

Organizations are increasingly realizing the myriad benefits of a unified platform-based approach to transforming their branch network and security strategies.

# Powering Branch Transformation with AI-Enhanced Secure Platforms, Advanced Automation, and Integrated Assurance

September 2025

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

## Introduction

The enterprise branch is in a state of transition. Enterprise branch locations are typically geographically distributed and diverse in terms of scale and enterprise IT needs, creating unique challenges from an IT and network perspective. Branch offices are also critically important to enterprises: They are the front lines where customers, partners, and employees interact with the business directly.

A complex set of disparate technologies combined to create a highly heterogeneous environment has predominantly defined past approaches to branch network architectures. Disaggregated approaches have been driven by misalignment of deployment or refresh cycles, organizations attempting to optimize individual technologies, or legacy installations of certain infrastructure. The result is too often the same. Management of nonintegrated systems results in manual, piecemeal approaches to engineering and operating varied components across wired and wireless LAN, routing/SD-WAN, security, and assurance. Moreover, inefficient operations inhibit business agility and can result in poor user experiences.

In the AI era, organizations need a new approach. An explosion of AI workloads is flooding branch office networks, prompting organizations to rethink the network designs and capabilities of branch offices. Almost every application the branch uses includes an AI element. AI workloads, particularly generative and agentic AI applications, have unique latency and jitter requirements, leading organizations to reconsider high-bandwidth, low-latency connectivity to ensure high-quality user experiences across mission-critical applications running in branch offices.

## AT A GLANCE

### KEY TAKEAWAYS

- » **Challenges in enterprise branch networking:** The distributed nature and scale of enterprise branches means organizations often rely on disaggregated systems that complicate management, inhibit agility, and degrade user experiences.
- » **Impact of AI on branch networks:** AI workloads, including generative and agentic applications, require high-bandwidth, low-latency connectivity in the branch. They are transforming network management through AI-powered automation, improving performance, user experience, and security.
- » **Unified platform-based approach:** IDC research shows the benefits of unified branch architectures that integrate wired, wireless, WAN, and security management with AI-powered automation and simplified operations, ensuring high-quality network performance and security.

AI is also fundamentally changing how organizations manage their networks. AI-powered engineering and enterprise networking represent a new era of network management, ushering in the ability to automate a range of tasks that have traditionally been manual. The aim is to ensure high-quality user experiences, network and application performance, and enhanced security. However, AI-powered network management systems — and automation toolsets more broadly — are inefficient (at best) and incapable (at worst) on disaggregated branch network and security infrastructure.

IDC research shows strong links between the use of AI-powered networking and platform-based approaches to network design and management. Unified platform-based approaches, which provide common architectural frameworks, advanced automation, and integrated security, enable a range of technical and operational benefits for branch network and security designs.

Fundamentally, a unified branch architecture integrates the management of wired/wireless/WAN and security with advanced infrastructure, AI-powered automation, and native, comprehensive assurance. This enables a platform-based approach that simplifies management, facilitates advanced AI-powered automation, and ensures high levels of network performance, user experience, and robust security.

This IDC Spotlight highlights the top factors driving organizations toward branch transformation, outlines the key elements that make a unified branch, and showcases the top benefits organizations can expect to achieve from unified branch strategies.

## Top Factors Driving Branch Transformation

A variety of factors drive organizations to transform their branch network and security strategies. Refreshing old equipment, mergers and acquisitions, and supporting return-to-office initiatives are some common factors that drive branch transformation. From a technology perspective, exciting innovations like Wi-Fi 7, SD-WAN/secure access service edge (SASE), and AI-powered management capabilities are also driving forces. Overall, key themes driving branch transformation include:

- » **Disparate technologies and tools at the branch:** A top reason that organizations are looking to transform their branch operations is that their current environments are a complex mix of separate infrastructure, management, and policies for wired, wireless, WAN, security, and assurance. Using different tools for different technologies sows complexity related to monitoring, optimizing, and managing the network and makes it challenging to standardize configurations, troubleshoot issues, and scale operations across sites. Ultimately, inefficient network engineering and operations leads to poor user experiences and security vulnerabilities, representing a risk to the business.
- » **Preparing for, and taking advantage of, AI:** AI is already embedded in almost every application enterprises rely on for their business operations, including finance, HR, and logistics/operational applications. The next wave of AI, focusing on AI agents, could place significant strain on the network. For every user, there could be a multitude of agents, each requiring low-latency, high-bandwidth connectivity. Furthermore, AI represents a fundamental shift in how enterprise networks can be deployed, optimized, secured, and managed via new generative AI interfaces with AI-powered automation capabilities. As a result, organizations are looking to ensure their infrastructure — particularly their network — is ready for AI workloads today and into the future, and they are looking to take advantage of AI's power to improve the engineering and operations of the network.

- » **A lack of structured automation:** Organizations use a variety of approaches to overcome inefficient operations, from service provisioning automation to automated incident response. But these approaches have challenges: Automation processes that are not structured properly to tightly integrate with network and security infrastructure are inefficient and difficult to implement and optimize. Worse, reliance on manual processes leads to errors and security vulnerabilities and impedes the ability to scale operations efficiently.
- » **The need for comprehensive assurance:** Disparate infrastructure components that require separate management make it difficult to gain visibility into network performance and operations across the entire branch, including networks controlled by IT, as well as "unowned" networks IT does not directly control. True end-to-end assurance and built-in visibility into network and security performance and operations are foundational for enabling advanced automation and ensuring high-quality experiences.

IDC survey data further contextualizes these points: IDC's 2024 *Future Enterprise Connectivity Survey* (n = 751) asked respondents to identify their top connectivity-related challenges. Top responses included network security, incorporating new technology, network reliability/resiliency, and transforming networks to be more virtualized, scalable, and agile. Combined, these challenges — and the factors driving organizations to transform their branch networks — represent potential risks to organizations. Poor network performance leads to suboptimal experiences for employees, customers, and other stakeholders, especially when the strain of large AI workflows floods the network. Meanwhile, IT teams struggle to manage this complex, disparate system, requiring swivel-chair approaches to monitoring, managing, optimizing, and securing the branch. AI workloads and data sets that aren't centrally monitored and managed represent significant security risks to organizations.

## Key Elements of a Unified Branch

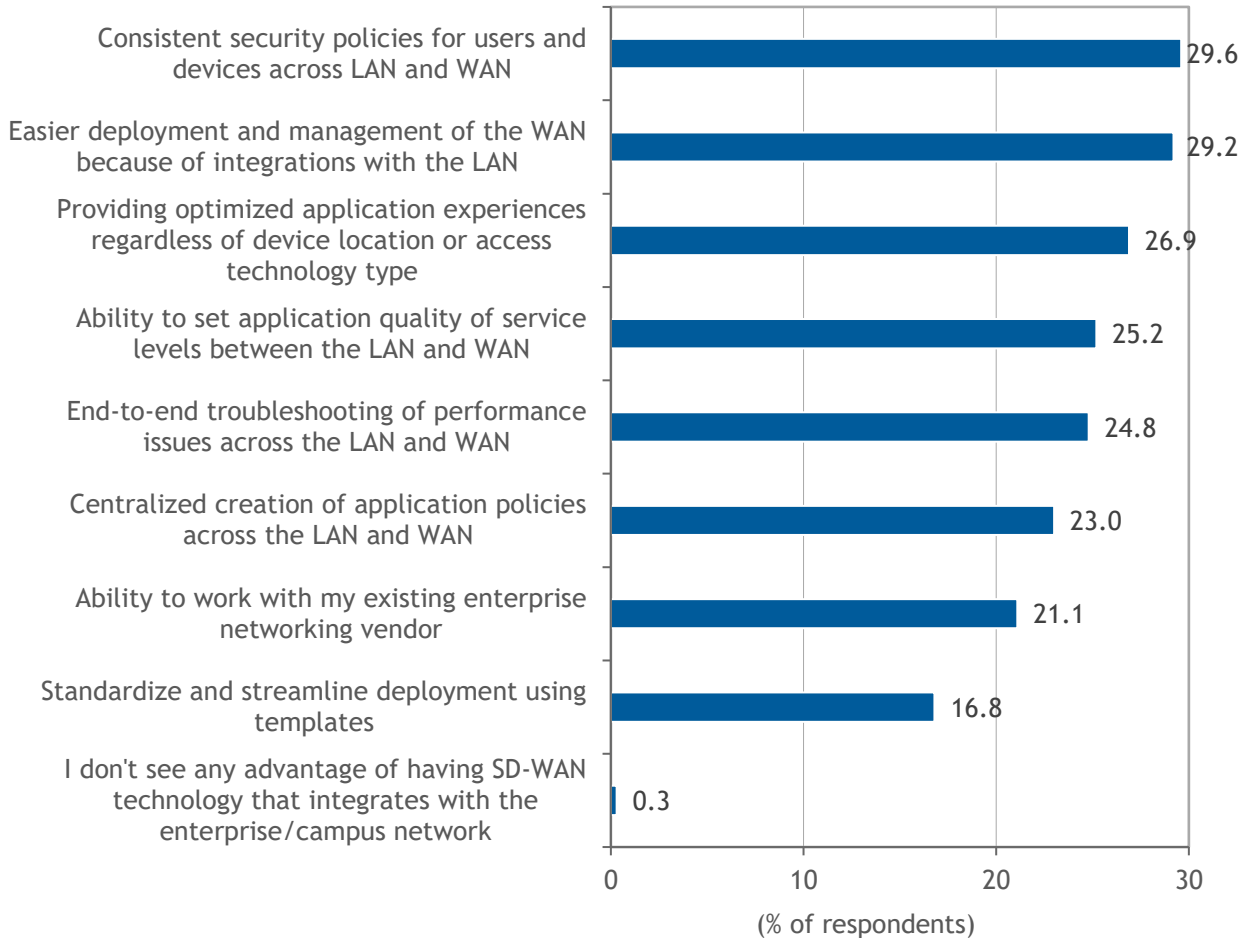
Organizations consider a variety of architectural elements when looking to transform their branch network and security strategies. The following are some of the key elements that make up a next-generation unified branch network and security strategy:

- » **Best-in-class elements managed via unified platform:** When considering a platform-based approach to branch architectures, there could be a trade-off between having high-quality components and centralized management. However, today's platform-based approaches have matured to the point where organizations can have both high-quality individual components (e.g., wired and wireless LAN, routing/SD-WAN, security, and assurance) and unified platform-based management with native security and advanced automation. IDC survey data reinforces the value IT end users gain from platform-based approaches to networking. IDC's 2024 *AI in Networking Special Report* found that 78% of survey respondents agreed or strongly agreed with the statement: "I am moving to an AI-powered platform approach to networking."
- » **Universal visibility and analytics:** A key element of a unified branch strategy is to have end-to-end visibility and real-time analytics across networks controlled by IT and those that are not. Real-time, historical, and predictive insights into network performance, security, user experiences, and service quality are key data. Consolidating insights across multiple individual components such as the LAN/WAN and security can provide a single view into network and security status. This approach enables faster detection, diagnosis, and resolution of issues and allows for proactive fault detection, consistent policy enforcement, and robust threat protection across all branch locations.

- » **AI-powered operations:** In addition to comprehensive visibility and analytics, organizations can apply AI-powered automation capabilities. Within a unified branch architecture, AI can enable zero-touch deployment, implement performance optimizations, and provide guided or automated issue resolution. AI can also enhance security through real-time threat detection and automated policy enforcement. IDC's 2024 *AI in Networking Special Report* found that 79% of respondents agreed or strongly agreed with the statement: "My efforts in network automation must be fueled by AI capabilities."
- » **Ability to leverage infrastructure-as-code (IaC) automation:** Being able to manage a unified branch architecture through DevOps-style automation toolkits enables consistent and accelerated deployment, configuration, and automation while reducing human error. Branch as code enables scalable, repeatable infrastructure deployment and management, which is especially critical in highly distributed branch locations where there may be limited onsite IT staff. It ensures security compliance through consistently applied policies and facilitates rapid recovery and updates, making branch network management efficient, reliable, and agile.
- » **Built-in security:** Security should be an in-built, core element of unified branch architecture. This includes strong security capabilities within each component of the unified branch architecture, from zero trust principles to SASE, as well as security tools, such as a next-generation firewall (NGFW) as a native component of a unified branch architecture that can be centrally managed via the unified platform and branch-as-code automation.

IDC survey data reinforces the opportunities enterprises see in more integrated management across their LANs and WANs. Figure 1 shows that the top benefits of more integrated wired and wireless LAN management with SD-WAN include more consistent security policies, easier deployment and management, and providing optimized application experiences.

FIGURE 1: **Top Benefits of Integrated Campus and Branch Networking (Wired/Wireless SD-WAN)**  
**Q What advantages, if any, do you see with SD-WAN technology that integrates with enterprise networking needs (wired and/or wireless)?**



n = 1,018

Source: IDC's SD-WAN Survey, 2024

## Benefits of a Unified Branch Approach

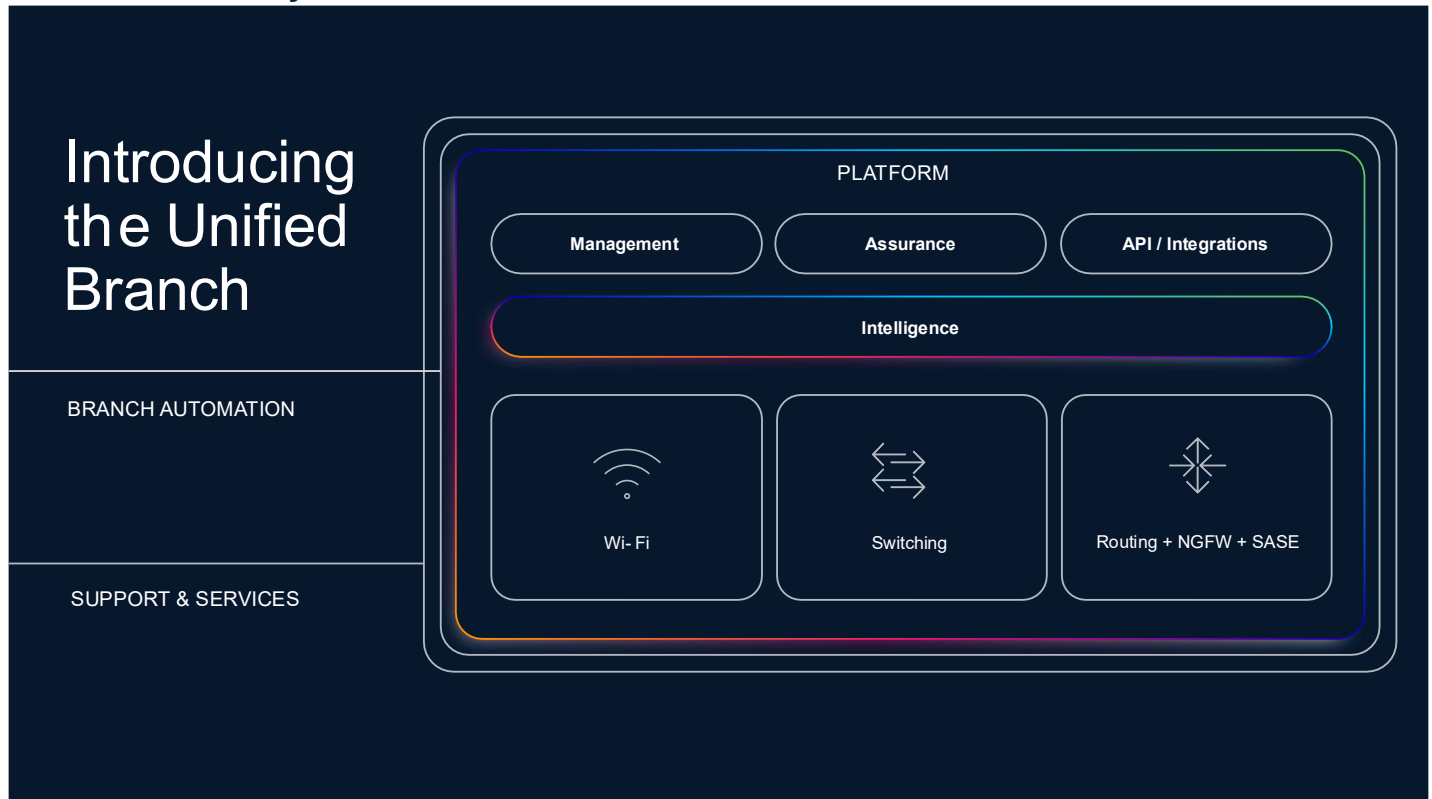
Combining the key elements of a unified branch enables a range of benefits, including:

- » **Operational simplicity and faster deployment:** Unified branch solutions enable zero-touch deployment and advanced automation, via both IaC and AI-powered automation. The result is faster deployment, streamlined scalability, reduced operational burden and complexity, and enhanced security and service quality.
- » **Robust and integrated security:** Having security fused into the network via next-generation firewall components provides faster security issue identification and resolution and stronger security defenses, enabling robust, consistent protection with locally enforced policies.

- » **End-to-end visibility and smarter troubleshooting:** Unified platforms consolidate data for full network and security visibility across network and security performance, end-user experiences, device health, and security posture management. By contrast, having disparate management of components across the LAN/WAN and security results in fragmented, incomplete views of the branch infrastructure and operations.
- » **Scalability and flexibility:** IaC and AI-powered automation capabilities enable rapid scaling and efficient ongoing management of branch configurations. Flexible platform-based approaches allow organizations to leverage a best-in-class system of integrated components to ensure branch infrastructure is rightsized for their use case.
- » **Enhanced user experiences:** The combination of advanced infrastructure, streamlined operations, and AI-enhanced assurance capabilities leads to improved network performance, reduced downtime, and faster security issue identification and resolution. In all, unified branch architectures enable enhanced experiences for users (e.g., employees, customers, partners) and IT.
- » **Future proofing the branch:** Platform-based approaches to unified branch architectures enable organizations to build a future-proof branch network and security strategy, ready to meet the needs of the business today, as well as being scalable and flexible to meet the needs of the future as more AI workloads flood the network.

### **Considering Cisco Unified Branch**

The Cisco Unified Branch offering is a modern, integrated branch network and security solution designed to simplify, secure, and accelerate branch deployments at enterprise scale. The full-stack solution unites Cisco's latest scalable AI devices ready for AI — including Cisco Smart Switches, Wi-Fi 7-supported wireless, Secure Routers with SD-WAN, and NGFW — all managed by a single platform. Cisco Unified Branch (see Figure 2) is a streamlined way for organizations to deploy and operate branch networks with enhanced security, performance, and operational efficiency.

FIGURE 2: *Cisco Unified Branch*

Source: Cisco, 2025

Key aspects of Cisco Unified Branch include:

- » **Integrated full-stack architecture:** The solution includes a set of tested and verified products that combine Cisco IOS XE software with best-in-class branch networking hardware built on Cisco silicon, including routing, switching, and wireless, plus integrated security. The Cisco Meraki Dashboard serves as the centralized management interface, offering unified visibility and control over physical and virtual branch infrastructure, enabling seamless updates, policy enforcement, and integrated AI-powered analytics.
- » **Cisco Validated Designs:** Cisco-validated and -tested design blueprints help accelerate branch deployments. These branch designs leverage Cisco's network and security architectural expertise so that best practices are followed for resilient, scalable, and secure branch infrastructures, reducing risk and deployment complexity.
- » **AI-powered operations:** Cisco Unified Branch leverages AI-powered operations, including the Cisco AgenticOps framework using the Cisco AI Assistant, to generate code templates and configurations and Cisco AI Canvas for generative, cross-domain, and multiuser customizable dashboards. Meanwhile, Cisco Unified Branch also supports a range of flexible automation capabilities. For simple automation tasks, Cisco Workflows provides prebuilt and custom automation templates for automating repetitive and time-consuming tasks across Wi-Fi, switching, WAN, datacenter, and so forth. For more advanced use cases, Cisco Unified Branch supports infrastructure-as-code and

DevOps automation principles using a branch-as-code toolkit. This enables automated provisioning, configuration, and change management at scale, accelerating deployments and minimizing human error and configuration drift.

- » **Zero-touch deployment:** Cisco Unified Branch rollouts are simplified and secure with zero-touch provisioning capabilities. Secure hardware and software from boot to runtime allows for trustworthy remote branch setups without the need for a local IT presence, reducing deployment time and operational costs.
- » **Comprehensive visibility and assurance:** Cisco integrates ThousandEyes within the unified architecture to provide end-to-end network visibility, real-time insights, and smarter troubleshooting. This capability helps quickly isolate issues across WAN, LAN, and cloud to provide high-quality user experiences and support rapid identification and resolution of network or security issues.
- » **Security fused into the network:** Security is deeply embedded within Cisco Unified Branch, with solutions such as integrated NGFW, post-quantum cryptography readiness, and support for secure access service edge. Cisco Unified Branch uses routers, switches, and wireless access points to support zero trust principles by continuously validating identities and enforcing segmented least privilege access. Unified management via IaC and AI-powered network automation helps ensure consistent security policy enforcement.

Cisco Unified Branch offers an advanced, software-defined branch architecture that seeks to transform how enterprises deploy, manage, and secure distributed networks, enabling branch deployment in moments, not months. By combining integrated networking and security, automation through automation toolkits, comprehensive assurance and analytics, and cloud-based management, Unified Branch provides a consistent, scalable, and secure branch experience that aligns with modern digital enterprise demands. This approach enables enterprises to conquer branch complexity and drive agility while maintaining robust protection against evolving cyberthreats.

### Challenges

Organizations face several challenges when implementing platform-based unified branch architectures. Some notable challenges for Cisco and its customers include:

- » Many organizations are at varying stages of maturity — and willingness — when it comes to leveraging advanced automation technologies such as IaC and AI-powered network operations. This is driven, in part, by difficulties among organizations in adopting DevOps principles, a lack of skill sets for managing configuration as code, and integrating AI-driven assurance. In response, Cisco has developed a range of automation toolkits to supplement dashboard-based ClickOps deployment. For example, Workflows is a GUI-based workflow builder that allows organizations to create step-by-step, validated workflow automation to deploy Unified Branch using Cisco Validated Designs and is powered by the Dashboard AI Assistant. For more advanced users, IaC toolkits are also available.
- » For AI-powered automation, Cisco offers a range of functions that are powered by AI to meet varying customer needs, from relatively low-risk use cases — such as analyzing large amounts of data for faster identification of network or security issues — to providing more advanced functions, such as human-in-the-loop recommended optimizations or automated remediations.
- » The widespread and distributed nature of branch networks can lead to operational complexity, including a lack of onsite IT staff, the risk of configuration drift, and increased security risks. Organizational challenges of managing staff and infrastructure resources across teams and sites contribute to the challenge. These challenges make consistent policy enforcement, rapid troubleshooting, and secure deployment difficult without streamlined

automation and centralized management platforms. Cisco's full-stack architecture and validated designs can help organizations overcome these challenges and accelerate their branch transformation.

These challenges underscore the importance of building organizational capabilities around automation and ensuring operational processes and tooling are aligned to support unified branch strategies effectively.

## Conclusion

A unified platform-based approach to branch network and security architectures simplifies operations by integrating networking and security functions into a single offering. This delivers consistent policy enforcement, end-to-end visibility, and enhanced security. Unified approaches that support zero-touch deployment, automation toolkits, and integrated security enable organizations to efficiently and securely manage and scale the edge of their network while ensuring high-quality user experiences and optimized network performance.

## About the Analyst



### ***Brandon Butler, Senior Research Manager, Enterprise Networks***

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 enterprise network management platforms. While contributing to ongoing forecast and market share updates, he also assists in end-user surveys, interviews, and advisory services and contributes to custom projects for IDC's Consulting and Go-To-Market Services practices.

## MESSAGE FROM THE SPONSOR

Cisco's Unified Branch is a comprehensive, full-stack solution that seamlessly integrates Secure Routers, Smart Switches Wi-Fi, visibility and assurance into a single, dashboard-managed system. As a Cisco validated solution, Unified Branch removes the complexity when deploying, managing and operating branch infrastructure at scale by consolidating services into one integrated platform rather than through multiple, separate appliances or services.

Unified Branch delivers AI-powered efficiency that gives IT teams a platform that configures, validates, and troubleshoots. The benefit of validated and versioned network automation enables IT teams to address operational inefficiencies and talent gaps. This unified approach shifts branch management from individual devices to orchestrating all services as a cohesive whole, enabling organizations to define operational intent that is automatically deployed across the network.

Unified Branch ensures branch office infrastructure is built for the speeds, low latency, and agility required by AI workloads and real-time applications. Unlike the multi-vendor approach, only Unified Branch enables both customized deployments and rapid scale through AI-powered automation and Cisco Validated Designs. Learn more here: <https://www.cisco.com/site/us/en/solutions/networking/campus-branch-networking/unified-branch/index.html>



The content in this paper was adapted from existing IDC research published on [www.idc.com](http://www.idc.com).

**IDC Research, Inc.**  
140 Kendrick Street  
Building B  
Needham, MA 02494, USA  
T 508.872.8200  
F 508.935.4015  
[blogs.idc.com](http://blogs.idc.com)  
[www.idc.com](http://www.idc.com)

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)

