Automated Assurance

Assure high-performance network services with confidence



© 2026 Cisco and/or its affiliates. All rights reserved.

Benefits

- **Expedite troubleshooting:** Identify and resolve problems before they affect service by leveraging end-to-end topology-based visualization and multilayer correlation to pinpoint the root cause of existing and potential problems.
- **Optimize Quality of Experience (QoE):** Monitor Key Performance Indicators (KPIs) in real time and make changes instantly with software-defined network control.
- **Unlock new revenue:** Deliver high quality services consistently and offer robust Service-Level Agreements (SLAs) to differentiate your services in competitive markets.
- **Simplify service lifecycle management:** Provision, assure, and optimize your network seamlessly with automated transport slicing, real-time monitoring, machine learning-powered analytics, and advanced traffic engineering.
- **Reduce costs:** Simplify assurance operations and increase efficiencies across multivendor, multilayer, and multidomain transport networks.

© 2026 Cisco and/or its affiliates. All rights reserved.

Imagine being able to execute intent-based, proactive service assurance across your entire multivendor, multidomain network. With Cisco Crosswork® Network Automation's automated assurance capabilities, you are empowered to optimize service performance, enabling you to deliver and monetize differentiated services that not only meet but surpass customer expectations.

Overview

Traffic continues to grow exponentially, and modern networks, with their multivendor, multidomain, and multilayer attributes, are becoming vastly more complex to manage. Yet despite this, customers still expect flawless network services.

Proactive, automated assurance is the key for Communications Service Providers (CSPs) who manage high-performance networks to deliver consistently exceptional experiences and adhere to the rigorous performance demands of the critical network services required by large enterprises.

Crosswork's automated assurance approach pairs advanced network automation with high-resolution performance monitoring for proactive, intent-based service assurance. See how your network performs end-to-end and monitor service health in real time with the ability to find and fix issues before customers are impacted, even as you rein in capital and operational expense.

Overcome complexity

Assurance is a key part of enabling superior digital experience. Yet the complexity of current assurance operations makes it challenging to deliver high-quality services consistently. Traditional assurance tools are simply not equipped to handle today's dynamic networking environment as the number of users, devices, and demands for services continue to skyrocket.

- Processes are mostly manual, which delays time to resolution and creates inefficiency.
- Troubleshooting is reactive and typically takes place after issues are identified.
- Context on performance issues is limited, with noise from alarms and alerts preventing a quick response to customer-impacting issues.

Complex assurance operations are time-consuming and slow, leading to poor service quality, high operating costs, and, ultimately, customer churn.

Drive a unified, and simpler, top-down approach

Crosswork's approach to intent-based service assurance is multilayered yet simplified, unifying domains as part of a top-down, service-centric approach.

The primary goal of the Service Operations Center (SOC) is to monitor that Service Level Agreements (SLAs) meet customer requirements. Operators view performance metrics on a single dashboard within Crosswork Network Controller and receive alerts in real time if a service is degrading or SLAs are being violated. Cisco Crosswork Assurance, actively monitors end-to-end service performance using embedded assurance sensors or probes, sending data and KPIs to the network controller dynamically to proactively identify service issues.

Crosswork Assurance sends granular reporting on network service performance to Crosswork Network Controller for deeper investigation when a degradation has been detected and flagged. Crosswork Assurance also enhances the customer experience with a personalized end-user portal designed with user-specific features to cater to different groups. This approach not only improves engagement but also opens up avenues for CSPs to offer additional capacity proactively when the portal detects potential issues.

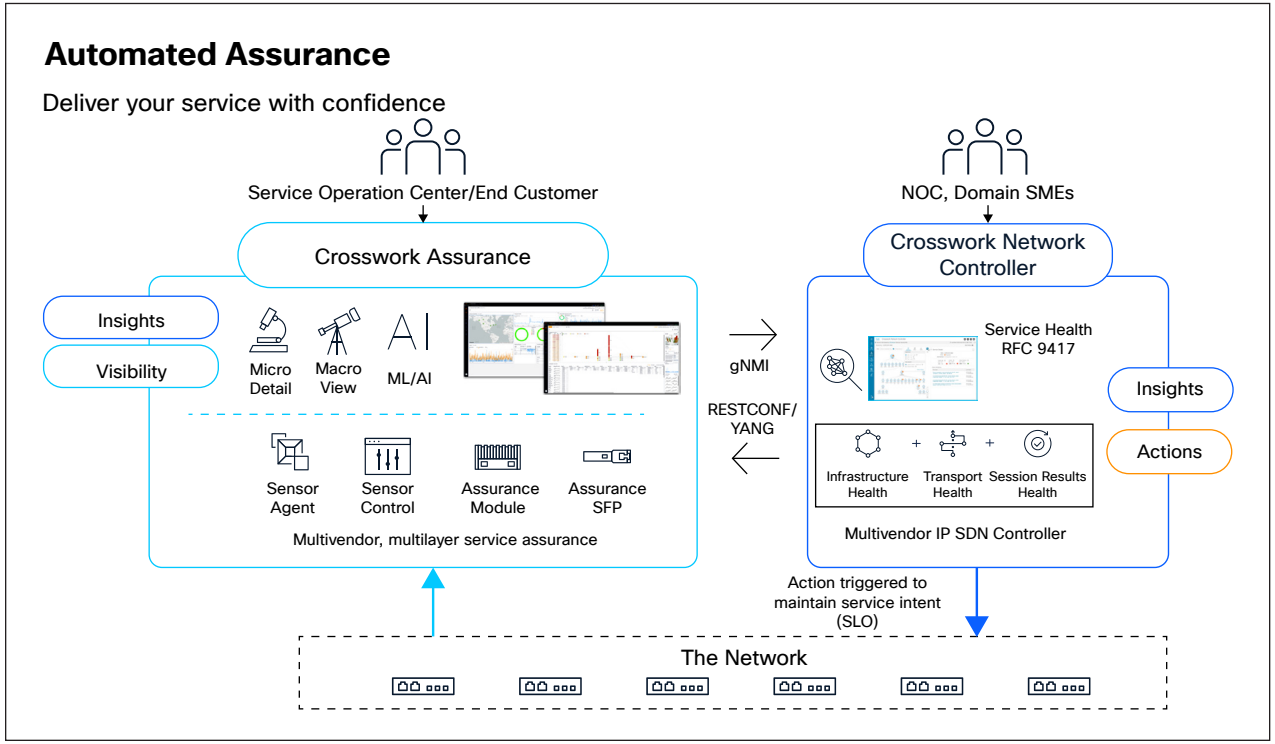


Figure 1. Crosswork Network Controller + Crosswork Assurance Integrated Solution

At the second layer, the Network Operation Center (NOC), operators use active topology maps enabled by Crosswork Hierarchical Controller (HCO) to drill down and find the root cause of issues. HCO is a multidomain controller with visibility that enables the NOC team to determine if issues are confined to a single domain or span multiple domains.

Equipped with these insights, domain-specific Subject Matter Experts (SMEs) can pinpoint and isolate components that impede network performance and service quality, taking corrective action to fix them.

The Crosswork platform seamlessly integrates and facilitates closed-loop, automated assurance operations, enabling a streamlined flow of information that is accessible and actionable for various teams. Whether it's the SOC, NOC, or domain SMEs, a clear and comprehensible view ensures quick understanding and fast remediation.

© 2026 Cisco and/or its affiliates. All rights reserved.

Deliver outstanding experience

An intent-based approach to service assurance helps you quickly understand if, where, and why services are degrading to accelerate issue resolution. You'll know when changing traffic conditions impact SLAs, and you'll be able to automatically optimize the network. You can also leverage AI-powered predictive analytics to mitigate anomalies before service is disrupted and customers are impacted.

Crosswork's advanced automation solutions work together to provide end-to-end visibility into network performance and service health. Continuous, data-driven insights make it easy to optimize dynamically and take swift action to resolve anomalies for consistent service quality, performance, and end-user experience. Intent-based automated assurance is how you deliver the outstanding experiences and differentiated services your customers expect.

How it works

Crosswork Assurance orchestrates and fully automates monitoring and assurance capabilities through the Crosswork Network Automation platform. Crosswork Network Controller and Crosswork Network Services Orchestrator drive automation decisions based on real-time network performance information and proactive alerting. Here's how it works:

- Assurance Sensors are deployed using Crosswork NSO as part of the automated workflow when new transport layers or VPNs are defined using service intent. Activation testing templates and other automated test sequences are used to activate service assurance.
- NSO triggers these templates using the NETCONF and YANG API to achieve closed-loop automation. This actively verifies that services work after being provisioned by NSO and continue to perform over the service lifecycle.
- Performance data and events can be further analyzed in Crosswork Assurance or can be sent back to Crosswork Network Controller to correlate KPIs with other events coming from the infrastructure. This process supports SLA management, AI/analytics, databus, and end-customer SLA reporting portals.

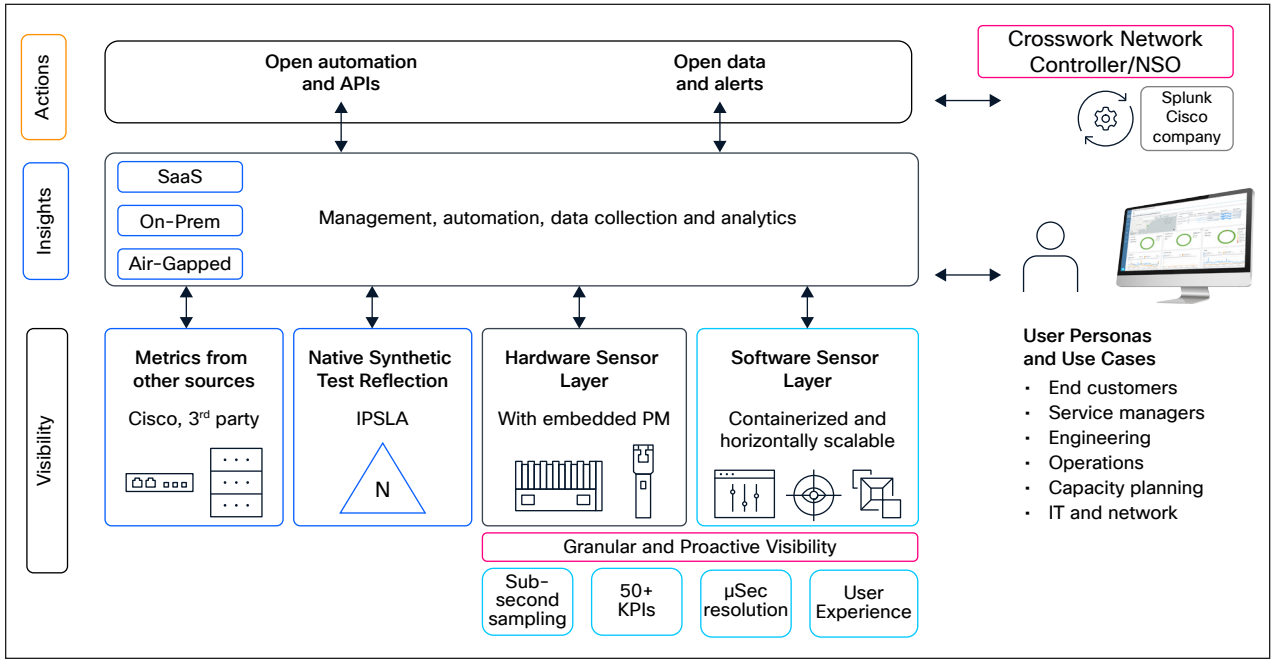


Figure 2. Crosswork Assurance: Closing the Loop for Autonomous Networks

© 2026 Cisco and/or its affiliates. All rights reserved.

Use cases

Table 1. Use cases

Use case	Description
Transport slicing automation and assurance	• Automate transport service provisioning and assurance. • Design, deploy and manage service slices across the entire lifecycle, monitoring the health of VPN services on Segment Routing over IPv6 (SRv6) networks. • Enhance service assurance with deeper insight via external sensors and dynamically optimize in real time.
Differentiated business services	• Leverage service assurance to enable SLAs to be offered for availability, latency and other KPIs. • Achieve proactive service health monitoring, enhanced with deep insight-critical for VPNs and latency-sensitive services. • Improve quality of experience and reduce customer churn, while driving down operational cost. • Enable upsell via end-customer reporting portals based on Crosswork Assurance.
Multivendor, multidomain, multilayer service lifecycle management	• Validate the service path at initial activation. • Automate service provisioning and assurance. • Continuously monitor the network and service layers throughout the service lifecycle. • Perform advanced troubleshooting and root cause analysis. • Gain real-time visibility into the network (underlay) service performance with proactive alerting on degradation or anomaly detection.

© 2026 Cisco and/or its affiliates. All rights reserved.

Benefits



ACG research confirms that automated assurance can reduce the time it takes to launch new, differentiated services by 85%.



Get to problem resolution 31% faster.



Lower your operational expenses by 55%.

Cisco Capital

Financing to help you achieve your objectives

Cisco Capital® can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For more information

Deliver a superior digital experience every time

Do you have the tools you need to meet QoE and QoS demands? Get proactive about service quality with automated assurance. See, understand, and act on network issues in real time, across domains and with agility—all while keeping operational costs low. For additional information, visit www.cisco.com/go/automatedassurance, then contact your Cisco Services sales representative.

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C22-2545260-04 06/26