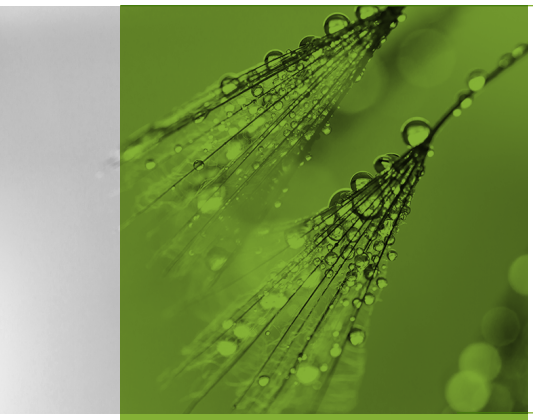
Juniper Networks | Driven by Experience™



BUILDING A THREAT-AWARE NETWORK FOR HEALTHCARE

Secure every point of connection to safeguard users, applications, and infrastructure

Challenge

According to the U.S. Department of Health and Human Services, 45 million individuals were affected by healthcare attacks in 2021, up from 34 million in 2020. These numbers prove that many healthcare organizations need a more effective security strategy to eliminate threats inside and outside the network.

Solution

Juniper Connected Security solutions provide an open, scalable way to block threats at every step of the cyber kill chain:

- *Security Director Cloud*
- *Secure Edge*
- *Next-generation firewalls*
- *Advanced Threat Prevention products*
- *SRX Series Firewalls*

Benefits

- *Expand threat visibility and enforcement capabilities across the entire network infrastructure*
- *Respond to threats with flexibility and agility*
- *Reduce time between threat detection and enforcement*
- *Easily manage and deploy security policies from a single UI across the entire healthcare enterprise*

Solution Brief

The digital economy is transforming healthcare. The pace of innovation is accelerating, patients' expectations are higher than ever, and new competitors are emerging from unexpected, nontraditional markets. To compound these challenges, the healthcare industry has long been a favorite target of cyberattackers. Despite firms' best efforts, cybersecurity threats are increasing, and attacks are more successful than ever. Healthcare firms need a more effective, adaptable approach to detecting and stopping cyberthreats.

The Challenge

Traditionally, network security has meant a strong perimeter defense. Firewalls sat at the network perimeter, checking everything coming into the network, ensuring that everything inside the network was trusted. That's no longer enough. Advanced threats can bypass traditional perimeter security defenses, enter the trusted network, and move undetected.

Unfortunately, compromised mobile devices are potentially connecting to the network every day, possibly unleashing malware and putting the entire organization at risk. The risk increases exponentially with the rise of the Healthcare Internet of Things that can span across medical devices that enable remote patient monitoring, to physical hospital assets with smart IoT sensors and connectivity such as smart beds and energy consumption equipment for power distribution, elevator operations, and others.

Virtualization and the cloud have brought increased agility to the data center, but modern security technologies have failed to keep pace with evolving threats. As a result, threats can persist unseen inside the network, giving criminals time to carefully plan the theft of high-value information, steal medical intellectual property, commit fraud, destroy the brand image, and disrupt revenue opportunities.

Employees and contractors depend on the network to access applications and other resources to do their jobs. Patients count on websites and mobile apps to interact with their caregivers, insurance companies, and other healthcare providers. Attackers commonly target facility resources, including mobile devices, because these systems have privileged access to business-critical applications such as provider and patient health records, payer insurance data, and institution, provider, staff, and patient financial information. This poses a challenge for security administrators to control and monitor today's highly distributed environments for suspicious activities. Security pros need greater visibility into business applications, whether in the data center or the cloud, and the operational tools to consistently apply security policies anywhere.

Data center networks are prime targets for attackers, since they house the core operations for healthcare firms and are home to the organization's most valuable information and applications. In addition to data theft and destruction, denial-of-service (DoS) attacks can overwhelm the data center, preventing workers and patients from accessing critical resources and personal healthcare information resulting in catastrophic consequences. A DoS attack can be as damaging to business viability as the exfiltration of high-value data.

Security professionals can no longer view internal networks as trusted and external networks as untrusted. We must consider all network traffic untrusted in today's cybersecurity threat landscape.

Juniper Connected Security

Now more than ever, everything from how users access the network, to data and applications, to making network connections must be secured. Security must be invisible to users, operationally efficient for IT teams to maintain, and provide effective threat prevention. This can only be achieved when security is built into

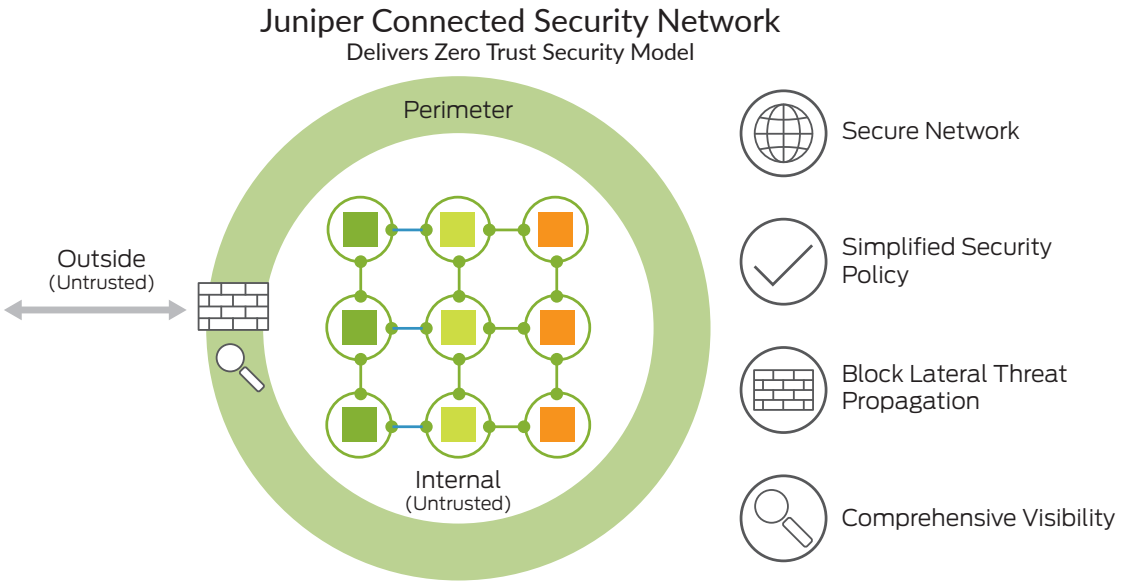


Figure 1: Juniper Connected Security is based on a zero-trust security model.

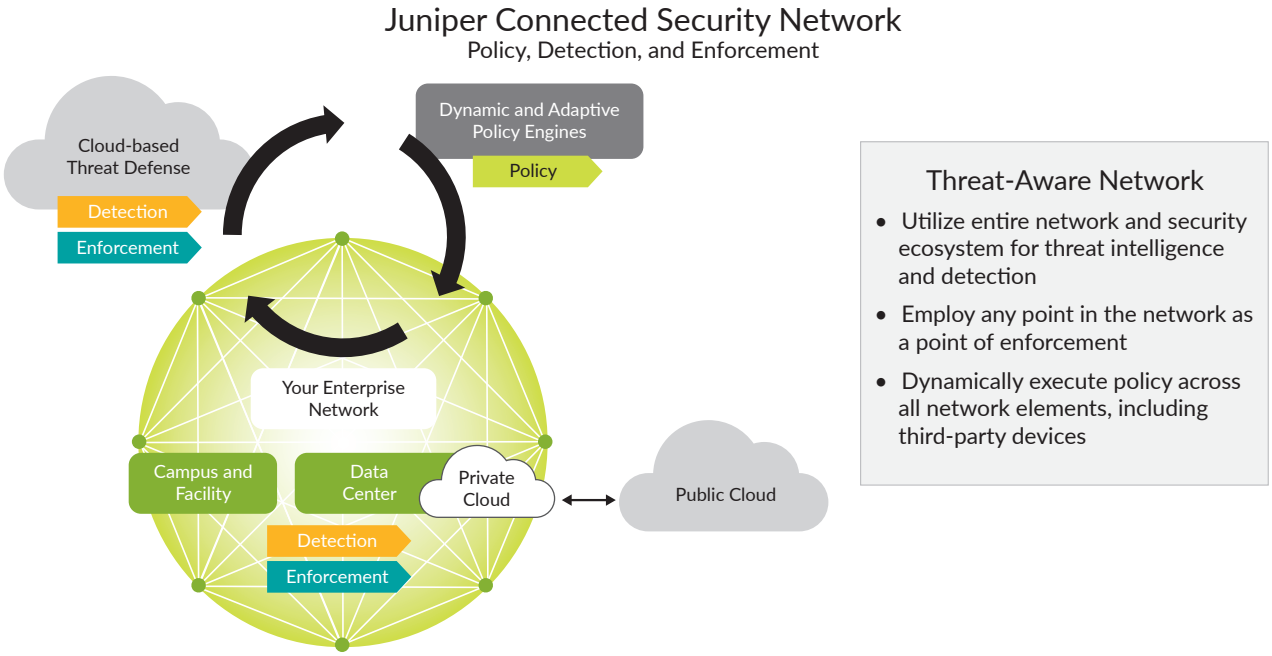


Figure 2: Juniper Connected Security simplifies creating security policies, detecting threats, and enforcing policies.

the same network infrastructure that provides connectivity and extends across every point of connection.

Juniper® Connected Security delivers the threat-aware network that today's healthcare organizations need, improving security while reducing complexity and streamlining management. When organizations empower the network to be threat-aware, attacks are detected sooner, and attackers are less likely to gain a foothold, safeguarding users, applications, and infrastructure.

With Juniper Connected Security, healthcare firms can shift from a traditional, siloed approach to viewing the network as a single enforcement domain. Network policy, detection, and enforcement become more adaptable, allowing firms to stop threats with greater accuracy. Security administrators can create and manage policies that are tightly aligned with business policies rather than micromanaging security for different VLANs and security zones.

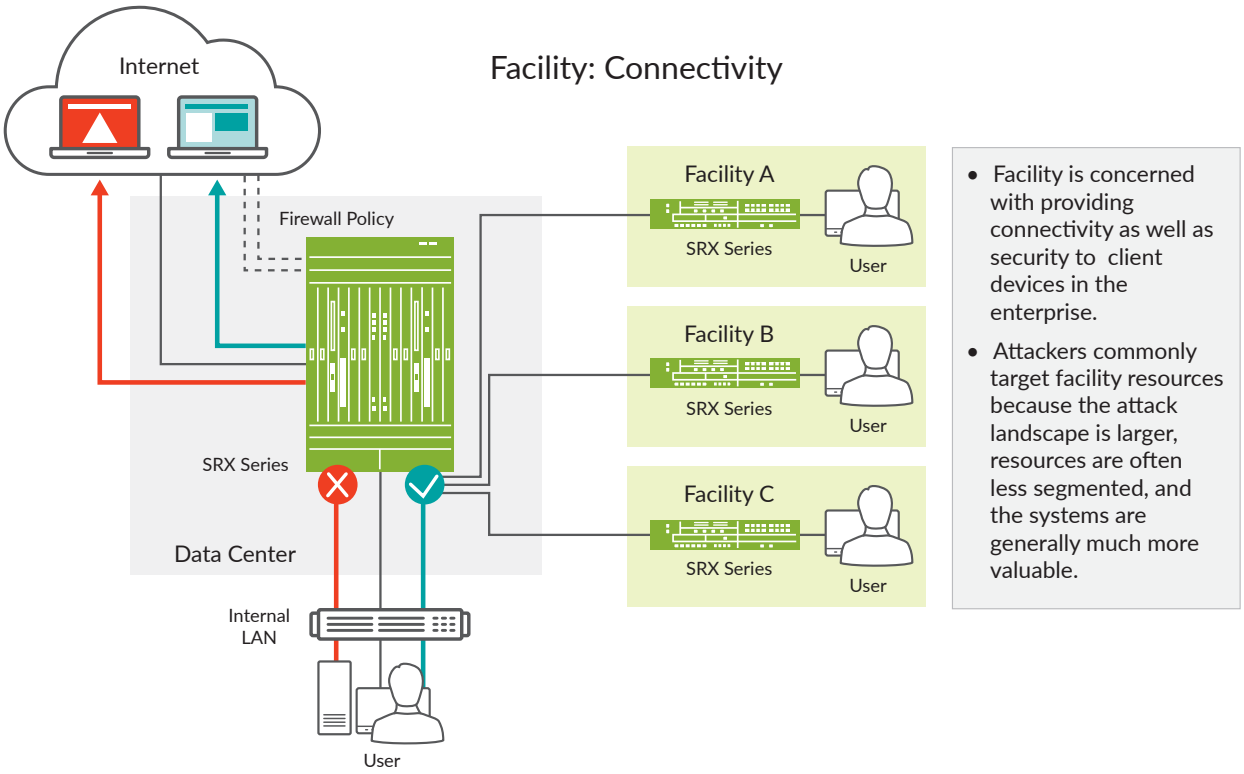


Figure 3: Secure network services architecture supports healthcare branches.

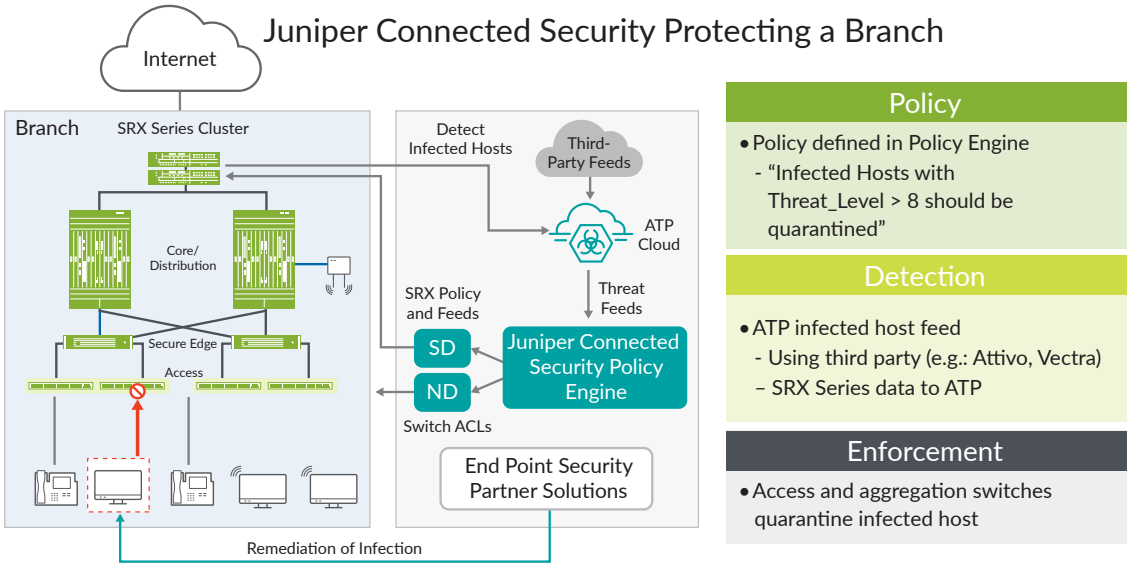


Figure 4: Juniper Connected Security makes it easier to protect facilities with consistent security policies, threat detection, and enforcement.

Juniper Connected Security Networks

Policy	Create and centrally manage security through a user intent-based system
Detection	Unify and rate intelligence from multiple sources, including dynamic event monitoring of your environment
Enforcement	Enforce policy in near real time across the network and. adapt to network changes

With the Juniper Connected Security strategy, threats can be detected sooner, even as they evolve, by leveraging threat intelligence from multiple sources, including third-party and customer-curated feeds, and tapping into the power of the cloud. Network security can adapt dynamically to real-time threat information to enforce security policies consistently, even in a nationwide healthcare enterprise. The building blocks of a Juniper Connected Security network include advanced firewalls for the facility and data center, threat intelligence, orchestration, and cloud-based protection.

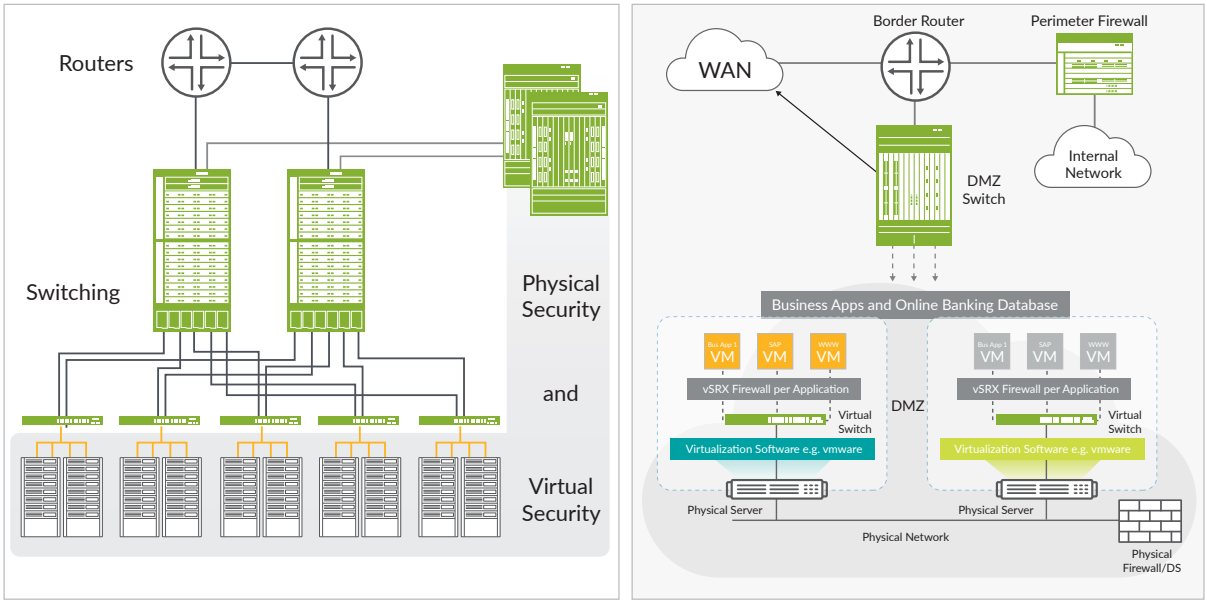


Figure 5: Microsegmentation allows zoning and segmentation created by SRX Series Firewalls (both virtual and physical).

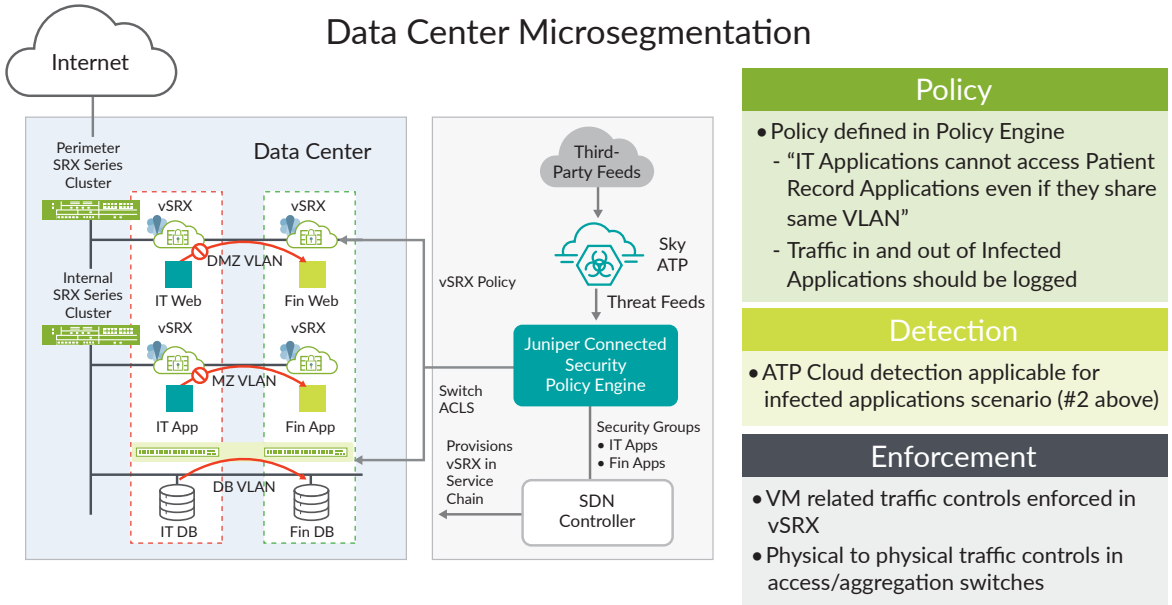


Figure 6: Juniper simplifies extending security to every segment in the data center using microsegmentation.

Securing Facility Networks in Healthcare

Juniper Networks® SRX Series Firewalls combine next-generation firewall and unified threat intelligence services with routing and switching in a single, high-performance, cost-effective network platform. SRX Series Firewalls provide network connectivity to regional or branch locations using standards-based routing protocols. A branch office SRX Series Firewall also provides switching to connect small numbers of endpoints. In contrast, a large SRX Series Firewall can provide WAN connectivity and switching for regional offices or campuses.

The SRX Series supports full, standards-based IPsec encryption to ensure secure transport of business data across networks that are not managed, controlled, or secured by the firm's security administrators, whether the organization uses a shared service provider network or the public Internet.

Features and Benefits

Securing Data Center Networks in Healthcare Through Micro-Segmentation

Healthcare firms of all sizes can defend their data centers with Juniper's portfolio of enterprise security solutions. SRX Series Firewalls are next-generation, anti-threat devices with advanced, integrated threat intelligence, delivered on the industry's most scalable and resilient platform.

SRX Series Firewalls have set new benchmarks with 100GbE interfaces, and they provide connectivity options for 1GbE, 10GbE, and 40GbE. Express Path technology enables up to 2 Tbps performance for the data center with less than 7 microseconds of throughput latency. All SRX Series Firewalls can encrypt and decrypt traffic across shared and public WANs using IPsec VPN while simultaneously supporting thousands of VPN tunnels.

In cloud and virtual environments, the Juniper Networks vSRX Virtual Firewall provides east-west separation for traffic that meets microsegmentation requirements, addressing today's virtual workloads. The vSRX is the industry's fastest virtual security platform, providing scalable, secure protection for data centers and cloud environments.

Advanced security extends to Docker Containers with Juniper Networks cSRX Container Firewall and brings greater agility and elasticity to virtual infrastructure. Featuring a microservices architecture, the cSRX makes deployment throughout the network easier without compromising performance.

Unified Security Enforcement with a Common Policy Engine

The SRX Series Firewall's security capabilities are consistent across the entire product family whether deployed as an appliance, a scalable chassis, a virtual device, or consumed as a service with a single policy framework. IT teams can apply firewall-based policies to remote users and branch sites. Policies only need to be created once and applied everywhere with unified policy management, including user and application-based access, intrusion prevention system (IPS), anti-malware, and secure Web access within a single policy.

Separation of Control and Data Planes

High volumes of traffic and processor overutilization can cause a firewall to become unmanageable. The firewall may block user access to business resources when designed with shared control and data planes. Junos® operating system, the foundational operating system of the SRX Series Firewalls, is designed with the separation of control and data plane. When under a DoS attack, an SRX Series device provides strict policing protection of the control plane so that administrators can maintain management connectivity with the platform. At the same time, screens and additional mechanisms minimize the impact that a DoS attack might have on the data plane.

Next-Generation Firewall Services and Application Inspection

SRX Series Firewalls provide security enforcement and deep inspection across all network layers and applications. Users can be permitted or prohibited from accessing specific business on-premises and Web applications, regardless of the network ports and protocols used to transmit those applications. Deep inspection is applied via intrusion prevention policies for any traffic allowed to pass through SRX Series Firewalls, ensuring that the desired traffic running across an organization's network is legitimate and not manipulated as an attack vector.

Application- and user-based firewall policies can be combined to ensure that users within a healthcare organization's network can only access the specific business applications they are authorized to access. Antivirus, content filtering, and antispam enforcements can be layered on top of these policies to round out the full spectrum of application-based services applied to network traffic running through the firewall.

Enhanced Threat Intelligence

To enhance traffic visibility and provide an additional layer of protection against advanced persistent threats, SRX Series Firewalls support IP address blocking via geo-IP and command-and-control botnet feeds. This additional threat intelligence is delivered via Juniper Advanced Threat Prevention, which is updated constantly to ensure that threat data employed in the firewalls is accurate and up to date.

IP address threat data is quickly applied within security policies without requiring a configuration commitment. The new threat data within firewall policies is applied in less than 60 seconds after being updated within the service. A healthcare organization can automatically enforce and block IP addresses on SRX Series Firewalls from internally created threat data or with data from a third-party threat feed. This threat data can be delivered and enforced on SRX Series Firewalls within 60 seconds.

Juniper Sky Advanced Threat Prevention

As malware attacks evolve and grow more insidious, conventional anti-malware products have difficulty defending against them. An excellent example of this is the recent increase in ransomware attacks on the healthcare market's data. These attacks cripple businesses by encrypting critical data and then charging a fee (ransom) to decrypt that data. Juniper ATP Cloud keeps the network free of these types of zero-day attacks and other unknown threats by delivering superior cloud-based protection, and scanning ingress and egress traffic for malware and indicators of compromise.

Juniper ATP Cloud, which employs a pipeline of technologies in the cloud to identify varying levels of risk, provides a higher degree of accuracy in threat protection. Integrated with SRX Series Firewalls, Juniper ATP Cloud delivers deep inspection, inline malware blocking, and actionable reporting.

Juniper ATP Cloud's identification technology uses various techniques to quickly identify a threat and prevent an impending attack. These methods include:

- Rapid cache lookups to identify known files
- Dynamic analysis that involves unique deception techniques applied in a sandbox to trick malware into activating and self-identifying

Additionally, machine-learning algorithms let Juniper ATP Cloud adapt to and identify new malware in an ever-changing threat landscape.

Manage Security Anywhere and Everywhere with Security Director

IIn today's complex environment, management solutions can be slow, unintuitive, or restrictive in their level of granularity and control. This negatively impacts network security management, which can become overly time-consuming and prone to error.

Juniper® Security Director Cloud provides extensive security policy management and control through a centralized, web-based interface. It enforces policies against emerging and traditional threat vectors, protecting physical, virtual, and containerized firewalls on-premises and across multiple clouds simultaneously. It provides detailed visibility into application performance and reduces risk while enabling users to diagnose and resolve problems quickly.

Providing extensive scale, granular policy control, and policy breadth across the network, Security Director delivers network-wide visibility and policy management for deployments on-premises, in the cloud, and as a service. Administrators can quickly manage all phases of the security policy life cycle for firewalls and next-generation firewall services, including zero-touch provisioning and configuration. They also gain insight into sources of risk across the network—all from a single user interface.

Empower the Work-from-Anywhere Workforce with Secure Edge

Juniper Secure Edge provides Firewall as a Service (FWaaS) in a single-stack software architecture managed by Juniper Security Director Cloud—empowering organizations to secure their workforce wherever they are. Users have fast, reliable, and secure access to the applications and resources they need, ensuring great experiences for users. IT security teams gain seamless visibility across the entire network while leveraging their existing investments, helping them transition to a cloud-delivered architecture at their own pace.

Secure Edge provides consistent security policies that follow the user, device, and application without copying or recreating rule sets. This makes it easy to deploy cloud-delivered application control, intrusion prevention, content and Web filtering, and effective threat prevention without breaking visibility or security enforcement.

Solution Components

A Juniper Connected Security healthcare network includes:

- SRX Series Firewalls to protect branches and data centers
- vSRX Virtual Firewall with Juniper Spotlight Secure cloud service for threat management
- Juniper Advanced Threat Prevention for advanced threat intelligence
- Juniper Security Director Cloud for policy management and control
- Juniper Secure Edge for consistent security policies that follow the user, device, and application

Summary—Stop Threats Faster with Juniper Connected Security

A threat-aware network can help security administrators in healthcare organizations stop threats faster and more accurately. It can also help them gain greater control over the applications and traffic on their regional, facility office, and data center networks while protecting business assets and patient health information against increasingly sophisticated—and successful—cyberthreats.

SRX Series Firewalls deliver next-generation firewall protection with application awareness, intrusion prevention system (IPS), and user role-based control options, in a best-in-class next-generation firewall (NGFW) to help protect and control healthcare business assets. Healthcare firms can choose from a broad range of options, from all-in-one security and networking appliances to highly scalable, high-performance chassis options, virtual and cloud-based enforcement platforms, and an easily consumable service.

Juniper's security intelligence for SRX Series Firewalls is designed to respond to a rapidly changing threat landscape. It is extensible as an open security intelligence solution based on business needs. ATP Cloud integrates with SRX Series Firewalls for detection and enforcement, providing dynamic, automated protection against known malware and advanced zero-day threats, resulting in instant threat response. Administrators can centrally manage all SRX Series Firewalls using Security Director and easily add security services to existing SRX Series platforms for a cost-effective and easily managed solution.

Next Steps

To bring the power of a Juniper Connected Security network to your firm, contact your Juniper representative, or go to www.juniper.net/us/en/solutions/security/.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

JUNIPER NETWORKS | Driven by Experience™

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

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

3510597-003-EN July 2022