SECURITY DIRECTOR DATASHEET

Product Overview

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

Product Description

Network security management is how administrators operationalize their firewall architecture, provide visibility across individual deployments, policies, and traffic, and gain insight from threat analytics across the entire network traffic.

It can be a curse if management solutions are slow or restricted in their level of granularity and visibility; or a blessing with intuitive wizards, time-saving orchestration tools, and insightful dashboards. Juniper's Security Director manages security policy for all physical, virtual, and containerized firewalls. Through an intuitive, centralized, web-based interface, Security Director reduces management costs and errors by providing visibility, intelligence, automation, and effective security across Juniper SRX Series Firewalls deployments in both public and private clouds concurrently.

Security Director Cloud

Security Director Cloud is Juniper's simple and seamless management experience delivered in a single UI to connect customers' current deployments with their future architectural rollouts. Management is at the center of the Juniper Connected Security strategy and helps organizations secure every point of connection on their network to safeguard users, data and infrastructure.

Organizations can secure their architecture with consistent security policies across any environment—on-premises, cloud-based, cloud-delivered, and hybrid—and expand zero trust to all parts of the network from the edge all the way into the data center and to the applications and microservices. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

Juniper meets our customers where they are on their journey, helps them leverage their existing investments, and empowers them to transition to their preferred architecture at a pace that is best for business by automating their transition with Security Director Cloud.

Figure 1: Security Director Cloud Architecture

The Security Director dashboard provides customizable, information-rich widgets offering visually intuitive displays that report security device status at a glance. A pallet allows you to easily navigate between firewall, threat, intrusion prevention system (IPS), application, throughput, and device-related information to create a customized view of the SRX Series firewall environment.

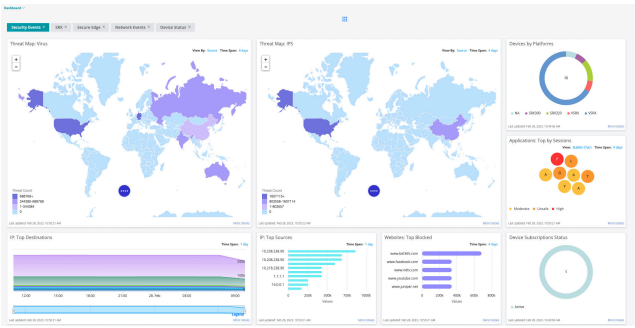

Figure 2: Security Director Dashboard

You can quickly determine which SRX Series devices have generated the most alarms or consume the most CPU cycles or RAM for a specific time period through the dashboard.

By drilling down on widgets, administrators can sort and search various events to effortlessly obtain detailed information such as top viruses blocked, top destinations, top sources, and other details to ensure the network is safe.

Security Director is an innovative solution for managing the application, user, and IP environments. Network administrators can choose between different views to see how applications and users affect the network, observe bandwidth utilization levels, or determine the number of sessions created. Admins can view granular usage details, such as the riskiest applications. Top talkers are easy to identify and remediate. You can also compare different time frames and determine when utilization is typically at its peak.

With most security management solutions, administrators must run a report or open several tabs to find the applications or users they want to manage. Then they must manually create the required firewall rules, determine where to place them, and hope they don't conflict with any existing rules, creating a host of new problems. This task is an exceptionally tedious, time-consuming, and error-prone process.

Security Director is extremely user-friendly and does not require users to run multiple reports, open multiple tabs, and manually analyze the data to find answers. Instead, Security Director allows administrators to quickly find crucial answers, at a glance, without digging through reports.

Using the actionable intelligence that Security Director provides, administrators can select one or more applications or user/user groups from the Application Visibility or User Visibility charts, then simply select "Block." Security Director automatically creates the requested rule or rules and deploys them in the optimal location within the rules base. It helps avoid anomalies and takes the guesswork out of managing the application and user environment.

Security Director also provides actionable intelligence when it comes to threat mitigation. For example, the Threat Map widget shows the number of IPS events detected per geographic location, giving you immediate awareness of threat activity and providing the means to remediate with one click.

Juniper Secure Edge

Juniper Secure Edge secures workforces anywhere with the fast, reliable, and secure access they need. Delivers full-stack SSE capabilities, including FWaaS, SWG, CASB with DLP, ZTNA, and advanced threat protection to protect access to web, SaaS, and on-premises applications and provide users with security that follows them wherever they go. Juniper meets customers where they are and takes them where they want to go by leveraging what they have and extending their zero-trust initiatives to a cloud-delivered architecture without breaking the bank or their ops team.

Juniper Secure Edge, managed by Security Director Cloud, uses a single policy framework that enables security policies to be created once to follow users, devices, and data wherever they go. Customers don't have to start from scratch when adopting cloud-delivered security. With our three-click wizard, customers can easily leverage existing campus edge policies and translate them into an SSE policy. Because it uses a single policy framework regardless of the deployment model, Secure Edge applies existing security policies from traditional deployments to its cloud-delivered model in just a few clicks, reducing misconfigurations and risk.

Whether securing remote users, campus and branch locations, private cloud, public cloud, or hybrid cloud data centers, Juniper provides unified management and unbroken visibility across all architectures. This makes it easy for ops teams to easily and effectively bridge their current investments with their future architectural goals, including SASE. Customers can manage security anywhere and everywhere, on-premises, in the cloud, and from the cloud, with security policies that follow users, devices, and data wherever they go, all from a single UI.

Users have fast, reliable, and secure access to the data and resources they need, ensuring great user experiences. 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.

Juniper Secure Edge provides consistent security policies that follow the user, device and data without having to copy over or recreate rule sets. It's easy to deploy cloud-delivered application control, intrusion prevention, content and Web filtering, and effective threat prevention without breaking visibility or security enforcement.

Juniper has been consistently validated by multiple third-party tests as the most effective security technology on the market for the past four years, with 100% security efficacy across all use cases.

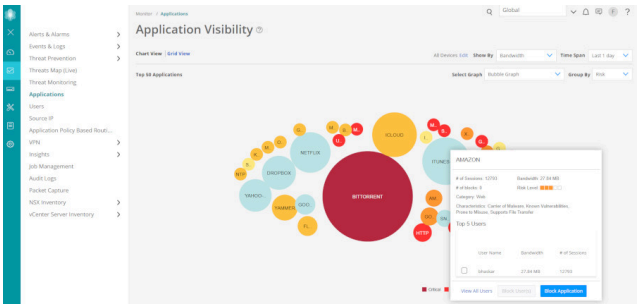

Figure 3: Application Visibility Dashboard

Security Director Insights

Security Director Insights expands end-to-end visibility by correlating and scoring threat events across the complete security stack. It offers a timeline view mapped to the MITRE attack framework so administrators can focus on the highest-priority threats. It unifies visibility across the network by correlating threat detection information, including detections from other vendor products, and enables one-touch mitigation to address gaps in defense quickly.

Security Director Insights empowers organizations to automate threat remediation and microsegmentation policies across the entire network with Security Director's built-in orchestration.

Figure 4: Security Director Insights Dashboard

Security Director Insights collects and automatically correlates data across multiple security layers—email, endpoint, server, cloud workloads, and network—so threats are detected faster, and security teams can improve investigation and response times. It also uses mitigation rules to prevent future attacks.

With Security Director Insights, customers can:

- Understand when and where an attack is happening by using it to correlate and prioritize security events from multiple security solutions across various parts of the network.
- Use custom threat and incident scoring so that security teams respond to and can mitigate attacks that have the potential to do the most harm to the business.
- Mitigate active threats across the network—on Juniper SRX Series firewalls—with one click.

Customers can use Security Director Insights to track attack indicators across their networks, from client to workload, regardless of which vendor product in their environment made the detection.

In Security Director, Policy Enforcer provides simplified user intent-based threat management policy modification and distribution tool.

Security Director provides automated enforcement and policy orchestration that allows updated security policies to deploy across Juniper SRX firewalls. The software helps automate threat remediation and microsegmentation policies across your entire network.

An intuitive user interface within Security Director allows administrators to control and modify network elements, enforcement groups, threat management services, and profile definitions.

Using Policy Enforcer, Security Director automatically updates policies based on the threats that Juniper Advanced Threat Prevention (ATP) identified. Additionally, SecIntel feeds are also available with the Policy Enforcer integration. Policy Enforcer distributes updated policies to enforcement points such as firewalls, ensuring real-time network protection.

Firewall Policy Analysis

With Firewall Policy Analysis, you can gain visibility into network anomalies by scheduling reports showing shadow or redundant firewall rules. Firewall Policy Analysis makes recommendations to fix all reported issues and uses automation to optimize your rule base.

Firewall Policy Analysis eliminates the need to run a monthly or quarterly anomaly report and fix all issues manually. You run the report once, and Security Director will adapt.

Table 1. Security Director Features and Benefits

Features	Description	Benefits
Secure Edge	Delivers full-stack Security Service Edge (SSE) capabilities, including FWaaS, SWG, CASB with DLP, ZTNA, and advanced threat protection to protect access to web, SaaS, and on-premises applications and provide users with security that follows them wherever they go.	Enables administrators to seamlessly secure their remote workforce with consistent security policies that follow the user wherever they go.
Security Director Insights	Collects and automatically correlates data across multiple security layers—email, endpoint, server, cloud workloads and network—so threats are detected faster, and security teams can improve investigation and response times. Prevents future attacks with mitigation rules.	• Understand when and where an attack is happening by using it to correlate and prioritize security events from multiple security solutions across various parts of the network. • Use custom threat and incident scoring so that security teams respond to and can mitigate attacks that have the potential to do the most harm to the business. • Mitigate active threats across the network—on SRX Series firewalls, Switches, wired and wireless access points driven by Mist AI, along with third-party solutions—with one click.
Policy Enforcer	Creates and centrally manages security policies through a user intent-based system, evaluating threat intelligence from multiple sources while dynamically enforcing policies in near real-time across the network. Enforces threat management policies at firewalls and access switches, aggregating threat feeds from Advanced Threat Prevention Cloud, SecIntel, and on-premises custom threat intelligence solutions with allow list and blocklist support.	• Reduces the risk of compromise by eliminating stale rules and automatically updating enforcement based on network threat conditions. • Improves protective posture by quarantining and tracking infected hosts. • Allows security practitioners to focus on maximizing security rather than writing tedious policy rules.
Firewall policy analysis	Provides the ability to schedule reports that show shadow or where redundant firewall rules are and recommends actions to fix all reported issues.	Allows administrators to maintain an efficient firewall rule base by quickly identifying ineffective and unnecessary rules.
Firewall rule placement guidance	Upon creating a new rule, analyzes the existing firewall rule base to recommend optimal position and application.	Significantly reduces shadowing rules.
Metadata-based policies	Enables administrators to create object metadata-based user-intent firewall policies.	Simplifies policy creation and maintenance workflows. In addition to making policies more readable from a user intent perspective, this feature streamlines firewall troubleshooting.
Dynamic policy actions	Enables security administrators to initiate different actions, including firewall, logging, IPS, URL filtering, and Antivirus, among others, under different conditions.	Reduces the time required to adjust the organization's security posture under different conditions and streamlines threat remediation workflows.
Firewall policy hit count	Shows hit counts for each firewall via meters and filters that display which rules are hit the least. Security Director also can keep a lifetime hit count.	Allows administrators to assess each firewall rule's effectiveness and quickly identify unused rules, resulting in a better-managed firewall environment.
Live threat map	Displays where threats originate in near real-time and allow you to take action to stop them.	Provides near-real-time insight into network-related threats. Allows you to block traffic going to or coming from a specific country with a single click.
Security Assurance	Automate security policies across the network, including firewalls and routers, for accurate enforcement, consistent security, and compliance.	Guarantee that security rules are always placed correctly for intended effectiveness.
Innovative application visibility and management	Provides an easy and intuitive way to see which applications use the most bandwidth, have the most sessions, or are most at risk. Know which users are accessing non-productive applications and by how much. Top talkers are displayed in an easy-to-understand manner. Block applications, IP addresses, and users with a simple mouse click.	Delivers greater visibility, enforcement, control, and protection over the network.
Simplified threat management	Reports where threats are originating and where they are going via a global map. Blocking a country is easy; simply mouse over the country to take action.	Provides insight needed to manage network-related threats effectively. Allows you to block traffic going to or coming from a specific country with a single click.
Snapshot support	Allows users to snapshot, compare, and roll back configuration versions.	Simplifies configuration changes and allows recovery from configuration errors.
Policy lifecycle management	Provides the ability to manage all phases of security policy lifecycles, including creating, deploying, monitoring, remediation, and maintenance.	• Enables central control over stateful firewall, AppFW, URL filtering, anti-virus, IPS, VPN, and NAT in one Security Director management console. • Eases administration by unifying common policy tasks within a single interface. • Reduces errors by enabling the reuse of policies across multiple devices.
Drag-and-drop	Allows firewall, IPS, and NAT rules to be reordered by simply dragging them to a new location.	Enables firewall, IPS, and NAT objects to be added or copied by dragging them from one cell to another or from a pallet located at the bottom of the policy table.
VPN auto-provisioning and import	Simply tell Security Director which VPN topology to use and which devices you want to participate in the topology, and Security Director will auto-provision the tunnels. If you have an existing Juniper VPN environment, Security Director can import the VPNs to provide an easy and effective way to manage them.	Makes pre-existing SRX Series firewall VPNs easier to manage.
Role-based access for policies and objects	Allows devices, policies, and objects to be placed within domains and assigns read/write permissions to a user.	Provides customers a way to segment administrative responsibility for policies and objects.
REST APIs for automation	Provides RESTful APIs used in conjunction with automation tools.	Automates configuration and management of physical, virtual, or containerized SRX Series firewalls.

Features	Description	Benefits
Logging and reporting application	Enables logging and reporting.	• Displays rules and events in the same window • Allows the administrator to easily shift views from logs to corresponding rules and vice versa Direct access to Security Director policies and objects: • Role-based access control (RBAC) • Event viewer for events aggregation and filtering • Dashboard with customizable graphs • Reports generated and automatically sent via email • Email alerts are automatically generated based on threshold SRX Series health monitoring - CPU utilization - Memory utilization - VPN monitoring System log forwarding to security information and event management (SIEM)

Ordering Information

To order Juniper Security Director and access software licensing information, please visit the How to Buy page at https://www.juniper.net/us/en/how-to-buy/form.html.

Files uploaded to the cloud for processing are destroyed afterward to ensure privacy. The Juniper Networks privacy policy can be found on the product Web portal at https://www.juniper.net/us/en/privacy-policy.html

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit https://www.juniper.net/us/en/products.html.

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.

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

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700

Juniper Networks | Driven by Experience™