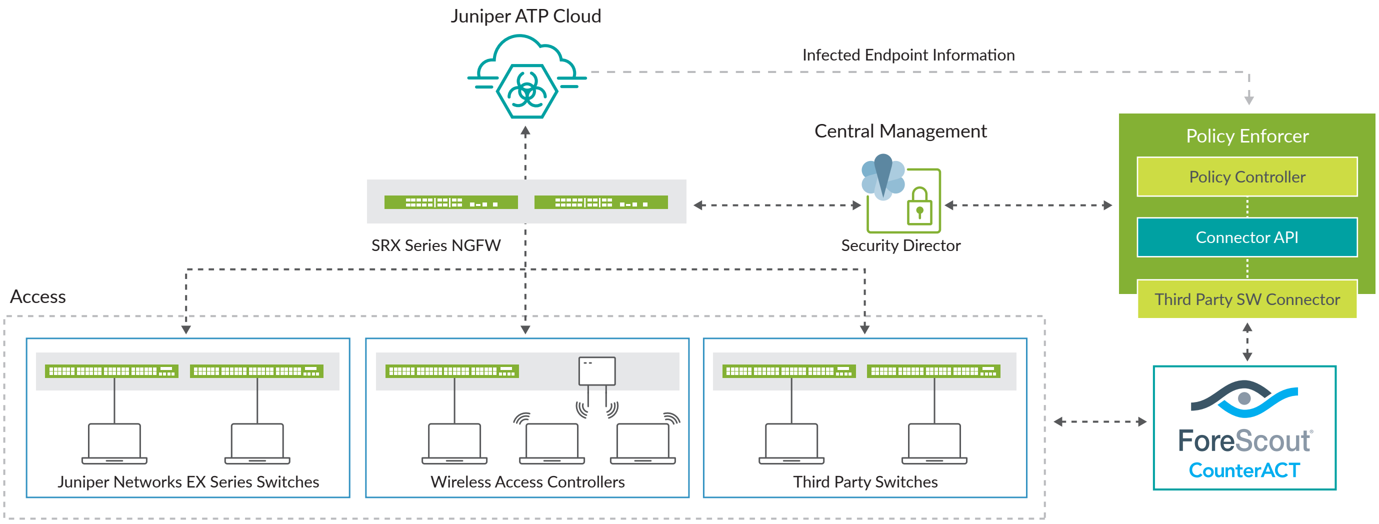

Figure 1: Juniper Connected Security and ForeScout CounterACT solution overview

its owner, purpose, and security posture.

These insights allow you to apply the appropriate level of network access control based on established security policies—for example, BYOD, guest, contractor, and IoT devices must be assigned to appropriate network segments. You must also be able to restrict access to noncompliant devices and quarantine them within secure VLANs. Given the dramatic growth of mobility and IoT devices, this level of control will ideally be achieved without manual implementation methods.

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 monitoring and mitigating endpoint security gaps, valuable time is lost. You must also be able respond to attacks and breaches quickly and automatically; any delay creates an opportunity for cyber threats to propagate within your network.

The Juniper Networks and ForeScout Solution

Juniper Connected Security delivers highly effective protection against today's sophisticated and ever-evolving threat landscape. With Juniper Connected Security's open architecture tightly integrated with ForeScout, enterprises can secure every point of connection across multivendor environments, including public and private clouds. With the automated threat remediation, real-time intelligence, and machine learning that the joint Juniper-ForeScout solution provides, your network will know when and how to protect your people, your data, and your infrastructure—no matter where they are.

With its agentless approach, ForeScout CounterACT occupies a unique space among network security solutions. Available as both a physical and virtual solution, ForeScout CounterACT uses active and passive techniques to discover and classify endpoints as they connect to the network, including BYOD/guest devices, nontraditional devices (IoT, handhelds, and sensors), and unknown and rogue endpoints (unauthorized endpoints, switches/routers, and wireless access points)—all without requiring management agents or previous device awareness. Using agentless visibility, CounterACT checks for device posture/compliance according to established security policies and then, depending on the device classification and/or posture, coordinates an automated host- or network-based response.

Working in concert with ForeScout CounterACT, EX Series and QFX Series switches offer layered security policy enforcement and control at the access, aggregation, core, and perimeter. This multilayer approach mitigates risk and noncompliance at multiple levels while increasing the network's security profile. Using standard protocols such as SNMP, CLI, and RADIUS, CounterACT classifies and assesses device compliance posture, then applies automated policy actions through the switches.

The joint solution empowers enterprises to defend themselves against the lateral movement of threats by blocking or quarantining infected hosts, even when users move and IP addresses change. This workflow is the same for endpoints that connect to the network via wireless access points.

Key Features and Benefits

The joint Juniper-ForeScout solution delivers the following features for enterprise customers seeking a comprehensive security solution.

Multilayer security	The joint Juniper-ForeScout solution provides layered security, policy enforcement, and control at the access, aggregation, core, and perimeter, greatly increasing the network security profile while reducing noncompliance risks and unauthorized access. It also ensures automated protection against malicious endpoints at both the perimeter and network levels.
Agentless	No endpoint agents are required for device profiling, compliance, remediation, and access control, allowing ForeScout CounterACT to see and control managed, unmanaged, and IoT devices. This greatly simplifies deployment.
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 infrastructure changes or upgrades.
802.1X and non-802.1X authentication	CounterACT can be deployed with Juniper switches using 802.1X authentication or a robust non-802.1X approach. The ForeScout-Juniper integration also supports hybrid deployments, giving customers a choice to authenticate traditional devices using 802.1X while nontraditional devices can connect using a non-802.1X approach.
Comprehensive endpoint visibility and assessment	CounterACT sees the network in incredible detail, identifying and evaluating network endpoints and applications as well as determining each device's operating 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—with or without 802.1X infrastructure.
In-depth visibility	CounterACT discovers and gains in-depth visibility on all endpoints. 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. This is in stark contrast to traditional access control solutions that typically do not discover every device on the network, offer few classification capabilities, and are often limited to displaying very basic endpoint properties.

Solution Components

SRX Series Services Gateways

Juniper Networks SRX Series Services Gateways are intelligent next-generation firewalls that deliver outstanding protection, market-leading performance, six nines reliability and availability, scalability, and services integration. Available in both physical and virtual form factors, SRX Series firewalls 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 carrier-grade SRX Series next-generation firewalls also offer advanced services such as application security, advanced security services, intrusion prevention system (IPS), and integrated threat intelligence services.

Juniper ATP Cloud

Juniper ATP is a cloud-based service that provides complete advanced malware protection. Integrated with SRX Series firewalls, Juniper ATP Cloud delivers a dynamic anti-malware solution that adapts to an ever-changing threat landscape.

Junos Space Security Director Policy Enforcer

Juniper's Policy Enforcer tool, a component of the Junos Space Security Director software, enforces threat remediation and microsegmentation policies on Juniper virtual and physical SRX Series firewalls, EX Series and QFX Series switches, MX Series 3D Universal Edge Routers, third-party switch and wireless networks, private cloud/SDN solutions like the Juniper Contrail® Platform and VMware NSX, and public cloud deployments. Juniper ATP's cloud-based malware detection, Command and Control (C&C), and GeoIP identification feeds, along with trusted custom feeds, act as threat detection mechanisms for Policy Enforcer to orchestrate remediation workflows.

EX Series Ethernet Switches

Juniper Networks EX Series Ethernet Switches are designed to meet the demands of today's high-performance businesses, letting companies 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.

QFX Series Data Center Switches

Juniper Networks QFX Series Switches are specifically designed for data centers. They provide the universal building blocks for creating and managing fabric architectures, improving performance, reliability, agility, and flexibility for multicloud environments.

Third-Party Switches and Wireless Controllers

The joint Juniper-ForeScout solution provides the same level of automated threat remediation for endpoint devices connected to third-party switches and wireless access points.

ForeScout CounterACT

ForeScout CounterACT is a physical and virtual security solution that dynamically identifies and evaluates traditional and nontraditional devices (security cameras, HVAC systems, and sensors) the instant they connect to a network.

CounterACT can be deployed using 802.1X authentication or a non-802.1X approach. In either scenario, CounterACT offers comprehensive endpoint discovery, classification, and assessment capabilities, allowing it to see and thoroughly profile endpoints that do not have or cannot support endpoint agents.

This agentless solution works with managed and unmanaged, mobile and virtual endpoints, both known and unknown. It quickly determines the user, owner, operating system, device configuration, software, services, patch state, and the presence of security agents. CounterACT then continuously monitors, controls, and remediates these devices as they come and go from the network. A broad range of responses across user, network, and endpoint are supported, including:

ORCHESTRATE
SEE
CONTROL
ForeScout

Figure 2: ForeScout CounterACT architecture

- Agentless 802.1X and non-802.1X solution
- Real-time visibility into wired and wireless endpoints
- Support for multivendor network devices, firewalls, and third-party SIEMs
- Integration with existing IT systems

Every CounterACT appliance, physical or virtual, ships with a built-inintegration module that interoperates with EX Series switches, QFX Series switches, and SRX Series firewalls. CounterACT works seamlessly with Juniper devices, requiring no infrastructure changes, upgrades, endpoint agents, or endpoint reconfiguration.

Solution Workflow: Juniper Connected Security and ForeScout

The Juniper and ForeScout solutions work together to detect and block attacks launched within the environment. The following bullets detail the full workflow.

- An endpoint device downloads a potentially malicious file from the Internet.
- An SRX Series firewall sends the file to Juniper ATP Cloud for analysis. Juniper ATP determines the threat level and communicates that information to the SRX Series firewalls and Policy Enforcer.
- SRX Series firewalls prevent the file from being downloaded based on predefined policies and the threat level score from Juniper ATP Cloud.
- At the same time, based on the threat intelligence received from Juniper ATP Cloud, Policy Enforcer determines that the host that downloaded the file is infected.
- Policy Enforcer reports the infected host's IP address to ForeScout.
- ForeScout enforces policy actions as defined by the user, including blocking or quarantining the infected host or device.
- Policy Enforcer mitigates lateral propagation of the threat by tracking infected host movement and taking remedial actions such as quarantining/blocking the host, even if its IP address changes.

Summary—End-to-End Monitoring, Automated Policy Enforcement, and Threat Mitigation

The joint Juniper-ForeScout security solution gives enterprises complete end-to-end monitoring, automated policy enforcement, and threat mitigation with unparalleled visibility into wired and wireless networks. Juniper Connected Security's open architecture, integrated with ForeScout's agentless CounterACT solution, delivers a consistent, easy-to-manage security posture deployment that effectively mitigates vulnerabilities and risks.

Next Steps

For more information about Juniper Networks security solutions, please visit http://www.juniper.net/us/en/products-services/security and contact your Juniper Networks representative.

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

About ForeScout

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology continuously assesses, remediates, and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows, and optimize existing investments. As of March 1, 2017, more than 2400 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate system-wide response. Learn how at www.forescout.com.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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

JUNIPER NETWORKS | **Engineering** Simplicity