JUNIPER PARAGON AUTOMATION—NETWORK TRUST AND COMPLIANCE

Automated, consistent, and reliable network trust and compliance

Application Note

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Today's networks are both complex and risky. As CSPs watch the complexities multiply, they may not be prepared for the additional risks to the network infrastructure. For example, tampered software and hardware in the network becomes more prevalent, network elements present security risks due to not conforming to trust compliance standards, and infrastructure is vulnerable to disruption and/or manipulation from both internal and external threats.

Juniper® Paragon Automation enables Network Trust and Compliance that confirms and quantifies network trust. The cloud-based, network automation solution continuously monitors network infrastructure to measure trust posture and the level of risk of compliance, vulnerability, and integrity impairments, offering valuable insights into equipment performance and early issue detection.

The Network Trust and Compliance in Paragon Automation allows you to:

- Quantify and demonstrate the trustworthiness of Juniper equipment objectively
- Maximize the reliability and security of Juniper devices
- Identify areas for improvement and optimize device performance over time
- Provide customers with peace of mind and confidence in their network infrastructure
- Streamline compliance processes by automating compliance checks and reporting
- Enhance cybersecurity posture by identifying vulnerabilities and taking proactive measures
- Optimize resource allocation by prioritizing improvements based on trust score insights

Introduction

Network trust is a measurable belief and confidence that the network is safe and reliable. The measurements can be represented as a combined value from historical data and an expected future value that is dynamic and changes over time. Identifying and measuring these values has never been easy, but automation, data analytics, and intelligent software are prepared for the challenge. Network operators are currently faced with many trust-related risks due to too many touch points for proper enforcement. Adding to the security risks are older versions of system software and a lack of firmware updates.

Network vulnerabilities can creep into play and lead to malicious attacks when network operators do not harden devices or perform regular patch updates. Unavailable vulnerability patches, outdated software, and outdated hardware present similar risks when network equipment at the customer premises is not replaced after reaching end of support.

Today, these pressing issues lead to connectivity disruption and outages that result in lost revenue, damage to reputation and trust, as well as declines in overall productivity.

Every CSP needs to trust the network and trust that it is in compliance. This is possible with a solution that:

- Provides valuable insights, benchmarks, and performance tracking to improve network infrastructure reliability and security
- Ensures compliance to the latest requirements and regulatory standards
- Reduces the risk of vulnerabilities
- Improves the cybersecurity posture of the network

Juniper Network Trust and Compliance

Juniper Paragon Automation provides automated, consistent, and reliable Network Trust and Compliance that can be used to verify, confirm, and quantify the trust aspects of the network, making it easier for network operators to run trustworthy networks. It measures the risk of integrity impairment and trust posture of network infrastructure. In parallel, it provides insight and nonintrusive validation of trustworthiness and reliability throughout the network.

While machines cannot demonstrate trust like humans, they can exhibit reliability and accuracy, which inspires confidence and trust in their abilities. The Network Trust and Compliance in Paragon Automation focuses on quantifying the trustworthiness of Juniper equipment and the networks in which they run. It highlights the reliability and trustworthiness of Juniper equipment and offers valuable insights into equipment performance and early issue detection.

With Paragon Automation, compliance checks can be automated, which reduces the risk of human error. Organizations can also demonstrate compliance with regulatory requirements and standards. Vulnerability assessments can be performed with proactive notifications that alert the operations team of known issues and offer guidance for resolution. End-of-life (EOL) dates can also be tracked for hardware and software to maintain security (Figure 1).

Paragon Automation provides an intuitive user interface with easy-to-use dashboards, alarms, and notifications on actionable integrity impairments, trust score graphs, and more. This helps to ensure that your networks stay trustworthy end-to-end. Key features and functionality include:

- A standardized and objective way to evaluate the trustworthiness of a device
- Trust-score calculation (Network Trust Score) based on prerequisite, variable, and reputational factors
- Customizable trust score calculation to suit different use cases and customer requirements
- Integration with compliance standards, vulnerability assessments, and more
- Comparative analysis and benchmarking of devices based on trust scores
- Visual representation of trust scores using graphs and indicators

With a Network Trust Score operators finally have a quantifiable measurement to indicate the level of trust in their networks. The score is calculated on three factor groups:

- Prerequisite: Conditions that must be met to receive a non-zero score
- Variable: Factors that provide a weighted trust contribution
- Reputational: Incremental trust contributions earned over time

Paragon Automation focuses on compliance, vulnerabilities, and integrity use cases. It then calculates a trust score based on these aspects of network trust.

Use Cases	Description
Compliance	Ensure best practice, hardened configuration compliance across the network, and automated analysis of network device compliance based on prepackaged, recommended hardening practices from the Center for Internet Security (CIS)
Vulnerabilities	Understand what Security Incident Response Team (SIRT) issues might be affecting your network and what their remediations might be; newly published SIRTs are automatically updated, keeping you aware of the latest threats and cyberattacks
Integrity	Analyze the EOL status of network hardware and software to simplify life-cycle management, reduce EOL security concerns of EOL devices and software, and decrease support issues
Trust score	Quantify trust with a percentage that allows operators to understand over time whether trust in the network is improving

Paragon Automation provides ready-to-use hardening rules to ensure day zero trust compliance. It can conduct periodic monitoring, auditing, and reporting of the hardware and software elements to ensure there is no deviation from standards. It also ensures that any system changes are applied uniformly and provides suggestions for fixes in case of deviations.

As part of its network trustworthiness monitoring and reporting Paragon Automation applies a deterministic method to establish metrics and measurements to provide a Network Trust Score for devices, or targets. Trust Scores are reported network-wide and on a device per device basis. The method to calculate the score can also be customed to meet organizational requirements and network expectations.

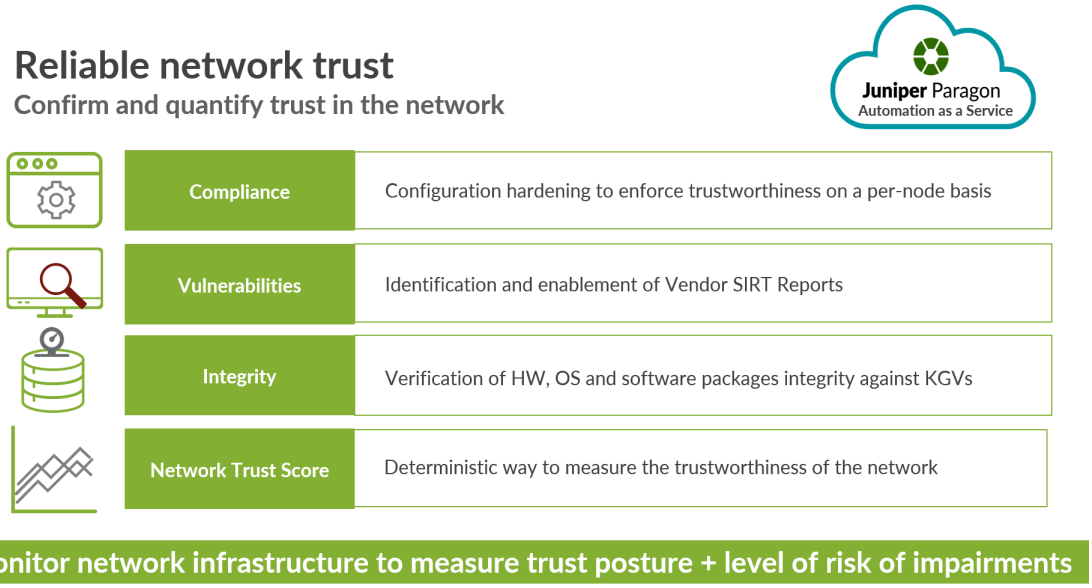
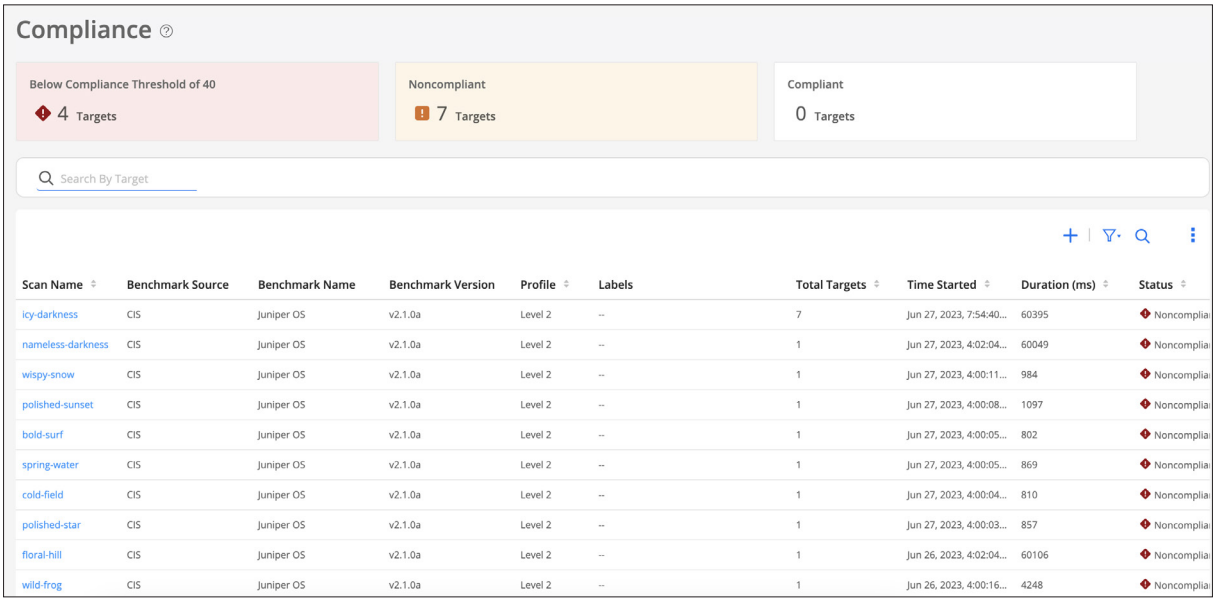


Figure 1: Paragon Automation monitors network infrastructure to measure end-to-end network trust and compliance

Compliance

The Scans web page in the user interface (Figure 2) provides a range of functions for device compliance scanning. Users can perform Create, Read, Update, and Delete (CRUD) operations related to device scanning within the system. Scanning verifies the compliance of one or more devices with a Security Content Automation Protocol (SCAP) Workbench document, which serves as a standard for evaluating device configurations.



Scan Name	Benchmark Source	Benchmark Name	Benchmark Version	Profile	Labels	Total Targets	Time Started	Duration (ms)	Status
icy-darkness	CIS	Juniper OS	v2.1.0a	Level 2	--	7	Jun 27, 2023, 7:54:40...	60395	Noncompliai
nameless-darkness	CIS	Juniper OS	v2.1.0a	Level 2	--	1	Jun 27, 2023, 4:02:04...	60049	Noncompliai
wispy-snow	CIS	Juniper OS	v2.1.0a	Level 2	--	1	Jun 27, 2023, 4:00:11...	984	Noncompliai
polished-sunset	CIS	Juniper OS	v2.1.0a	Level 2	--	1	Jun 27, 2023, 4:00:08...	1097	Noncompliai
bold-surf	CIS	Juniper OS	v2.1.0a	Level 2	--	1	Jun 27, 2023, 4:00:05...	802	Noncompliai
spring-water	CIS	Juniper OS	v2.1.0a	Level 2	--	1	Jun 27, 2023, 4:00:05...	869	Noncompliai
cold-field	CIS	Juniper OS	v2.1.0a	Level 2	--	1	Jun 27, 2023, 4:00:04...	810	Noncompliai
polished-star	CIS	Juniper OS	v2.1.0a	Level 2	--	1	Jun 27, 2023, 4:00:03...	857	Noncompliai
floral-hill	CIS	Juniper OS	v2.1.0a	Level 2	--	1	Jun 26, 2023, 4:02:04...	60106	Noncompliai
wild-frog	CIS	Juniper OS	v2.1.0a	Level 2	--	1	Jun 26, 2023, 4:00:16...	4248	Noncompliai

Figure 2: Compliance Scans are based on CIS benchmarks

Users can initiate a CIS Junos® Compliance scan against a device managed under Paragon Automation. Behind the scenes, an Open Vulnerability and Assessment Language (OVAL) document is utilized to define the commands and criteria used to evaluate the compliance of the device configurations with the CIS standards.

The Scans web page features an Insights bar that displays crucial information about compliance targets. The operations team can find details about the number of targets below the compliance threshold, the count of non-compliant targets, and the number of compliant targets. This overview allows users to quickly assess the compliance status of their targets and identify areas that require attention.

A search tool enables users to search for a specific target. When a search is performed, the rows displayed in the scans table are filtered accordingly, making it easier for users to locate and manage specific scan results.

The scans table on the web page presents a comprehensive view of all historic scans performed within the system. These scans may have been triggered either according to a predetermined schedule or through user-initiated operations. Users can trigger new scans by clicking on the plus icon on the page, allowing for on-demand compliance checks.

Overall, the Scans web page provides a convenient interface for users to manage device compliance scanning. It offers insights into compliance status, search capabilities for specific targets, and a comprehensive view of scan history, empowering users to ensure the trustworthiness and security of their network devices.

The Checklists web page (Figure 3) is a central hub for managing Checklist documents. Users can assess and document the compliance of devices against specific benchmark documents, such as Security Content Automation Protocol (SCAP) Benchmark documents from CIS.

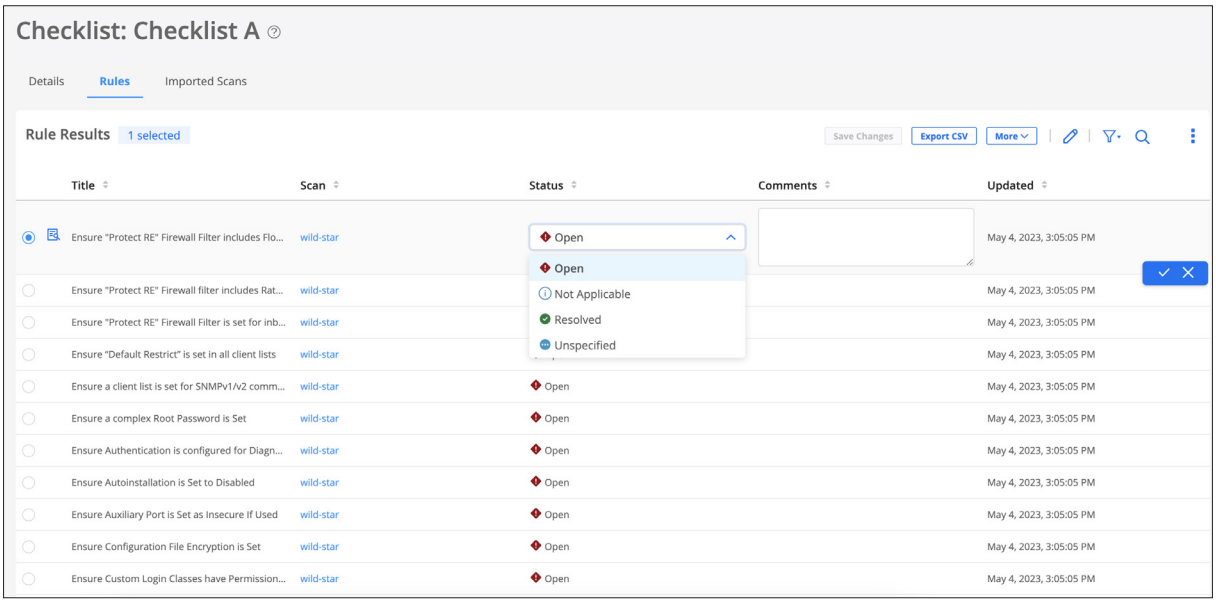


Figure 3: The Checklist compares device compliance with industry benchmark documents

The web page provides CRUD functions for the Checklist document repository. Users can create new Checklist documents, view existing ones, make updates, and remove documents as needed.

Checklist documents are user generated and are associated with specific devices. They indicate whether a device is compliant or noncompliant with the rules and standards outlined in a benchmark document. Users can utilize a Compliance Scan to streamline the process of populating Checklists. The Compliance Scan takes a scan as input and automatically sets one of the four allowable values for each rule: open, not applicable, resolved, or unspecified. This seeding process prepopulates the Checklist document with initial compliance results.

Once seeded, users can manually update the Checklist document for each rule. They can modify the status value assigned to a rule or include comments to provide additional context. For example, if a rule is marked as open, the user can add a comment explaining why it is acceptable in that specific scenario.

When the Checklist document is complete for a device, users can generate a Comma-Separated Values (CSV) file containing information from the Checklist. This CSV can be exported and used by other applications or processes, allowing for seamless integration with external systems that may require Checklist data.

The Tailoring Documents web page (Figure 4) allows users to create and manage tailoring documents for compliance scans. Users can customize the values within a benchmark document during a compliance scan against a specific target.

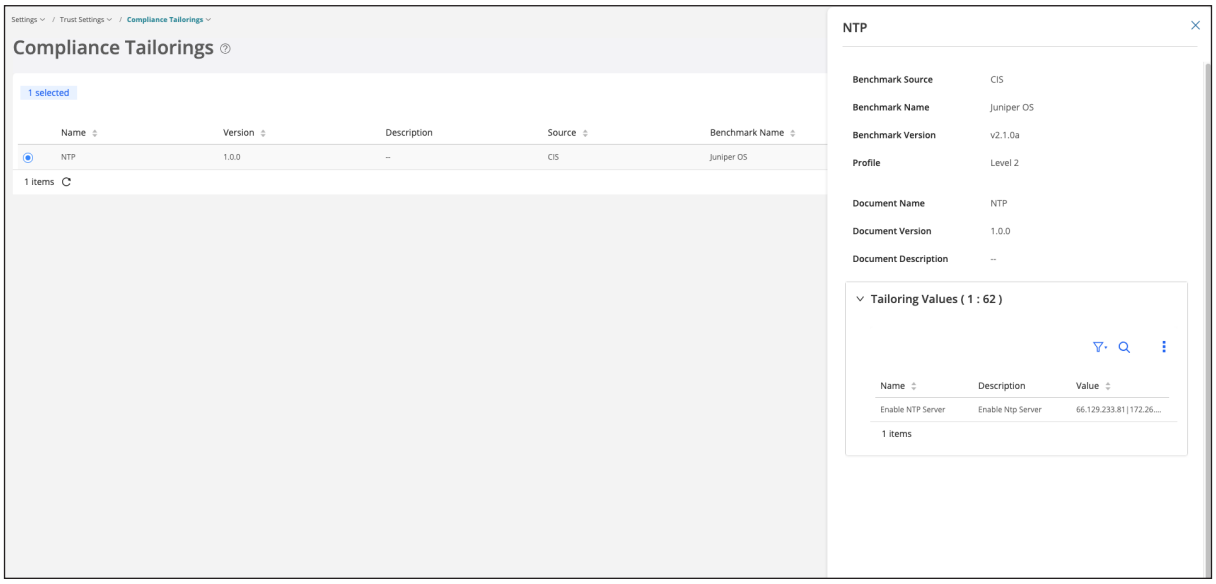


Figure 4: Tailoring Documents improves compliance scans

The web page provides Create, Read, and Delete (CRD) functions for the Tailoring document repository. Users can create new Tailoring documents, view existing ones, and remove documents as needed. Note there is no update. Tailoring documents are immutable, as once they are used, they need to be maintained/tracked against a compliance scan execution.

The web page consists of a table where each row represents an instance of a tailoring document. To create a new document, users can click on the plus icon in the screen's top right-hand corner. This action opens a form or dialog where users can specify the details and configurations for the new tailoring document.

Each tailoring document is associated with a specific benchmark and profile. This association is visible within the row in the table, providing users with a clear overview of the documents and their corresponding benchmarks and profiles.

Once a tailoring document is created, it can be selected during a compliance scan against one or more targets as long as the scan is executed with the same benchmark. Users can define custom values and configurations used in the compliance scan, tailoring it to their specific requirements.

By providing the ability to create and manage tailoring documents, the Tailoring Documents web page enables users to customize compliance scans and ensure that they align with their specific benchmark and profile needs. This flexibility allows for more accurate and tailored compliance assessments of the network environment.

The Benchmarks web page allows users to analyze the rules defined in benchmark documents (Figure 5). These benchmark documents consist of rules defined in Extensible Configuration Checklist Description Format (XCCDF), which describe the compliance requirements for a specific standard.

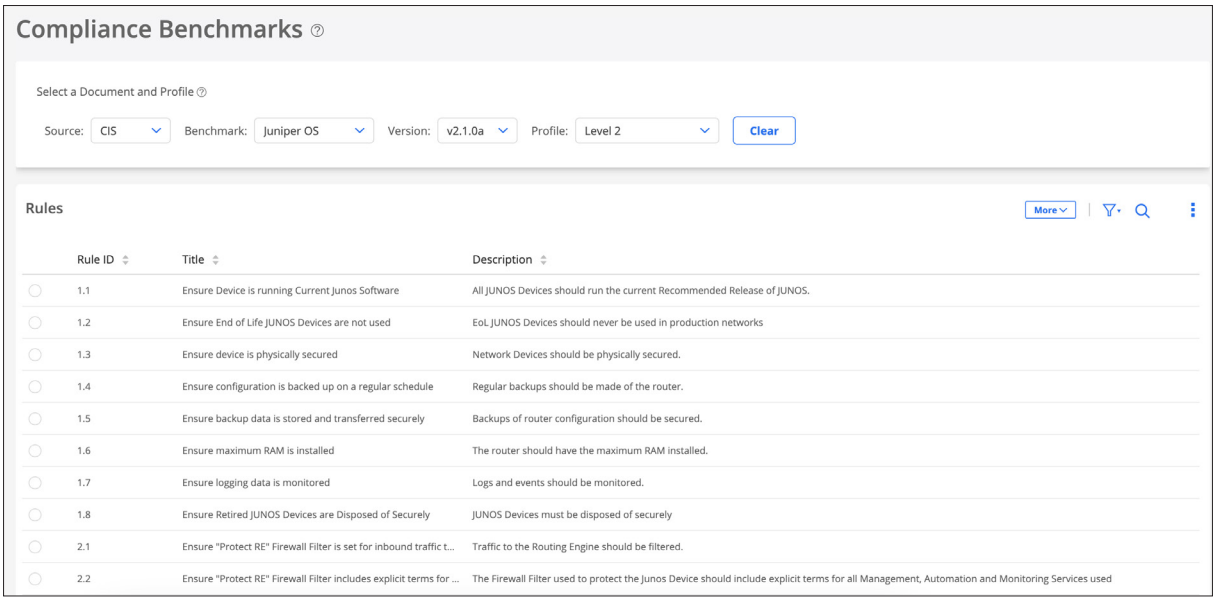


Figure 5: Benchmarks helps users analyze the rules defined in benchmark documents

Upon accessing the Benchmarks web page, users view a list of the supported benchmark documents. These benchmark documents are displayed in dropdown filters, allowing users to select a specific benchmark and profile of interest.

By selecting a particular benchmark and profile in the filters, the table on the web page is dynamically updated to show the relevant rules of the selected filter. Each table row represents a specific rule within the benchmark document.

Users can expand a rule row to view the full details of that rule as defined by the standard body. This provides users with comprehensive information about the compliance requirements and expectations specified by the standard.

It primarily supports benchmark documents from CIS. However, the platform is designed to incorporate other standards, such as the Defense Information Systems Agency (DISA) STIGs, in future releases. This will allow users to analyze and assess compliance with a broader range of industry standards.

The Benchmarks web page offers users a user-friendly interface to explore and analyze the rules defined in benchmark documents. By providing access to detailed rule information and supporting multiple standards bodies, it assists users in understanding and meeting compliance requirements based on industry standards.

Vulnerabilities

The SIRT Advisories web page is a valuable resource for users to identify vulnerabilities in the software running on their network equipment. The Insights bar gives an overview of the vulnerability counts categorized by critical, high, medium, and low severity levels (Figure 6). Users can quickly assess the severity of the vulnerabilities present in their network.

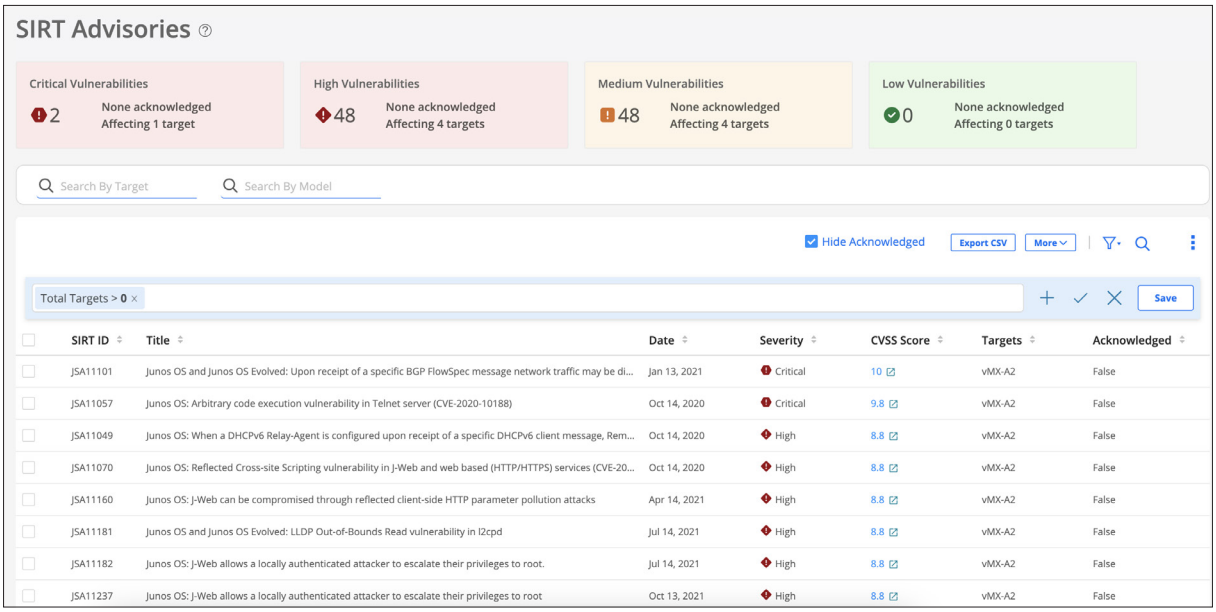


Figure 6: SIRT Advisories provides an overview of equipment vulnerabilities

The web page also includes search functionality, allowing users to search for specific targets or models. Users can narrow the results to the equipment or software they are interested in, making it easier to find relevant information.

A table on the web page presents summary information of Juniper Security Advisories (JSAs) that match the equipment or software running in the network. The rows in the table are ordered based on severity, with the most severe vulnerabilities listed first. This ordering helps users prioritize their remediation efforts and address the most critical vulnerabilities first. Each row in the table provides critical details about the advisory, such as the title, severity level, and release date. Users can click on the Common Vulnerability Scoring System (CVSS) Score, a numerical value representing the severity of the vulnerability, to access a third-party web page that provides a breakdown of the assessment. This additional information allows users to better understand the vulnerability and its potential impact.

Overall, the SIRT Advisories web page provides users with an organized and informative view of vulnerabilities in their network equipment. Users can identify and prioritize vulnerabilities for remediation, enhancing the security and reliability of their network infrastructure.

Integrity

The Software EOL web page is a valuable resource for users to identify software that has reached its EOL. It provides essential understandings through an Insights bar that displays information about the number of software versions that have reached EOL and the number of versions approaching EOL (Figure 7). This data helps users understand the status of their software versions and plan for necessary updates.

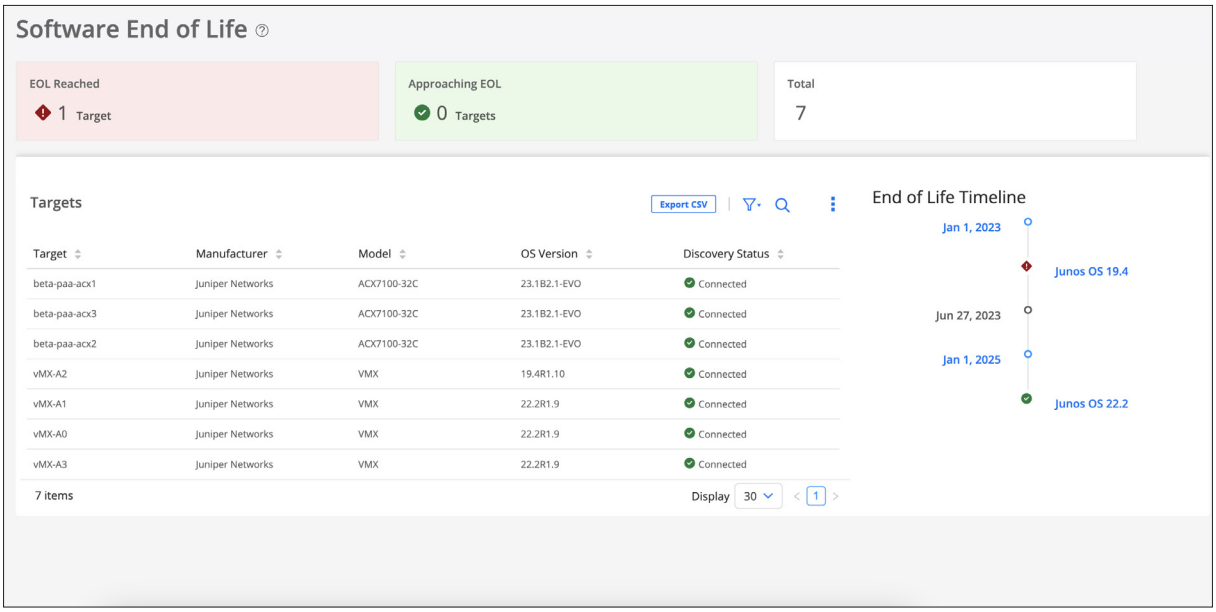


Figure 7: Software EOL reports EOL timelines for software versions

One critical feature of the web page is the timeline, which visually represents the current software versions running in the network. The timeline provides pointers to users, indicating when they should consider updating to a newer release. Users can identify the software versions that are nearing or have already reached EOL, enabling them to take proactive actions.

The web page also includes a table presenting summary information about targets and their software versions. The rows in the table provide key details, such as the target name and the corresponding software version, enabling users to quickly identify the software versions used across their network.

To enhance usability, filter the table by selecting a specific software version or date in the timeline widget. Users can focus on particular software versions of interest, assess the impact of EOL, and plan for necessary updates or replacements.

Overall, the Software EOL web page provides users with comprehensive insights into software versions that have reached their EOL. Combining an Insights bar, a visual timeline, and a filterable table ensures that users can quickly identify EOL software, plan for updates, and maintain a secure and up-to-date software environment.

The Hardware EOL web page is a valuable tool for users to identify hardware that has reached its EOL. The Insights bar displays information about the number of devices that have reached EOL and the number of devices approaching EOL (Figure 8). This data helps users understand the current status of their hardware inventory and plan for necessary replacements.

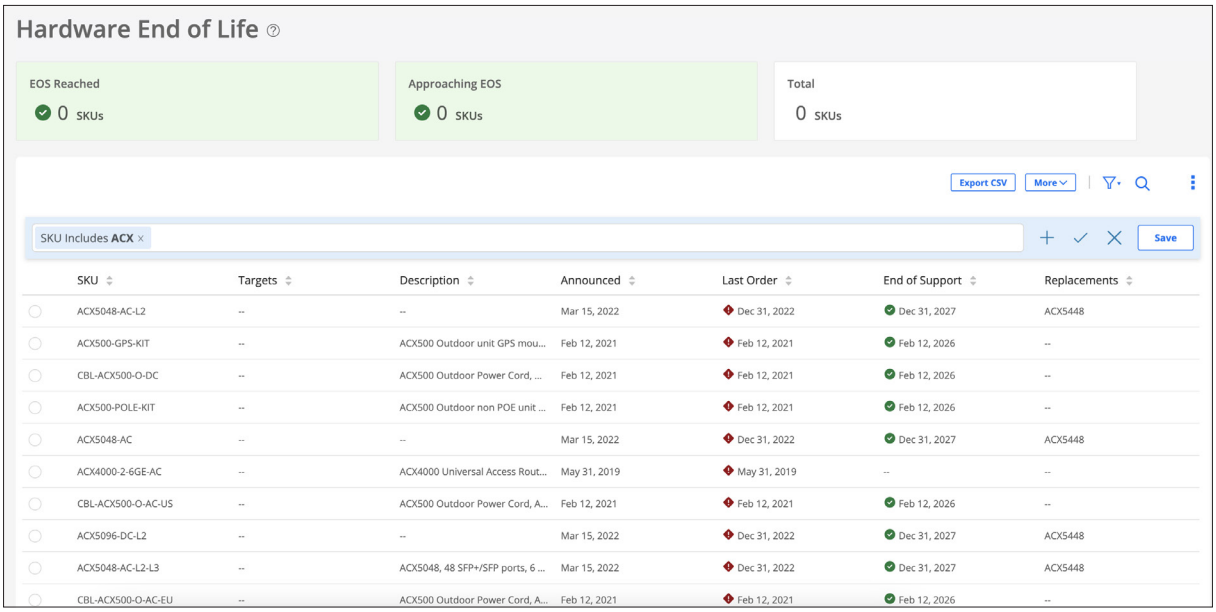


Figure 8: Hardware EOL helps maintain network inventory and plan upgrades

The web page includes search functionality, allowing users to search for specific targets or hardware models. Users can quickly find information about EOL hardware that interests them, making it easier to identify affected devices.

A table on the web page presents summary information about Stock Keeping Units (SKUs) that have reached EOL in the network. The rows in the table provide relevant details such as the SKU name, EOL date, and recommended replacement SKUs for the EOL hardware. Users can quickly understand which devices are affected and gain guidance on suitable replacement options.

By including recommendations for replacement SKUs, the web page assists users in planning hardware upgrades or replacements. This ensures the network remains secure, reliable, and up-to-date, even after EOL hardware is phased out.

Overall, the Hardware EOL web page provides users with a clear overview of hardware reaching EOL in their network. It offers insights, search functionality, and a table with essential information and replacement recommendations. Users can effectively manage their hardware lifecycle, make informed decisions, and maintain trustworthy and up-to-date network infrastructure.

Trust Scores

On the 'Trust Scores' web page users can select a specific plan and view the trust scores of devices over time. A line graph displays the trust scores for the selected device, allowing users to track the device's trustworthiness over a certain period (Figure 9).

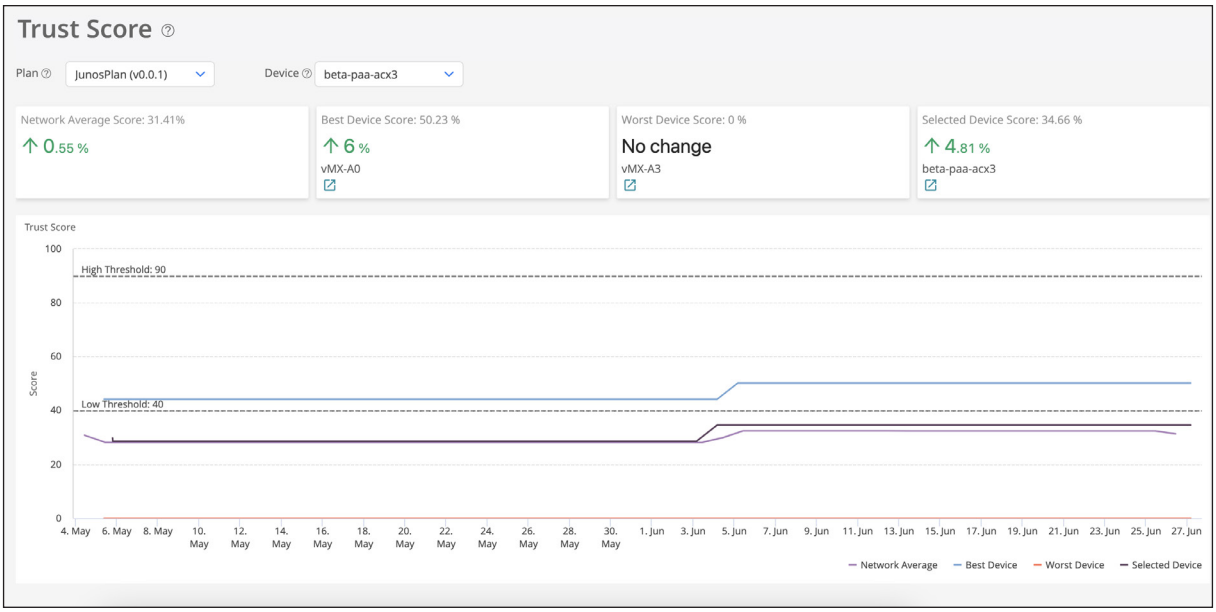


Figure 9: Trust Scores track a device's level of trust over a time period

To enhance the visualization and provide more insights, the line graph overlays additional information. Best Device Score represents the highest trust score achieved by any device within the network, and the Worst Device Score represents the lowest trust score recorded. These overlay lines give users a clear understanding of the range of trustworthiness across devices in the network.

Additionally, the graph displays the average score for the network, which provides an overall measure of trustworthiness for the entire network infrastructure. This average score helps users assess the overall performance and reliability of their network devices.

Low and high thresholds further assist users in interpreting the graph. These thresholds define the acceptable range of trustworthiness for the network devices. By setting these thresholds, users can easily identify if a device's trust score falls within the desired range or if it deviates from the expected level of trustworthiness.

The scores displayed in the line graph and their corresponding hyperlinks offer users a seamless transition to the Snapshots web page. By clicking on a specific score, users can navigate to the Snapshots web page to access detailed information about the device at that particular point in time. Snapshots capture and preserve the state of the device, providing a comprehensive and accurate representation of its trustworthiness factors, configuration, and other relevant details.

Overall, the Trust Scores web page presents a comprehensive and visual representation of the trust scores for devices over time, allowing users to track the trustworthiness of their network and quickly identify any devices that may require attention or improvement.

The Snapshots web page provides users with a comprehensive view of device snapshots and their corresponding trust scores (Figure 10). Users can select a specific Plan (for a specific vendor device model) and then choose a Target (device) to explore its trust score trends and changes over time.

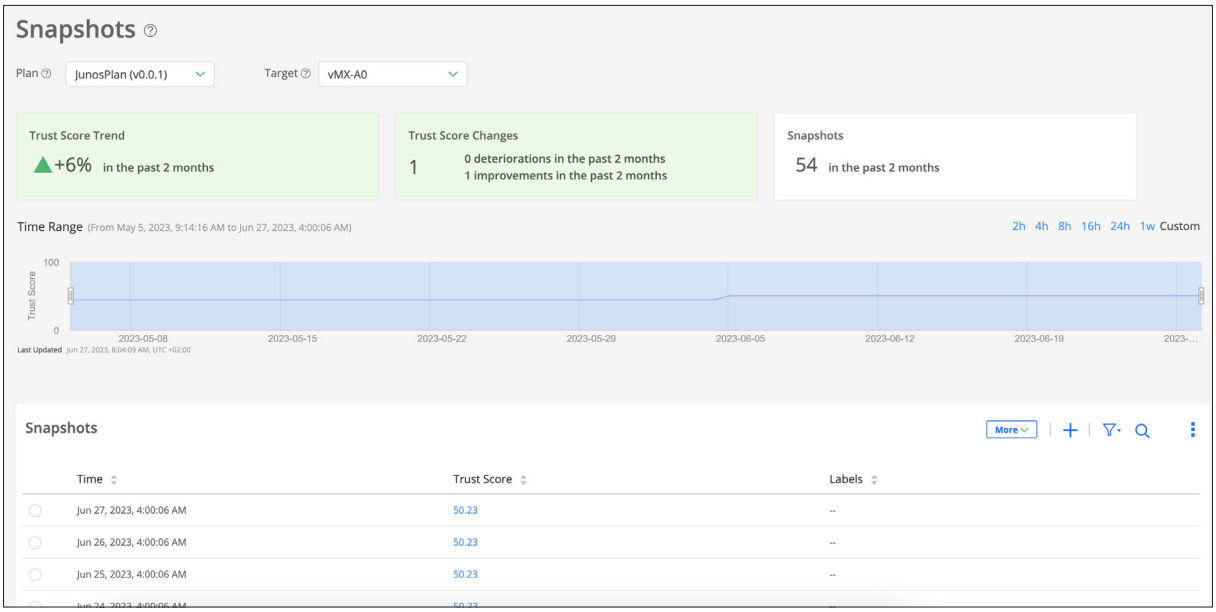


Figure 10: Snapshots highlight the trust scores of specific devices

An Insights bar displays key information about the selected Target. This information typically includes the Trust Score Trend, which shows the overall trend of the target's trust score, whether it is increasing, decreasing, or remaining stable. Additionally, the Trust Score Changes indicate the number of times the trust score has changed for the selected target. The Insights bar also provides the total number of Snapshots available for the selected target, giving users an idea of the historical data available for analysis.

To switch between different targets within the selected Plan, users can utilize the dropdown widget located at the top of the screen. This allows for easy navigation and comparison of trust scores across multiple devices.

The line graph on the Snapshots web page presents the trust score history of the selected target. It visualizes how the trust score has changed over time, providing a clear representation of trends and patterns. Users can interpret the graph to identify periods of high or low trustworthiness and track the device's overall performance.

In addition to the line graph, users can view a table that captures detailed information about historic snapshots for the selected target. This table presents rows of data, each representing a specific snapshot. The information typically includes details such as the date and time of the snapshot, the trust score at that point, and any relevant metadata or configuration information associated with the snapshot. This tabular view allows users to explore specific snapshots in more detail and extract insights from the historical data.

By selecting a specific trust score in the table row, users can navigate to the Plans page for the selected device. Users can access a detailed breakdown of the trust score, a comprehensive view of the factors contributing to the score, and an understanding of the strengths and weaknesses of the target's trustworthiness.

To enhance usability and filter snapshots based on the desired time scale, the line graph includes a slider. By adjusting the slider, users can change the scale shown on the line graph, zooming in or out on specific time intervals. This interactive feature provides a more granular view of trust score changes and dynamically updates the table by filtering the displayed snapshots based on the selected time scale.

Additionally, the Snapshots web page includes a plus icon, which allows users to generate ad hoc snapshots for the selected target. By clicking on the plus icon, users can create an ad hoc snapshot at the current point in time, capturing the device's trust score and associated information. This feature enables users to capture snapshots on demand and obtain real-time insights into the trustworthiness of the device.

Overall, the Snapshots web page offers users a powerful tool to analyze and explore trust score trends, changes, and historical snapshots for specific targets within a selected Plan. The combination of line graphs, interactive sliders, and a comprehensive table facilitates data exploration and assists in identifying patterns, making informed decisions, and gaining valuable insights into the trustworthiness of devices.

The Plans web page provides users with detailed information about how the trust score was calculated for a specific Plan, target, and score. It offers a comprehensive breakdown of the individual factors and values that influenced the score, categorized by factor groups.

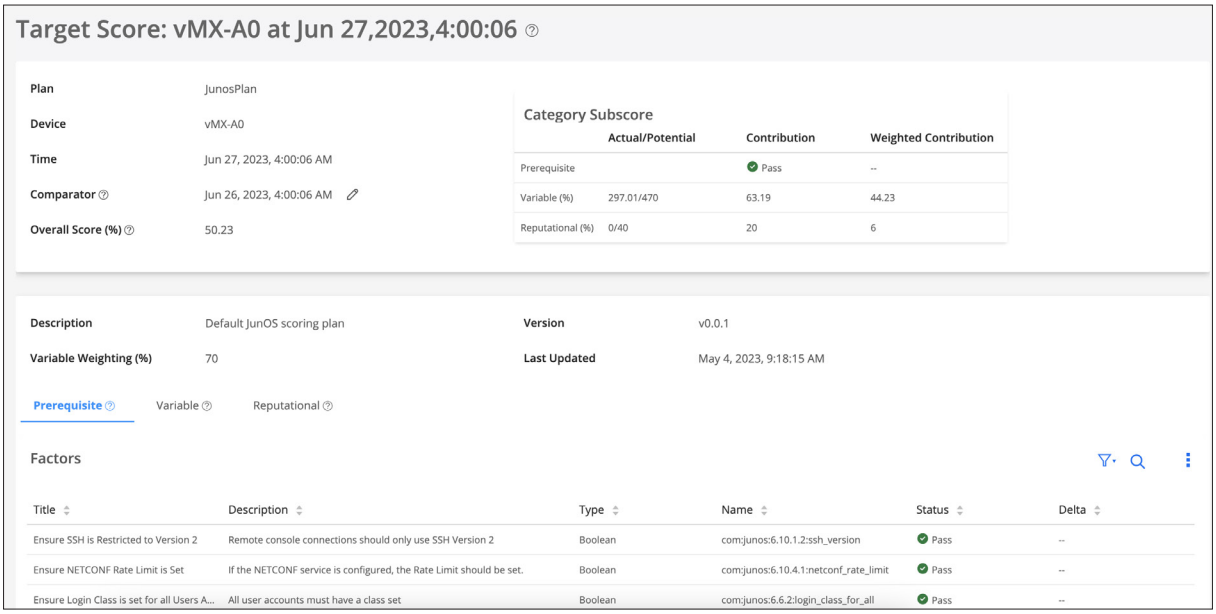


Figure 11: Plans displays information about a selected Plan, target device, and trust score for that device

Upon accessing the web page, users will find a top-level panel that displays summary information about the selected Plan, target, and score. This summary provides an overview of the key details, allowing users to quickly understand the context of the score analysis (Figure 11).

In addition to the summary information, the web page allows users to compare a target device to an alternate score. Users can explore and understand the factors that contributed to a target trending upwards or downwards. By selecting an alternate score, users can identify any significant differences in the individual factors and values, gaining insights into the specific elements that influenced the change in trustworthiness.

The main panel of the web page presents a detailed breakdown of the individual factors and values that influenced the score. These factors are grouped into factor categories, providing a structured view of the various aspects that contribute to the overall trust score.

Within each factor category, users can explore the specific factors and their corresponding values. This breakdown helps users understand the relative importance of each factor in determining the trust score and provides transparency into the calculations.

By analyzing the individual factors and values, users gain a deeper understanding of why a particular score was assigned to the target. They can identify areas of strength or weakness in the target's trustworthiness and take appropriate actions to address any areas that require improvement.

Overall, the Plans web page offers users a detailed breakdown of how the trust score was calculated for a specific Plan, target, and score. With the summary information, the ability to select alternate scores, and the breakdown of individual factors and values, users can gain comprehensive insights into the trustworthiness assessment and make informed decisions to optimize network reliability and security.

Ensuring Network Trust and Compliance during Device Onboarding

Juniper Cloud Metro routers come pre-integrated with a secure Trusted Platform Module (TPM2.0) chip and unique Device identifier (DevID) that allow Paragon Automation to ensure the authenticity and tamper-proofness of the hardware. Zero-trust security capabilities also include secure ZTP and software integrity checks. These capabilities help Paragon Automation ascertain a Network Trust Score and continuously monitor that score over time with changes to the network hardware and software. During the device onboarding process, the workflow supports automated steps that include device trust validation checks. When investigating device onboarding issues with Paragon Automation device lifecycle and network observability, operators can leverage the built-in, integrated network trust and compliance.

Integration into Device Life-cycle Management and Network Observability

For device life-cycle management, the NOC engineer can troubleshoot and gain visibility into network trust and compliance issues using Paragon Automation's network observability application. Specifically, when viewing the software installed on a device, network trust and compliance in Paragon Automation can also see the device's EOL date and any related SIRT advisories that exist. In addition, they can see a configuration compliance score for the device derived from Paragon Automation's integrated network trust compliance, and explore any existing configuration compliance issues.

Conclusion

Automation accelerates innovation, increases operational efficiency, and delivers amazing customer experiences. It saves you time, money, and resources, while allowing you to introduce new service enhancements at your own pace and protect network performance and quality. Time to automation matters. When you have a reliable network, your customers and your business realize better outcomes.

With Paragon Automation, you can enable Network Trust and Compliance and empower operation teams to confirm and quantify network trust by continuously monitoring your network infrastructure to measure trust posture and the level of risk of impairments. Operators can have peace of mind—and quantifiable data—that their network infrastructure can be confidently trusted. Organizations can also better enforce the latest requirements and regulatory standards for compliance while automating the process for continuous monitoring and reporting. Network trust and compliance can be prioritized and maintained—automatically.

Next Steps

Learn more about Paragon Automation and how it supports autonomous networks.

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
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