

# JUNIPER WAN ASSURANCE

## Produktübersicht

Die [Cloud-Services der Mist™ Plattform](#) bringen den IT-Betrieb im Zeitalter des KI-nativen Unternehmens näher an das intelligente Self-Driving Network™. [Juniper® WAN Assurance](#) bietet einen einfacheren Betrieb, eine kürzere mittlere Reparaturzeit (MTTR) und eine bessere Transparenz der Endbenutzererfahrung im gesamten [WAN](#).

## Produktbeschreibung

Juniper WAN Assurance ist ein Cloud-Service, der automatisierte Abläufe und Servicelevels auf die Zugriffsebene des Unternehmens am WAN-Edge bringt. WAN Assurance ist eine Schlüsselkomponente der HPE Juniper Networking KI-gestützten SD-WAN-Lösung, die es IT-Teams ermöglicht, erstklassige Benutzererfahrungen im gesamten WAN zu bieten. Bei Verwendung in Verbindung mit [Juniper® Wired](#) and [Wireless Assurance](#), der Service transformiert und vereint alle Abläufe über [Netzwerk-Switches](#), [IoT-Geräte](#), [Access Points](#), Server, Drucker und andere Geräte. [Juniper® Session Smart® Router](#) (SSR) und Service Gateways der [SRX-Serie von Juniper®](#) bieten umfassende Streaming-Telemetrie, die den Anwendungszustand, den WAN-Verbindungszustand sowie Gateway-Zustandsmetriken und Anomalieerkennung ermöglicht.

Die [Mist AI™](#) Engine und der virtuelle Netzwerkkassistent vereinfachen die Fehlerbehebung weiter und optimieren den Helpdesk mit selbstfahrenden Aktionen, die Probleme automatisch beheben. [Marvis® AI Assistant](#) verwandelt Einblicke in Aktionen und transformiert den IT-Betrieb von reaktiver Fehlerbehebung in proaktive Behebung.

Die Cloud-Services der Mist Plattform sind mit OpenAPI für die vollständige Automatisierung und/oder Integration in Ihre IT-Anwendungen zu 100% programmierbar.

## WAN-Erlebnisse auf Serviceebene

Erhalten Sie betriebliche Einblicke in die WAN-Erfahrungen der Benutzer mit Service-Level-Erwartungen (SLEs) für SSRs oder SRX-Gateways. Messen Sie die Auswirkungen des Zustands von Gateway- und WAN-Schaltkreisen auf die Anwendungserfahrungen der Endbenutzer. Ein WAN Link Health SLE, der Netzwerküberlastungen, Kabelprobleme und ISP-Netzwerkverfügbarkeit berücksichtigt, liefert Einblicke in die Auswirkungen dieser Faktoren auf einen bestimmten Netzwerkbenutzer oder eine bestimmte Anwendung. Das Juniper Mist™ SLE Dashboard hilft, die Ursachen suboptimaler Anwendungserfahrungen mit nur wenigen Klicks zu identifizieren, um proaktiv „needle-in-a-haystack“ - Probleme zu isolieren (Abbildung 1).

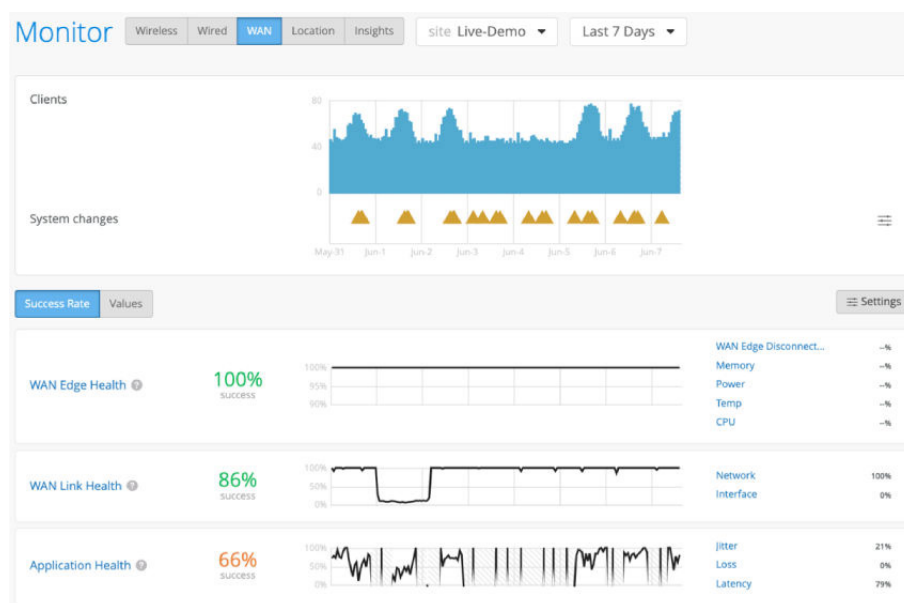


Abbildung 1. WAN SLEs

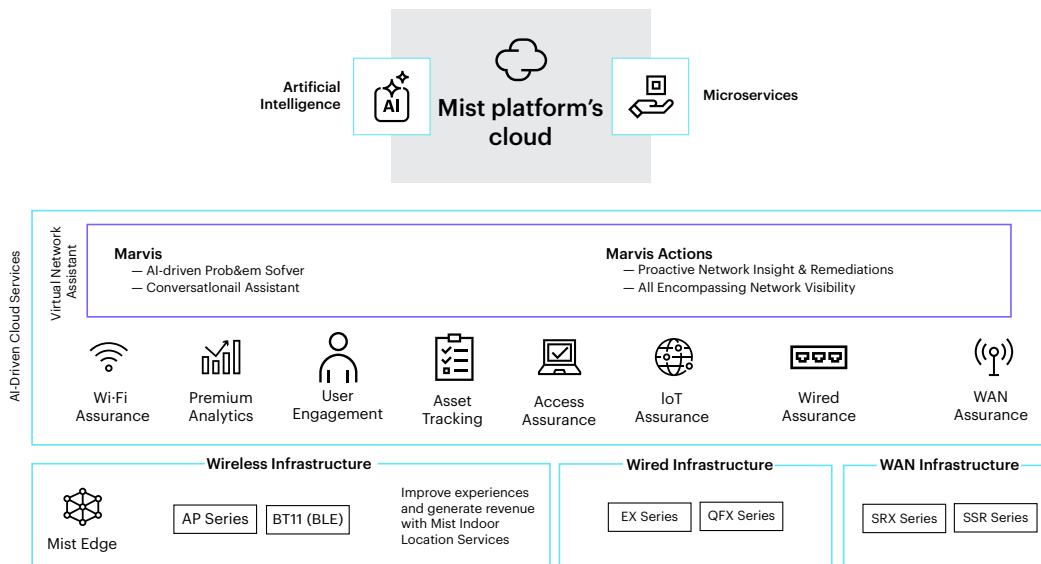


Abbildung 2. KI-nativer Unternehmensportfolioüberblick

## WAN-Einblicke mit Mist AI

Wissen Sie genau, wie SSRs oder SRX-Gateways funktionieren, mit Metriken und Einblicken bis hinunter zur Portebene. Dazu gehören CPU, Speicherauslastung, übertragene Bytes, Datenverkehrsauslastung und Stromverbrauch. WAN Assurance protokolliert auch Gateway-Ereignisse wie Konfigurationsänderungen und Systemwarnungen. WAN- und IPSec-Nutzungseinblicke zeigen Ihnen, wie viel Datenverkehr Ihren verschlüsselten Tunnel im Vergleich zu Ihrem lokalen Breakout durchläuft. Außerdem erhalten Sie einen Einblick in die Leistung und Erfahrungen pro Benutzer und pro Anwendung (Abbildung 3).

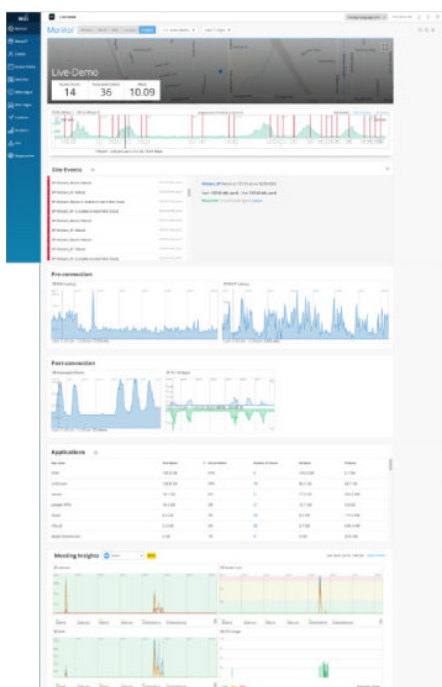


Abbildung 3. WAN-Einblicke

Der Congestion SLE informiert Betreiber darüber, ob ihre Netzwerkschnittstellen überlastet werden und zu einer schlechten Benutzererfahrung führen. Mit App Routing Insights können Betreiber herausfinden, was überproportional mit Bandbreite umgeht und wie das Problem am besten behoben werden kann. Optionen können darin bestehen, mehr Bandbreite zu erwerben, die Kapazitätsplanung anzupassen oder bestimmten Datenverkehr zu drosseln. Typ (Abbildung 4).



Abbildung 4. Einblicke in das App Routing

Dynamische Paketerfassung (dPCAP) gibt den Betreibern Einblicke, wie sie die MTTR verkürzen und einfach nach Nadel-in-a-Hystack-Problemen suchen können. Anstatt Probleme im Netzwerk neu zu erstellen, um die richtigen Pakete zu erfassen, bemerkt Mist AI, wenn ein Problem auftritt, und erfasst automatisch die entsprechenden Pakete zur Analyse.

## Marvis, der KI-native virtuelle Netzwerkasistent für WAN

Marvis AI Assistant verlagert den IT-Betrieb näher an das Self-Driving Network mit vereinfachter Fehlerbehebung und Leistungsanalyse für Helpdesk-Mitarbeiter und Netzwerkadministratoren.

Marvis® Actions ist ein zentrales Informationscenter, das Einblick in standortweite Netzwerkprobleme bietet, die sofortige Aufmerksamkeit erfordern. Verwenden Sie Marvis Actions, um Probleme zu finden, die sich auf die Benutzererfahrung auswirken, und um Empfehlungen zu Lösungen zu erhalten (Abbildung 5).

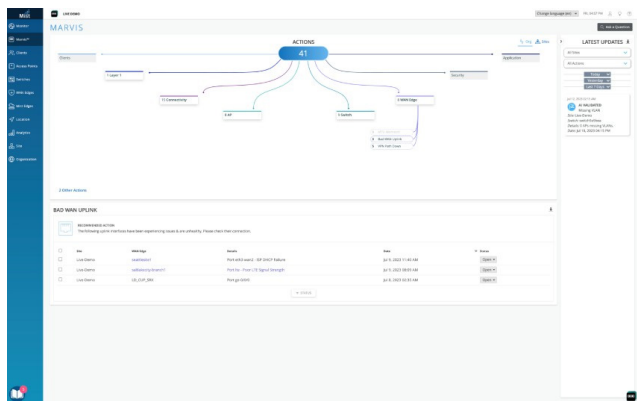


Abbildung 5. Marvis-Aktionen

Der Marvis Conversational Interface Service ermöglicht es IT-Teams, schnell Antworten auf Fragen zur Fehlerbehebung zu erhalten. Stellen Sie einfach eine Frage in natürlicher Sprache, wie z. B. „Warum ist die Videoanruferfahrung meines Benutzers schlecht?“ und Marvis gibt Empfehlungen zur Verbesserung dieser Erfahrungen. Abbildung 6 zeigt, dass Marvis die IT über ein WAN-Problem informiert, das dazu führt, dass der CEO ein schlechtes Videoanruferlebnis hat. [Marvis® Minis](#) führen automatisierte Geschwindigkeitstests durch, mit denen Unternehmen sehen können, ob sie die gesamte Bandbreite erhalten, die sie erworben haben. Selbst wenn Benutzer nicht anwesend sind, werden Betreiber auf vorgelagerte Netzwerkprobleme aufmerksam gemacht. Dies gibt Betreibern die Möglichkeit, an der Lösung von Problemen zu arbeiten, bevor Endbenutzer im Büro erscheinen.

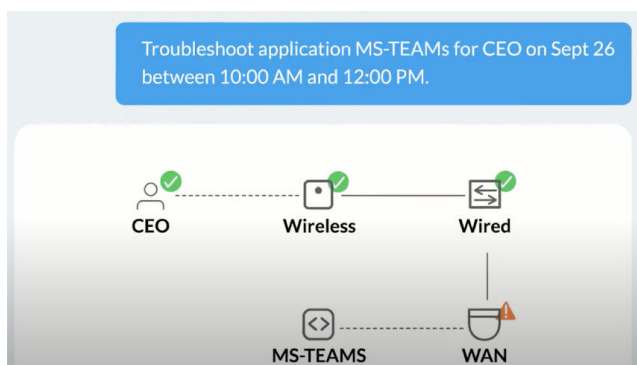


Abbildung 6. Fehlerbehebung bei einer Anwendung

### SD-WAN, unterstützt durch Session Smart

WAN Assurance bietet nicht nur [AIOps](#) für den Betrieb am zweiten Tag, sondern auch Lifecycle-Management und -Betrieb. Dazu gehören der Betrieb an Tag 0 und Tag

1 für die HPE Juniper Networking KI-gestützte SD-WAN-Lösung mit Session Smart Routern, die eine fortschrittliche, serviceorientierte Netzwerklösung unterstützen. Session Smart-Technologie bietet ein erfahrungsbasiertes SD-WAN mit umfassender Sitzungstransparenz und -einblicken sowie feinkörniger Sitzungskontrolle. Sein tunnelfreier Ansatz ermöglicht agile, sichere und ausfallsichere WAN-Konnektivität mit bahnbrechender Wirtschaftlichkeit und Einfachheit. Mit WAN Assurance können IT-Teams SSRs und SD-WAN mit folgenden Vorgängen integrieren, konfigurieren und bereitstellen:

- Zero-Touch Provisioning (ZTP) und einfaches Onboarding mit Mist Claim Code
- Einfache Vorlagenerstellung für schnelle Bereitstellungen im großen Maßstab
- Pfad- und Peering-Präferenzen
- Service- und Anwendungsrichtlinien
- Sicherheitsrichtlinien
- Netzwerk- und NAT-Konfiguration

Session Smart Router sind auf dedizierten Appliances verfügbar (Tabelle 1).

Tabelle 1. SSR-Appliances und vorgeschlagene Standorte

System	Empfohlener Einsatzort	Max. Durchsatz (Unverschlüsselt)	Relevantes Datenblatt
SSR120	Kleine Zweigstelle	1.5 Gbit/s	<a href="#">Router der SSR100-Reihe</a>
SSR130	Mittlere Zweigstelle	2 Gbit/s (Leitungsrate an Ports)	<a href="#">SSR1000 Router-Reihe</a>
SSR1200	Große Zweigstelle oder kleines Datacenter/Campus	10 Gbit/s	
SSR1300	Mittleres Datacenter/Campus	20 Gbit/s (max. Durchsatz auf NIC)	
SSR1400	Großes Datacenter/Campus	40 Gbit/s	
SSR1500	Extra großes Rechenzentrum/Campus	50 Gbit/s (max. Durchsatz auf NIC)	

Die Hardwaredatenblätter enthalten Standardspezifikationen wie Schnittstellenoptionen, Anzahl der Schnittstellen, verschlüsselter Durchsatz, Arbeitsspeicher und Festplattenkapazität.

SSRs sind auch in anderen Formfaktoren verfügbar, einschließlich zertifizierter Whiteboxen (siehe Datenblatt [Session Smart Routing](#)) oder des Netzwerks der Juniper® NFX-Serie Services-Plattformen.

WAN Assurance unterstützt auch die folgenden [Firewalls der SRX-Serie](#), wenn sie als WAN-Gateways bereitgestellt werden:

- [vSRX](#)
- [SRX 300](#)
- [SRX 320](#)
- [SRX 340](#)
- [SRX 345](#)
- [SRX 380](#)
- [SRX 1500](#)
- [SRX 1600](#)
- [SRX 2300](#)
- [SRX 4100](#)
- [SRX 4200](#)
- [SRX 4300](#)
- [SRX 4600](#)

### Auswahl eines WAN-Edge-Geräts

Bei der Auswahl einer WAN-Edge-Plattform innerhalb von Juniper WAN Assurance werden SSRs im Allgemeinen für ihre Effizienz bei der Netzwerkauslastung, dem schnellen Failover, der umfangreichen Telemetrie und der integrierten Sicherheit empfohlen, wobei Secure Vector Routing und KI-gestütztes Cloud-Management genutzt werden.

Für Netzwerke, die bereits HPE Juniper Networking SRX Gateways verwenden, verbessert die Integration dieser Gateways in Juniper Mist ihre Funktionen und bietet einen schrittweiseren Übergang zu SD-WAN. Dies ermöglicht sofortige Vorteile für das KI- und Cloud-Management und ermöglicht gleichzeitig vertraute Umgebungen.

Darüber hinaus können Unternehmen ihre Sicherheitsfunktionen über das Juniper Mist Framework direkt auf dem SSR und/oder dem SRX konfigurieren. Letztendlich sollte die Wahl zwischen SSR und SRX

Passen Sie sich Ihren spezifischen Anforderungen und Zielen an und gewährleisten Sie eine nahtlose Integration mit dem einheitlichen Management-Dashboard von Juniper Mist.

### Erweitertes Sicherheitspaket

Session Smart Router Advanced Security Pack (Abbildung 7) integriert weitere Sicherheitsfunktionen in die Routing-Fabric:

- URL-Filterung verhindert den Zugriff auf und von bestimmten Websites und erfüllt besondere Geschäftsanforderungen
- Ein System zur Erkennung und Prävention von Eindringlingen ([IDS/IPS](#)) schützt vor fortschrittlichen böswilligen Angriffen



**Abbildung 7.** Grundlegende SSR-Router-Sicherheit und das Advanced Security Pack

Diese Funktionen machen zusätzliche Sicherheits-Appliances in der Zweigstelle überflüssig und bieten diese erweiterte Funktionalität im Juniper Mist Ökosystem von kabelgebundenen, drahtlosen und SD-WAN. Wenn mehr Cloud-integrierte Sicherheit erforderlich ist, haben Kunden die Möglichkeit, [Juniper® Secure Edge](#) zu der Umwelt.

### Treffen Sie sich dort, wo Sie sich befinden

HPE Juniper Networking möchte Sie dort treffen, wo Sie sich befinden, wenn es um Ihre Netzwerksicherheit geht. Das Advanced Security Pack kann daher eigenständig oder zusammen mit einer Firewall der SRX-Serie von Juniper in Ihrer Zweigstelle oder Ihrem Rechenzentrum installiert werden.

Das Advanced Security Pack kann auch verwendet werden, um Sie bei Ihrer SASE Journey zu unterstützen, und bietet Ihnen Schutz in der Zweigstelle oder im Rechenzentrum, bevor Sie diesen Datenverkehr einfach an einen SSE wie [Juniper Secure Edge entlasten](#).

## Risikoprofilierung, angetrieben durch KI

WAN Assurance ist eine Schlüsselkomponente der Risk Profiling-Lösung, die Netzwerksicherheit am verteilten Netzwerkrand bietet. Risk Profiling bietet Einblick in infizierte kabelgebundene oder drahtlose Clients, die in der Cloud der Mist-Plattform beobachtbar sind, und weist einen Bedrohungswert zu, der von Juniper® Advanced Threat Prevention bestimmt wird. Von der Cloud der Mist-Plattform aus können Sie infizierte Geräte geospatial lokalisieren und Maßnahmen zur Eindämmung mit nur einem Berührungskontakt ergreifen, wie z. B. Verbot oder Authentifizierung.

## Informationen zu HPE

HPE ist führend in der wesentlichen Unternehmenstechnologie und vereint die Leistungsfähigkeit von KI, Cloud und Netzwerken, um Unternehmen dabei zu unterstützen, mehr zu erreichen. Als Wegbereiter der Möglichkeiten fördern unsere Innovation und unser Fachwissen die Art und Weise, wie Menschen leben und arbeiten. Wir befähigen unsere Kunden branchenübergreifend, die betriebliche Leistung zu optimieren, Daten in Vorausschauende umzuwandeln und ihre Auswirkungen zu maximieren. Setzen Sie mit HPE Ihre kühnsten Ambitionen frei. Erfahren Sie mehr unter [HPE.com](https://www.hpe.com).

**Haftungsausschluss:** Dieses Blatt wurde mithilfe künstlicher Intelligenz maschinell für Sie in die Sprachen Deutsch/Französisch/Italienisch/Spanisch/Japanisch/Koreanisch übersetzt. Bitte beachten Sie, dass die Übersetzung nicht überprüft oder von menschlichen Übersetzern Korrektur gelesen wurde. Daher können Fehler oder leichte Abweichungen in der Sprache auftreten. Die genauesten und zuverlässigsten Informationen finden Sie in der ursprünglichen englischen Version des Datenblattes.

[HPE.com besuchen](https://www.hpe.com)

## Jetzt chatten

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise (HPE) ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Die hier enthaltenen Informationen stellen keine zusätzliche Garantie dar. Hewlett Packard Enterprise haftet nicht für hierin enthaltene technische oder redaktionelle Fehler oder Auslassungen.

a00150846dee

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

