SPOTLIGHT

Sponsored by: Cisco

Modern WAN platforms empower organizations with secure, agile, and scalable connectivity for the unique challenges AI applications pose.

Reinventing the WAN for AI: Intelligent, Secure, High-Performance Connectivity

April 2026

Written by: Brandon Butler, Senior Research Manager, Enterprise Networks

Introduction

The AI era is fundamentally reshaping WAN requirements, driving a shift from traditional cloud-centric networking to architectures optimized for distributed AI workloads. Unlike in the cloud era, enterprises now face a surge in application diversity, agentic workflows, and multimodal traffic (voice, video, and data and telemetry), all of which place simultaneous and highly variable bandwidth and latency pressures on the network.

In the agentic era, AI runs on continuous interactions between users, agents, models, and tools — often across branches and clouds — putting network performance directly on the critical path of work. The rise of application-to-application communications, driven by agentic workflows with strict latency budgets, will make performance assurance and policy management more challenging.

AT A GLANCE

KEY STATS

IDC's 2025 *AI in Networking Special Report Global Survey* found that 78% of respondents agreed or strongly agreed with the statement: "My efforts in network automation must be fueled by AI capabilities."

The same survey found that most AI applications (55%) will be implemented within cloud provider platforms, necessitating a renewed need for optimized and secure WAN connectivity for AI workloads.

In many environments, AI workloads create traffic flows that are often bursty and unpredictable, raising the bar for consistent performance. The growing role of inference at the edge and the need for ROI from distributed AI are accelerating the demand for WAN platforms that assure performance, security, and operations across hybrid environments.

Meanwhile, AI is ushering in a new era of network management, enabling meaningful operational efficiencies in the engineering and assurance of the network. IDC's 2025 *AI in Networking Special Report Global Survey* found that 78% of respondents agreed or strongly agreed with the statement: "My efforts in network automation must be fueled by AI capabilities."

To address these challenges, organizations must:

- **Optimize networking for AI:** Support high-performance, low-latency connectivity for distributed AI workloads, agentic app-to-app interactions, and multicloud management, particularly in the WAN. This increasingly requires automated identification and classification of emerging AI applications; manual discovery and tuning cannot keep pace.

- **Secure AI:** Implement governance and control for AI usage (including shadow AI and agent-to-agent policy enforcement). This includes applying the appropriate level of contextually aware security controls without introducing friction that degrades latency-sensitive workflows.
- **Embrace AI-powered operations:** Embed AI into WAN platforms for assurance, automation, and proactive troubleshooting, enabling cross-domain collaboration and improved user/application experience.

This IDC Spotlight explores the critical role that next-generation, AI-driven WAN platforms with native, quantum-safe security play in accelerating organizations' secure and optimized use of AI applications to drive business growth.

Key definitions

Below are explanations of key drivers of WAN modernization.

- **Platform-based networking:** This refers to an integrated system of network hardware, software, policy management, and APIs with an intuitive user interface and advanced AI-powered telemetry, analysis, and automation, enabling unified management across disparate domains. In an AI-driven environment, networking platforms are increasingly critical for supporting assured connectivity and simplified policy management, as well as applying AI-enhanced operations and AI-powered security controls, including visibility into new AI-driven traffic patterns and governance of AI usage.
- **Software-defined wide area network (SD-WAN):** An SD-WAN is a virtual WAN architecture that enables enterprises to securely connect users to applications, leveraging centralized control, dynamic path selection, and integrated security across multiple transport types. In 2026 and beyond, SD-WAN platforms are expected to deliver AI-driven assurance, policy enforcement, and support for distributed inference workloads.
- **Secure access service edge (SASE):** This cloud-delivered architecture converges networking and security functions, such as SD-WAN, firewall, and zero trust network access, into a unified service for secure, scalable access to applications and data. SASE platforms must increasingly provide AI-aware security controls, including policy enforcement over agent-to-agent interactions and shadow AI governance.
- **Quantum-safe networking:** This refers to the implementation of cryptographic protocols and network architectures designed to withstand future quantum computing threats, ensuring data integrity and confidentiality against "harvest now, decrypt later" attacks.
- **AI security/governance:** This is the ability to automatically identify AI applications and control access and usage, including fine-grained controls for shadow AI (allow/monitor/block) and policy enforcement over agent-to-agent interactions (semantic proxy concepts and zone-based segmentation for AI apps).

Key trends driving the WAN market

As organizations across the globe embrace AI-driven business models, the WAN market is undergoing rapid evolution. SD-WAN and SASE architectures are now foundational to enabling secure, resilient, and high-performance connectivity for distributed applications, users, and AI workloads. However, the AI era has introduced a set of new challenges and opportunities for the WAN market.

The following trends are shaping the future of WAN platforms, with direct implications for SD-WAN and AI networking strategies.

- **Assuring WAN performance for distributed AI workloads:** The proliferation of AI applications, especially those requiring real-time inference at the edge, demands WAN platforms that deliver low-latency, high-bandwidth, and application-aware connectivity. Networks must now support a surge in app-to-app communications, highly variable traffic patterns (voice, video, data, telemetry), and agentic workflows. This shift from cloud-centric to distributed AI architectures makes performance assurance and policy enforcement more complex and critical. Enterprises need WAN solutions that can dynamically optimize traffic flows, prioritize latency-sensitive AI workloads, and adapt to evolving application patterns to maximize ROI from distributed AI investments. Because new AI applications and tools can emerge faster than IT teams can manually classify and tune policies, automated discovery, classification, and intent-based optimization are necessary to maintain predictable performance.
- **Transforming WAN operations and management through AI:** AI is increasingly embedded into WAN platforms to drive automation, assurance, and proactive troubleshooting. Advanced AIOps capabilities enable predictive analytics, guided remediation, and closed-loop optimization across network domains. AI-powered tools facilitate cross-team collaboration (NetOps + SecOps), moving beyond simple chat interfaces to shared, context-rich workflows. Simplified operations and reduced mean time to resolution (MTTR) are essential as network complexity grows. AI-powered management improves user and application experience, streamlines troubleshooting, and enables scalable operations as AI traffic volumes and variability increase.
- **Securing AI (governance, policy, and quantum-safe networking):** The rise of AI introduces new security challenges, including shadow AI governance (controlling which users/apps can access AI), policy enforcement over agent-to-agent interactions, and the need for quantum-resistant encryption. WAN platforms must integrate advanced security features, such as zero trust, SASE, and support selective security inspection of AI-related traffic when deeper analysis is required. As AI-driven threats and regulatory requirements evolve, organizations require WAN solutions that can enforce granular policies, detect anomalous behaviors, and safeguard sensitive data against future cryptographic risks.

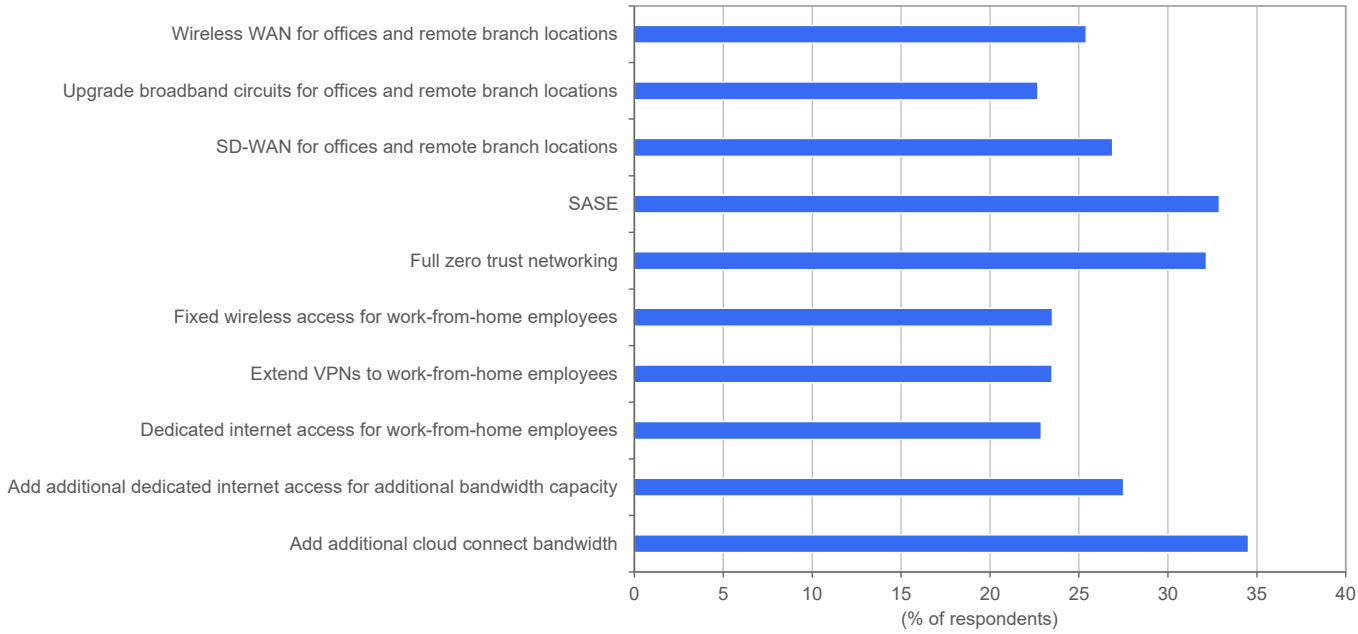
Core characteristics of an AI-driven, secure WAN platform

Modern WAN platforms are defined by their ability to unify networking, security, and operational intelligence into a single, integrated system. These platforms go beyond traditional connectivity, offering advanced features such as AI-driven analytics, dynamic policy enforcement, and seamless cloud integration.

Figure 1 shows results from an IDC global survey in which respondents were asked what their top network configurations are to support the future state of their business. The results show the striking power of a WAN platform that is inclusive of networking, security, and direct cloud connectivity.

FIGURE 1: ***The top network configurations for future business needs highlight the benefits of WAN platform capabilities***

Q ***As you look to the future state of your business, including hybrid work, what are the top 3 network configurations that your company will prioritize and implement?***



Source: IDC's *Future Enterprise Connectivity Infrastructure and Services Survey* (August 2025); n = 758

The following core characteristics distinguish leading WAN solutions and enable enterprises to meet the demands of distributed applications, hybrid workforces, and AI-powered business models in the AI era.

- **Comprehensive portfolio:** A comprehensive portfolio includes hardware and software solutions spanning networking, security, and assurance, with flexible offerings to meet diverse customer requirements, and combines best-in-class components with the advantages of a platform that enables "better together" solutions.
- **Traditional enterprise routing:** This includes support for broadband, MPLS, and cellular connectivity technologies, with reliable routing for established enterprise use cases.
- **SD-WAN capabilities:** These include dynamic management of multiple WAN connections, optimized for AI workloads, including agentic and app-to-app communications, with automatic assurance of performance, cost optimization, and enhanced resiliency. SD-WAN capabilities also include the ability to identify and classify rapidly evolving AI applications and to dynamically steer latency-sensitive flows based on intent and performance.
- **Integrated security/SASE support:** Native cloud-based secure services edge (SSE) integrations combine SD-WAN with universal zero trust, secure web gateway, and cloud access security broker, with a strong emphasis on AI security tools, controlling what AI tools users and applications are allowed to use, with fine-grained guardrails. For AI-era workflows, integration should enable policy-consistent security and governance while preserving WAN

performance (e.g., selectively steering AI traffic for deeper inspection when required.) Quantum-safe security capabilities natively embedded across the system are also critical.

- **Support for SD-Branch**: WAN platforms that integrate with wired/wireless local area network management enable further operational and security efficiencies and expand the scope of what AI-powered management capabilities can be applied to.
- **Detailed visibility and analytics**: Deep insights into user, application, and network telemetry, and insights into "owned" and "unowned" networks are foundational for delivering assured experiences.
- **Advanced AI-powered management:** This refers to cross-domain AI-driven functions, particularly in the areas of analysis, optimization, security, and prediction for assurance and predictive operations. They include AI-assisted diagnosis and closed-loop automation and support of collaborative, cross-domain operations when incidents span networking, security, and application performance.
- **Direct connections into public clouds and cloud edges:** These include POP-based architectures that connect directly to IaaS and SaaS clouds and integrate with cloud middle-mile vendors and cloud WAN services, enabling more predictable access to cloud-hosted AI services, models, and distributed applications.

Benefits of a platform-based approach to the WAN

Adopting a platform-based WAN strategy delivers meaningful advantages for enterprises navigating the demands of distributed applications, hybrid workforces, and AI-powered business models. Modern WAN platforms unify networking, security, and operational intelligence, enabling organizations to simplify management, accelerate innovation, and optimize performance in an increasingly complex environment.

Today, having fine-grained and powerful security tools for protecting sensitive corporate data is critically important. Key benefits include:

- **Future proof WAN for the AI era:** The AI era is rapidly reshaping traffic patterns, particularly in the WAN. AI-driven platforms must adapt to support diverse and distributed applications with highly variable bandwidth and latency qualities. IDC's 2025 *AI in Networking Special Report Global Survey* found that most (55%) AI applications will be implemented within cloud provider platforms, necessitating a renewed need for optimized and secure WAN connectivity for AI workloads. WAN platforms that combine advanced infrastructure with powerful and secure AI-driven operations will be future proofed to seamlessly support the rise of agentic workflows, application-to-application communications, and multimodal traffic patterns while ensuring performance, security, and operational agility. As AI usage scales, automated classification and intent-based policy become essential to prevent business-critical AI workflows from competing with non-critical AI traffic and experiencing variability.

  Why it matters: This enables enterprises to ensure that the WAN is a strategic enabler of networking requirements, rather than a bottleneck.

- **AI-powered automation, assurance, and predictive operations:** Embedding AI into WAN platforms enables advanced analytics, proactive troubleshooting, and closed-loop optimization. AI-driven assurance improves user and application experience, while predictive operations help forecast issues and automate remediation across network domains. IDC's 2025 *AI in Networking Special Report Global Survey* found that 31% of organizations'

campus and branch network management tasks are augmented by AI, a figure projected to grow to more than half (51%) in two years, indicating the rapidly growing use of AI-powered network operations, including in the WAN.

Why it matters: Enhanced operational efficiency and reliability are essential as network complexity and performance demands increase, especially for latency-sensitive AI workloads.

- **Integrated security and governance:** Platform-based WANs converge networking and security, delivering zero trust, quantum-safe encryption, and granular policy controls for shadow AI and agent-to-agent interactions. SASE architectures provide unified enforcement and real-time threat detection across hybrid environments.

  Why it matters: As AI-driven threats and regulatory requirements evolve, organizations need WAN solutions that safeguard data, ensure compliance, and constantly evolve to enforce security policies at scale.

- **Simplified operations and cross-domain management:** Platform-based WANs provide unified management across networking, security, and cloud domains, streamlining configuration, monitoring, and troubleshooting. AI-powered automation and guided remediation reduce operational overhead and MTTR while enabling NetOps and SecOps teams to collaborate from a common view. This is critical because most WAN pain points occur post-deployment, during day 2 operations, reducing operational friction and the integration burden associated with point tools.

  Why it matters: Advanced, AI-driven WAN platforms become the basis for organizations' connectivity strategies in the AI era, enabling enterprises to manage complex, multicloud environments more efficiently, reducing risk and freeing IT resources for strategic initiatives.

- **Accelerated innovation and agility:** Unified WAN platforms allow organizations to rapidly deploy new applications and services, including AI workloads, without redesigning the network for each new workflow. Integrated SD-WAN and SASE capabilities support flexible deployment models and seamless cloud connectivity, enabling faster adoption and simpler life-cycle management.

  Why it matters: Businesses can respond quickly to changing requirements, support distributed workforces, and maximize ROI from AI and cloud investments.

These benefits position platform-based WAN solutions as critical enablers for enterprises seeking to thrive in the AI era, delivering operational simplicity, security, agility, and performance across increasingly distributed and dynamic environments.

Considering Cisco

Cisco offers a unified WAN platform designed to support seamless and secure connectivity across hybrid and distributed work environments. The solution integrates SD-WAN, SASE, and SD-Branch architectures within a single management console, enabling organizations to manage networking and security functions from a centralized interface.

Advanced AI capabilities include next-generation infrastructure for supporting the needs of high-bandwidth, low-latency AI traffic patterns, combined with automated visibility into emerging AI application flows and adaptive traffic optimization to maintain predictable performance. AI-enhanced management capabilities are embedded throughout the platform. Integrated security includes components for securing AI workloads and preparing for a quantum-safe future.

Key elements include:

- **Platform-based management and deployment flexibility:** Cisco's approach emphasizes platform-based management, providing universal hardware and licensing across the Catalyst and Meraki portfolios. The solution supports cloud-based and on-premises deployments, allowing organizations to select the operational model that best fits their requirements.
- **AI-enabled network operations:** Cisco's AI Assistant and AI Canvas are designed to democratize AI-powered network management. These tools offer natural language interfaces, automated diagnostics, and a shared, context-rich workspace that helps teams collaborate across domains, supporting more efficient and accessible network operations.
- **Secure AI workloads:** Cisco secures enterprise AI with network-embedded guardrails, policy-based access control, continuous runtime monitoring, and fine-grained data loss prevention, protecting against shadow AI, unsafe outputs, and sensitive data exposure across clouds and SaaS.
- **Quantum-safe SD-WAN fabric:** The platform incorporates quantum-resistant encryption and secure boot capabilities, aiming to prepare organizations for future cryptographic threats and defend data in transit against emerging risks.
- **Integrated security features:** Security is addressed through features such as Hybrid Mesh Firewall and Zero Trust Access, which provide unified policy enforcement, and real-time threat detection across physical, virtual, and cloud-native environments.
- **Cloud and multicloud connectivity:** Cisco SD-WAN enables secure, high-performance connectivity across public cloud, multicloud, and hybrid environments through integrated cloud on-ramp capabilities and automated multicloud access. The platform supports direct high-performance connectivity to hyperscalers, emerging specialized cloud service providers, and distributed applications as well as to IaaS, SaaS, and AI datacenter environments, helping enterprises deliver consistent application performance at scale. Its cloud-agnostic approach and centralized operational control help maintain consistent policy across distributed deployments while addressing evolving sovereignty, resiliency, and AI infrastructure access requirements.
- **Telemetry, assurance, and observability:** The platform is designed to deliver measurable outcomes through advanced telemetry, AI-powered assurance, and observability, with integrations to tools such as ThousandEyes and Splunk for enhanced visibility and analytics.
- **Extensibility and ecosystem support:** Cisco's WAN solution supports API integrations, third-party management systems, and flexible hardware options, enabling organizations to tailor deployments to diverse enterprise requirements.

This platform-centric approach is intended to address the operational, security, and connectivity needs of modern enterprises, supporting distributed applications, hybrid workforces, and evolving AI-driven business models.

Challenges

As organizations adopt advanced WAN platforms and integrate AI-powered applications, Cisco and its customers face several key challenges:

- **Varied organizational maturity for AI adoption:** Enterprises are at different stages in leveraging AI-powered applications and network automation. This disparity can complicate deployment strategies, training, and the realization of operational benefits across diverse environments. Vendors such as Cisco must offer a simple road map of AI-driven solutions that enable organizations to gain operational value from AI while maintaining control. Cisco's AI Assistant and AI Canvas provide a range of use cases with detailed logging capabilities, enabling organizations to leverage a range of guided to automated AI-powered actions.
- **Rapid proliferation of AI applications and evolving threats:** The fast-paced growth and adoption of AI applications introduce new security risks and operational complexities. WAN platforms must continuously evolve to address emerging AI-based threats and ensure robust governance and policy enforcement. Vendors such as Cisco are investing in advanced capabilities that improve visibility and control over AI-driven traffic, including deeper semantic inspection and classification of both generative and agentic AI applications. These capabilities enable organizations to identify AI usage patterns, apply granular policies, and strengthen their security posture as AI adoption accelerates.
- **Networking and security investments aligned to business outcomes:** Cisco and its customers must ensure that investments in networking and security technologies are closely aligned with strategic business initiatives and desired outcomes. This requires ongoing collaboration between IT and business stakeholders and is particularly relevant in the AI era, when organizations are looking to move fast and not fall behind competitors that are leveraging AI tools. Embracing AI-based applications while assuring security and performance is a key priority.

Conclusion

With the rise of AI, organizations are fundamentally rethinking their network strategies. In the WAN, the need to support distributed applications, agentic workflows, and multimodal traffic across hybrid and multicloud environments is heightened with a flood of variable and latency-sensitive AI workloads. In response, enterprises are increasingly adopting platform-based approaches that unify networking, security, and operational intelligence, enabling them to optimize performance, simplify management, and accelerate innovation. SD-WAN and SASE architectures are now foundational components, providing the flexibility and assurance needed to meet the demands of AI-powered business models. Advanced AI-driven operations and quantum-safe security features are becoming essential to future proof the network. By leveraging modern WAN solutions, organizations can position themselves to thrive in an increasingly dynamic and AI-driven digital landscape.

About the Analyst

Brandon Butler, *Senior Research Manager*

Brandon's research focuses on market and technology trends, forecasts, and competitive analysis in enterprise campus and branch networks. His coverage includes technologies used in local and wide area networking, such as Ethernet switching, routing/SD-WAN, wireless LAN, and AI-powered enterprise network management platforms.

MESSAGE FROM THE SPONSOR

As organizations adopt AI-driven applications and distributed workflows, network architectures must evolve to support new traffic patterns, operational requirements, and security expectations. AI workloads introduce highly dynamic, latency-sensitive interactions between users, applications, cloud environments, and emerging AI infrastructure, increasing the importance of consistent connectivity, policy control, and operational simplicity across the WAN.

Cisco believes modern WAN platforms should combine intelligent traffic awareness, adaptive optimization, and integrated security to help organizations deliver predictable performance while maintaining governance across hybrid and multicloud environments. By unifying networking and security operations and embedding AI-driven assurance into the platform, organizations can simplify management and prepare their infrastructure for evolving AI and cloud requirements, including future cryptographic resiliency.

Learn more about Cisco SD-WAN:

cisco.com/go/sd-wan

Read ebook

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com