eBook

Modernize Your Network for the AI Era

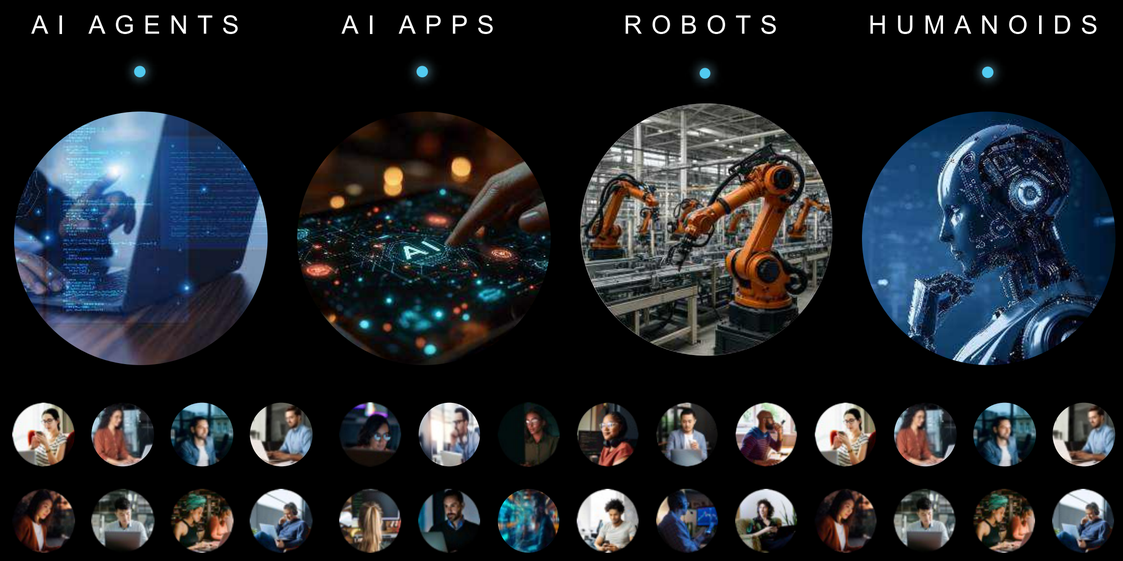
A Guide to Cisco AI-Ready Secure Network Architecture

eBook

Networks at the Edge of Change: Why Modernization Can't Wait

Modern networks weren't built for AI, immersive apps, or machine-speed operations. Today's access, switching, wireless, and WAN layers are stressed beyond design intent. Add in the evolving threat landscape—quantum risk, infrastructure threats like Salt Typhoon, and encrypted traffic blind spots—and the need to modernize becomes a strategic imperative.

Cisco AI-Ready Secure Network Architecture addresses this challenge head-on, combining agentic AI-powered operations, scalable high-throughput infrastructure, and security fused into every layer of the network. The result is a network built not just for today's traffic, but for tomorrow's intelligent workloads.



eBook

The current state of enterprise networks

Enterprise networks have evolved over time, but many foundational elements still reflect the design priorities of earlier IT eras that focused on office productivity, limited cloud use, and perimeter-based security. As a result, key layers in today's networks often exhibit a broad mix of legacy and modern configurations. This section outlines common architectural characteristics across access, campus, wireless, WAN, segmentation, and cryptography based on leading industry research.

Layer	Typical deployment	Insights from industry research	Source
Access switching	1 GbE ports still dominate enterprise access networks	~90% of enterprise access ports are still 1 GbE or below in campus and branch environments, per IDC's global switch shipment data.	"https://my.idc.com/getdoc.jsp?containerId=prUS52590024"IDC Finds Mixed Results for Q2 2024 in the Worldwide Ethernet Switch and Router Markets , IDC, September 12, 2024
Campus uplinks	1–10 GbE shared uplinks	Common uplink speeds remain in the 1–10 GbE range, with upgrades to 25 GbE or 40 GbE reserved for larger campus backbones.	IDC, Enterprise Campus Trends, 2024
Wi-Fi	Wi-Fi 5 and Wi-Fi 6 dominate deployments	Wi-Fi 5 throughput typically averages 300–400 Mbps per client; Wi-Fi 6 delivers higher capacity but is still rolling out widely.	2024 Global Networking Trends Report, Cisco, 2024
WAN edge	Hybrid MPLS + internet DIA; bandwidth typically 50–200 Mbps	TeleGeography's 2023 WAN Manager Survey reports typical MPLS branch bandwidth at 10–100 Mbps and DIA circuits at 100–200 Mbps for most enterprise sites.	https://blog.telegeography.com/wan-configurations-are-shifting"WAN Configurations Are Shifting , TeleGeography, March 15, 2023
Cryptography	AES-128 with manual certificate lifecycle management	AES-128 remains common; NIST and Gartner recommend a transition to post-quantum cryptography over the next 3–5 years.	NIST IR 8105; Gartner, Post-Quantum Cryptography Preparedness, 2023
Operations	Siloed tools, fragmented UIs, human-driven troubleshooting	Issue resolution often takes hours or days across multiple teams. Manual diagnostics can't keep pace with real-time application demands or AI workloads.	Gartner, 2024 Network Observability Trends; IDC, AI in IT Operations Survey, 2023

cisco

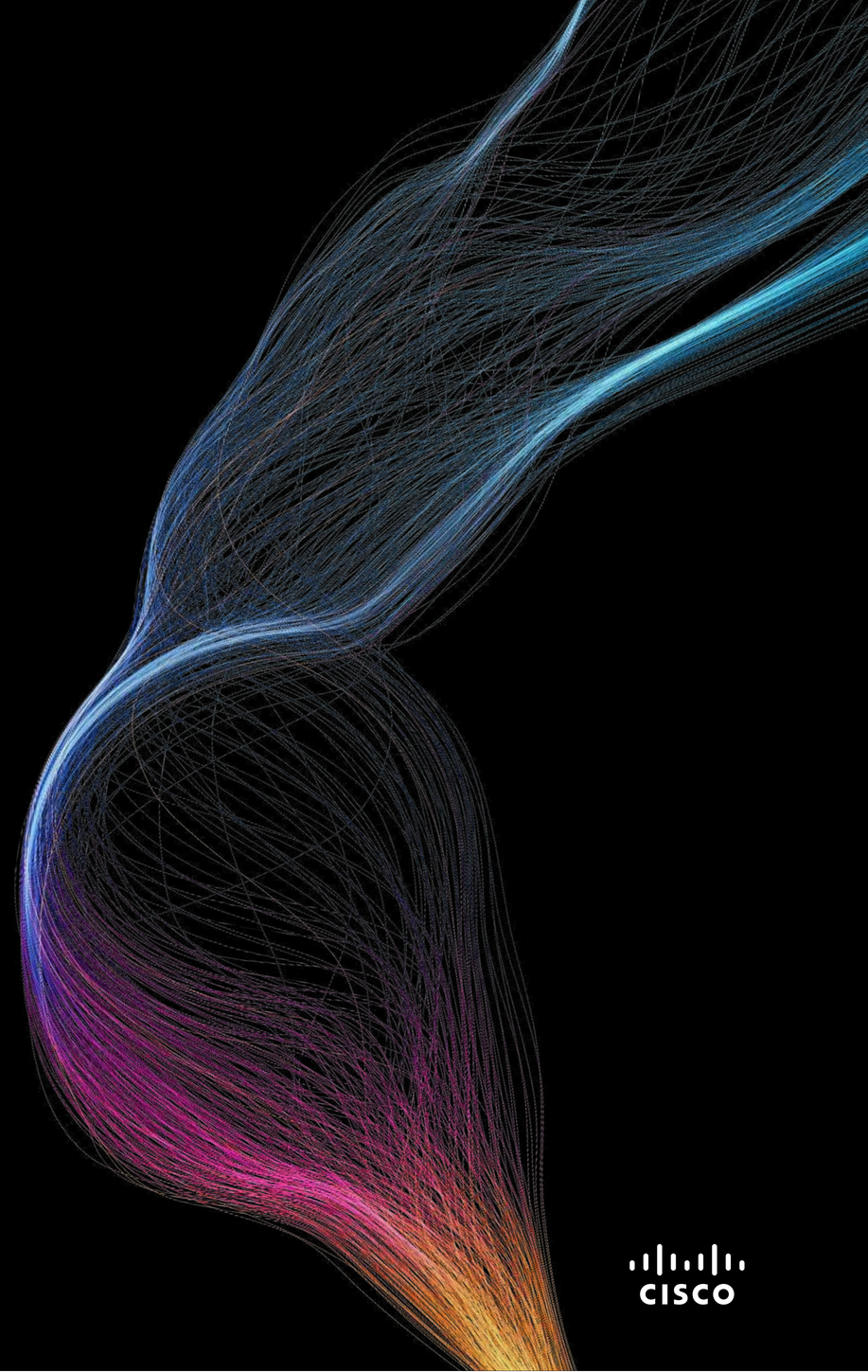
eBook

What's breaking the network? Use cases you can't ignore.

Enterprise networks are under growing pressure—not just from emerging AI applications, but from everyday digital operations. Video meetings, cloud-based POS systems, and sensor-driven telemetry already demand more bandwidth, lower latency, and greater reliability than legacy networks were designed to deliver.

Now, with AI-powered meeting assistants, smart surveillance, and machine vision entering the mainstream, the stakes are even higher. These applications introduce bursts of inference traffic, sustained HD video streams, and real-time data requirements that stretch infrastructure limits—especially at the access, wireless, and WAN layers.

This section explores real-world use cases—both AI-driven and traditional—across campus, branch, and industrial factory environments. Together, they illustrate how modern demands are outpacing yesterday's networks and why modernization is no longer a future initiative—it's a present-day imperative.



Campus

AI use case: AI-powered meeting summaries

Description: AI assistants in collaboration platforms (e.g., Webex, Zoom, Teams) transcribe meetings, generate summaries, and flag action items.
What it needs: Sub-150 ms latency to exchange real-time inference data with cloud application programming interfaces (APIs).
Where current networks fall short: 1 GbE access ports and Wi-Fi 5 introduce jitter and delay.
Result: Summaries are incomplete or delayed, undermining productivity in high-stakes meetings.

Non-AI use case: 4K video collaboration

Description: Conference rooms rely on high-definition 4K video for executive briefings and hybrid work.
What it needs: 300–500 Mbps per room, with jitter-free performance.
Where current networks fall short: Lack of multigigabit uplinks and insufficient QoS policies degrade audio/video quality.
Result: Video freezes, dropped audio, and poor user experience during important sessions.

Branch

AI use case: smart surveillance with edge analytics

Description: AI-enabled cameras analyze security footage in real time to detect incidents and optimize store layouts.
What it needs: 160 Mbps per 4K stream plus 90W PoE for edge inference modules.
Where current networks fall short: 1 GbE uplinks and limited PoE budgets constrain sustained video feeds.
Result: Frame loss and inference lag compromises safety and decision-making.

Non-AI use case: cloud POS and CRM

Description: Point-of-sale systems and customer databases rely on cloud platforms like Salesforce, Shopify, or ServiceNow.
What it needs: 20–40 Mbps per user with sub-100 ms round-trip latency.
Where current networks fall short: Low-bandwidth WAN links (e.g., 50 Mbps) quickly saturate during busy periods.
Result: Slow checkouts, customer relationship management (CRM) sync failures, and delayed service impact revenue and customer experience.

Industrial factory

AI use case: machine vision for quality inspection

Description: AI-driven cameras inspect products for defects in real time, catching anomalies early and ensuring consistent output.
What it needs: Reliable, low-latency uplinks between HD cameras, edge servers, and control systems.
Where current networks fall short: 1 GbE uplinks and flat networks can't prioritize or segment real-time video inference traffic.
Result: Missed defects or delayed detection leads to rework, waste, and lost productivity.

Non-AI use case: real-time sensor control for critical equipment

Description: Industrial machines rely on high-frequency telemetry—temperature, pressure, and vibration—from sensors to make instant control decisions that prevent breakdowns and ensure safety.
What it needs: Reliable, sub-10 ms latency to deliver thousands of sensor updates per second to control systems.
Where current networks fall short: Flat, oversubscribed networks with 1 GbE links introduce unpredictable jitter and delay.
Result: Delayed safety responses can cause equipment damage, production downtime, or worker safety risks.

Bottom line: use cases are outpacing the network

Today's AI and non-AI workloads demand more from the network, including greater bandwidth, lower latency, and dynamic segmentation. Legacy infrastructure with 1 GbE links, Wi-Fi 5, and static policies fall short.

Whether it's video calls, smart surveillance, or machine vision, the network can no longer be the bottleneck. Modern use cases require a modern foundation built for real-time, intelligent, and distributed operations.

Designing the AI-ready network: principles for the next decade

Summary

Enterprise networks weren't built for AI. From real-time inference to autonomous agents, the demands of AI-powered applications introduce a new set of performance, visibility, and security requirements. Modernization must start with rethinking how networks are designed, managed, and secured—not just upgraded.

This section outlines the three essential design principles for building a network that can support the future:

1. Intelligent operations that scale with AI.
2. High-performance infrastructure built for real-time workloads.
3. Security fused into the fabric of the network.

eBook

Intelligent operations that scale with AI

In the AI era, network operations can't be reactive. The volume of telemetry, the pace of change, and the complexity of multi-domain environments has outgrown human-scale monitoring and siloed tools.

Key principles for modern operations:

Unified observability across domains

Visibility must extend beyond switches and routers, encompassing cloud paths, Software as a Service (SaaS), third-party infrastructure, and AI endpoints.

AI-augmented troubleshooting

With AI-generated traffic patterns, operations must shift from dashboards and alerts to dynamic workflows that explain, recommend, and resolve issues with minimal manual effort.

Agentic operations

The next frontier is agentic systems—autonomous workflows that can be triggered by context (not just thresholds), adapt to anomalies, and coordinate actions across domains.

Insight: In large enterprises, more than 50% of incident response time is spent on root-cause isolation. By augmenting operations with agentic AI and domain-specific intelligence, enterprises can reduce mean-time-to-resolution (MTTR) by 60–80%, even for complex, multi-layer issues.

High-performance infrastructure built for real-time workloads

Today's applications, such as AI agents, augmented reality/virtual reality (AR/VR), 4K video, and immersive collaboration, demand deterministic performance across the network. The infrastructure must not only be fast—it must be predictable and scalable.

Key design considerations:

Multigigabit access and deterministic wireless

Wi-Fi 6E/7 and multigigabit switching ensure that edge congestion and latency do not bottleneck user experiences or inference pipelines.

Low-latency core and WAN pathing

Campus cores, branch routers, and WAN edges must support sub-50 ms latency and bursty traffic flows, especially where inference workloads, video analytics, or edge compute are involved.

PoE at scale for AI-edge devices

GPU-powered endpoints like smart cameras and AI assistants require consistent Power over Ethernet (PoE)++ delivery and high throughput, often simultaneously.

Insight: Many enterprises have upgraded servers and apps for AI—but the network remains the silent bottleneck. Infrastructure modernization must align with app behavior: latency-sensitive, burst-prone, and increasingly east-west in nature.

eBook

Security fused into the fabric of the network

AI workloads are expanding the enterprise attack surface—from AI-generated malware to rogue agents embedded in legitimate apps. Traditional perimeters, static rules, and bolt-on firewalls can't keep up.

Modern network security must be built in, not layered on.

The new security mandate

In the AI era, effective defense demands

Identity- and context-aware access
Decisions based on who/what is connecting, not just IPs or VLANs.

Adaptive microsegmentation
Policies that follow users, devices, and apps to prevent lateral movement.

Post-quantum readiness
Encryption that protects data—today, and into a quantum future.

Embedded enforcement
Protection that starts at the connection point, not downstream in the cloud.

Why the old model falls short

Attackers now target infrastructure, impersonate identities, and bypass inspection points through encrypted traffic. With SD-WAN, direct internet access (DIA), and hybrid access models, visibility gaps widen and perimeter-based security can't respond fast enough.

A network that defends itself

Security must be fused into every layer:

1. **Infrastructure:**
Secure boot, hardened operating system (OS), and runtime protection block firmware-level exploits.

2. **Access:**
Software-defined policies grant least-privilege access based on real-time identity and posture

3. **Data in motion:**
Post-quantum MACsec and IPsec encrypt every session without compromising performance.

4. **Application access:**
Zero-trust network access (ZTNA) enforces continuous trust across users, devices, and locations.

How Cisco Helps You Modernize: Built for Change, Not Just Speed

Most networks weren't designed for AI-powered assistants, real-time video, or IoT at scale. They still rely on siloed tools, static policies, and infrastructure from a simpler time.

At Cisco, modernization means more than faster switches or smarter software—it's about transforming from static, productivity-focused designs to intelligent, adaptive operations. The **Cisco AI-Ready Secure Network Architecture** delivers this through three integrated pillars:

The three main pillars:

Operational simplicity powered by AI

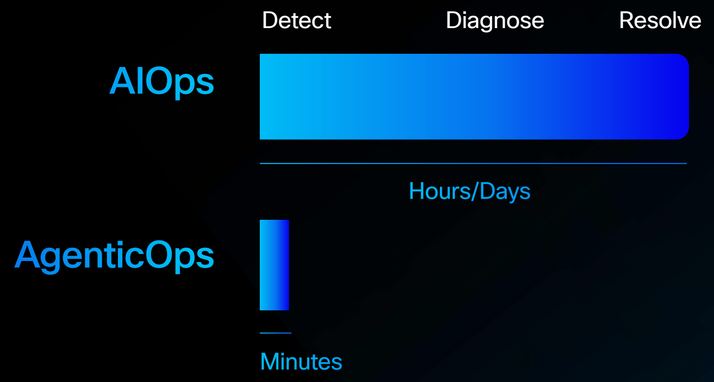
Scalable devices ready for AI

Security fused into the network

cisco

Operational Simplicity Powered by AI

A single, unified operations platform—centered on the Meraki Dashboard—manages campus, branch, cloud, and WAN. Embedded **ThousandEyes** provides full-stack visibility from Wi-Fi to SaaS. **AgenticOps** automates with intelligence, using Cisco AI Canvas, Cisco AI Assistant, and our Deep Network Model to diagnose, recommend, and remediate in minutes—not hours.



Scalable Infrastructure for AI Demands

Cisco's latest **Catalyst 9000 switches, Wi-Fi 6E/7 access points, and 8000 Series Secure Routers** are built for high-throughput, low-latency, and converged networking + security.

We enable **modular transformation**—modernize where it matters most, reusing existing investments where possible.

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 (1300, 1200, Business 350) [2]

Routing

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

Security Fused into the Fabric of the Network

Security isn’t bolted on—it’s built in at every layer:

Secure the device: Secure Boot with quantum-safe algorithms, hardened kernels, and LiveProtect runtime defense stop zero-days like Salt Typhoon without downtime.

Secure access: Cisco ISE with SDA and SGTs enforces Zero Trust—identity, posture, and context-driven least-privilege access for users, devices, and IoT.

Secure data in motion: MACsec, IPsec, and WAN MACsec with post-quantum readiness protect traffic end-to-end, extending segmentation and threat inspection to the cloud edge.

Secure application access: Universal ZTNA, delivered via Cisco SASE, applies continuous risk and posture checks for every session—across SD-WAN, DIA, and remote access—with post-quantum encryption and policy-based segmentation.

This is modernization with security woven into every connection, every packet, and every policy—ready for AI-scale operations today and resilient for what’s next.

Securing the device

Protecting and ensuring compliance of devices

Securing network access

Securing connectivity to the network

Securing network connectivity

Safeguarding and optimizing network connections

Securing users, clients & apps

Protecting user access and application interactions

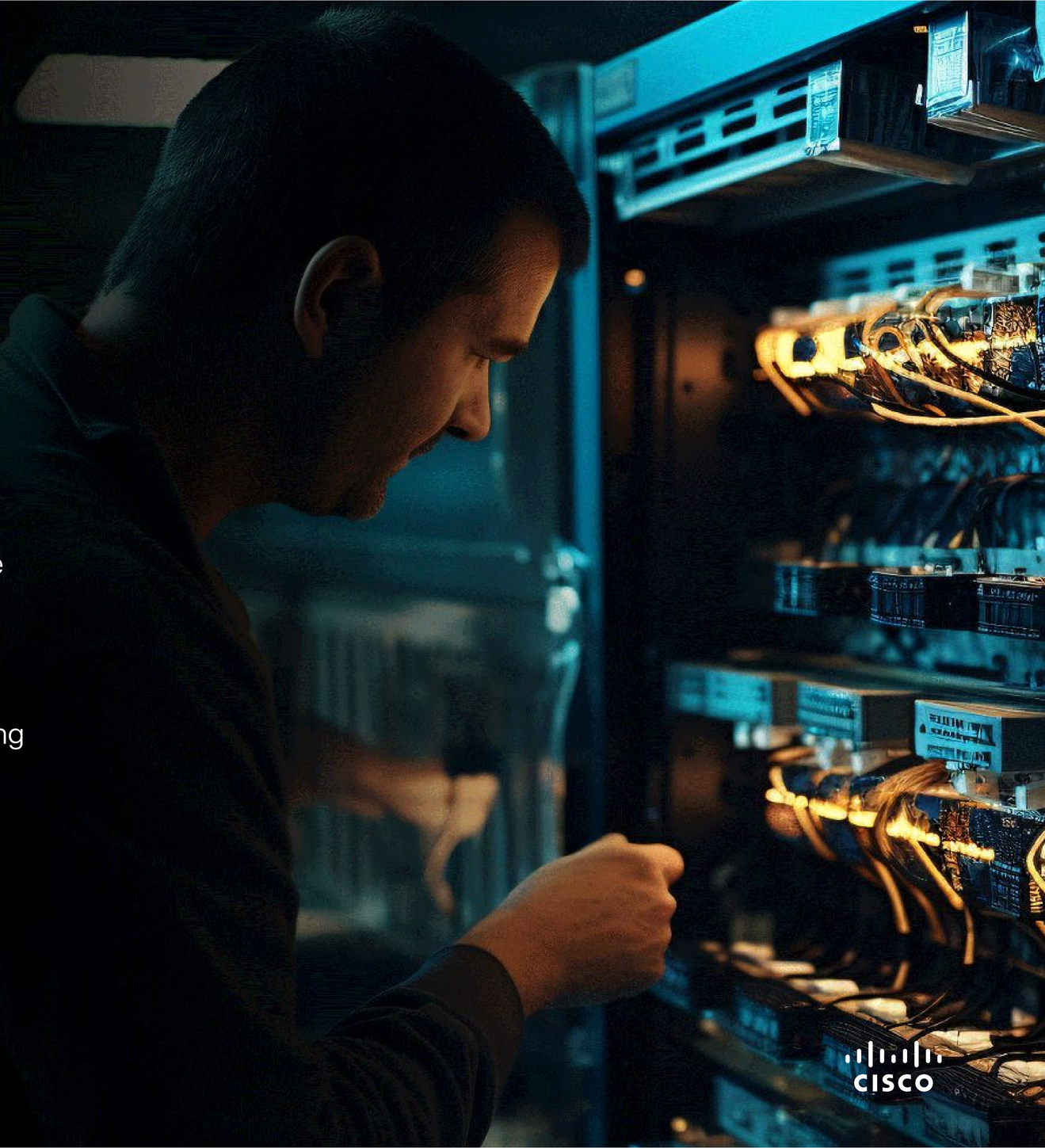
cisco

eBook

Modernization without disruption: a smarter way to transform

We get it—network refreshes are never just a technical project. They're strategic and they affect users, operations, and budgets. That's why our approach to modernization is pragmatic, phased, and designed to minimize disruption.

We don't ask you to rip and replace. We help you build forward, starting with software-first upgrades and expanding into infrastructure where needed.



Phase 1:

Strengthen security first

Security is non-negotiable. With cloud-delivered ZTNA, identity-based segmentation, and adaptive policy enforcement, you can improve your security posture now without waiting for a hardware refresh.

Phase 2:

Simplify operations and gain visibility

Move to unified operations with the Meraki dashboard. Layer in ThousandEyes and Cisco AI Assistant to reduce time-to-resolution and give your team better tools to manage what's already in place.

Phase 3:

Upgrade where it matters most

Refresh access switching, wireless, or WAN where bandwidth bottlenecks, real-time traffic, or high-stakes security make the business case obvious. We help you prioritize based on your workload; it's not a one-size-fits-all mandate.

This isn't transformation for transformation's sake. It's targeted modernization with ROI, security, and operational sanity as your North stars.

Why Cisco? A platform that's ready for what's next.

Every vendor will tell you they're ready for the future. But at Cisco, we've spent decades building the foundation that makes that claim real.

We understand that modernization isn't about isolated features. It's about architecture. It's about bringing intelligence, visibility, performance, and security into one integrated platform.

But what sets Cisco apart isn't just the tech, it's the strategy. The conviction that modernization should be modular, customer-paced, and relentlessly focused on outcomes, not checklists.

You've already begun your journey. We're here to help you finish it—faster, smarter, and without regrets.

With Meraki and Catalyst under one cloud-managed umbrella, you get control without compromise.

With ThousandEyes, you see what users see—across the LAN, WAN, internet, and cloud.

With AgenticOps, you turn intent into action—with AI that guides, recommends, and automates.

With purpose-built infrastructure, you scale confidently, from access to core to cloud.

cisco

Cisco is your partner

If you'd like to understand more about how IT leaders like you are planning for the future, you may be interested in our recent Cisco IT Networking Leader Survey, alternatively, if you'd like to learn more about any of the product or technologies listed here please feel free to reach out to your Cisco account team.