JUNIPER PARAGON AUTOMATION—NETWORK TRUST AND COMPLIANCE SOLUTION BRIEF

Automated, Consistent, And Reliable Network Trust And Compliance

Challenge
Today's networks are both complex and risky. As the complexities multiply, CSPs may not be prepared for the additional risks to the network infrastructure, such as from tampered software and hardware, infrastructure vulnerabilities and security risks due to not conforming to trust compliance standards.

Solution
Juniper Paragon Automation confirms and quantifies network trust. It 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.

Benefits
- Quantifies trustworthiness
- Maximizes reliability/security
- Identifies areas for improving device performance
- Provides customers with peace of mind/confidence in their network
- Eases compliance by automating checks/reporting
- Identifies vulnerabilities to take proactive measures
- Prioritizes improvements from trust score insights

The Challenge

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 Unavailable vulnerability patches, outdated software, and outdated hardware present similar risks when network equipment at the customer premises is not replaced after reaching end of support.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 Communications Service Provider (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

Network Trust and Compliance with Juniper Paragon Automation

Juniper® Paragon Automation provides automated, consistent, and reliable Network Trust and Compliance that can verify, confirm, and quantify the trust aspects of the network, making it easier for network operators to run trustworthy networks. The cloud-based, automation solution 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

Features and Benefits

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

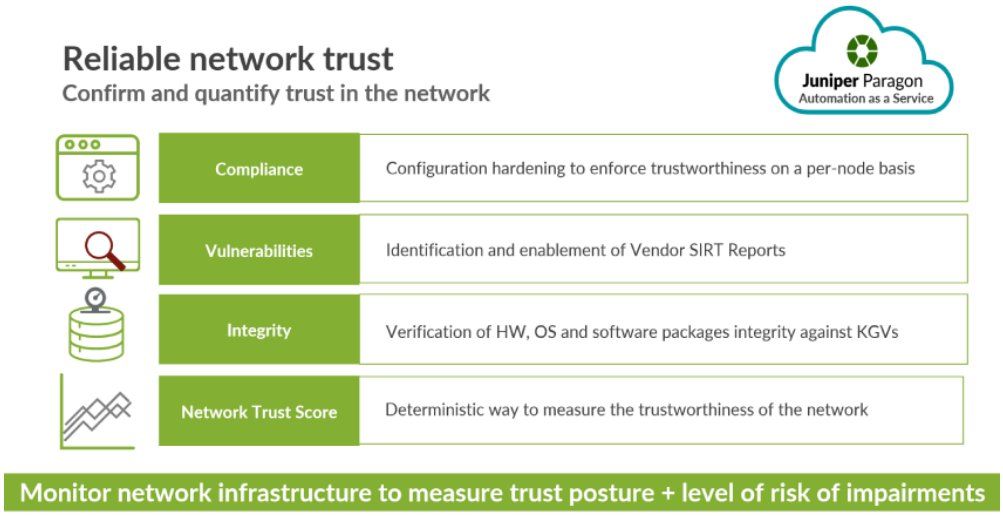

Figure 1: Paragon Automation monitors network infrastructure to measure end-to-end network trust and compliance

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

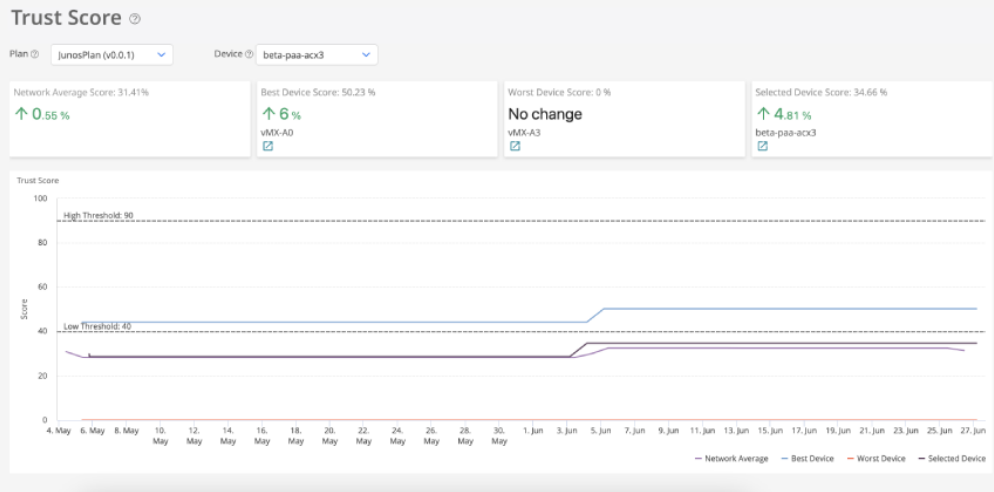

Figure 2: Trust Scores track a device's level of trust over a time period

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 networkwide and on a device-per-device basis. The method to calculate the score can also be customized to meet organizational requirements and network expectations..

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 life-cycle management and network observability, operators can leverage the built-in, integrated network trust and compliance.

Learn more about how Paragon Automation simplifies device onboarding by reading the Solution Brief on Device Life-cycle Management.

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. Specifically, when viewing the software installed on a device, Paragon Automation can show engineers the device's EOL date and any related Security Incident Response Team (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.

Learn more about our network observability by reading the Solution Brief on Network Observability.

Solution Components

Network Trust and Compliance is powered by **Paragon Automation**, which provides intent-based network automation. The solution makes network automation intuitively easy while enabling organizations to evolve to AIOps and better support their network and service life cycle, from Day 0 to Day 2. With Paragon Automation, organizations can reduce time to revenue, accelerate service delivery, and significantly reduce mean time to know (MTTK) and mean time to repair (MTTR). It dramatically boosts productivity and speed, along with continually enabling amazing experiences, both for end users and the operators that run the networks.

Summary—Automated Network Trust and Compliance that Scales with Your Needs

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 Network Trust and Compliance by reading this Application Note.

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:**

+31.0.207.125.700