Cisco Unified Branch

Solution Brief

August 2025

Strategic Branch Modernization: The Unified Solution.

Modernizing corporate branches is a strategic imperative that dramatically enhances both digital and in-person interactions, significantly boosting customer experience and driving operational efficiency. This is particularly true as the branch stands as the prime platform for delivering a business model to the customer, serving as the very place where digital experiences are delivered to them.

These advantages resonate across diverse industries. Financial institutions, for example, can use modernized branches with financial wellness pods to allow customers to use biometrics to securely connect with specialized advisors via video, making services like mortgages and wealth management more personal. In retail, updated branches enable seamless online-offline shopping. A customer can browse products on an app, then use a smart mirror in the fitting room to see their selections and receive personalized suggestions. Similarly, healthcare providers benefit from streamlined processes. Patients can check in at a self-service kiosk, and doctors can then use a tablet to access records and share information on a large screen. These examples highlight how a modern, unified branch architecture optimizes operations and improves customer or patient experiences regardless of the sector.

When building and refreshing branch IT infrastructure, organizations must choose between unified solutions from a single vendor, or a best-of-breed approach integrating multivendor solutions. The best choice depends on an organization's specific needs and priorities, balancing the integrated capabilities and simplified management of a unified branch approach against the high customization sometimes required for complex environments with unique requirements.

For branch networks, a unified solution provides key advantages over a best-of-breed approach, such as:

- Guaranteed Service Level Agreements (SLAs). A unified branch solution simplifies the process of defining, monitoring, and guaranteeing Service Level Agreements (SLAs) for network performance and application delivery. With a single platform providing comprehensive visibility and control, IT teams can more easily track key metrics, identify potential bottlenecks, and proactively address issues to meet predefined service levels. In a fragmented, multi-vendor environment, correlating data across disparate systems to ensure SLA compliance becomes a significant challenge, making it difficult to confidently offer and meet stringent service guarantees to end-users or business units.
- Centralized configuration. Only a unified, single-vendor solution can enable centralized configuration for all branch (network and security) devices, whether delivered through a graphical user interface (GUI) or powered by Infrastructure as Code (IaC) automation. In contrast, a best-of-breed, multi-vendor approach inevitably forces IT teams to juggle fragmented configurations across disparate vendor-specific GUIs and operating systems. This significantly increases the likelihood of human error, complicates troubleshooting, and drastically escalates operational complexity.
- Simplified Day N operations. A unified architecture dramatically simplifies lifecycle monitoring, troubleshooting, and maintenance by offering a single pane of glass for all branch IT functions, from networking to security. This contrasts sharply with a best-of-breed, multivendor approach, which typically fragments management across disparate tools, increasing operational complexity.
- Lower total cost of ownership. A unified branch architecture significantly lowers total cost of ownership through simplified licensing, reduced integration efforts, and streamlined operational efficiency. Specifically, a platform approach makes it incremental to add and operate new technologies, offering a single platform for assurance. In sharp contrast, a best-of-breed, multivendor approach often increases TCO through multiple licensing fees, costly integration efforts, and increased training and support overhead.
- Comprehensive Application Visibility. A unified architecture is inherently more capable of providing end-to-end application visibility across the entire network than a multi-vendor environment. This

comprehensive insight is crucial for enhancing security, accelerating troubleshooting efforts, and ensuring common policy enforcement, as it eliminates blind spots and provides a cohesive view of application behavior and dependencies.

- Enhanced security posture. A unified branch architecture significantly enhances security posture by providing integrated features, consistent policy enforcement, and centralized threat visibility across the entire network. Conversely, a best-of-breed, multivendor approach often creates security gaps due to fragmented controls, inconsistent policies, and complex integration challenges. between disparate security solutions

Cisco Unified Branch: The Integrated Platform for Modern Networks

The Cisco Unified Branch offers a comprehensive, full-stack **platform** for organizations that want advanced capabilities and simplified management at the branch. It includes a curated set of products, tested and verified together, that integrate routing with next-generation firewall capabilities, Wi-Fi, and switching into a robust suite of services. All these components are centrally managed through a common dashboard.

This platform represents a fundamental shift from managing individual network and security devices to orchestrating all branch services as a cohesive whole. Organizations can define their operational " intent" – specifying desired capabilities, performance, and security—which is then automatically deployed across all underlying technologies. This platform-centric approach delivers significant benefits, including operational and integration simplification, consistent configurations, accelerated deployments, and a dramatically improved security posture

By treating the entire branch as a single, centrally managed entity, Cisco Unified Branch also enables a faster time to detect and restore problems. The platform is further enhanced by the inclusion of Cisco ThousandEyes, which provides full visibility, smarter troubleshooting, and the ability to quickly pinpoint issues, ensuring businesses run smoothly.

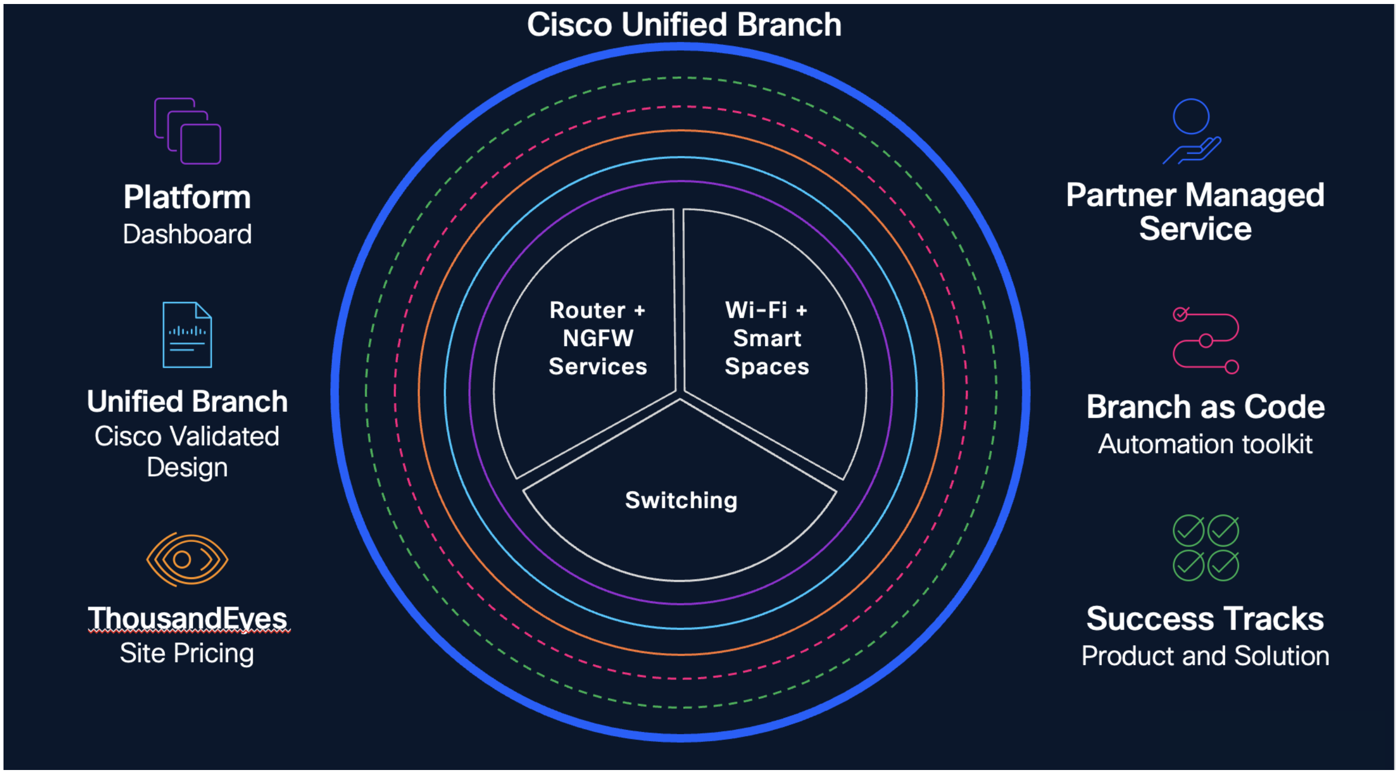

Figure 1. **Cisco Unified Branch Platform Services**

Platform Dashboard

At the heart of the platform, a cloud-delivered dashboard functions as the network conductor, providing a single, intuitive interface where all critical data is processed, analyzed, and acted upon. From this dashboard, IT teams gain complete, real-time visibility into the health, performance, and security posture of every aspect of the branch network—from Wi-Fi and LAN switching to WAN routing and integrated security services. It's the command center for device configurations, defining and enforcing policies, monitoring user experience, detecting anomalies, and orchestrating automated responses, translating complex operational data into actionable intelligence that enables proactive management and rapid issue resolution.

Core Services

The foundation of the unified branch lies in its core services, which are designed to provide robust, secure, and reliable connectivity for all users and devices. These services are the bedrock upon which all branch operations depend.

Cisco Secure Routing: Router with integrated Next Generation Firewall (NGFW)

A cornerstone of this platform is the integration of Unified Threat Management (UTM) and Next-Generation Firewall (NGFW) functionalities directly into Cisco Secure routers, offering the best of routing and firewall in a single device with a common OS. Secure routing provides a suite of crucial services that orchestrate data handling within the branch office (LAN) and its connections to external networks like headquarters, the Internet, or cloud services (WAN). This includes segmentation, which isolates different user and device classes into smaller, secure network sections, significantly reducing the attack surface, containing breaches, and improving access control. It also encompasses SLA-driven policies to prioritize critical applications, secure tunnels (SD-WAN) for encrypted multi-path connectivity, and secure direct Internet access (DIA) with comprehensive threat protection using integrated Next-Generation Firewalls (NGFWs). Together, these services ensure a highly secure, efficient, and well-managed branch network.

Secure Wired Access: Cisco LAN Switching

For a branch, secure wired access through LAN switches is vital for protecting sensitive data. It ensures Ethernet connections are authorized and effectively preventing unauthorized devices from gaining access. This is achieved through network segmentation (VLANs), which divide the LAN into isolated Layer 2 segments for different traffic types (e.g., employees, guests), preventing unauthorized access and mitigating the impact of security threats like malware. Port security prevents unauthorized devices from connecting to switch ports, while 802.1X authentication mandates login, requiring credentials or certificates before granting network access, ensuring only trusted devices join.

Secure Wireless Access: Cisco Wireless

Secure Wireless Access provides ubiquitous and highly performant Wi-Fi connectivity throughout the branch, prioritizing both the protection of sensitive data and an exceptional user experience. This is achieved through Enterprise-Grade Wi-Fi 7 technology, which delivers superior coverage, higher throughput, and lower latency, significantly enhancing overall network performance. It also employs strong authentication (like 802.1X with individual credentials) for robust encryption and accountability, moving beyond simple shared passwords. When deployed in a unified branch, the service utilizes multiple SSIDs with separate policies to create distinct wireless networks (e.g., " Employee-Secure," " Guest-WiFi"), each with tailored security rules and optimized performance profiles.

Smart Spaces

Cisco Smart Spaces transforms physical environments into intelligent, optimized areas by integrating IoT devices and leveraging existing network infrastructure (Wi-Fi, switches, cameras) as a powerful sensor and control fabric, all centrally managed via the Cisco Spaces cloud platform. This optimizes operational efficiency through automation, enhances user experience, strengthens security, and provides actionable insights. For instance, occupancy sensors can automatically adjust lighting and HVAC based on real-time space utilization, while integrated cameras and Wi-Fi location services can dynamically deploy staff to busy areas in retail, improving customer service.

Assurance Services - Artificial Intelligence for IT Operations (AIOps)

In today's complex and highly distributed IT environments, NetOps and SecOps teams are grappling with an overwhelming influx of alerts, siloed data, and labor-intensive processes. Reactive troubleshooting, fragmented visibility, and the vast volume of data generated by modern networks and security tools make proactive management and rapid incident resolution extremely challenging. This is where Cisco AIOps becomes an indispensable solution.

Cisco AIOps leverages a wide range of telemetry data, including real-time monitoring of external network and internet performance via Cisco ThousandEyes, alongside insights from traditional network infrastructure, applications, and diverse security systems. By intelligently correlating this wealth of data, Cisco AIOps delivers unparalleled end-to-end visibility and actionable insights that traditional, manual NetOps and SecOps workflows simply cannot achieve.

ThousandEyes: A Foundation for Cisco AIOps

A cornerstone of Cisco's AIOps capabilities within the Unified Branch architecture is the deep and comprehensive visibility provided by ThousandEyes (TE). Now natively integrated into Cisco routing platforms through embedded Enterprise Agents, TE delivers immediate, hop-by-hop insights into network infrastructure, complete with detailed path and performance metrics. This visibility extends to overlay networks and critical SaaS applications, enabling proactive monitoring of performance and reliability. By integrating ThousandEyes, Cisco Unified Branch solutions can rapidly activate agents at scale, offering immediate visibility into web applications and WAN link performance.

Design and Deployment Services

Designing and deploying a Cisco Unified Branch is streamlined through specialized services that ensure success throughout the lifecycle, from blueprint to operations. These include Cisco Validated Designs (CVDs), expert assistance from partner-managed services, comprehensive support via Cisco CX Success Tracks, and a Branch as Code toolkit.

Cisco Validated Designs (CVD)

Cisco Validated Designs (CVDs) are thoroughly tested blueprints offering prescriptive guidance for deploying Cisco solutions across multiple technologies and places in the network (PINs). They empower customers by significantly reducing deployment risk and accelerating implementation through product information, detailed instructions, and configuration examples for common network and security use cases. CVDs address performance, reliability, and security, while embedding Cisco's best practices to foster standardization and simplify the overall design, deployment, and operational experience.

Branch as Code (BaC) Toolkit

Branch as Code (BaC) is Cisco's innovative approach to applying DevOps " Network-as-Code" principles specifically to unified branch office deployments. This method empowers network administrators to declaratively configure all branch services using pre-defined templates that embed Cisco's proven best practices for routing, security, and both wired and wireless infrastructure.

This capability fosters deep standardization across diverse network topologies, ensuring consistent support for varying branch requirements across multiple industries and for offices of all sizes–from small to large. Ultimately, BaC significantly reduces the administrative burden of deploying and managing numerous branch locations compared to traditional, manual methods for device and policy configuration.

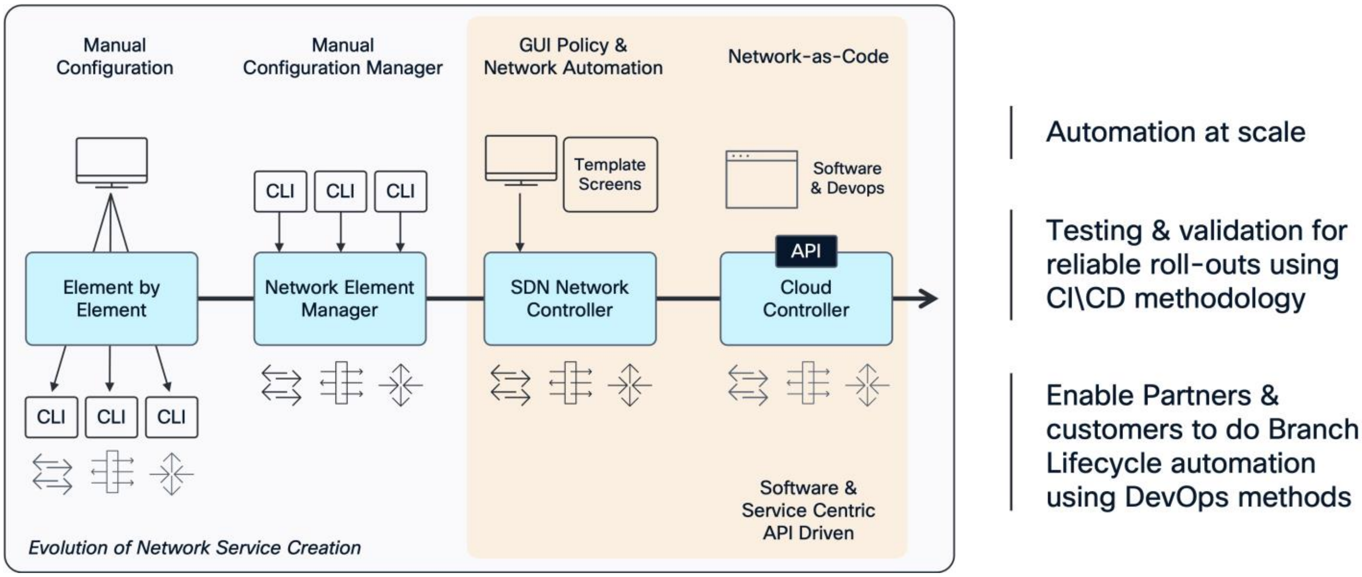
Manual Configuration
Manual Configuration Manager
GUI Policy & Network Automation
Network-as-Code
Template Screens
Software & Devops
CLI
CLI
CLI
API
Element by Element
Network Element Manager
SDN Network Controller
Cloud Controller
CLI
CLI
CLI
Software & Service Centric API Driven
Evolution of Network Service Creation
Automation at scale
Testing & validation for reliable roll-outs using CI\CD methodology
Enable Partners & customers to do Branch Lifecycle automation using DevOps methods

Figure 2. Evolution of Network Service Creation

For organizations adopting DevOps practices in lieu of traditional GUI-based configurations, the BaC Toolkit is a crucial component that empowers the declarative, service-oriented deployment of unified branch networks. The toolkit includes a dedicated Terraform provider, which serves as the programmatic interface to interact with the high-level Branch as Code data models and subsequently translate these intentions into device-specific configurations via their respective APIs. Complementing this provider is a comprehensive set of validated YAML files. These YAML files function as pre-engineered templates, embedding Cisco's best practices for deploying a CVD-based unified branch. Each template is crafted to encompass optimal settings for core network services, including robust routing configurations, stringent security policies, high-performance wireless and Ethernet switching parameters. Together, the Terraform provider and these validated templates enable organizations to rapidly and consistently deploy complex branch infrastructures with built-in best practices, significantly reducing manual effort and potential errors.

Partner Managed Services

For organizations aiming to establish or optimize a unified branch architecture, partnering with a specialized managed services provider offers significant advantages. Our partners bring deep expertise in designing, deploying, and operating complex branch networks, ensuring best practices for security, performance, and scalability. Cisco Unified Branch is designed with partners in mind – to help them deliver outstanding branch experiences on the Unified Branch platform. Unified Branch to customize and extend the Branch as

Code (BaC) data models, allowing organizations to tailor network and security services to unique operational demands or integrate with existing IT ecosystems.

Success Tracks

Success Tracks from Cisco Customer Experience (CX) services are designed to help organizations maximize the value of their Cisco technology investments throughout the entire lifecycle of a solution, from planning and deployment to adoption and optimization. They go beyond traditional technical support by offering a more proactive, guided, and outcome-driven approach. In addition to planning, design and implementation guidance, success tracks include knowledge transfer sessions from experts on emerging technologies such as Infrastructure as Code, network automation, SD-WAN and cloud networking.

Conclusion

Modernizing corporate branches is vital for enhancing customer experience and driving operational efficiency. While multi-vendor approaches introduce complexity, a unified solution provides compelling advantages for branches, offering centralized management, simplified operations, lower TCO, comprehensive visibility, proactive assurance, and enhanced security.

The Cisco Unified Branch Architecture delivers these benefits by shifting from individual device management to orchestrating full stack branch services as a cohesive whole. This platform-centric approach allows organizations to define their operational " intent" and automatically apply it, leading to profound simplification, consistent configurations, accelerated deployments, and faster problem resolution.

Through centralized cloud management, integrated security, and intelligent automation, the Cisco Unified Branch Architecture provides pervasive protection and enhances user experience with optimized routing and unparalleled visibility via AIOps and ThousandEyes. This strategic platform consolidates infrastructure, streamlines operations, and boosts business agility, creating a secure, high-performing foundation for the future of hybrid work and digital interactions.