eBook

Modernizing the Branch for the AI Era

A Guide for IT Leaders

Executive Summary

Fueled by modern applications and the transformative power of AI, the branch is evolving from a service touchpoint into a critical hub for digital experiences and customer engagement. Regardless of industry, organizations are reimagining the branch to meet the demands of cloud, mobility, and advanced digital capabilities.

The surge in mobile, IoT, and AI workloads is overwhelming traditional branch infrastructure—driving up operational complexity and widening security gaps. Cisco's 2025 Networking Research found that over 77% of organizations have experienced major outages, often due to misconfigurations or cyberattacks, underscoring the strain on already stretched IT teams.

As traffic patterns shift and threats grow more sophisticated, businesses face mounting challenges in maintaining performance, visibility, and protection across distributed environments.

This e-book explores the challenges of legacy branch environments, examples of AI use cases, and the technologies required to build secure, scalable, and simplified branch networks without costly disruptions.

77%

of organizations have experienced major outages, often due to misconfigurations or cyberattacks, underscoring the strain on already stretched IT teams.

cisco

eBook

The evolution of the branch

Branch offices serve as critical touchpoints where companies engage directly with customers, making them high-stakes environments that demand reliable performance, uninterrupted operations, and robust future-ready security.

Yet IT teams continue to face mounting challenges, including managing legacy infrastructure, scaling operations, ensuring compliance, and supporting hybrid work models. While technologies like SD-WAN, cloud, automation, and zero trust have helped address some of these pain points, integration, security, and consistent management remain complex.

Traditionally, branch traffic flowed north-south to centralized data centers for basic services like email, centralized applications, and web access. Today, cloud-based apps, IoT, and AI are accelerating east-west traffic between branches, driven by peer-to-peer collaboration and distributed workloads. This architectural shift, combined with AI's growing footprint, is placing unprecedented strain on lean IT teams tasked with managing vast, decentralized networks—often without local support.

The following use cases are intended to illustrate that, while they deliver business benefits, there's an impact to the branch infrastructure's performance, security, and operational complexity.

Use Cases	Business Benefits	Branch impact
Mobile ordering and loyalty apps	Increased convenience and customer retention	Drives heavy app-to-cloud traffic and requires strong encryption for transactions, synchronization between systems, and mixed north-south and east-west flows. [1]
Hybrid work/secure access	Operational flexibility with secure access from anywhere	Involves dynamic routing, encrypted access control, centralized policy enforcement, and mixed traffic paths from users to cloud and branch resources. [2]
Telehealth or remote diagnostics	Broader care access and faster patient service	Demands high-bandwidth, low-latency video; strict data privacy compliance; resilience in limited IT environments; and north-south traffic for virtual consultations. [3]

[1] Modern Retail Article: Starbucks mobile ordering strategy, September 2024
[2] Market Research: 2025 Strategic Roadmap for Enterprise Networking, October 2024.
[3] Cisco Meraki Case Study: Kindred Healthcare; Article: CVS MinuteClinic, December 2015

Branch workloads like mobile ordering, hybrid work, and telehealth increasingly exceed the capabilities of traditional infrastructure. Limited uplink speeds, especially below 100 Mbps, can cause delays in real-time transactions, inventory sync, and video consultations. These issues are compounded by Wi-Fi 5 or early Wi-Fi 6 access points, 1 GbE switches, and restricted PoE budgets, which constrain device density, bandwidth, and performance.

This creates operational bottlenecks just as branch demands are surging, which can impact your applications, your workforce, and the customer experience.

With CEOs planning to adopt and incorporate AI (or more AI) into their business—whether for forecasting inventory, smart surveillance, or video analytics—the impact to branch infrastructure is expected to increase.

AI Use Case	Business Benefits	Branch requirements
AI-powered voice and vision kiosk	Delivers faster, inclusive service with fewer errors and data-driven operational optimization	Generates high-bandwidth video and audio streams requiring edge processing, encrypted transmission, and real-time analysis. Creates east-west traffic between devices and analytics engines, potentially saturating uplinks in already strained branch networks. [4]
Smart surveillance and video analytics	Real-time threat detection, pattern recognition, and operational insights	Generates high-bandwidth video requiring edge processing, encrypted transmission, and real-time analysis with east-west traffic from devices to analytics engines saturating uplinks. [5]
Computer vision for store audits	Automated compliance checks, reduced human error, improved efficiency, and insights of store operations	High-bandwidth, low-latency connectivity to support video data processing; secure transmission, edge/cloud integration, and network segmentation are essential for performance and compliance. [6]

[4] Article: The Wall Street Journal, March 2025

[5, 6] Blog: Cisco Meraki Physical Security, March 2025; Blog: Cisco Meraki Smart Spaces, March 2022

AI fundamentally changes network behavior—not just by increasing traffic, but also by making it dynamic, real-time, and cross-domain. A single prompt from a branch can trigger several application programming interface (API) calls across SaaS apps, infrastructure, and backend systems. These unpredictable interactions bypass traditional security boundaries, challenging visibility and control. To maintain performance and protect sensitive data, IT must adopt zero-trust models, enforce strong identity controls, and deploy real-time threat detection across distributed environments.

Forces breaking the traditional branch

The branch needs to become purpose-built for the modern application demands and requirements created by AI agents and machine-to-machine communication. Failing to do so increases the risk of breaking the traditional branch in three main areas:

Augmented operational challenges

Increased security threats

Network congestion

Augmented operational challenges

Modern applications are dynamic, distributed, and API-driven. The introduction of AI increases these demands by adding real-time, cross-domain interactions that strain traditional IT operations. Managing branch environments at scale now requires a shift from manual workflows to automated, policy-based infrastructure.

Inadequate speed, scalability, and automation: Branch networks are struggling to keep up with the speed and responsiveness that modern applications demand. With AI workloads requiring sub-50 ms responses and generating more alerts than ever, manual processes can't keep pace.

Talent and resource gaps: Many branches don't have enough skilled IT staff, and manual changes often lead to delays or errors. Without automated lifecycle management—including configuration, updates, and rollbacks—IT risks falling behind on reliability and performance.

Lack of centralized visibility and closed-loop operations: IT teams often lack a clear, real-time view of what's happening across devices and applications. Gaps in centralized monitoring and AI-driven automation increase the detection, diagnosing, and troubleshooting of issues.

Without comprehensive observability, IT teams struggle to gain real-time insights into device health, application performance, and cross-domain dependencies. Siloed platforms hinder the ability to automate changes and compliance enforcement across domains, impacting service levels and governance across distributed locations.

Increased security threats

As branches evolve into digital experience hubs, they play a bigger role than ever in business operations and customer experience. However, many still rely on outdated security models that can't keep pace with today's threats, let alone post-quantum threats. Limited resources, inconsistent policies, and rising complexity make branches prime targets, requiring a shift toward security that is embedded and built for scale.

Emerging AI-driven threats: AI introduces new risks, such as impersonation and synthetic attacks, while the explosion of connected devices amplifies the attack surface. Traditional networks often lack the segmentation, encryption, and monitoring capabilities needed to detect and contain threats across distributed environments.

Inability to address sophisticated attacks: Legacy systems fail to defend against advanced threats, such as "harvest now, decrypt later," which compromise encrypted data, across east-west flows and cloud-bound data for future exploitation. The advent of post-quantum computing raises the urgency even further.

Performance bottlenecks for AI traffic: Traditional branch security tools introduce excessive latency, making them unsuitable for the dynamic, high-performance needs of AI-driven applications, leaving critical workloads exposed to potential breaches.

Network congestion

Branch networks are under growing strain as users, devices, and cloud applications compete for bandwidth from access to core. Real-time and AI workloads increase pressure, leading to congestion, latency, and performance gaps while traditional architectures lack the flexibility and intelligence to keep up.

Inability to meet low-latency requirements: Legacy routers, switches, and Wi-Fi systems struggle to support sub-10 ms WAN performance or the sub-50 ms responsiveness AI agents demand for real-time interactions.

Traffic-management inefficiencies: Traditional devices create bottlenecks by failing to optimize internal (device-to-device) network traffic and east-west data flows, as well as cloud-bound data. This limits the performance of modern applications as well as the demands of AI workloads.

Inadequate support for high-concurrency demands: From access to the core, legacy networking equipment cannot handle the high-concurrency requirements of AI-intensive environments or maintain consistent performance under high-jitter conditions.

eBook

Introducing Cisco's Unified Branch

The Cisco Unified Branch solution unites routing with next-generation firewall (NGFW) capabilities, Wi-Fi, and switching—all managed by a unified platform that can also leverage Branch-as-Code (BaC) capabilities. It delivers full visibility, smarter troubleshooting, and the ability to quickly pinpoint issues to keep businesses running smoothly. This architecture empowers organizations to deliver a modern, AI-ready solution that simplifies operations, enhances security, and ensures seamless connectivity to future-proof the branch.

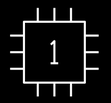
Operational simplicity, powered by AI. AI-first operations across the network make management simpler than ever.

Security fused into the network. Ensure that networks are protected at every layer to proactively defend against new attacks.

Scalable devices, purpose-built for AI. Innovative new hardware to deliver the scale and performance needed for the AI era across every domain.

The three main pillars:

Operational simplicity powered by AI



Scalable devices ready for AI

Security fused into the network

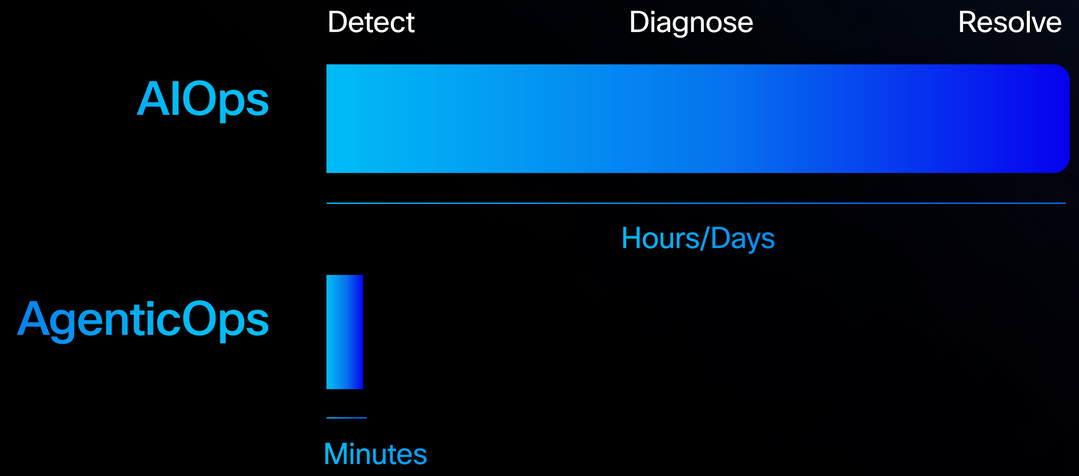
Operational simplicity, powered by AI

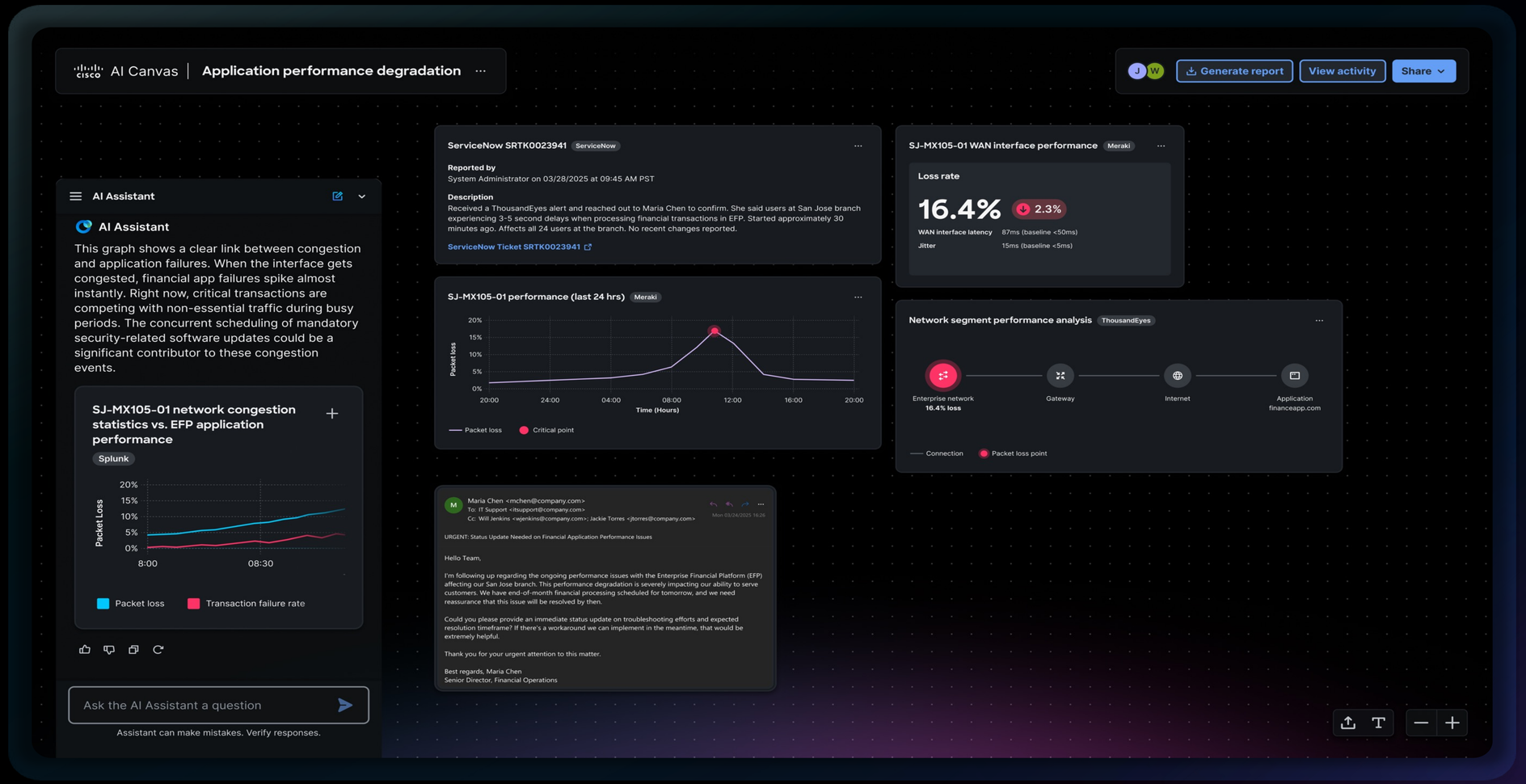
Managing large-scale branch environments with fragmented tools and manual processes is unsustainable. With 60% of outages tied to aging and complex infrastructure, operational inefficiency is a major risk. Cisco solves this with unified automation, telemetry, and orchestration, removing system friction and enabling scalable, AI-ready operations.

Unified management and multi-layered assurance
Cisco's unified platform integrates networking and security management across the branch, providing full-stack visibility and centralized control. With embedded Cisco ThousandEyes, it monitors both owned (LAN/WAN) and unowned (internet, cloud, and SaaS) environments to detect performance-impacting issues and support automated closed-loop operations.

Agile deployment with Branch-as-Code
Cisco provides the option to manage branches as software-defined assets, enabling rapid deployment of full branch stacks—SD-WAN, switching, wireless, and security—through APIs and policy templates. Zero-touch provisioning ensures consistent and compliant setups.

AgenticOps for autonomous troubleshooting and remediation at AI-scale Cisco combines AI and human expertise built for scale, intelligence, and collaboration across teams.





Cisco AI Canvas provides a shared generative workspace that correlates telemetry across domains, enabling collaborative, real-time root-cause analysis. AI and human expertise work side by side. Cisco AI Assistant offers a conversational interface to surface issues to diagnose root causes, recommend fixes, and assist with tasks like config changes and migrations, while keeping humans in control. Powered by the Cisco Deep Network Model, a Cisco-trained large language model (LLM), AgenticOps transforms operations from slow, reactive troubleshooting to autonomous, real-time decision-making—compressing the entire lifecycle from Observe → Diagnose → Decide → Act.

Security fused into the network

Branch environments often rely on separate devices for routing, SD-WAN, and firewalls—driving up costs, complicating integration, and causing inconsistent policy enforcement. This fragmentation slows the adoption of secure access service edge (SASE), leads to inefficient traffic backhauling, and weakens zero-trust strategies due to gaps across remote, branch, and cloud access. Cisco addresses this with a converged secure WAN edge that unifies routing, SD-WAN, NGFW, and SASE—including universal zero-trust network access (ZTNA)—into a single policy-driven architecture. With integrated telemetry, policy enforcement, and cloud-delivered security, Cisco eliminates operational silos and simplifies secure connectivity at scale.

Converged edge platform

Cisco Secure SD-WAN routers combine enterprise-grade routing, application-aware SD-WAN, and embedded NGFW features like deep packet inspection, intrusion prevention, malware protection, and URL filtering—all managed centrally for operational simplicity and policy consistency.

Cloud-ready SASE architecture

Cisco's built-in SASE stack supports both native and third-party secure service edge (SSE) solutions, offering Secure Web Gateway (SWG), cloud-access service broker (CASB), data loss prevention (DLP), Firewall as a Service (FWaaS), and ZTNA in a unified cloud-delivered model.

Consistent security with universal ZTNA

Cisco enforces identity, device posture, and contextual access across branches, remote users, and cloud apps—leveraging WAN edge, NGFW, and SD-WAN fabric. With centralized control through Cisco SD-WAN Manager and SecureX, organizations gain unified visibility and policy enforcement across users, apps, and locations. Post-quantum cryptography ensures future-ready investment protection.

Securing users, clients & apps

Protecting user access and application interactions

Securing network access

Securing connectivity to the network

Securing network connectivity

Safeguarding and optimizing network connections

Securing the device

Protecting and ensuring compliance of devices

cisco

Scalable devices, purpose built for AI

From monolithic to distributed and now AI-native applications, traffic patterns have fundamentally changed. AI-driven applications generate dynamic traffic patterns for inferencing, automation, and peer-to-peer decisions—putting new pressure on branch networks. Cisco delivers the performance, concurrency, and responsiveness required to support intelligent workloads seamlessly across thousands of locations.

Routers Consolidate SD-WAN, NGFW, and post-quantum encryption in a single device, delivering up to 3x the throughput of previous generations. Support for multi-gig uplinks and real-time path optimization drives round-trip latency below 10 ms—ideal for AI-sensitive future applications.

Switches Deliver wire-rate switching with up to 1Tbps backplane capacity, ensuring no traffic bottlenecks during peak branch activity. It also enables deterministic performance for high-concurrency workloads, such as multiple video feeds or endpoint AI agents.

Wireless Access Points Enable low-jitter, high-speed wireless performance—even in ultra-dense environments. Integrated ultra-wideband (UWB) delivers centimeter-level location precision, unlocking AI-powered applications in retail, healthcare, and logistics.

Routing

Catalyst 8000 Edge Platforms (8200, 8300), Cisco 8000 Secure Routers (8100, 8200), Meraki MX Series (MX6x, MX7x, MX9x, MX1xx) [3]

Switching

Catalyst 9000 Series (9300, 9200), Meraki MS Series (Access), Catalyst Smart/SMB Switches

Wi-Fi 6/6E/7

Catalyst 9100 Wi-Fi 6 & 6E Series, Catalyst 9100 Wi-Fi 7 Series, Meraki MR Wi-Fi 6E/7 Series

1 Catalyst = controller-managed, Secure Routers = secure WAN with SD-WAN, Meraki = cloud-managed branch security & SD-WAN
2 Stackable access, compact/SMB form factors, PoE for APs, IoT, and cameras
3 (CW = same hardware for cloud (Meraki) or controller (C9xxx) management); supports smaller scale than campus, optimized for branch layouts

cisco

Modernize for experience, security, and performance at your own pace

Every organization is on a different path to branch transformation. With Cisco, your existing infrastructure becomes the foundation for the Cisco AI-Ready Unified Branch, enabling selective upgrades without disruption. As modern workloads like 4K video collaboration, AI-driven security, and advanced analytics strain legacy systems, Cisco allows you to evolve at your own pace while optimizing for both current and future demands. For example:

Cisco helps you modernize without disruption—enhancing today's user experience while enabling the AI-powered services of tomorrow. Whether you're optimizing key branches or building toward full-scale transformation, we're ready to help you take the next step.

Initiative	Business benefit	Branch requirements
Modern collaboration	Enable HD video meetings and IoT video use cases	Wire-speed LAN/WAN, sub-50ms latency, prioritized video backhaul
Security and compliance	Protect sensitive data and maintain regulatory compliance	Real-time threat inspection, MACsec + PQC-ready encryption for video streams and SaaS data, identity validation
AI-Ready Edge	Run AI video analytics for operational efficiency	High-density, low-jitter connectivity; prioritized alert routing; end-to-end observability

Conclusions

AI is fundamentally reshaping how organizations operate—demanding a new level of agility, intelligence, and security at the branch. To unlock its full potential, infrastructure must be scalable, adaptive, and deeply integrated. Only Cisco brings together the innovation, scale, and operational maturity to modernize every branch without compromise.

Scalable performance for AI workloads

As modern apps and connected devices drive more edge-to-cloud traffic, the Cisco Unified Branch delivers the scale, speed, and reliability required today –and is ready for tomorrow's AI demands. Secure routers enable sub-10ms latency for real-time services, Cisco Smart Switches provide wire-speed concurrency, Wi-Fi 7 access points ensure seamless wireless in dense environments, and embedded ThousandEyes agents assure every WAN and cloud path. Together, Cisco provides the performance, visibility, and resilience branches need now, with the scalability to meet AI workloads at enterprise scale.

Security that starts at the edge

The Cisco secure WAN edge converges routing, SD-WAN, embedded NGFW, and built-in SASE (with universal ZTNA) into one architecture. This centralized approach enables real-time threat detection, continuous access control, and identity-based segmentation—securing the user, device, and application from edge to cloud.

Effortless operations, built in

AI is fundamentally reshaping how organizations operate—demanding a new level of agility, intelligence, and security at the branch. To unlock its full potential, infrastructure must be scalable, adaptive, and deeply integrated. Only Cisco brings together the innovation, scale, and operational maturity to modernize every branch without compromise.

Start your journey today

With Cisco, the branch isn’t just keeping up—it’s moving ahead. Modernize confidently with a platform built for the next decade of growth, intelligence, and customer experience.