Building the AI-Ready Secure Network

A practical guide to consistent performance, identity-driven security, and agentic operations

CHAPTER 1

The network is becoming part of application execution

A shift in the role of the network

Enterprise networks are no longer simply supporting applications; they are increasingly becoming part of how those applications execute.

Most production environments today were designed around a different operating model—one characterized by intermittent, human-driven traffic where demand fluctuated and systems had time to recover between bursts. In that context, oversubscription, buffering, and some degree of latency variability were acceptable trade-offs.

That assumption is no longer holding.

Modern environments operate under conditions where demand is continuous, interdependent, and increasingly sensitive to performance variability. AI-assisted workflows, real-time collaboration, distributed application architectures, and persistent telemetry streams generate traffic that doesn't subside between events. These workloads depend on consistent performance across wireless, campus, WAN, and cloud domains as a single execution path.

Changing operating conditions

The broader operating environment has also evolved in ways that compound this shift.

Users, devices, and workloads are more distributed. Applications are more modular, driving increased east–west traffic within the network. Encryption is pervasive, reducing visibility while also adding processing overhead. At the same time, security enforcement can no longer rely on fixed perimeters and must follow identity wherever communication occurs. Individually, these changes are manageable. Together, they alter how the network behaves under sustained load.

The emerging disconnect

In many enterprise environments, a consistent pattern is emerging.

Network metrics indicate acceptable utilization and infrastructure appears stable, yet users experience inconsistent application performance. Troubleshooting often requires coordination across multiple domains before root cause can be isolated.

A common example illustrates this clearly. In a typical campus environment, users on a video collaboration platform may experience intermittent audio drops or lag, even when dashboards show low overall network utilization. Closer inspection often reveals a combination of factors—wireless contention affecting airtime scheduling, transient queue buildup at the access switch, and minor packet loss along the WAN path. Each condition, in isolation, appears insignificant. Together, they degrade application experience in a way that is difficult to diagnose using domain-specific tools.

This reflects a growing disconnect between how networks are measured and how applications behave.

The network is still being evaluated with a throughput-centric lens, while applications are increasingly sensitive to consistency.

→ Implication

The issue isn’t simply a lack of bandwidth.

It is a structural misalignment between network design and modern workload behavior. As a result, the network is no longer a passive transport layer—it has become an active component in application execution, directly influencing responsiveness, reliability, and ultimately, business outcomes.

CHAPTER 2

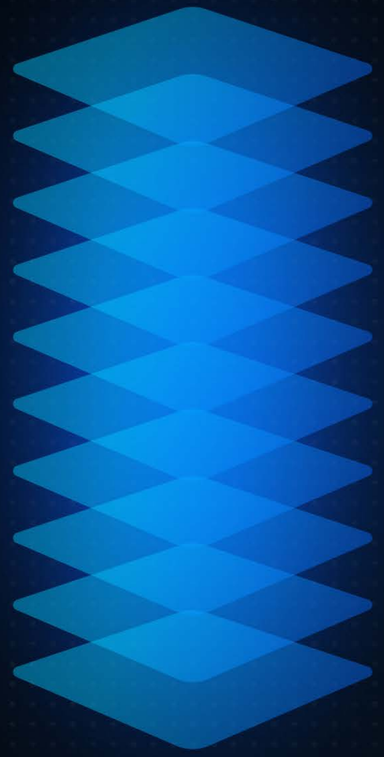
Where current network designs fall short

Legacy design characteristics

Most enterprise networks in operation today reflect design decisions that were appropriate for an earlier era.

Access layers are often built around 1 GbE connectivity with oversubscribed uplinks. Wireless networks are designed primarily for coverage rather than sustained concurrency. WAN architectures frequently rely on best-effort internet paths, introducing variability in latency and packet loss. Security is commonly enforced at centralized inspection points, and operational visibility is fragmented across domain-specific tools.

Under intermittent workloads, these designs perform adequately. Under continuous demand, their limitations begin to surface.



Design assumptions vs. current requirements

Domain	Traditional assumption	Current requirement
Access	Intermittent load	Sustained concurrency and east–west traffic
Wireless	Coverage first	Density and scheduling efficiency
WAN	Variability acceptable	Predictable latency and low jitter
Security	Perimeter-based	Identity-driven enforcement
Operations	Domain-specific	Cross-domain visibility

→ Nature of the gap

This isn’t a single bottleneck that can be addressed in isolation.

Each layer continues to function as designed, but the system as a whole struggles to deliver consistent outcomes because it was not built for sustained cross-domain execution.

CHAPTER 3

The shift to continuous and layered traffic

From burst-and-recover to sustained demand

Traditional enterprise networks were designed around a burst-and-recovery model, where traffic increased, buffers absorbed load, and the system returned to a steady state.

Modern environments operate differently. A continuous baseline of demand is now present, driven by persistent application activity, with additional burst activity layered on top.

Traffic patterns

This shift can be understood through two dominant patterns:

- **Sustained traffic,** driven by real-time collaboration, AI co-pilots, and continuous telemetry
- **Bursty traffic,** driven by analytics, synchronization, and AI inference workloads

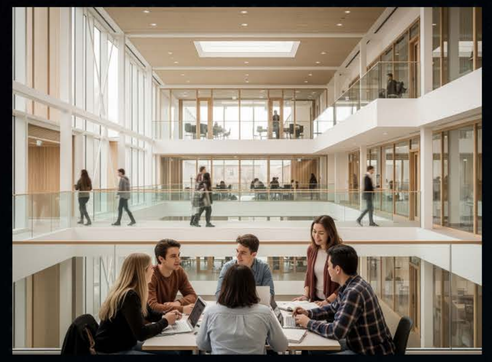
Architectural impact

In a sustained-plus-bursty model, queues remain active for longer periods, and scheduling efficiency becomes more important than peak throughput. Latency variability increases even when overall capacity appears sufficient.

This explains a common failure mode:
Networks show acceptable utilization yet fail to deliver consistent application performance.

CHAPTER 4

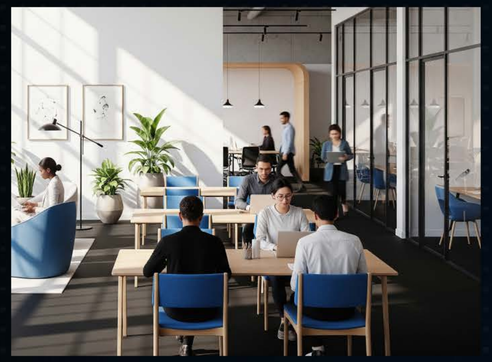
How constraints surface across environments



Campus environments

Campus networks are increasingly wireless-first, with growing device density and continuous bidirectional traffic. These conditions place sustained pressure on airtime scheduling, leading to contention and variability during periods of high concurrency.

Even when aggregate throughput appears sufficient, users often experience inconsistent application behavior.



Branch environments

Branch environments are now tightly coupled to application experience, particularly for SaaS workloads. Variability in internet paths introduces latency and packet loss that are difficult to predict and isolate.

As a result, issues are often perceived as application problems, even when the root cause lies within the network path.

Industrial and edge environments

Industrial environments introduce stricter requirements for determinism. Continuous telemetry, video analytics, and control systems generate sustained demand, while latency and jitter directly impact operational outcomes.

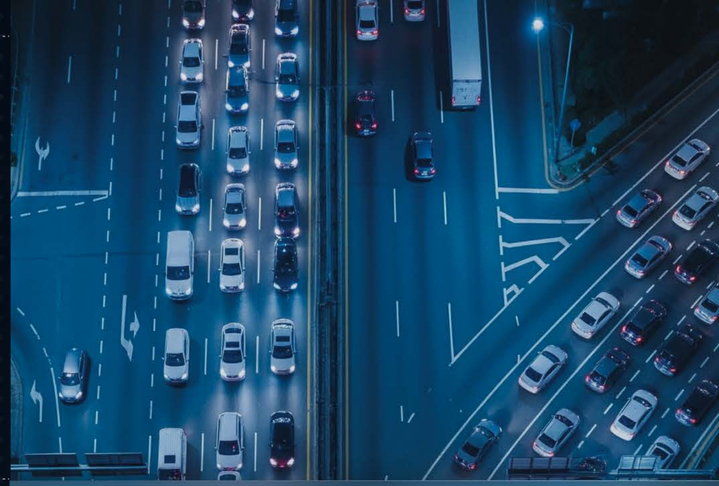
→ Common patterns

Across all environments, three patterns are consistent:

- → **Traffic is continuous rather than intermittent**
- → **Application execution spans multiple domains**
- → **Failures propagate across systems rather than remaining isolated**

CHAPTER 5

Why incremental improvements are no longer sufficient



The limits of incremental change

A common response to emerging performance issues is to add bandwidth, upgrade specific segments, or deploy additional monitoring tools. While these actions can provide short-term improvements, they don't address the underlying structural mismatch.

Drivers of increasing complexity

As environments evolve, several forces compound complexity:

- **Increased concurrency across users and devices**
- **Growth in east–west traffic**
- **Additional overhead from encryption and inspection**
- **Stronger dependencies across wireless, LAN, WAN, and application layers**

Failure progression

Over time, constraints tend to accumulate in a predictable way:

Stage	Constraint
STAGE 1	**Wireless contention**
STAGE 2	**Uplink oversubscription**
STAGE 3	**WAN variability**
STAGE 4	**Operational fragmentation**

→ Business impact

As these constraints build, troubleshooting becomes more complex, mean time to resolution (MTTR) increases, and application performance becomes inconsistent. At that point, the issue extends beyond network engineering and begins to affect business operations.

CHAPTER 6

Design principles for AI-ready networks

Evolving the operational model

Modern environments generate more telemetry than traditional operational models can effectively interpret in real time. Alert-driven domain-specific workflows aren't well suited to issues that span multiple domains.

An effective model must correlate signals across domains, understand cause-and-effect relationships, and support timely response.

Designing for sustained performance

Infrastructure must be designed to maintain consistent latency and behavior under continuous load rather than optimizing solely for peak throughput.

Unifying visibility across the execution path

Visibility must extend across the full path, from user to application, reducing the time required to isolate root cause and enabling faster resolution.

Embedding security into the network

Security must be integrated into the network fabric, with policy enforcement based on identity and applied consistently across environments.

→ Design implications

Layer	Traditional approach	AI-ready approach
Access	1 GbE	multigigabit/10G
Core	Peak throughput optimized	Low-latency fabric
Wireless	Coverage driven	High density
WAN	Best effort	Application-aware
Operations	Siloed	Cross-domain
Security	Centralized	Distributed, identity-driven

CHAPTER 7

Why Cisco—and why now?

A system-level problem requires a system-level architecture

The challenges outlined earlier—continuous demand, cross-domain dependencies, and rising operational complexity—don't originate within any single layer of the network. They emerge from how infrastructure, operations, and security interact under sustained load.

Most solutions in the market address parts of this problem:

- **Better visibility within a domain**
- **Faster correlation across signals**
- **Incremental improvements in performance or security**

What they don't address is the system itself.

Modern networks fail less because of individual components—and more because those components aren't designed to operate together under continuous, cross-domain conditions.

Cisco AI-Ready Secure Network Architecture is built around this distinction: the network must operate as a **coordinated system**, not a collection of tools.

Operations

Simplified operations powered by AgenticOps

Most enterprise environments today rely on a combination of domain-specific tools and artificial intelligence for IT operations (AIOps) platforms. While these systems improve visibility and correlation, they still depend on human interpretation and sequential workflows.

This creates a structural limitation:

- **Issues span domains**
- **Data is fragmented**
- **Resolution remains manual**

AgenticOps from Cisco addresses this by introducing a closed-loop operational model that combines telemetry, domain-aware reasoning, and controlled execution.

What's different?

The difference isn't incremental—it's architectural.

Capability	Traditional/AIOps	Cisco AgenticOps
Data	Aggregated telemetry	Cross-domain, system-level telemetry
Analysis	Correlation	Causal reasoning (DNM)
Action	Human-driven	System-assisted execution
Outcome	Faster troubleshooting	Continuous performance maintenance

How it works in practice

AgenticOps operates as a continuous loop:

Observe → reason → plan → execute → validate

Observe: Unified telemetry across wireless, campus, WAN, and application layers (including ThousandEyes for end-to-end visibility)

Reason: The **Cisco Deep Network Model (DNM)** applies protocol, topology, and policy awareness to identify root cause—not just correlated signals

Plan and execute: Actions such as traffic steering, quality of service (QoS) changes, or configuration updates are applied through the control plane (SD-WAN, Catalyst Center, Meraki) with built-in guardrails

Validate: Outcomes are verified using post-change telemetry before closing the loop

Why this matters

A single user experience issue may involve:

- **Radio frequency (RF) contention**
- **Switch queue buildup**
- **WAN packet loss**
- **Software-as-a-service (SaaS) latency**

Most tools surface these independently.

Cisco's approach is designed to understand and act on them as one system, which is the difference between diagnosing issues and maintaining consistent performance at scale.

Infrastructure

Scalable devices ready for AI

As traffic shifts toward sustained demand, the limiting factor is no longer peak throughput—it's how infrastructure behaves under load.

Traditional architectures often introduce latency variability as utilization increases, driven by shared buffers, pipeline contention, or oversubscription.

Cisco infrastructure, built on Silicon One, is designed differently.

What's different?

- **Deterministic latency under sustained load**
- **High concurrency without performance degradation**
- **Integrated, real-time telemetry without external instrumentation**

This isn't simply higher performance—it's **predictable performance** under real operating conditions.

Why this matters

In modern environments:

- **AI workloads create sustained east–west traffic**
- **Collaboration tools depend on consistent latency**
- **Small variations compound across domains**

Networks do not fail because they run out of bandwidth. They fail because they cannot maintain consistency under continuous load.

Cisco's infrastructure is designed specifically for this condition.

Security

Security fused into the network

Traditional security models assume traffic can be routed through centralized inspection points. In distributed environments, this creates blind spots and inconsistent enforcement.

Cisco takes a different approach by embedding security into the network fabric itself.

What's different?

- **Identity as the control plane (ISE, SGT)**
  [ISE – Identity Services Engine, SGT – Security Group Tags]
- **Segmentation enforced across the network (SD-Access)**
  [SD-Access – Software-Defined Access]
- **Distributed enforcement across all traffic paths (Hybrid Mesh Firewalling)**

This enables policy to follow the user, device, or workload—regardless of location.

Why this matters

- **Lateral movement is restricted by default**
- **Policy remains consistent across campus, branch, WAN, and cloud**
- **Security scales with the network rather than constraining it**

This is particularly critical as encrypted and east–west traffic increase.

The real differentiation: Integration across domains

→ Individually, these capabilities are valuable. Collectively, they are what differentiate Cisco.

Domain	Traditional approach	Cisco approach
Visibility	Tool-specific	End-to-end (client → app)
Operations	Correlation	Reasoning + execution
Infrastructure	Peak throughput	Deterministic performance
Security	Centralized	Distributed, identity-driven

Most vendors optimize for one or two of these areas. Cisco's architecture is designed to operate across all of them as a **single system**.

Why this matters now

The shift to continuous, latency-sensitive workloads is already underway. As it accelerates, the cost of inconsistency increases—not just in user experience, but in operational complexity.

At the same time, environments built on fragmented tools and manual workflows face a widening gap between visibility and resolution.

The implication isn't immediate failure, but a steady erosion of predictability.

The question is no longer whether the network can handle peak demand, but whether it can operate consistently under continuous demand.

Cisco's architecture is designed for this transition—aligning infrastructure, operations, and security with how modern applications actually behave.

CHAPTER 8

A practical starting point

Evaluating the network through application execution

A practical starting point is to evaluate the network from the perspective of application execution. This involves identifying critical application paths, assessing how performance behaves under sustained load, and understanding how issues are diagnosed across domains.

Indicators of structural strain

Certain patterns often indicate that the network is operating outside its design assumptions:

- **Persistent performance variability despite acceptable utilization**
- **Increasing time to isolate root cause**
- **Security policies tied to location rather than identity**
- **Dependence on multiple tools and teams for troubleshooting**

A phased approach to modernization

Modernization doesn’t require a complete overhaul. It requires a phased approach that addresses performance, visibility, and security in a coordinated way.

Cisco works with organizations to assess the current state, identify gaps, and define a roadmap aligned with business priorities.

Final perspective

Enterprise networks are no longer constrained solely by bandwidth. They are constrained by their ability to operate under continuous demand, maintain consistent performance, and manage cross-domain complexity.

As these requirements evolve, the network becomes more than infrastructure.

It becomes a critical component of how applications execute—
and how the business operates.

Take the next step in modernizing your network.

View webinars → Discover more →