Closing the readiness gap

How secure networking is defining future success

Contents

Cisco secure networking

India is entering a new phase of digital acceleration. Cloud adoption is rising, AI is moving from pilots to production, and hybrid work has permanently expanded the boundaries of the enterprise.

For any business leader, this creates a high-stakes reality: the network is now asked to deliver more performance, more visibility, and more security than it was ever designed for - at a scale few markets face.

This paper is Cisco India's point of view on secure networking - the fundamental advantage of having a single, unified infrastructure, where connectivity and security are intrinsically built as one. The paper serves as a practical blueprint for leaders looking to modernize infrastructure, reduce risk, and scale AI-ready operations with a more unified and simplified approach.

The paper also outlines why many organizations are hitting a readiness gap between digital ambition and operational resilience - and why the traditional response of adding more tools, more overlays, and more complexity is no longer sustainable.

It includes

- A clear framing of India's readiness gap - and why it is an architectural issue, not a single-domain problem
- The converging pressures of hybrid work, multi-cloud, SaaS, and AI, and what they demand from modern networks
- Why the network has become the first line of defence and the 'convergence layer' where visibility, policy, and enforcement meet
- Examples of overlapping capabilities (networking and security-based) that delivered exponential outcomes when they were designed to work together
- India-relevant models and outcomes that show what great looks like in practice

This paper is a practical blueprint for leaders looking to modernize infrastructure, reduce risk, and scale AI-ready operations with a more unified and simplified approach.

The network imperative

Securing India's digital future

India is on track to become the world's third-largest economy by 2028, with nearly 1 billion people online. This rapid digital expansion, coupled with the rise of AI, presents extraordinary opportunities, but also significant challenges for business and IT leaders.[1]

How can organizations navigate a complex, rapidly evolving threat landscape while staying competitive and capitalizing on emerging technologies? In India, this tension is particularly acute due to scale, diversity of infrastructure maturity, and accelerated digital adoption.

Simplifying complexity

Complicated problems are rarely solved by adding complexity, but that is just what many companies have done. Across networking, data processing, and user experience, Cisco focuses on reducing clutter, providing clear lines of sight, and delivering operational clarity. This unifying approach drives better decisions, faster responses, and more resilient outcomes.

India's digital acceleration

India's enterprise landscape is evolving faster than traditional infrastructure can support. Applications are no longer confined to data centers, users access resources from multiple locations and devices while data is generated and consumed across cloud, SaaS, and edge environments.

This expansion increases the attack surface dramatically. Many businesses have responded with increasingly complex security stacks, but more tools alone cannot solve operational and security challenges. Add the exponential growth of traffic and compute demands from AI workloads, and organizations quickly find themselves unable to keep up.[2]

1. EY India. India Towards Becoming the Third Largest Economy in the World. Economy Watch. 2023.
2. Cisco Systems, Inc. Cisco Hybrid Work Solutions Overview. Cisco.com. Latest edition.

The C-Suite challenge

Cisco's 2025 AI Briefing highlights the pressures on senior executives:

- 53% of CEOs globally fear missed growth opportunities due to underinvestment in technology.[3]
- 74% believe outdated infrastructure is already limiting innovation.[3]
- CISOs face expanded attack surfaces across endpoints, networks, clouds, and applications, often protected by disconnected tools and inconsistent policies.
- CIOs are tasked with deploying AI initiatives and modernizing infrastructure without escalating cost or complexity.

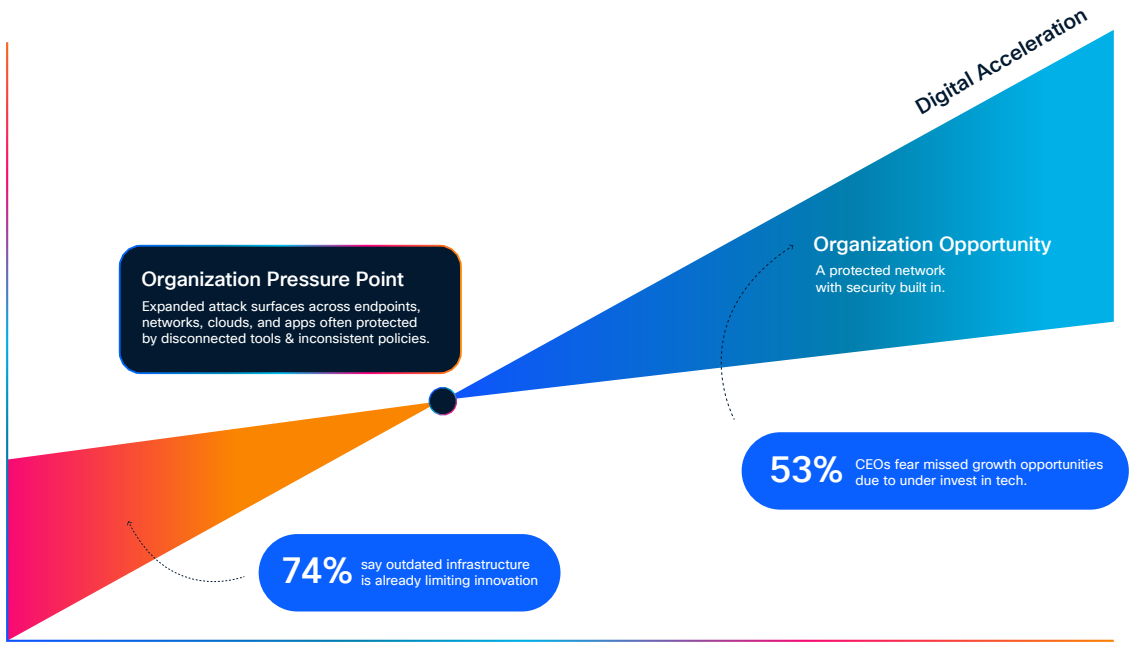
While CEOs look to their colleagues to deliver security and growth, these challenges may seem distinct, but they stem from the same underlying capacity constraints.

The platform approach

At Cisco we believe that a unified, secure networking foundation that aligns performance, visibility, and security is the way to meet these challenges. By operating through a single platform across networking, security, and observability, organizations no longer need to choose between speed and safety – reducing complexity and delivering an all-important layer of clarity and simplicity for the end user.

CIOs and CISOs can now innovate, scale, and protect simultaneously, turning India's digital acceleration into a sustainable competitive advantage, and maybe CEOs can sleep at night knowing they are not missing out on the next innovation.

Security & infrastructure readiness



3. Cisco Systems, Inc. Cisco 2025 AI Briefing: CEO Edition. February 2025.

India's readiness gap

Closing the divide between ambition and operational resilience

India is in the midst of a remarkable digital acceleration, and organizations are rapidly adopting cloud, AI, and automation to transform operations, deliver superior customer experiences, and compete globally.
Yet, according to Cisco's 2025 Cybersecurity Readiness Index, the gap between digital ambition and operational readiness remains significant.

While 7% of Indian organizations have achieved a 'Mature' level of cybersecurity readiness, slightly ahead of the global average of 4%, this still leaves 93% of companies in a precarious state, vulnerable to downtime, data loss, and operational disruption.[4]

The stakes are high: it's estimated that businesses on the Forbes' Global 2000 lose $200 million annually per organization in direct costs such as lost revenue, fines, and service interruptions.[5]

Legacy networks and fragmented tools

Many Indian enterprises operate on legacy network infrastructures that struggle to deliver consistent performance and visibility across campuses, branches, clouds, and SaaS platforms. Fragmented security controls, inconsistent telemetry, and limited automation slow detection and response to cyber threats.

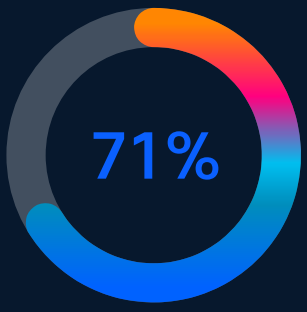
4. Cisco Systems, Inc. Cisco Cybersecurity Readiness Index 2025. 2025.
5. Cisco Systems, Inc. The Hidden Costs of Downtime. Security Outcomes Study (Cisco & External Economic Analysis). 2024.

Cisco research highlights the magnitude of the challenge

86–95% have experienced at least one AI-related security incident in the past year[4]

Talent shortages, particularly in senior security and network architecture roles, continue to constrain execution.

This is not just a security problem, or even a networking problem, it is an architectural issue. Addressing it requires CIOs and CISOs to align on shared platforms, shared data, and shared outcomes.



71% of organizations expect business disruptions from cyber incidents within the next 12–24 months.[4]

AI and integrated solutions: Closing the gap

A growing number of Indian enterprises are turning to AI-powered solutions to enhance resilience. In fact, 56% of companies that have adopted network protection solutions now significantly incorporate AI into their defenses.[6]
These AI-driven tools:

- Detect anomalies in real-time
- Prioritize threats based on risk context
- Enable faster, automated responses

Cisco's network and AI threat detection solutions – powered by platforms such as Splunk – offer integrated telemetry and analytics, correlating signals across endpoints, networks, and applications to accelerate Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). These capabilities allow Indian enterprises to move from reactive operations to predictive, automated threat management.

> "By embedding AI across networking and security, organizations can significantly improve their cyber posture and reduce operational risk."

4. Cisco Systems, Inc. Cisco Cybersecurity Readiness Index 2025. 2025.
6. Cisco Systems, Inc. Security Outcomes Study: AI & Automation Edition. 2024.

Long-term resilience

The appetite for sustainable cybersecurity is strong in India, with 56% of Indian businesses planning to implement network segmentation within the next year and 37% intending to implement segmentation in the following one to two years. This reflects a fundamental shift toward proactive security, emphasizing architectural modernization, real-time visibility, and automation.

Integrated, end-to-end cybersecurity strategies are now essential, combining AI-powered threat detection and response with high-quality, reliable data and modernized network infrastructure. These solutions fuel AI analytics and deliver networks capable of supporting cloud, SaaS, and AI workloads.

India generates roughly 20% of the world's data, but hosts only 3% of global data centre capacity, and there is an increasing desire for cloud infrastructure to be housed within the same territory as operations.[7]

Cisco's solutions provide Indian organizations with a complete, AI-native platform, from secure networking with embedded visibility to analytics and threat intelligence via Splunk, powered by cloud capacity from Meraki India Region.

Indian businesses plan to implement network segmentation in the:

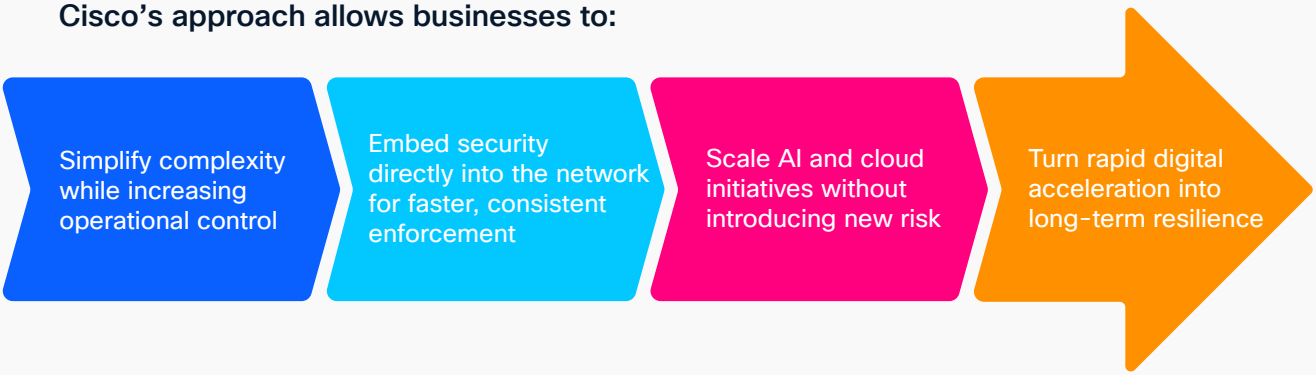
Next 12 Months

Next 1-2 years

The Cisco path forward for India

Closing India's readiness gap requires a unified architecture that integrates networking, security, observability, and AI into a single operating model. The gap is not caused by insufficient tools, but by the absence of this converged model.

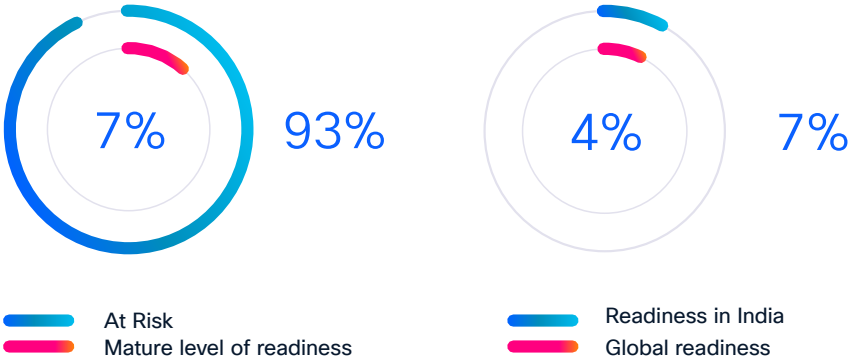
Cisco's approach allows businesses to:



7. Fortune India. The Coming Data Centre Boom. 2024.

By modernizing infrastructure, integrating AI-powered security, and aligning CIO and CISO objectives, Indian enterprises can close the readiness gap, reduce risk, and unlock the full value of digital transformation.

In a market where ambition is high but operational maturity is uneven, Cisco offers the clearest, most complete blueprint for secure, scalable, AI-ready networking in India.



> “only 7% of Organizations in India have achieved a mature level of cybersecurity readiness.”

Converging risks and demands

Hybrid work, multi-cloud, and AI

The enterprise network is no longer defined by walls, campuses, or data centers. Hybrid work, multi-cloud adoption, and AI-driven innovation have permanently reshaped how organizations operate and, just as importantly, how risk accumulates.

These forces are not isolated trends. They are converging pressures that expose gaps in visibility, security, and operational resilience. Organizations that continue to rely on fragmented tools and siloed operating models will struggle to deliver reliable digital experiences, protect critical assets, and scale for AI-driven growth.

Hybrid work has redefined the perimeter

Hybrid work has dissolved the traditional network perimeter. Employees now access applications from home offices, corporate campuses, and public networks using a mix of managed and unmanaged devices. SaaS applications have become the backbone of daily operations, often accessed directly over the internet rather than through centralized data centers.[8]

For CIOs, this shift introduces new challenges around application availability, performance, and user experience. For CISOs, it dramatically expands the attack surface across identities, endpoints, networks, and cloud services. Visibility gaps emerge when users, devices, and applications sit outside traditional monitoring and enforcement frameworks.

The result is a fragile operating environment where IT teams must maintain uptime and security across locations they no longer fully control.

8. Cisco ThousandEyes. Internet & Cloud Insights Reports. Cisco ThousandEyes Research.

Multi-cloud complexity multiplies risk

We have seen through the deployment of the Meraki India Region how many businesses prefer their cloud infrastructure to have a physical base in their own region. This helps to streamline regulatory requirements and gives an extra layer of assurance. However, many organizations have no choice but to operate multi-cloud environments, often across many territories.

Multi-cloud strategies promise flexibility and innovation, but they also introduce operational complexity. Each cloud provider brings its own networking constructs, security controls, logging formats, and management tools. Teams are forced to stitch together disparate platforms, often without consistent policy enforcement or end-to-end visibility.

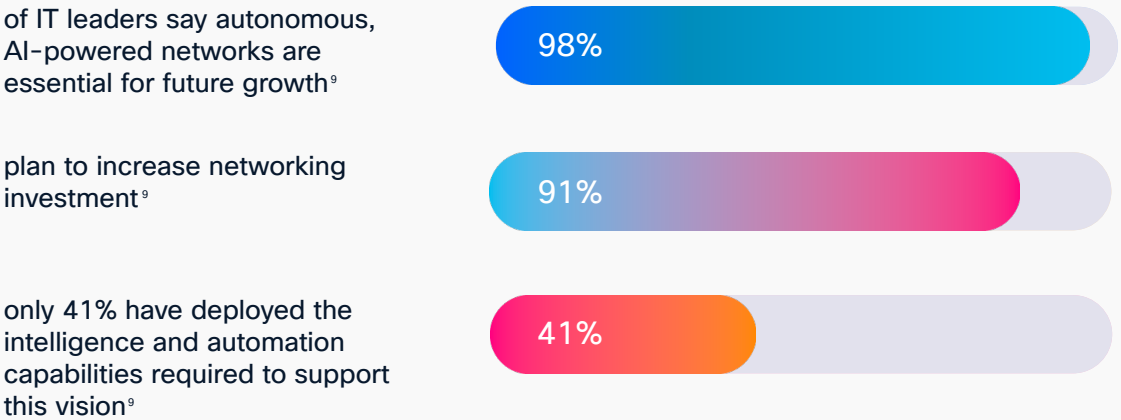
This fragmentation slows troubleshooting and increases the likelihood of misconfigurations. It also makes it difficult to correlate performance and security events across environments. When something breaks, the mean time to resolution increases, and so does business impact.

A unified secure networking approach across on-premises, cloud, and SaaS environments is no longer a 'nice-to-have, it is fundamental to resilience.

AI is raising the stakes for network resilience

AI workloads intensify these pressures. AI requires fast, uninterrupted access to data across distributed environments, while generating massive east-west traffic and placing new demands on network performance and reliability.

According to Cisco's AI readiness index



9. Cisco Systems, Inc. Cisco AI Readiness Index 2025: Realizing the Value of AI. 2025.

At the same time, network resilience is under strain

77%

of organizations experienced major outages in the last two years[10]

Leading causes include congestion, cyberattacks, and software or configuration errors

52%

say revenue is the business area most impacted by disruptions[10]

A single severe outage can cost businesses billions collectively, adding up to an estimated $160bn globally per year[10]

“These outages are more than downtime, they directly affect revenue, productivity, customer trust, and growth.”

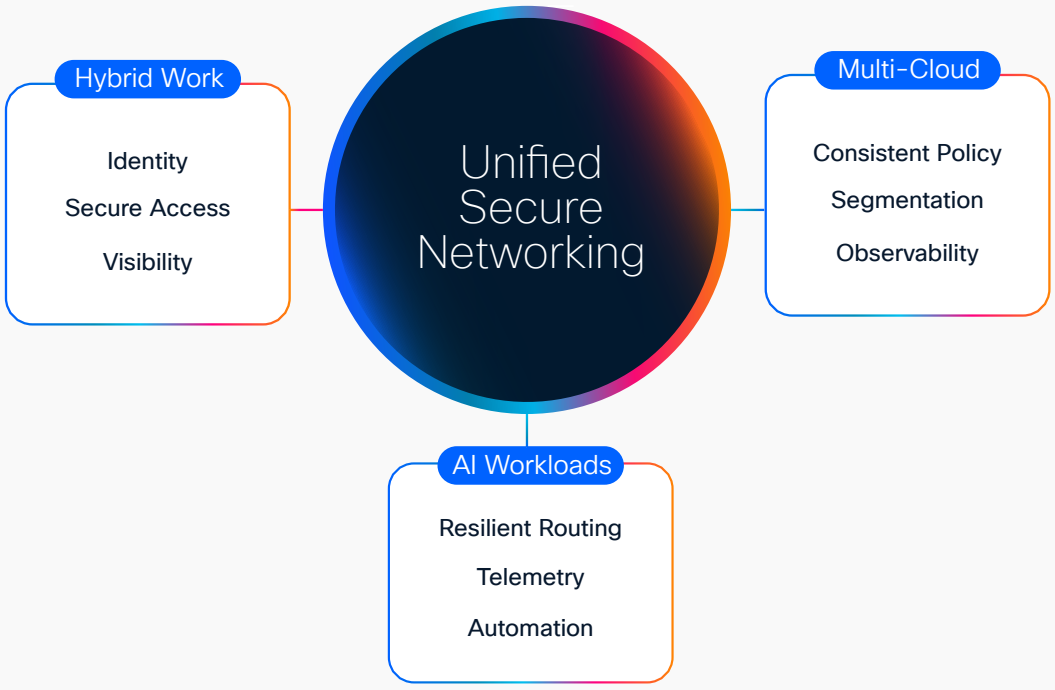
Why siloed tools are no longer enough

The traditional approach to cybersecurity has often been to add more point solutions, more dashboards, more alerts, more tools. This can lead to siloed systems that create blind spots, operational friction, and inconsistent policies, all the while increasing costs and complexity.

The goal is not to deploy more tools, but to simplify operations, improve visibility, and build a resilient foundation that can scale with hybrid work, multi-cloud, and AI. The organizations that succeed will be those that approach their security and networking as one seamless system - to create a more agile, secure, and better-run business.

Building for what's next

Hybrid work, multi-cloud, and AI are here to stay, and if they are not already, will soon be part of 'business as usual'. The organizations that succeed will be those that simplify their environments, unify operations, and embed intelligence across their infrastructure. Cisco is helping enterprises make this transition, securely, intelligently, and at scale.



Why the network is now the first line of defense

The multiplication of threats we discussed earlier means a strong network has to be underpinned by a zero trust strategy. These strategies succeed or fail at the network edge, where users connect, devices authenticate, and traffic flows between applications and data, often across environments that extend far beyond the corporate campus.

From a security perspective, it is vital that access policies are enforced consistently, traffic is segmented to limit lateral movement, threats are detected using behavioral and contextual signals, and that enforcement happens at machine speed, not human speed.

With these measures in place, the network becomes the telemetry hub, providing real-time visibility into application and user experience, faster fault isolation and remediation, and the all-important data foundation required for AI-driven operations and automation.

When security is built directly into the network, rather than bolted on as an overlay, CIOs and CISOs gain a shared source of truth. This alignment reduces friction, shortens response times, and enables coordinated decision-making across performance, availability, and risk.

AI, IoT, and cloud Are redefining network expectations

We know from Cisco's 2025 Networking Research that nine out of ten IT leaders expect AI, IoT, and cloud to have the biggest impact on their networks in the next two years, and that they are planning to invest in modernizing their networks to help deploy them.[11]

AI workloads, in particular, place unprecedented demands on networks. They require low-latency, high-throughput, and highly resilient connectivity across distributed environments. At the same time, AI increases the blast radius of outages and security incidents.

Networks were previously defined by speed and capacity, but there is now a real shift to think in terms of network intelligence, high degrees of automation, and an expectation of security by design.

9/10 IT leaders expect AI, IoT, and cloud to have the biggest impact on their networks in the next two years. [11]

> "When security is built directly into the network—not bolted on—CIOs and CISOs gain a shared source of truth."

11. Cisco Systems, Inc. Cisco 2025 Networking Research. 2025.

The network is the value: Turning infrastructure into business impact

It is often tempting to think of networks as cost-centres, fraught with vulnerabilities, but the reality is far different. Over half of the IT leaders we've spoken to are delivering measurable business value from their networks, with improved customer experience and increased operational efficiency. There is also a recognition that networks enable innovation.

The business case for smarter and more secure networks is compelling. An impressive 89% of those surveyed in our research said improved networks will directly drive revenue, with 93% expecting meaningful cost savings through smarter operations, fewer outages, and reduced energy consumption. It's for this reason that Cisco defines the Power Pair strategy as synonymous with secure networking - one cohesive infrastructure that represents the future of how organizations will build and scale.[11]

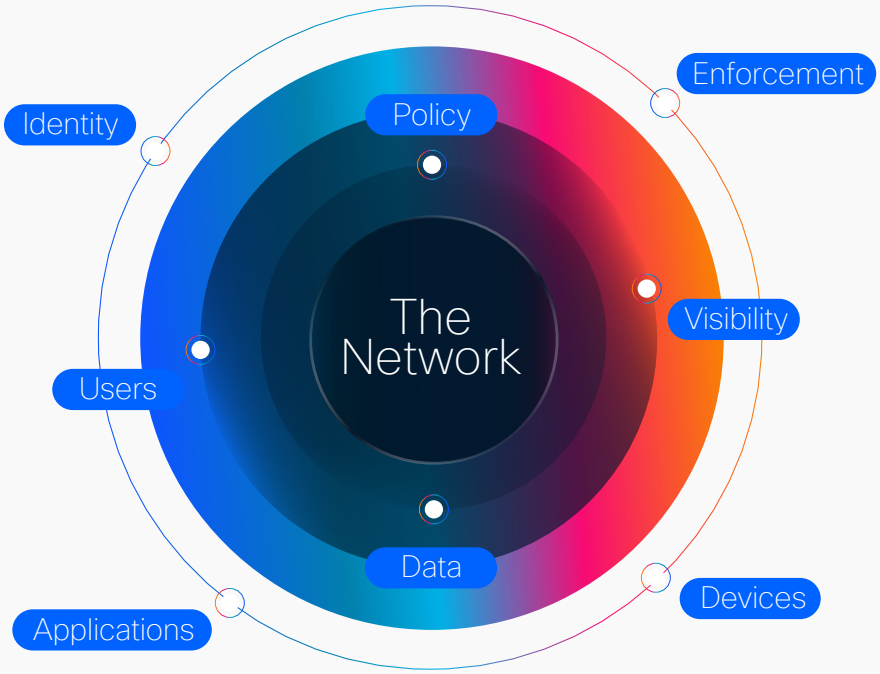
It is important, however, to sound a note of warning, as many organizations are relying on infrastructure that was never designed for AI-driven scale or real-time operations. Organizations in this situation have to address siloed or partially integrated systems, incomplete deployments, and systems that rely too heavily on manual oversight if they are to realize the growth potential of their networks.

89%

of those surveyed in our research said improved networks will directly drive revenue.[11]

93%

expecting meaningful cost savings through smarter operations, fewer outages, and reduced energy consumption.[11]



Cisco's secure networking point of view

One platform, shared outcomes

Traditional approaches treat networking and security as separate domains, often managed by different teams using different tools. This separation creates blind spots, inconsistent policies, and operational friction, especially in hybrid, multi-cloud environments.

Cisco's secure networking point of view starts from the premise that security is not an overlay or add-on, it is embedded into the infrastructure itself.

This enables CIOs and CISOs to operate from a shared foundation, with common telemetry, consistent enforcement, and aligned outcomes. The result is a platform model that simplifies operations while strengthening security and resilience.

> Security is not an overlay or add-on — it is embedded into the infrastructure itself."

Unified policy with distributed enforcement

At the core of Cisco's approach is a unified policy model with enforcement distributed across the entire environment. This is achieved through campus and branch networks, WAN and SD-WAN environments, and data center and multi-cloud infrastructure, ensuring consistent access control, segmentation, and threat prevention, regardless of where users, devices, or applications reside.

Technologies such as Cisco Identity Services Engine (ISE), Cisco Secure Access, Cisco SD-WAN, Cisco Secure Firewall, and Cisco Secure Workload work together to deliver consistent access control, segmentation, and threat prevention regardless of the location of users, devices, or applications. This enables zero trust principles to be applied uniformly, while still allowing fine-grained enforcement close to the source of activity.

> At the core of Cisco's approach is a unified policy model with enforcement distributed across the entire environment."

Security and visibility embedded in the network

Visibility determines both performance outcomes and security effectiveness. Rather than relying on external tools alone, Cisco embeds visibility and security directly at the network and operating system, delivering a unified, secure network. This approach improves detection accuracy using contextual network signals. It also reduces blind spots created by encrypted traffic and enables faster, more confident responses to anomalies and threats.

Much of what we have covered so far is unified by bringing simplicity to complex environments. Cisco delivers cloud-managed operations through unified dashboards that span networking, security, and observability domains. Platforms such as Cisco Meraki, Catalyst Center, and Secure Access provide simplified configuration and lifecycle management, end-to-end visibility across environments, and reduced operational overhead for IT teams.

AI-native operations powered by telemetry

High-fidelity telemetry is the fuel for intelligent operations, and it enables faster root-cause analysis, automated remediation, and improved service assurance at scale. Cisco's AI-native approach uses advanced analytics and machine learning to transform raw telemetry into actionable insight across networking and security domains.

Capabilities such as Cisco AI Network Analytics and automation detect anomalies, predict failures, and recommend or execute remediation actions, reducing downtime and human error. When combined with Splunk's analytics platform, organizations gain deeper correlation across network, security, and application data, enabling faster root-cause analysis and more effective incident response.

This convergence is giving rise to a new operational model: the Resilience Operations Center. Here NetOps, SecOps, and AppOps teams collaborate using shared data, shared tools, and shared objectives. Instead of operating in silos, teams work from a common operational truth.

> “Cisco embeds visibility and security directly at the network and operating system level.”

Secure-by-design infrastructure

Cisco's secure networking platform is underpinned by infrastructure that is secure by design with hardware and software trust mechanisms, including Trust Anchors, Secure Boot, MACsec encryption, and native segmentation. These features help ensure platform integrity, protect data in motion, and reduce the risk of supply chain and insider threats.

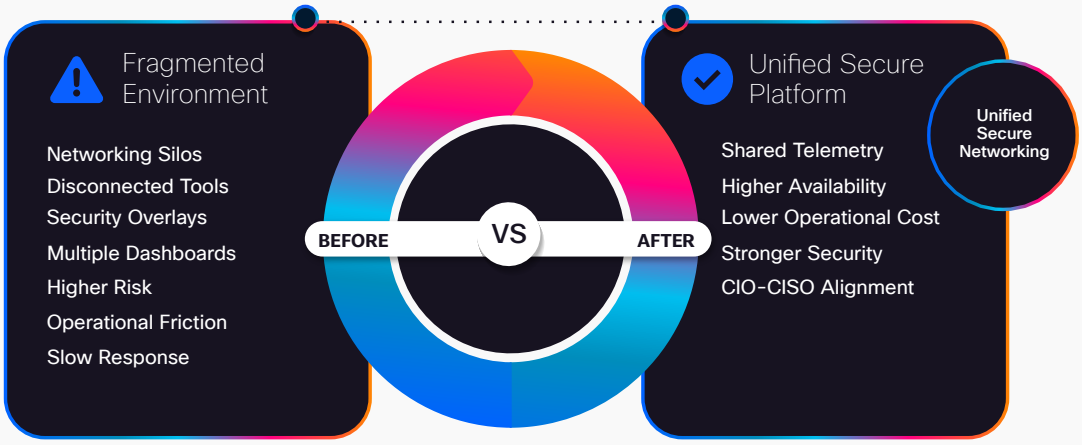
For organizations supporting AI workloads, sensitive data flows, and regulated environments, these capabilities establish zero trust principles at the foundation of the network, not just at the user and application layers.

Shared outcomes, real results

Cisco's Secure Networking point of view is about delivering both performance and protection through a single, integrated platform. By embedding security into the network, simplifying operations through cloud management, and applying AI-driven intelligence at scale, Cisco enables companies to lead from a common foundation, turning complexity into clarity and acceleration into sustained readiness.

A secure and resilient network is a strategic enabler for AI, cloud, and future growth, and perhaps most importantly, it reduces complexity without sacrificing control.

Architectural simplification



12. This chapter draws on insights from Cisco Global Networking Trends Report (2025) and Cisco 2025 Networking Research.

Integrated by design

Turning overlapping capabilities into exponential outcomes

In hybrid, multi-cloud, and AI-driven environments, value is created when visibility is directly connected to enforcement, when telemetry feeds intelligence, and when security is built into the network as a single system.

Cisco's integrated portfolio is intentionally built around the Power Pair philosophy – security and networking operating on a shared foundation. By connecting this strategy with observability and analytics, Cisco enables organizations to reduce complexity, strengthen protection, and accelerate outcomes with greater clarity and control.

Below are key examples of how a secure networking approach transforms operations.

Visibility + enforcement: ThousandEyes + Cisco SD-WAN

Visibility without action creates insight, but not outcomes. By integrating Cisco ThousandEyes with Cisco SD-WAN, organizations gain both.

ThousandEyes delivers deep, end-to-end visibility across the internet, cloud providers, and SaaS applications, revealing exactly where performance degradation occurs. When combined with SD-WAN, those insights can directly inform policy-based routing and enforcement.

The result is a closed-loop system where

Internet and cloud issues are identified in real-time

Traffic is dynamically steered away from problem paths

User experience is protected without manual intervention

> This integration turns the network into an active participant in experience assurance – not just a passive observer."

Routing + DDoS Defense: Cisco IOS® XR Routers + Cisco Secure DDoS Edge Protection

Resilience has to begin at the earliest point threats can enter the system, and at internet scale, this means at the routing layer. Distributed denial-of-service (DDoS) attacks increasingly target core routing infrastructure, cloud interconnects, and AI-driven services, threatening availability long before traditional security controls can respond.

Cisco IOS® XR-based routers provide the high-performance, carrier-grade routing foundation required to operate at massive scale, supporting advanced telemetry, programmability, and resilient control planes. When paired with Cisco Secure DDoS Edge Protection, these routers become an active line of defense against volumetric and protocol-based attacks.

Together, they enable

Early detection of DDoS attacks using routing and traffic telemetry

Automated mitigation at the network edge, before congestion spreads

Protection of critical services without sacrificing throughput or latency

By addressing infrastructure with a Power Pair approach, CIOs and CISOs gain a unified system to maintain availability for mission-critical services while mitigating large-scale attacks at the point of entry, where response is fastest and most effective.

> The Power Pair strategy allows CIOs to maintain availability for mission-critical services while enabling CISOs to mitigate large-scale attacks at the point of entry, where response is fastest and most effective."

Kubernetes networking, visibility, and security: Isovalent (Cilium + Tetragon)

Cloud-native environments demand cloud-native security. Isovalent, built on Cilium and Tetragon, brings networking, observability, and runtime security directly into Kubernetes.

Cilium provides high-performance, eBPF-based networking and segmentation, while Tetragon delivers deep visibility into process execution and system behavior at runtime.

Together, they enable

Fine-grained, identity-based networking at the Kubernetes layer

Real-time detection of anomalous or malicious activity

Security enforcement without sidecars or performance penalties

This integration allows DevOps and security teams to secure containerized workloads without slowing innovation.

Cloud-native segmentation across north-south and east-west traffic: Multi-cloud defense + secure workload

To tackle inconsistent segmentation and fragmented policy enforcement in multi-cloud environments, Cisco Multicloud Defense focuses on protecting ingress and egress (north-south) traffic, while Secure Workload provides deep visibility and microsegmentation for east-west traffic within and across workloads.

Together, they deliver

Consistent segmentation policies across data centers and clouds

Reduced attack surfaces and lateral movement risk

Simplified compliance and governance across environments

This pairing enables zero trust segmentation at cloud scale.

Networking + security at the edge: Catalyst + Cisco Secure Firewall

Security is most effective when it is enforced as close to the source as possible. The integration of Cisco Catalyst platforms with Cisco Secure Firewall embeds threat detection and enforcement directly into the campus network.

This combination enables

Unified policy across switching, wireless, and firewall domains

Faster detection and containment of threats at the edge

Reduced reliance on backhauling traffic for inspection

By collapsing the distance between networking and security, organizations improve both performance and protection.

Management control + policy engine: Catalyst center + Identity Services Engine (ISE)

Manual segmentation and static network policies are unable to cope with increasingly dynamic environments with dispersed users, devices, IoT, and AI-driven systems. Cisco Catalyst Center and Cisco Identity Services Engine (ISE) work together to deliver centralized control with identity-based enforcement.

Catalyst Center provides centralized network management, assurance, and automation across campus and branch environments. Cisco ISE acts as the policy engine, using identity, device posture, and contextual signals to determine access and segmentation.

Together, they enable

Identity-based segmentation across users, devices, and things

Centralized policy definition with distributed enforcement

Automated onboarding and consistent access control across the network

This pairing simplifies network operations while giving precise, scalable control over who and what can access the network, without relying on manual VLANs or static rules.

Universal identity + zero trust enforcement: Duo + secure access

Identity is the cornerstone of zero trust, but enforcement must follow the user everywhere. Cisco Duo and Cisco Secure Access work together to make that possible.

Duo provides strong, continuous identity verification, while Secure Access enforces zero trust policies across users, devices, and applications, regardless of location.

Identity-based access decisions with continuous verification

Consistent zero trust enforcement across on-prem and cloud apps

Secure, seamless access for hybrid workforces

This integration ensures that trust is never assumed and always verified.

Telemetry + analytics: Cisco infrastructure + Cisco XDR

Raw telemetry becomes powerful when it is correlated and analyzed at scale. By integrating Cisco infrastructure telemetry with Cisco XDR, organizations gain cross-domain threat detection and response.

Network, endpoint, email, and cloud signals are correlated to

Detect sophisticated, multi-vector attacks

Reduce alert fatigue through contextualized incidents

Enable faster investigation and response workflows

This integration transforms telemetry into actionable security intelligence.

Application and security telemetry: AppDynamics + Splunk

Performance issues and security incidents often share the same root cause. AppDynamics and Splunk together provide a unified view across applications, infrastructure, and security data.

This integration enables

Faster root-cause analysis across code, network, and infrastructure

Improved MTTD and MTTR through shared context

Better collaboration between NetOps, SecOps, and DevOps teams

The result is faster resolution and more resilient digital experiences.

Analytics + threat intelligence: Splunk + Talos

Advanced analytics are only as good as the intelligence behind them. Splunk integrated with Cisco Talos brings world-class threat intelligence into analytics workflows.

Talos provides:

- Real-time threat intelligence from global telemetry
- Indicators of compromise and adversary insights

When combined with Splunk's analytics and automation, teams can

Detect emerging threats faster

Prioritize incidents based on real-world risk

Automate response with greater confidence

This pairing turns data into decisive action.

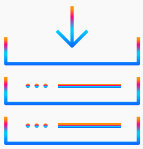
AI for security and security for AI: AI-infused security + AI defense

As AI is embedded across an organization, security must evolve in two directions at once: using AI to improve security, and securing AI itself.

Cisco's AI-infused security capabilities apply machine learning to

Detect anomalies and threats at machine speed

Predict and prevent outages and attacks



Automate response across the security stack

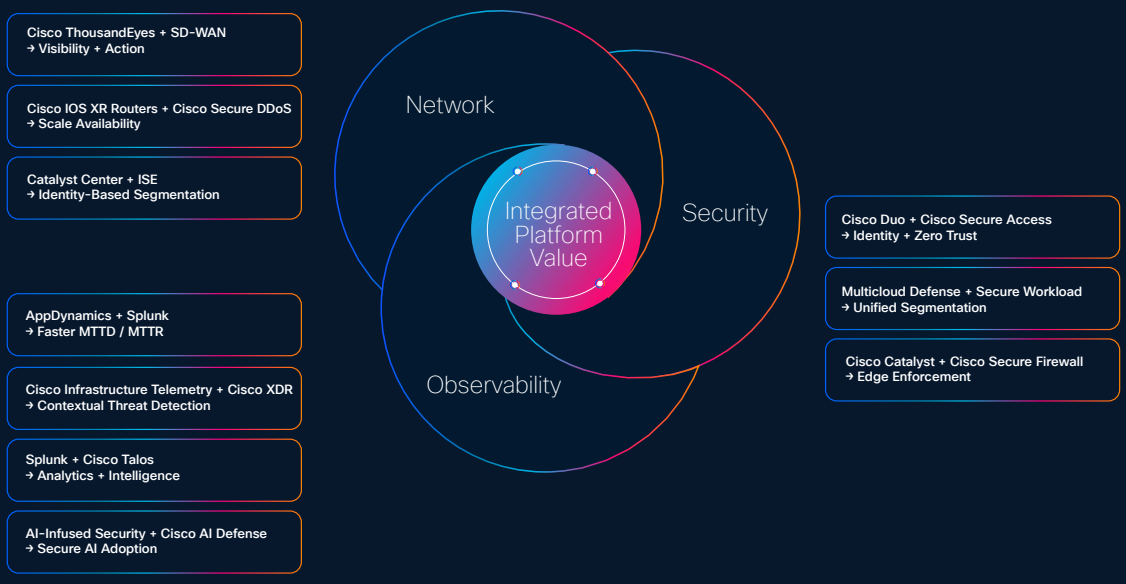
At the same time, Cisco AI Defense focuses on protecting AI models, data, and pipelines from misuse, poisoning, and exploitation.

Together, they ensure that AI accelerates innovation without becoming a new source of risk.

Stronger Together

Each of these integrations delivers value on its own, but together, they form a cohesive platform where visibility drives action, intelligence drives automation, and security is built in by design.

This is how Cisco helps organizations move from tool sprawl to operational leverage, and from reactive operations to resilient, AI-ready infrastructure.



India-focused models and outcomes

Measurable impact through secure, intelligent networking

Across India's enterprise landscape, organizations that have embraced secure, modern networking architectures are already unlocking measurable benefits. We've helped them to deliver greater resilience and performance, as well as faster incident response and lower operational cost.

Two compelling examples illustrate how integrated platforms deliver real-world outcomes, while enabling teams to shift from reactive firefighting to proactive optimization.

LTIMindtree

Securing global scale with simplified, AI-enabled access

LTIMindtree, one of India's largest IT services and consulting firms, faced a unique set of challenges as its workforce expanded rapidly around the world. With a global footprint spanning dozens of offices and tens of thousands of users, maintaining consistent, secure access for hybrid work was essential.

Working with Cisco, LTIMindtree deployed a modern secure access foundation that embeds zero trust principles at scale. By consolidating access controls and modernizing security with Cisco technologies, LTIMindtree significantly reduced operational complexity while strengthening cyber resilience and user experience.

The result was a more secure hybrid work environment that supports global collaboration without burdening IT teams with fragmented controls or manual policy management.

This outcome highlights that when identity, access, and networking are converged and AI-empowered, organizations gain consistent policy enforcement, fewer incidents, and simplified operations. All of these are key ingredients for digital readiness.

> “The result was a more secure hybrid work environment that supports global collaboration without burdening IT teams with fragmented controls or manual policy management.”

Birla Opus Paints

Connected factories, resilience by design

Birla Opus Paints entered India's competitive manufacturing sector with the bold vision to build six next-generation factories and a nationwide distribution network from day one. Cisco was selected to provide the digital backbone, delivering a secure, intelligent, and resilient architecture across factories, depots, and R&D operations.

By embedding Cisco technologies, including zero trust security, ThousandEyes end-to-end observability, and Cisco Industrial Network Director for centralized management, Birla Opus achieved 99.9% uptime, rapid automated deployment across 145+ depots, and consistent operational visibility.[12] These outcomes translated into continuous production, stronger supply chain resilience, and reliable quality control metrics without the operational overhead traditionally associated with scaling manufacturing networks.

More importantly, Birla Opus's experience underscores how secure networking platforms empower new enterprises to build resilience into their foundation, not as an afterthought but as an inherent business enabler.

Birla Opus achieved

99.9%
uptime achieved across the digital infrastructure.

145+
depots with rapid automated deployment and consistent visibility.

> "Birla Opus built resilience into its foundation — not as an afterthought, but as an inherent business enabler."

12. Cisco Systems, Inc. Birla Opus Paints: Connected Factories with Cisco. Customer Case Study.

Moving beyond case studies

Broader India outcomes

These case studies reflect a broader shift among Indian enterprises toward platform-based architectures that deliver strategic outcomes.

These are:

- Resilience and uptime: High-availability operations with measurable reductions in outages and disruptions.
- Operational simplicity: Automated deployment and centralized management delivering consistency across hybrid environments.
- Security posture: zero trust applied everywhere, from factories to remote offices, backed by real-time visibility and enforcement.
- Efficiency gains: Reduced mean time to detect and respond, freeing critical talent to focus on innovation rather than firefighting.

Integrated platforms improve visibility, reduce risk, and can help accelerate digital transformation. They also remove legacy silos and give teams a single source of truth, as well as bringing some much-needed simplicity.

Conclusion

Building India's digital future: secure, resilient, AI-ready networking

As we have seen, India is experiencing an unprecedented wave of digital acceleration from cloud adoption and hybrid work to AI-driven innovation across the enterprise, government, and services sectors. But speed without structure introduces risk. Enterprises cannot scale securely or confidently if networks remain fragmented, overly complex, or reactive. Architectural simplification with security built in is essential.

To meet these demands, networks must become intelligent, resilient, and AI-ready platforms capable of delivering seamless performance, continuous security, and real-time observability across hybrid and multi-cloud environments. This evolution transforms the network from a passive utility into a strategic foundation for innovation.

Cisco offers the clearest and most complete path to achieving this transformation in India. The Power Pair / secure networking strategy represents an interwoven approach across networking, security, observability, and AI, delivering exponential value. By operating through a single integrated model, Indian enterprises can close readiness gaps, reduce operational and security risk, and build AI-ready resilience at scale. Embracing this Power Pair methodology allows teams to move from reactive troubleshooting to predictive, automated operations, turning infrastructure into a true business enabler.

Just as we have shown how pairing complementary capabilities delivers outstanding performance, the same is true on a larger scale. Cisco has shown its commitment to aligning with India's growth trajectory and digital ambitions through its India Go Big strategy and investment in infrastructure.[13]

13. Cisco Systems, Inc. Cisco India Go Big Initiative. Press Release. 2023.

The Power Pair of Secure Networking