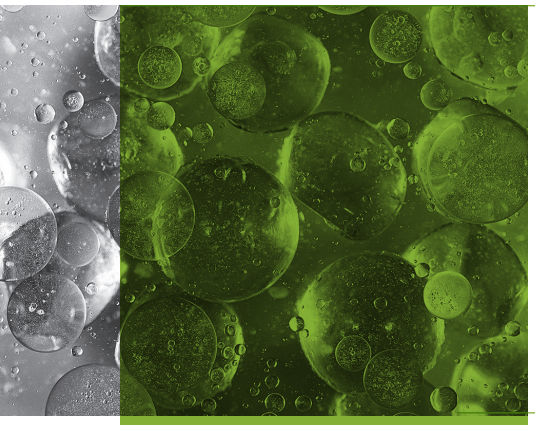

SECURE YOUR NETWORK SMARTER AND FASTER

Unmatched visibility, management, and security intelligence

Challenge

Network managers struggle to gain network-wide visibility into and control over applications, user activities, and potential threats due to the large number of point products, a lack of data correlation and actionable intelligence, and the number of steps required to take remedial action.

Solution

Junos Space Security Director offers an intuitive and modern interface, powerful actionable security intelligence, and automated workflows, allowing administrators to quickly identify vulnerabilities, perform forensic analysis, automate compliance, and remediate threats faster across all firewalls deployed throughout the enterprise.

Benefits

- *Detects and remediates sophisticated attacks as early as possible with actionable intelligence*
- *Reduces the expertise needed to detect and manage threats and vulnerabilities*
- *Reduces risk of human error and enhances operational efficiency through superior automation*
- *Provides massive scalability for managing thousands of firewalls*

In today's complex and constantly changing environment, administrators need complete visibility into network behavior to maintain a robust security posture. Attackers are finding increasingly creative ways to infiltrate networks, and the architectures employed by many organizations make it difficult to acquire actionable cyber threat intelligence, detect malicious activity, and enforce security policies against these attacks. The ability to see and understand threats across the network and take immediate remedial action is essential, if security teams are going to keep their organizations safe. Juniper Networks® Junos Space® Security Director, with its tight integration with the Juniper Secure Analytics (JSA) platform, provides correlated and actionable information on applications, users, and threats, allowing you to quickly enforce security policies, neutralize risks, and make smarter and faster security decisions.

The Challenge

Today's networks are borderless, supporting a growing number of applications and millions of connections across wide geographic areas. This widespread deployment makes it difficult to effectively and completely monitor and block high-risk behavior and applications, eliminate policy anomalies, reduce noise, and take immediate remedial action when attacks are detected. Organizations also realize that network complexity, a lack of real-time security intelligence, and minimal or no integration with security solutions render traditional security information and event management (SIEM) offerings ineffective, putting them at tremendous risk. To regain control, enterprises need fully integrated security intelligence platforms that are scalable, easy to use, and offer a single point of management across all security elements. These high-performance platforms need to be able to effectively analyze large data sets and provide actionable intelligence to reduce business risk, protect critical data from unauthorized access, and quickly remediate threats while improving user productivity and operational efficiency.

Junos Space Security Director Solution

The Juniper Connected Security framework, powered by Junos Space Security Director, centrally manages all security policies for physical and virtual Juniper Networks SRX Series Services Gateways deployed at headquarters or in the cloud throughout the infrastructure. Both physical SRX Series appliances and the vSRX Virtual Firewall register with a single instance of Security Director. Once policies

Junos Space Security Director Features and Benefits

Table 1: Junos Space Security Director Visibility and Management Benefits

Capabilities	Features	Benefits
Greater visibility with simplified and intuitive management	• Customizable dashboard • Application, user, IP bubble charts, and heat map • Live threat map • Visibility into application, user, and IP behavior and activity • Mobile app for Google's Android and Apple's iOS systems	• Visibility, simplified management, and actionable security intelligence on applications, users, IPs, and threats help network managers make better security decisions. • Simple user interface allows even new users to quickly become proficient. • Remote mobile monitoring capabilities provide visibility and enhanced flexibility.
Faster detection and remediation with actionable intelligence	• Block applications, users, or IPs with one click • Fully integrated policy creation with monitoring and management	• Action-oriented design allows users to detect risky applications and threats across the network as they happen and apply immediate remedial action with a single click.
Enhanced operational efficiency through superior automation and shorter learning curves	• Single security intelligent rule wizard • Automated workflows for updating policy enforcement based on network threat conditions	• Reduces risk of compromise and human error by allowing administrators to focus on maximizing security and accelerating operations with a simple, concise rule set. • Tells policy creators the optimal position for firewall rules.
Massive scalability	• Manage up to 15,000 devices	• Scalable and automated solution with a single centralized management interface provides actionable intelligence to reduce business risk.
Unmatched security intelligence	• Log analytics • Threat analytics • Compliance management • Vulnerability management • Risk management	• Uses state-of-the-art machine learning and data mining tools. • Offers the best search speed in the industry when correlating petabytes of data across hundreds of nodes. • Enables more effective threat management while producing detailed data access and user activity reports.

are pushed to select devices, data is synchronized across all firewalls no matter where they are deployed. Security Director allows users to centrally manage thousands of firewalls, physical and virtual, providing complete visibility into and control over the complete enterprise.

Regardless of the type of deployment, large enterprises typically have multiple firewalls deployed throughout their network. Unfortunately, minor differences, complexities, and inconsistencies between individual devices make achieving unified visibility into and control over these firewalls a challenge. Junos Space Security Director delivers the tools required to regain control over the secure enterprise.

Solution Components

Junos Space Security Director

Juniper's scalable and intuitive Junos Space Security Director enables network administrators to make precise security decisions by providing complete end-to-end visibility into applications, users, and threats in their network. Through its comprehensive network view, rich security feature set, and quick actionable intelligence, Security Director allows network managers to quickly identify risky applications and immediately take necessary remedial actions, as well as quickly create simplified security policies that improve user safety and productivity.

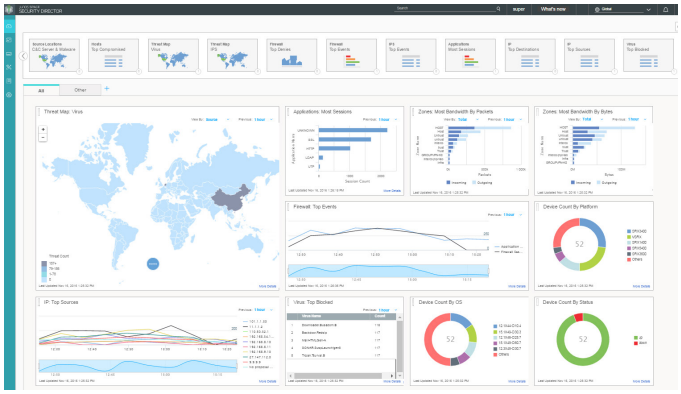

Figure 1: Junos Space Security Director

Junos Space Security Director 19.1 runs on Junos Space 19.1 and later releases. To learn more about Security Director, visit www.juniper.net/us/en/products-services/security/security-director.

Cloud Advanced Threat Prevention

A cloud-based service that is integrated with Junos Space Security Director and SRX Series firewalls, Juniper Cloud Advanced Threat Prevention constantly adapts to an ever-changing threat landscape, using a sandboxing technique to perform dynamic data analysis and protect against sophisticated "zero-day" threats.

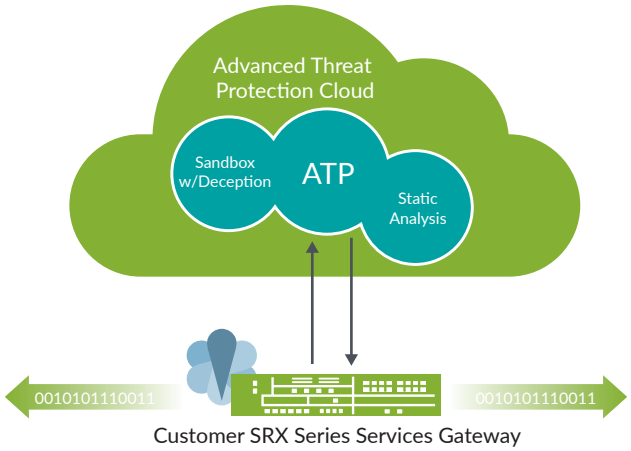

Figure 2: Cloud Advanced Threat Prevention

To learn more about Juniper ATP products, visit www.juniper.net/us/en/products-services/security/advanced-threat-prevention/.

Juniper Networks Secure Analytics

JSA Series Secure Analytics Appliances combine, analyze, and manage an unparalleled set of surveillance data—network behavior, security events, vulnerability profiles, and threat information—empowering companies to automate the analysis of large data sets and efficiently manage business operations on their networks from a single console. JSA Series platforms, key components of the Juniper Connected Security framework, also integrate with Security Director, providing real-time threat intelligence for quick threat remediation and direct policy enforcement across the network. The JSA Series solutions, offered in both physical and virtual form factors, include JSA SIEM, Log Manager, Vulnerability Manager, Risk Manager, and Flow Collectors.

To learn more about JSA Series Security Analytics, please visit www.juniper.net/us/en/products-services/security/secure-analytics.

SRX Series Services Gateways and vSRX Virtual Firewall

Offering a broad range of options from all-in-one, integrated physical and virtual security networking devices to highly scalable, chassis-based data center solutions, SRX Series Services Gateways and vSRX virtual firewalls can protect enterprise data center and service provider networks of any size. The SRX Series provides high-performance security with advanced, integrated threat intelligence, delivered on the industry's most scalable and resilient platform. SRX Series gateways set new benchmarks with 100GbE interfaces and feature Express Path technology, which enables up to 2 Tbps performance for the data center. Junos Space Security Director enables you to centrally manage all physical and virtual SRX Series firewalls and enforce security policies across your network.

To learn more about SRX Series Services Gateways and vSRX virtual firewalls, visit www.juniper.net/us/en/products-services/security/srx-series/.

Use Cases

Junos Space Security Director can be used in different deployment scenarios including: enterprise branch offices; enterprise regional offices; public cloud/hybrid cloud; and data center/private cloud. The following sections detail a number of specific use cases and describe how Security Director helps businesses gain complete control over their enterprise-wide security.

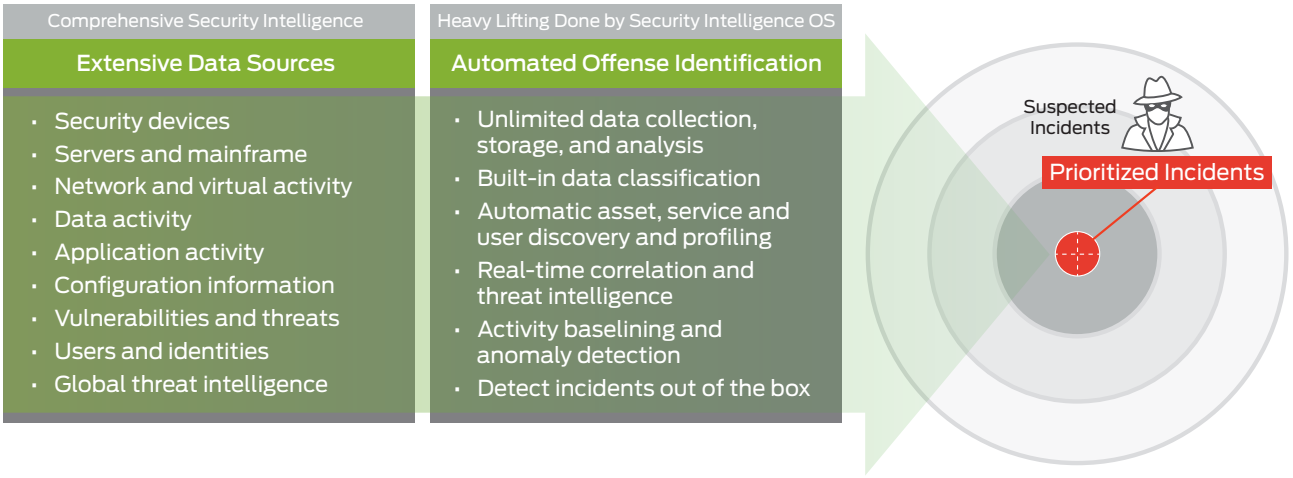

Figure 3: JSA Series Secure Analytics in a nutshell: automated offense identification

Use Case 1: Monitor Applications

Security Director's Application Visibility view provides information on bandwidth consumption, session establishment, and the risks associated with applications. This analysis yields useful security management information such as abnormalities that can lead to data loss, bandwidth hogging, time-consuming applications, and personal applications that can increase business risks. By understanding the overall application risk posture and the way resources are being used, it is possible to effectively control application consumption and secure the network in a way that is much smarter and faster.

Efficiently Manage Applications in Your Network

Seasoned administrators don't have to devote much time or effort to optimize application access and consumption. Automation features built into Security Director help less experienced administrators perform like veterans, allowing you to manage access and usage to effectively block applications and users with confidence.

Quickly Identify and Block Risky Applications

The following example describes the process of identifying high-risk applications and will show how to quickly and easily take immediate remedial action to reduce business risk. You will be able to understand the overall risk posture of your application environment and see which applications are most popular.

The Security Director IP Visibility view allows you to pinpoint network bottlenecks and bandwidth hogs, and take quick remedial action when network usage is exceeded. Simply log in to Security Director and navigate to the Application Visibility view under Monitor > Applications (Figure 4).

Monitor Applications Running in Your Network

Simply glancing at the innovative application view lets you quickly see risky and non-risky applications currently in use. Generally speaking, bigger means "more" and red means "bad." Figure 4 shows that Bittorrent, Kaspersky-update, and Oracle are using the most bandwidth and are very popular.

Once you select a time range, all data presented in the view is refreshed automatically, complete with device-level visibility on network-wide application traffic that lets you effectively manage security for all or parts of the network.

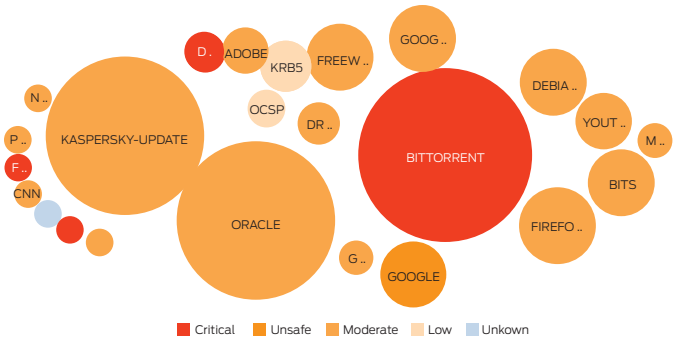

Figure 4: Application Visibility view

Identify Applications with the Highest Risk

A color-coded bubble graph allows you to quickly identify the most risky applications currently in use. You can then immediately isolate and block these applications to eliminate the risk to your network.

Figure 5 shows that Bittorrent, Doubleclick, and Facebook-Access pose the greatest risk to your environment.

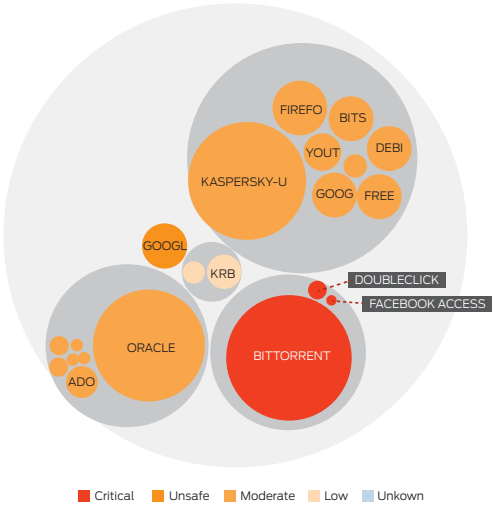

Figure 5: Risky application view

Quickly Block High-Risk Applications

After identifying high-risk or nonproductive applications, you can quickly block a risky application or a set of risky applications for a specific user or group of users.

Simply click the blue "Block Application" button and the system does all the work, allowing you to fix the issue quickly, intelligently, and confidently by eliminating the risk of human error.

Monitor and Control User-Level Application Consumption

To comply with productivity standards and organizational policies, it is important to identify top users consuming the most application bandwidth.

Simply click on the application bubble and Security Director will automatically correlate application and user information so you can immediately see which users are associated with this application—there is no need to sort, filter, search, or drill down to learn user-level application details.

In this example (Figure 6), Tina and Frank are using the most bandwidth with the largest number of sessions. To block them, simply check their names and click on "Block User(s)" tab.

To see the complete list of users for this application, click on "View All Users." You can then sort the resulting list based on different characteristics like bandwidth or number of sessions. To block the application for users in the detailed view, simply select the users and click on the "Block User" tab.

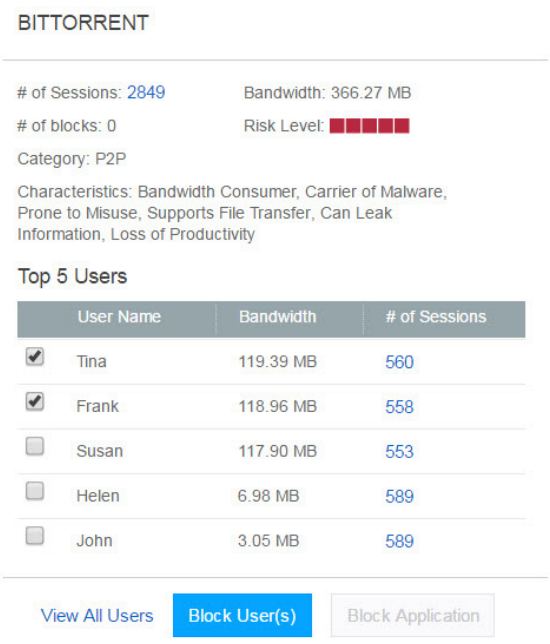

Figure 6: Top 5 application users

Use Case 2: Monitor Users

Security Director provides complete visibility into application users, helping you reduce business risk and allowing you to move quickly from knowing to doing by applying remedial actions in near real time. Analyzing user application consumption yields useful information such as which applications are most popular with users, who are the top bandwidth consumers, and which applications are used by a specific user. Abnormal user activities can lead to data loss, bandwidth hogging, poorly performing applications, and personal applications that can increase business risk. By understanding the overall business risk posture and how resources are being used, you can effectively control application consumption and secure your network quickly and smartly.

Improve Organizational Productivity and Reduce Human Errors

Security Director's user view reduces business risk, helping you comply with your organization's productivity standards without having to navigate multiple tabs and reports. Security Director lets you quickly identify and block nonproductive users and risky applications.

Monitor User Activity in Your Network

Glancing at the innovative User view helps you quickly identify which users are consuming the most bandwidth in your network. Once you select a time range, all data presented in the view is refreshed automatically.

If you want to correlate user information with specific applications, simply mouse over a user's bubble to see which applications they are using—no need to sort, filter, search, or drill down.

Efficiently Manage Users in Your Network

Security Director's IP Visibility view lets you pinpoint network bottlenecks and bandwidth hogs and take quick remedial action when network usage is exceeded. Simply log in to Security Director and navigate to the User Visibility view under Monitor > Users (Figure 7).

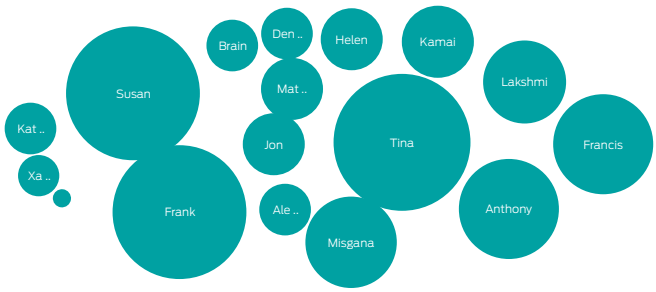

Figure 7: User bubble graph

Quickly Block Users Consuming the Most Bandwidth

To comply with your organization's productivity standards and policies, it is important to monitor applications and identify users consuming the most bandwidth in order to block them.

Figure 8 shows that mousing over Frank on the user bubble graph produces a table of the applications he is using, the amount of bandwidth he is consuming, and the number of

sessions associated with each application. For Frank, Bittorrent is the top application with the most bandwidth consumed: 121.31 MB.

To completely block this user, simply click the blue "Block User" button and the system will do all the work, allowing you to fix this issue quickly and easily.

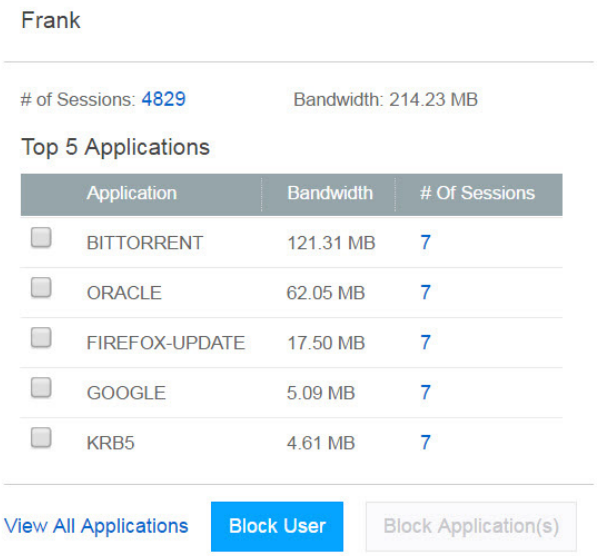

Figure 8: User Top 5 applications consumption

Use Case 3: Monitor Unidentified Traffic in Your Network

If you do not use user verification methods like Lightweight Directory Access Protocol (LDAP) with your firewalls, Security Director will still allow you to monitor and control applications based on source IP address, providing another perspective on application traffic in your network. Security Director provides complete visibility into unidentified network traffic relative to applications, helping you reduce business risk. Analyzing application consumption from source IP addresses in your network yields useful information such as which applications are consumed the most, which are the top IPs with the most bandwidth usage, and which applications are used the most by a specific IP address. By understanding the overall business risk posed by unidentified traffic and the way your resources are being used, you can effectively control resource consumption and secure your network smarter and faster.

Improve Organizational Productivity and Reduce Human Errors

Security Director's Source IP view allows you to reduce business risk and comply with your organization's productivity standards. You can control application consumption and create effective IP-level application policies for requests coming from IP addresses in your network.

Efficiently Manage Unidentified Traffic in Your Network

Security Director allows less experienced network administrators to manage network traffic coming from source IPs that do not have any user names associated with them. Users can effectively block source IPs and applications used by these IPs with confidence by using automation built into Security Director.

The Security Director IP Visibility view allows you to pinpoint network bottlenecks and bandwidth hogs and take quick remedial action when network usage is exceeded. Simply log in to Security Director and navigate to the IP Visibility view under Monitor > Source IP.

Monitor Application Traffic in Your Network

Simply glancing at the innovative Source IP view lets you quickly identify which IPs are consuming the most resources in your network. Once a time range is established, all data is refreshed automatically.

To correlate source IP information with specific applications, simply mouse over the Source IP bubble (see Figure 9) to see which applications are used by this IP—no need to sort, filter, search, or drill down to learn the details.

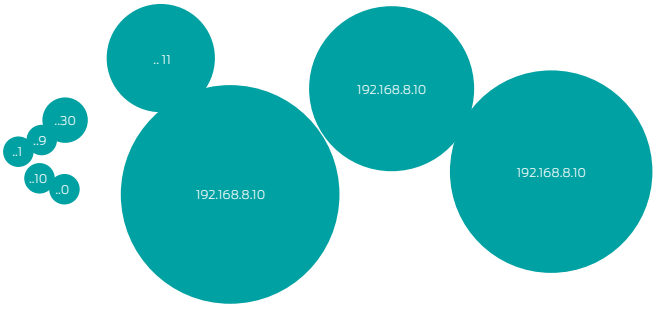

Figure 9: Source IP bubble graph

Quickly Block Source IPs Using the Most Bandwidth

Security Director allows you to quickly identify and block IPs that are consuming the most bandwidth in your environment in violation of corporate productivity standards and organizational policies.

Mousing over source IP address 192.168.8.10 on the Source IP bubble graph reveals a table that shows the source IP, top applications used by the IP address, and the amount of bandwidth consumed and number of sessions associated with each application. As seen in Figure 10, Bittorrent is the top application used by this IP address and has consumed the most bandwidth: 377.85 MB.

To completely block this IP address, simply click the blue "Block IP" button and the system will do the rest, allowing you to fix the issue with a simple mouse click while eliminating the risk of human error.

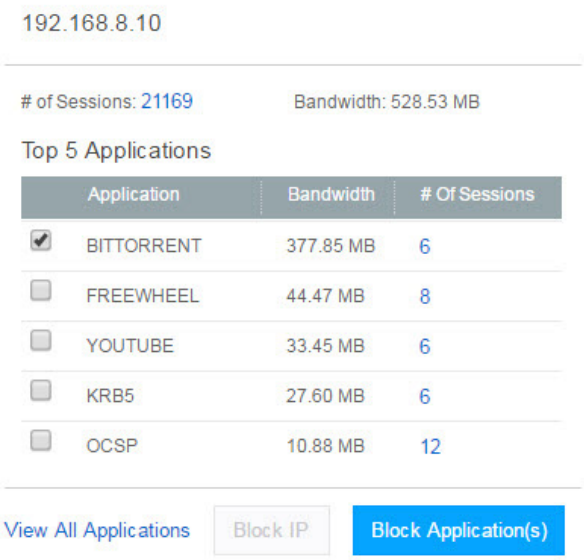

Figure 10: IP address top application consumption

Quickly Identify and Block Nonproductive Application Requests

After identifying which IPs are consuming the most bandwidth, you can quickly block nonproductive applications for that particular IP. Security Director correlates application and IP information; simply mouse over the bubble on the display to immediately see which applications are associated with the selected IP address.

In this example (Figure 10), after mousing over source IP 192.168.8.10 on the bubble graph, you can select Bittorrent and click the "Block Application(s)" button. The system does the rest.

Clicking on "View All Applications" produces a complete list of all applications used by this IP address. Applications can be sorted based on characteristics like bandwidth usage or number of sessions.

To block applications for this IP address from the detailed view, simply select the applications and click on the "Block Application(s)" button.

Use Case 4: Detect and Remediate Threats Faster

Network security monitoring is time-consuming. A slow security management solution gives attackers more time to infiltrate the network and threats more time to spread. Security Director's Threats Map analyzes threat behavior, allowing you to close your network's exposure window. Faster detection and actionable intelligence helps you quickly reduce the risk associated with threats in your environment.

Security Director's Threat Visibility view helps you quickly understand overall business risks and threats in your network and take immediate remedial actions with no need to sort, filter, search, or drill down to learn the details. Log in to Security Director and navigate to the IP Visibility view under Monitor > Threats Map (Figure 11).

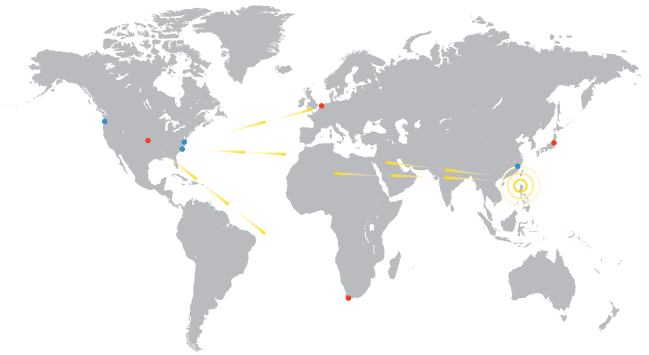

Figure 11: Threat Visibility view

Visualize Geographic Regions for Incoming and Outgoing Threats

Glancing at the innovative Threats Map view helps you quickly see where threats are coming from and going in your network.

Event counts for each attack object can be viewed by clicking a specific geographical location. This is useful for viewing unusual activity that could indicate a possible attack.

If you have deployed firewalls around the world, you can find which countries are launching the most attacks against your firewalls by using the threat map. You can perform further attack analysis by clicking the attack type and viewing the filtered list of events from the Event Viewer.

Identify and Block IPs for Top Attackers

Clicking on any individual source or destination point on the threat map reveals information about threat events, including the number, type, time, source IP, and destination IP.

Figure 12 shows the detail window for China, which reports the number of inbound or outbound threats, the top IPs sending them, and the number of events associated with each IP.

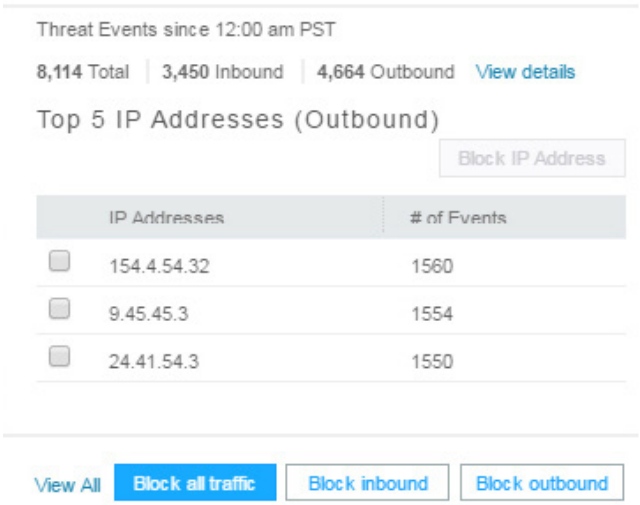

Figure 12: Threat detail window

Blocking Threats Is Quick and Easy

After clicking on a country, it is possible to block all traffic simply by clicking the "Block all traffic" button (Figure 12). Likewise, inbound and outbound traffic can also be blocked. The system does all the work, eliminating the risk of human error.

Quickly Know What Types of Threats You Are Receiving

After clicking on a country, clicking on "View All" will open a side window (Figure 12) that provides additional details on types of threats. Threat types are color-coded; mousing over a country and clicking on "View details" provides details such as:

- Blocked and allowed threat events based on feeds from intrusion prevention system (IPS), antivirus, and antispam engines
- Unsuccessful login attempts for the devices
- Top IP addresses for outbound traffic

Easily Access Details about the Threat

To view all events for a country and get a more detailed view, click on "View all IP addresses" under Threat Events to see the following:

- Intrusion detection and prevention (IDP) attacks detected by the IDP module. Reported attack information includes:
  - Source of attack
  - Destination of attack
  - Type of attack
  - Session information
  - Severity
  - Existing policy information
  - Traffic permitted or dropped
- E-mail spam detected based on blacklist spam e-mails. Reported attack information includes:
  - Source
  - Action: e-mail rejected or allowed
  - Reason for identifying as spam
- Virus attacks detected by the antivirus engine. Reported attack information includes:
  - Source of the infected file
  - Destination
  - File name
  - URL used for accessing the file

Quickly Block Threats from the Detailed View

It is also possible to block all traffic from the Detailed View window by clicking the "Block all traffic" button (Figure 13). Inbound and outbound traffic can also be blocked. The system does all the work, without human intervention.

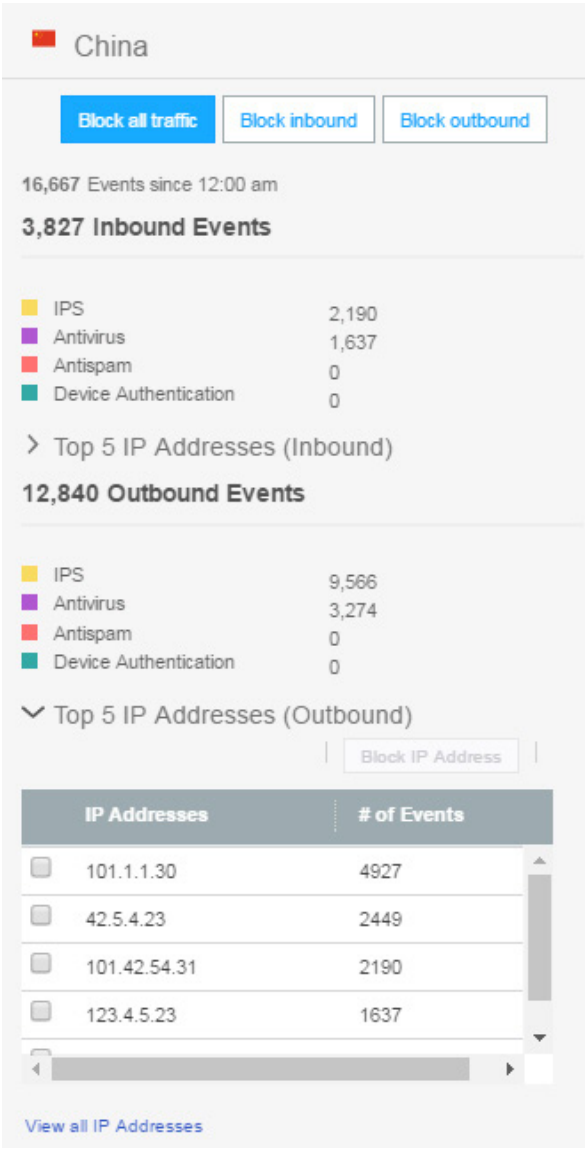

Figure 13: Block all traffic display

Summary—Security Director Returns Control to the Enterprise

Providing extensive scale, granular policy control, and policy breadth across the network, Security Director helps enterprises manage all phases of the security policy life cycle. You can achieve complete visibility into users and applications, which helps you detect and respond to threats in near real time and move from "knowing" to "doing." The tight integration with JSA Series Secure Analytics Appliances makes applying security easier and more effective by automating analysis across all available data and quickly delivering actionable security intelligence that allows organizations to make better security decisions against sophisticated attacks. Security Director reduces management costs and errors by providing actionable intelligence, automation, efficient security policy, intuitive workflows, and a powerful application and platform architecture.

Next Steps

For more information on Junos Space Security Director, please visit us at www.juniper.net/us/en/products-services/security/security-director and contact your Juniper Networks representative.

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