

BUILDING A CONNECTED AND SECURE RETAIL ENVIRONMENT

Enabling automated threat remediation to protect customer data and business continuity

Challenge

Network security is a main concern in today's omnichannel environment. This concern increases with the added number of connected devices that make the network more vulnerable to security threats, putting retailers at risk of losing brand reputation, customer trust, employee and customer retention, and revenue.

Solution

As retail digital transformation efforts continue with a focus on providing enhanced customer experiences, retailers must balance these efforts with escalating data security threats and privacy compliance.

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

Benefits

- Expand threat visibility and enforcement capabilities across the entire network infrastructure
- Improve flexibility and agility in responding to threats
- Reduce time between threat detection and enforcement
- Manage security anywhere and everywhere, on-premises and in the cloud, from the cloud, all within a single UI
- Create policies once and apply them anywhere and everywhere with unified policy management

The Challenge

Retail networks are complex, constantly changing environments. If anything disrupts them or impacts their availability, business grinds to a halt. When a customer can't make a purchase, they will likely go elsewhere—and that lost transaction could mean a lost customer forever. As a result, retailers must ensure the ongoing availability and reliability of their network while protecting sensitive personal information and transactional data to deliver great consumer experiences.

Accomplishing these goals takes greater visibility into network activities and strong, flexible defenses that can detect and prevent attacks and enforce security policies throughout the network. A fully protected network can neutralize risks and maintain business continuity across retail branches, the data center, and the cloud for better in-store and online customer and staff experiences.

Juniper Connected Security

Juniper Networks® Connected Security helps retailers safeguard their business with a threat-aware network that maintains the integrity and availability of their retail operations. Retailers gain a holistic security ecosystem that extends security to all connection points on the network. They can react in near real time to current and evolving intelligence to protect against known and unknown threats. Juniper Connected Security delivers a zero-trust model for information security, combining visibility, intelligence, and enforcement with a comprehensive product portfolio that centralizes and automates security to keep retail businesses running.

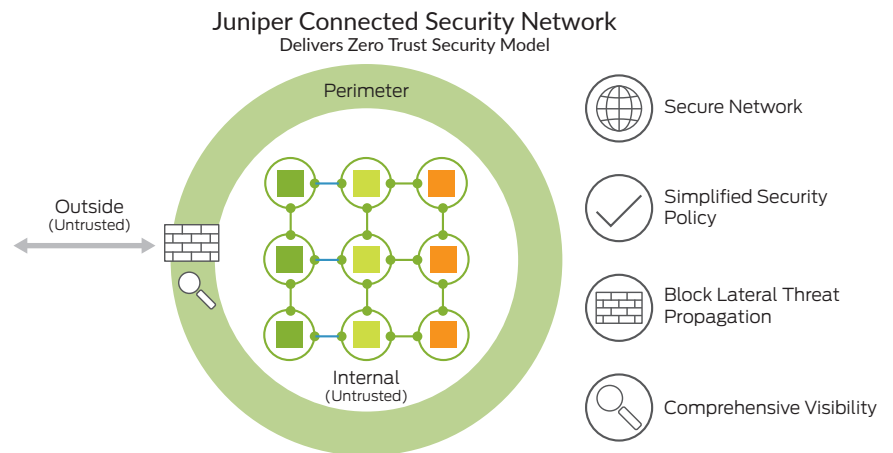


Figure 1: Juniper Connected Security is based on a zero-trust model.

Features and Benefits

Pervasive Security

Retailers can deploy zero trust and extend security to every layer of the network, including switches, routers, Wi-Fi access points, and the firewall layer, to combat the rising risks retailers face. Juniper Connected Security helps retailers build a threat-aware network with end-to-end security to protect their operations, customers, and staff against increasingly sophisticated and successful cyber threats.

Flexibility and Agility with an Open, Multivendor Ecosystem

Juniper Connected Security takes an open approach, allowing retailers to leverage their existing investments while transitioning to a more secure network. Juniper Connected Security offers a truly collaborative and comprehensive approach to complete network security by partnering with other network and security vendors.

Juniper supports different deployment models, from an on-premises physical deployment or private clouds (VMware NSX and Juniper® Contrail Networking) to public clouds (Amazon Web Services, Microsoft Azure, and Google Cloud Platform). Juniper Connected Security means retailers don't have to compromise in their pursuit of robust security.

Accelerated Detection and Enforcement

When retailers empower the network to be threat-aware, attacks are detected sooner; attackers are less likely to gain a foothold in the network, which safeguards users, applications, and infrastructure. Retailers can leverage threat intelligence from multiple sources (including third-party threat feeds and customer curated ones) and tap into the power of the cloud with Juniper® Advanced Threat Prevention. Network security can adapt dynamically to real-time threat information to enforce security policies consistently, even in a nationwide retail environment. 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.

Dynamic, Automated Threat Remediation

Juniper Connected Security helps security administrators in retail organizations identify and stop threats in their tracks while reducing overall risk and improving security posture. Juniper Policy Enforcer can automatically take corrective action against threats, blocking or quarantining them almost immediately at the network layer. This reduces administrative overhead and facilitates a faster, more manageable approach to security as the network expands.

Greater Visibility and Simplified Management with Global Policies

A significant challenge for retailers is consistent security across the entire network. The whole network must be secure from the corporate office to retail stores. Managing these locations can cause major headaches for IT and security teams.

Security Director enables retailers to manage security anywhere and everywhere, on-premises and in the cloud, with unified policy management that follows users, devices, and applications wherever they go. Policies can be created once and applied everywhere. Security Director gives retailers network-wide visibility and policy management for deployments on-premises, in the cloud, and as a service.

Managed by Security Director, Juniper® Secure Edge helps retailers easily manage and deploy security policies from a single UI across all environments. Create policies once and apply them everywhere with unified policy management, including user and application-based access, IPS, anti-malware, and secure web access within a single policy. Automate threat remediation and micro-segmentation policies across the entire network with Policy Enforcer, Security Director's built-in security orchestration.

Juniper gives retailers a consistent security policy they can use to protect employee data, customer payment information, and transactions while also maintaining PCI compliance and protecting in-store Internet of Things (IoT) devices.

Solution Components

A Juniper Connected Security retail network includes:

- Juniper Networks® SRX Series Services Gateways to protect branches and data centers
- Juniper Networks® vSRX Virtual Firewall with Spotlight Secure cloud service for threat management
- Advanced Threat Prevention for advanced threat intelligence
- Security Director for policy management and control
- Secure Edge for all next-generation firewall (NGFW) features as a service

Summary—Realize a Zero Trust and Threat-Aware Network with Juniper Solutions

Juniper Connected Security delivers the threat-aware network that safeguards users, applications, and infrastructure by extending security to every point of connection, from client to cloud, across the entire network. Ultimately, the network should work and never negatively impact the user experience. It must be seamless and secure. Retail customers and staff shouldn't

have to think twice about the network or its security. They should be able to do their job and make their purchase without worrying about the security of their data.

That is what a threat-aware network does. Juniper Connected Security helps retailers provide a seamless and secure user experience.

Next Steps

To find out more about how Juniper is helping retailers defend themselves against sophisticated attacks and protect customer data, please visit [What Is Secure Retail?](#)

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.



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

Copyright 2022 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, Junos, and other trademarks are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.