

Branch transformation powered by AI-enhanced platforms

Platform-based approaches to branch networking feature integrated security, advanced AI-powered operations, and comprehensive assurance.



Brandon Butler
Senior Research Manager,
Enterprise Networks, IDC

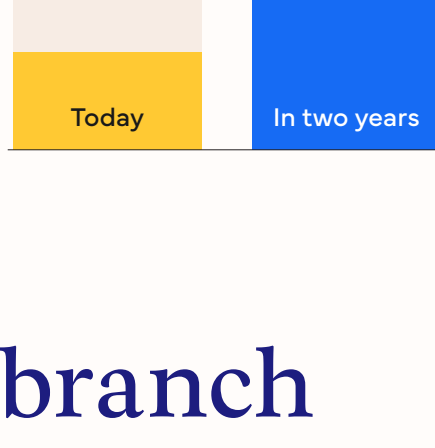
Significant network transformation is underway

“I am moving to an AI-powered platform approach for networking.”



of respondents agreed or strongly agreed with the statement.

Organizations whose connectivity strategy is “extensively connected,” where networks are “intelligent, edge-enabled, and self-aware.”



Note: Data weighted by IT spending by country.
n = 758; Source: IDC's Future Enterprise Connectivity Infrastructure and Services Survey, August 2025.

Top factors driving branch network transformation

Branch offices — where customers, partners, and employees directly interact with the business — are a key area of network transformation, due to:



Business and technology drivers

- Business drivers include equipment refreshes, mergers and acquisitions, and return-to-office initiatives.
- Tech drivers include Wi-Fi 7, SD-WAN/SASE, and AI-powered management capabilities.



Disparate technologies

- Disaggregated systems in the branch across wired and wireless LAN, routing/SD-WAN, security, and assurance complicate management, inhibit agility, and degrade user experiences.



Artificial intelligence

- AI applications, including generative and agentic AI, are flooding the network.
- AI-powered network automation improves how networks are deployed, optimized, secured, and managed.



Enhanced automation and comprehensive assurance needs

- Disparate infrastructure components with separate management tools make it difficult to gain visibility into network performance and operations across the branch.
- Manual processes lead to errors and security vulnerabilities.
- Unstructured and decoupled automation tools are difficult to implement and optimize.

Top connectivity challenges

From a networking perspective, what are the top 3 ranked connectivity-related challenges your organization faces?



Network security



Network reliability and resiliency



Aligning network infrastructure to AI applications



Aligning network infrastructure with cloud connectivity requirements



Managing and optimizing hybrid networks



Incorporating new/emerging access/networking technologies (e.g., 5G, LEO Satellite, Wi-Fi 7, SD-WAN, Private LTE/5G, cloud)

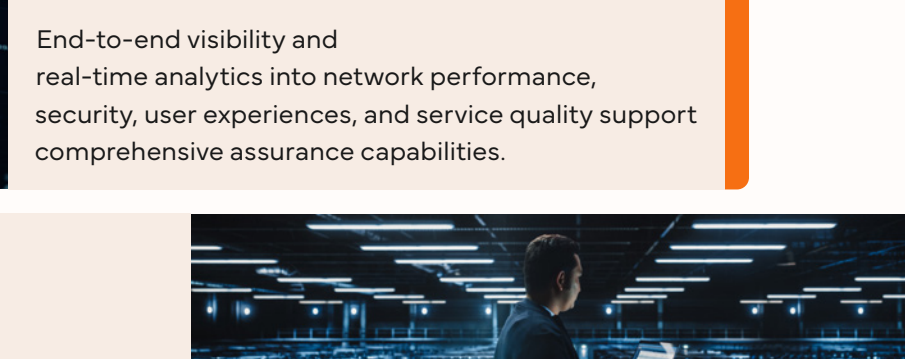
Note: Data weighted by IT spending by country; multiple dichotomous table-total will not sum to 100%.
n = 758; Source: IDC's Future Enterprise Connectivity Infrastructure and Services Survey, August 2025.

Key elements of a unified branch platform

Next-generation unified branch network and security strategies include:

Advanced hardware, managed centrally:

Platform-based unified branches should feature best-in-class network and security hardware components, managed via a unified system.



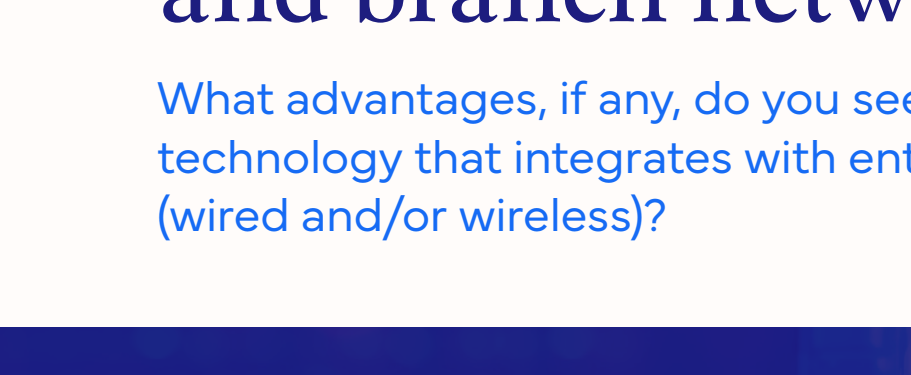
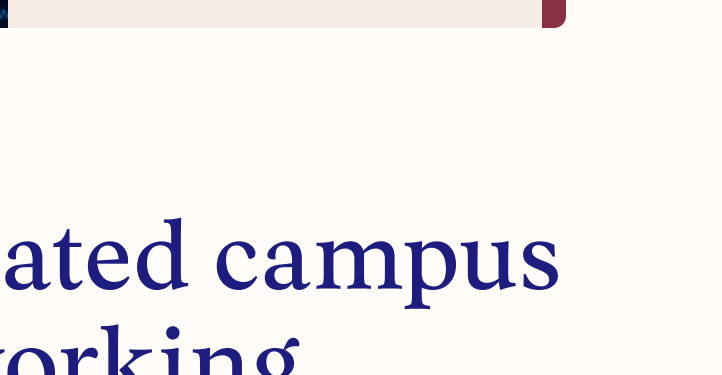
Universal visibility and analytics:

End-to-end visibility and real-time analytics into network performance, security, user experiences, and service quality support comprehensive assurance capabilities.



Advanced automation:

AI-powered operations and infrastructure as code (IaC) facilitate consistent scalable deployment and management, improving performance optimization and automating issue resolution.



Built-in security

Zero trust and SASE support reliable secure connectivity for all users and devices.

Benefits of integrated campus and branch networking

What advantages, if any, do you see with SD-WAN technology that integrates with enterprise networking needs (wired and/or wireless)?

Consistent security policies for users and devices across LAN and WAN

30%

Easier deployment and management of the WAN because of LAN integrations

29%

Optimized application experiences regardless of device location or access technology

27%

Note: Multiple dichotomous table-total will not sum to 100%.
n = 1,018; Source: IDC's IDC's SD-WAN Survey, 2024.

Advice for implementing unified branch strategies



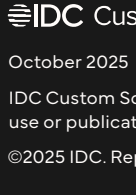
Future-proof with AI-ready infrastructure:

Branch network infrastructure should be scalable and flexible, ensuring readiness for evolving business needs, specifically generative and emerging AI workloads.



Ensure native security:

Security components should be built-in, not bolted on to the unified system.



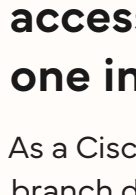
Leverage best-in-class components with unified management:

Optimize performance and reliability with best-in-class components; gain centralized visibility, analytics, and more rapid problem identification and resolution with unified management.



Simplify operations:

Adopt advanced automation, including IaC and AI-powered tools, to enhance security and service quality while reducing operational complexity.



Focus on optimizing user experiences:

Advanced infrastructure and AI-driven assurance enable reliable network performance, streamline operations, and enhance resiliency by minimizing downtime and security risks.

Message from the sponsor



Cisco Unified Branch is a full-stack platform approach to branch office IT ensuring networking, security, cloud access, visibility and management are consolidated into one integrated solution.

As a Cisco validated solution, Cisco Unified Branch simplifies, secures, and accelerates branch deployments, providing the necessary capacity to handle the demands of distributed applications, AI workloads and Agents.

[Learn more](#)