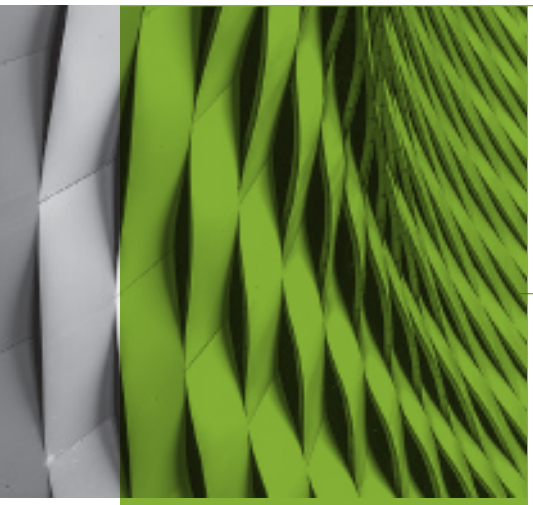

# JUNOS SPACE SECURITY DIRECTOR

## Product Overview

*In today's complex environment, network security management can become overly time consuming and prone to error if management solutions are slow, unintuitive, or restricted in their level of granularity, control, and visibility. Junos Space Security Director provides security policy management for all physical, logical, container, and virtual firewalls (SRX Series Services Gateways) through an intuitive, centralized, web-based interface that offers enforcement across emerging and traditional risk vectors.*

*With the addition of Policy Enforcer, Security Director automatically updates policies based on threats identified by Advanced Threat Prevention Cloud, as well as those found by on- premises threat intelligence solutions. Updated policies are then distributed to enforcement points such as firewalls, switches, and wireless solutions, ensuring up-to-the-minute network protection.*

## Product Description

Juniper Networks® Junos® Space Security Director, an application that runs on the innovative, intuitive, and intelligent Junos Space Network Management Platform, provides detailed visibility into application performance, reducing risk while enabling users to move quickly from "knowing" something is wrong to "doing" something to fix the problem.

Providing extensive scale, granular policy control, and policy breadth across the network, Security Director helps administrators manage all phases of the security policy lifecycle for stateful firewall, URL filtering, anti-virus, intrusion prevention, application firewall (AppFW), VPN, and Network Address Translation (NAT) through a centralized web-based interface. Security Director reduces management costs and errors by providing actionable intelligence, automation, efficient security policy, intuitive workflows, and a powerful application and platform architecture, allowing users to detect threats as they happen and apply remedial actions in real time.

Policy Enforcer simplifies and automates the process of deploying up-to-the-minute enforcement. An intuitive user interface gives administrators the flexibility to selectively control and modify network elements, enforcement groups, threat management services, and profile definitions.

Security Director Insights expands end-to-end security visibility by correlating and scoring threat events across many different security solutions, offering up a timeline view to focus on the highest priority threats. One-click mitigation is available to block active threats across the network.

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, which can be used to create a customized view of the Juniper Networks SRX Series Services Gateways firewall environment.

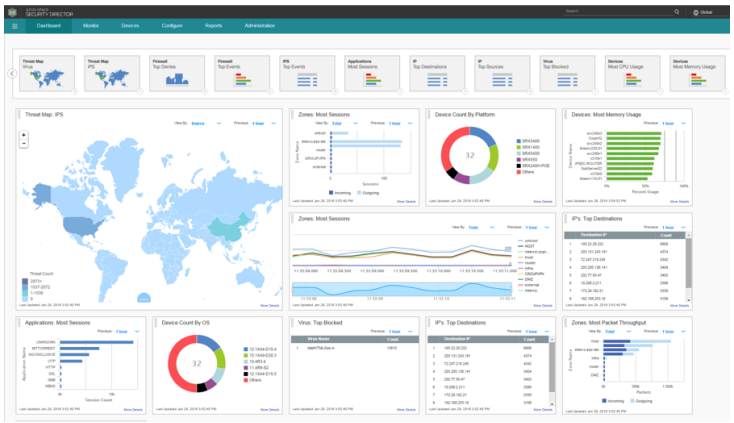

*Figure 1: Junos Space Security Director dashboard*

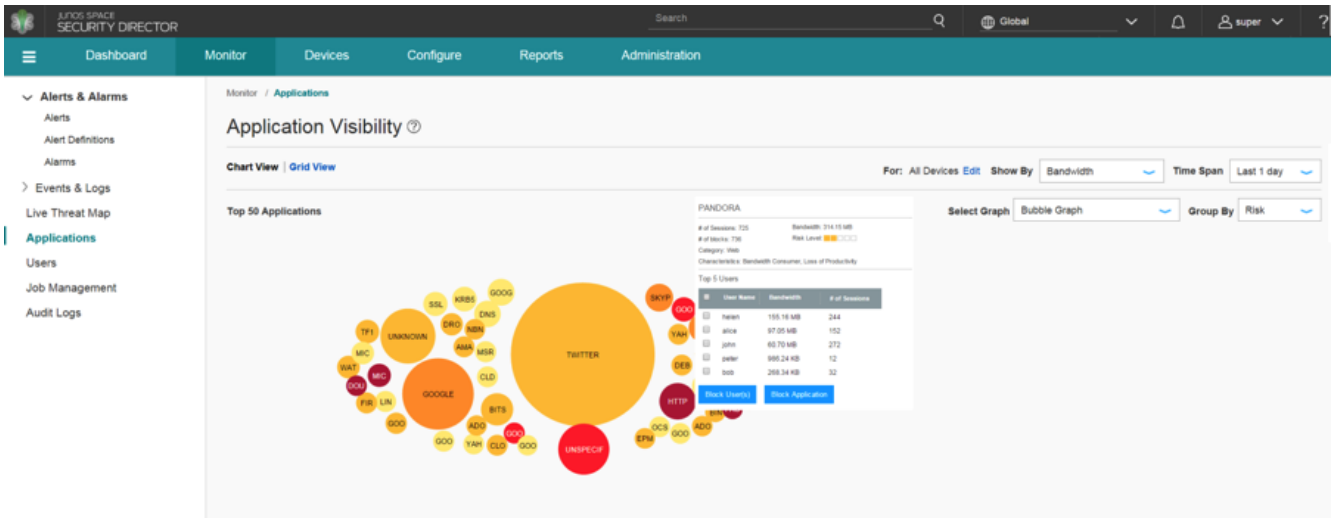


*Figure 2: Application Visibility dashboard feature*

Through the dashboard, you can quickly determine which SRX Series devices have generated the most alarms, or which have consumed the most CPU cycles or RAM for a specific time period. A Threat Map widget shows the number of IPS events detected per geographic location, giving you industry-leading information gathering and remediation capabilities.

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 that can be used to ensure that the network is safe.

Security Director offers the industry's most innovative solution for managing the application, user, and IP environment. Network administrators can choose between three different views to see how applications and users are affecting the network, observe bandwidth utilization levels, or determine the number of sessions created. Granular usage details, such as which applications are the riskiest, can be viewed. Top talkers are easy to identify and remediate. Different time frames can also be compared to determine when utilization is typically at its peak.

Unlike other products, Security Director does not require users to run multiple reports or open multiple tabs and then manually analyze the data to determine who is using which applications and to what extent. Instead, Security Director allows administrators to easily correlate users to applications by simply selecting an application icon or a user/user group icon.

Blocking traffic from a specific country is also easy and intuitive. Using Security Director's Live Threat Map, it's not only possible to see where threats are originating, you can also block traffic coming from or going to a selected geographic location.

## Actionable Intelligence

With most security management solutions, administrators have to 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 those rules, and hope they don't conflict with any existing rules, thereby creating a host of new problems. This is a tedious, time-consuming, and error-prone process.

Security Director offers an Actionable Intelligence feature that eliminates the need to engage in this antiquated exercise. Using Actionable Intelligence, 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, avoiding any anomalies and taking the guesswork out of managing the application and user environment.

Actionable Intelligence is even more powerful when used in conjunction with Juniper Secure Analytics (JSA) or IBM's QRadar SIEM solutions. When malicious activity is detected and a warning is generated, a "Block" button available in the Security Director JSA/QRadar application allows you to automatically create and deploy a firewall rule in the optimal location within your rule base to remediate the offending IP addresses. Working together, Security Director and the SIEM solution help you more effectively protect your network.

Table 1. Junos Space Security Director Features and Benefits

| Features | Description | Benefits |
|---|---|---|
| **Security Director Insights** | Provides the tools needed to ingest, prioritize, and correlate security events across multiple security solutions. Integrated with Juniper ATP Cloud, Security Director Insights provides one-click mitigation, enabling devices with active threats to be added to the ATP Cloud infected host feed. This list can be used to block active threats across Juniper Networks SRX Series Services Gateways and Juniper Networks EX Series and QFX Series switches, along with third-party wired and wireless solutions. Security Director Insights normalizes security alerts using threat scoring and displays them in a timeline, allowing Security Operations Center (SOC) analysts to focus on the highest priority threats. | • Reduce the number of alerts across disparate security solutions.<br>• Quickly react to active threats with one-click mitigation<br>• Improve the SOC teams' ability to focus on the highest priority threats. |
| **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 allowlist and blocklist support. | • Reduces risk of compromise by eliminating stale rules and automatically updating enforcement based on network threat conditions.<br>• Improves protective posture by quarantining and tracking infected hosts.<br>• Allows security practitioners to focus on maximizing security rather than writing tedious policy rules. |
| **SIEM integration** | With a single mouse click, Juniper Secure Analytics and IBM QRadar work with Security Director to block malicious IP addresses contained within an offense. | • Increases speed at which malware can be blocked.<br>• Reduces the expertise needed to harness the power of IBM QRadar and Juniper Secure Analytics products. |
| **Firewall policy analysis** | Provides ability to schedule reports that show which firewall rules are shadowed or redundant and recommends actions to fix all reported issues. | Allows administrators to maintain an effi-cient firewall rule base by easily identifying ineffective and unnecessary rules. |
| **Firewall rule placement guidance** | Upon creation of a new rule, analyzes 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 Anti-virus 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, as well as filters that display which rules are hit the least. Security Director also has the ability to keep a lifetime hit count. | Allows administrators to assess effectiveness of each firewall rule and quickly identify unused rules, resulting in a better managed firewall environment. |
| **Live threat map** | Displays where threats are originating in near real time and allows 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. |
| **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 address, 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 effectively manage network-related threats. 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 life cycle management** | Provides ability to manage all phases of security policy lifecycles, including create, deploy, monitor, remediate, and maintain. | • Enables central control over stateful firewall, AppFW, URL filtering, anti-virus, IPS, VPN, and NAT in one Junos Space Security Director management console.<br>• Eases administration by unifying common policy tasks within a single interface.<br>• Reduces errors by enabling 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. |

| Features | Description | Benefits |
|---|---|---|
| **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 that can be used in conjunction with automation tools. | Automates configuration and management of physical, logical, or virtual SRX Series firewalls. |
| **Logging and reporting through Junos Space Log Director application** | Enables integrated logging and reporting. | Tight coupling with Junos Space Security Director:<br>• Displays rules and events in same window<br>• Allows administrator to easily shift views from logs to corresponding rules and vice versa<br>Direct access to Junos Space Security Director policies and objects:<br>• Role-based access control (RBAC)<br>• Event viewer for events aggregation and filtering<br>• Dashboard with customizable graphs<br>• Reports generated and automatically sent via e-mail<br>• E-mail alerts automatically generated based on threshold<br>SRX Series health monitoring:<br>• CPU utilization<br>• Memory utilization<br>• VPN monitoring<br>System log forwarding to security information and event management (SIEM) |

## 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 www.juniper.net/us/en/products-services.

## Ordering Information

### Junos Space Appliance

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

| Product Number | Description |
|---|---|
| JA2500-A-BSE | Base Appliance |

### Junos Space Security Director

Junos Space Security Director software is licensed based on the number of security devices you will manage. For example, if you will be managing 100 SRX Series Services Gateways, then you would purchase a single license for JS-SECDIR-100.

| Product Number | Description |
|---|---|
| JS-SECDIR-5 | Junos Space Security Director license for 5 devices |
| JS-SECDIR-10 | Junos Space Security Director license for 10 devices |
| JS-SECDIR-100 | Junos Space Security Director license for 100 devices |

## 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
**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