



AUTONOMOUS NETWORKS POWERED BY ARTIFICIAL INTELLIGENCE

This paper explores how artificial intelligence is transforming network operations from rule-based automation to systems that learn, reason, and adapt in real time. It outlines the shift toward autonomous networking—where networks manage performance, security, and assurance proactively—helping enterprises achieve greater agility, reliability, and efficiency across hybrid environments.

Cisco and Infosys: Advancing the Future of Autonomous Networks

Building the foundation for autonomous networks

Enterprises are reaching the limits of traditional network automation. Growing complexity, distributed environments, and AI-driven workloads demand a new model that can learn and adapt on its own. This paper explores how Cisco and Infosys are enabling that evolution through AI-powered autonomy that delivers greater resilience, efficiency, and insight.

Ideal audience:

- Network and IT operations leaders
- Network architects and engineers
- Digital transformation and infrastructure strategists

You will learn:

- Why traditional automation is no longer enough
- How AI-driven autonomous networks improve performance and assurance
- How the combination of Cisco's network intelligence and AgenticOps platform with Infosys's AI-First, human-centric Cloud & Infrastructure Services delivers a unified operational fabric where AI and humans collaborate seamlessly to enable autonomous, resilient, and adaptive networks.

Today's networks built for yesterday's demands

Enterprise and service provider networks, originally designed for centralized applications, on-site users, and predictable traffic patterns, have become the backbone of global digital operations. Configuration relied on manual processes, policies were static, and visibility ended at domain boundaries. Engineers managed each device, ticket, and alert individually, in a model that depended heavily on human expertise and constant attention.

At the same time, networks have become more critical to business performance. Every outage, policy misconfiguration, or degradation of service directly affects user experience, productivity, and revenue. A single human error can disconnect thousands of users or expose sensitive data. 70% of IT pros say alert fatigue is a top challenge, as many teams receive over 10,000 alerts per day.¹ As businesses depend more heavily on digital services and distributed connectivity, operational risks continue to grow.

Complexity is compounded by hybrid and multi-vendor environments. Many organizations run a mix of Cisco and third-party platforms across wired, wireless, and security domains. Each system can have its own interface, telemetry, and policy definitions. Correlating data across these domains is time-consuming and often incomplete. Infosys engineers describe this as complexity debt, a growing burden of integration, visibility, and configuration management that consumes valuable operational capacity. Every new device, API, or cloud instance adds to that debt.

The human impact is also significant. The global shortage of skilled IT professionals is expected to persist, with nearly two-thirds of organizations anticipating an IT skills gap by 2026.² Meanwhile, operations teams spend most of their time managing incidents and troubleshooting issues instead of driving innovation or improving performance, as fragmented visibility and manual workflows further constrain progress. Engineers focus on maintaining stability rather than enabling new digital services. This imbalance restricts agility at a time when organizations must move faster to stay competitive.

From a technical perspective, networks now generate more data than teams can process. Each device, client, and application produces telemetry that reflects performance, reliability, and security posture. Cisco® data shows that operators can see symptoms but often lack context. The result is reactive troubleshooting instead of predictive assurance. Traditional network-management tools struggle to correlate billions of data points quickly enough to isolate problems before they affect users. The system produces information faster than humans can interpret it.

Security adds another layer of pressure. As east-west traffic grows within enterprise networks, the potential attack surface expands. Manual segmentation cannot adapt to the dynamic nature of workloads and user mobility. Static policies either leave blind spots that attackers exploit or over-constrain legitimate traffic, slowing performance. Maintaining the right balance between security and agility requires context-aware intelligence that can evaluate risk in real time.

Hybrid work models have further increased operational strain. Employees and devices now connect from anywhere, at any time, across public and private networks. This creates more endpoints to monitor, more variables to manage, and more opportunities for failure. Traditional network architectures built for fixed locations and predictable demand cannot keep pace with this distributed reality. The complexity of managing such environments has outgrown what even the most experienced teams can handle manually.

¹ How to Address Cybersecurity Alert Fatigue with AI: <https://www.msspalert.com/native/how-to-address-cybersecurity-alert-fatigue-with-ai>

² Gartner - Strategies to Address Skill Gaps: <https://www.gartner.com/en/human-resources/insights/skills-gap>

The business implications are clear. Network reliability, once a back-office concern, is now a boardroom priority. Downtime disrupts customer engagement, delays transactions, and undermines brand trust. Slow incident response translates directly into lost productivity and revenue. As networks become more central to digital operations, the tolerance for disruption continues to shrink. Enterprises need infrastructure that can respond to conditions automatically, not after human intervention.

The limits of manual and reactive network management have become impossible to ignore. While many organizations have adopted automation to improve speed and consistency, these tools were never designed for the scale and dynamism of today's environments. Understanding how traditional approaches evolved—and where they now fall short—reveals why the next leap must be toward autonomous networking.

Traditional approaches: Progress that reaches its limits

For many years, organizations have addressed network complexity through automation and centralized management platforms. The goal has been clear: streamline operations, reduce human error, and improve consistency. These traditional approaches have delivered measurable benefits but were built for a different era. As network environments have become more dynamic and distributed, these methods now show their limits.

Automation and orchestration

Early automation replaced repetitive manual configuration with reusable scripts and templates. Orchestration frameworks extended this concept, allowing teams to apply changes across many devices or sites simultaneously. Platforms such as Cisco DNA® Center and Meraki® Dashboard help standardize configuration and policy deployment, reducing time to service and improving compliance through consistent enforcement of security and performance policies.

However, these systems remain rule-based. They follow human-defined instructions and react to conditions that were anticipated when the workflow was created. When an unexpected event occurs, such as a new application, a sudden traffic surge, or a novel security threat, human operators must still diagnose the issue and determine the response. Automation accelerates execution but does not necessarily improve decision-making.

Intent-based networking

Intent-based networking (IBN) emerged to simplify management further. Instead of configuring individual devices, operators define the desired outcome, such as secure access for a group of users, and the system translates that intent into specific configurations. IBN represents an important step forward. It improves consistency, accelerates change control, and reduces the potential for manual error.

Yet IBN also depends on static models of policy and limited analytics. It understands what the network should do but not necessarily what it is doing at any given moment. When network conditions, user behavior, or applications change, the intent model must be manually updated. In practice, intent-based systems often become another layer of configuration that still requires expert oversight.

Advantages and disadvantages

Traditional automation and IBN have provided meaningful progress:

- **Advantages:** Consistency, speed, improved compliance, and simplified provisioning
- **Disadvantages:** Limited adaptability, high maintenance, and continued reliance on human expertise for analysis and troubleshooting

These methods address how networks execute tasks but not how they think. They automate processes but not problem-solving. As data volumes and event rates continue to grow, even the best-scripted workflows may not interpret or act on information fast enough.

The industry now stands at a turning point. The tools that once simplified operations have themselves become complex to manage. They remain valuable foundations but lack the cognitive capabilities required for real-time optimization and predictive response. This sets the stage for the next evolution: autonomous networking.

The path forward: Autonomous networks powered by AI

The evolution from automation to autonomy requires more than incremental change. It calls for a new operational foundation built on intelligence, reasoning, and collaboration between humans and AI. Cisco and Infosys each bring a distinct but complementary approach to achieving this vision, beginning with Cisco's innovation in network intelligence.

Cisco's approach: The AI Canvas and the era of AgenticOps

Cisco's approach to autonomous networking centers on a powerful new foundation: the Cisco AI Canvas (Figure 1), part of its broader vision for Agentic Operations (AgenticOps). This evolution moves beyond automation and AIOps to an environment where AI models can reason, interact with systems, and take guided action across network and security domains. It represents a shift from command execution to contextual reasoning and guided action.

The AI Canvas delivers a single, cross-domain workspace where NetOps, SecOps, and IT teams can collaborate with AI agents that learn continuously from Cisco's Deep Network Model. The result is an intelligent interface that transforms how teams troubleshoot, analyze, and automate network functions. It offers a generative, reasoning-based user experience that unifies human expertise and machine intelligence within a shared operational view.

ALPHA | OCTOBER

AI Canvas

Troubleshooting and execution across multiple domains

Collaboration across multiple users (NetOps, SecOps and execs)

Built on the foundation of the Deep Network Model

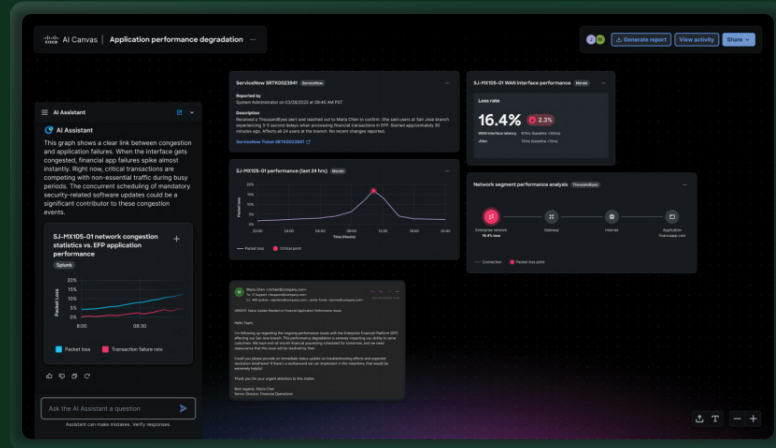


Figure 1 Cisco AI Canvas, Generative UI for cross-domain IT-a shared, intelligent workspace that brings real-time telemetry, AI insights, and team collaboration into one view.

At the heart of this innovation is the Cisco Deep Network Model, purpose-built for networking and refined over more than 40 years of Cisco expertise, telemetry, and support insights from Cisco Technical Assistance Center (TAC) and Customer Experience (CX) teams. This model evolves continuously with live data, enabling precise reasoning for troubleshooting, configuration, and optimization. It delivers domain-specific accuracy that generic large language models cannot achieve, combining Cisco's proprietary data scale with decades of protocol knowledge.

Within the AI Canvas, these capabilities come to life. Operators can ask natural-language questions such as "Is our SD-WAN having problems?" The system interprets the query through a large language model and agent architecture that calls tools like ThousandEyes®, Meraki®, or Splunk® to gather telemetry, logs, and performance metrics. The AI agent reasons on that data, identifies potential root causes, and presents actionable recommendations or executes pre-approved remediations automatically.

Unlike static dashboards or rule-based automation, the AI Canvas provides a live, collaborative environment for multi-team problem solving. Network engineers, security analysts, and business leaders can all view the same data context and insights, accelerating mean time to resolution and aligning technical actions with business priorities. This unification replaces manual investigation with guided reasoning, fragmented tools with shared intelligence, and reactive responses with predictive assurance.

Cisco's AI Canvas serves as the platform for an era of AgenticOps, where AI agents augment human expertise across the full IT lifecycle. By combining reasoning, automation, and collaboration, Cisco delivers a fundamentally new operational paradigm where networks are not only automated but intelligent, adaptive, and autonomous.

Infosys's approach: AI-First transformation through Topaz

Infosys Cloud & Infrastructure Services (CIS) is the accountable delivery and operations organization that embeds AI-First transformation into enterprise infrastructure. Within CIS, Infosys Topaz functions as the AI operating layer that powers this transformation.

The AI Operating Layer: Topaz

Topaz is not a single product, but a comprehensive enterprise AI platform and execution framework, providing cognitive models, generative AI, domain-specific agents, governance controls, and reusable accelerators. CIS deploys, governs, and continuously optimizes Topaz within client environments, ensuring that AI capabilities are embedded into network, cloud, edge, security, and service operations at scale.

In this model, Topaz provides the intelligence layer, and CIS provides the operational authority, lifecycle management, and human-AI orchestration required to translate that intelligence into measurable enterprise outcomes.



Infosys Agentic Operations Framework

While Cisco’s AgenticOps advances network-domain intelligence, Infosys Agentic Operations represents the enterprise operating model that governs how AI agents are designed, deployed, orchestrated, and continuously improved across complex hybrid estates.

At its core, Infosys Agentic Operations is built on closed-loop intelligence. AI agents monitor real-time telemetry, reason across cross-domain signals, execute within defined guardrails, and refine future decisions through feedback. This model advances traditional automation toward adaptive, continuously improving workflows.

Powered by Topaz and operationalized through CIS, Infosys Agentic Operations spans network, cloud, edge, security, data, and service management domains. It integrates human oversight, responsible AI governance, and enterprise-grade lifecycle controls to ensure autonomy remains explainable, auditable, and aligned with business objectives. This framework provides the structural foundation upon which Topaz assets, accelerators, and industry playbooks are deployed.

In this architecture, Cisco provides domain-native network intelligence, while Infosys Agentic Operations governs the enterprise-scale deployment and orchestration of that intelligence across hybrid environments.

The Infosys Human–AI Operating Model

A defining element of Infosys Agentic Operations is its Human–AI operating philosophy. Infosys views AI agents not as replacements for human expertise, but as digital co-workers designed to augment, scale, and elevate human capability.

Within this model, AI agents assume high-volume, data-intensive, and repetitive operational tasks, while human engineers focus on judgment, innovation, architecture, exception handling, and strategic decision-making. This redistribution of work shifts operational effort toward higher-value contributions.

Infosys applies measurable Human–AI operating ratios to guide transformation. As AI maturity increases, organizations move from predominantly human-led operations to blended models in which AI agents handle a growing percentage of incident detection, correlation, and remediation workflows under human supervision. The outcome is workforce evolution, with reduced operational toil and increased focus on innovation and strategic impact.

This co-working model operates within enterprise governance guardrails, including explainability, auditability, and continuous skill transformation, helping to ensure AI remains accountable and aligned with performance objectives.

Scaling the Framework: Assets, Governance, and Accelerators

Topaz embodies the Infosys principle of AI-First by Design, embedding intelligence at the core of digital operations rather than layering it on top. It provides the foundation for organizations to adopt AI responsibly, accelerate automation, and amplify human potential. With more than 80 reusable AI assets, 25 industry playbooks, and domain-specific blueprints, Topaz helps enterprises scale innovation while maintaining governance and compliance.

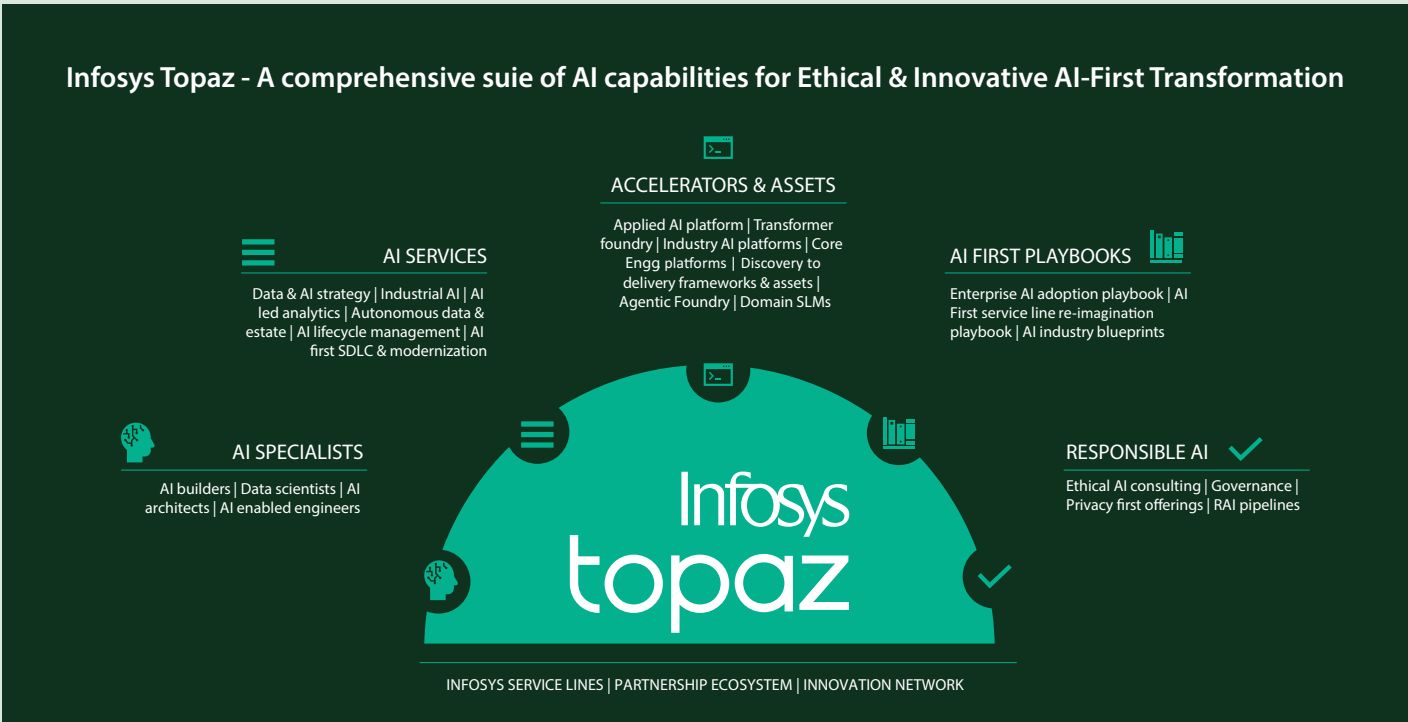


Figure 1 Cisco AI Canvas, Generative UI for cross-domain IT-a shared, intelligent workspace that brings real-time telemetry, AI insights, and team collaboration into one view.

At the heart of Topaz are three building blocks:

- **AI specialists** who integrate cognitive and generative models into client environments
- **AI services** that deliver outcomes through applied analytics, AIOps, and autonomous data management
- **AI accelerators and assets** such as the Applied AI Platform, Cognitive Automation Studio, and Agentic Foundry, which provide pre-trained models and reusable workflows to speed deployment

Topaz powers the Infosys Agentic Operations Framework, where human-in-the-loop AI agents automate decision-making across complex service chains. Predictive-maintenance models detect anomalies and trigger pre-defined remediation actions, while natural-language assistants surface insights for network and operations teams. The Agentic Foundry provides industry-specific agents and horizontal skills, including anomaly detection, Optical Character Recognition (OCR), audio processing, and code interpretation, that can be composed to automate unique workflows across sectors.

Responsible AI underpins Topaz. Infosys embeds ethical AI principles through its SCAN, SHIELD, and STEER framework, which governs model transparency, privacy, and bias mitigation. Every AI asset and workflow within Topaz complies with zero-trust security and global regulatory standards.

AI-Led Change and Governance

Beyond ethical AI principles, Infosys applies an AI-Led approach to operational governance and change management. AI-Led does not mean autonomous decision-making without oversight. Instead, it represents a structured model where AI agents participate in evaluating risk, dependency impact, policy alignment, and historical change outcomes before execution.

Within this model, Agentic Change Advisory processes augment traditional CAB (Change Advisory Board) workflows. AI agents analyze telemetry, configuration dependencies, past incident data, and compliance constraints to provide contextual risk assessments and recommended mitigation steps. Human leaders retain final accountability, while AI accelerates analysis and reduces blind spots across complex hybrid environments.

This AI-Led governance approach helps organizations move from reactive approval cycles to proactive, intelligence-informed change orchestration, supporting faster execution while maintaining enterprise-grade control, transparency, and auditability.

Incremental Transformation: Micro Changes for Mega Outcomes

Infosys also applies a “Micro Changes for Mega Outcomes” philosophy, aligning transformation with agile sprints. Incremental improvements guided by behavioral-change frameworks and human-AI collaboration build organizational confidence and accelerate adoption.

Together, these governance and change mechanisms reinforce the scalability of the Topaz platform. In practice, Topaz unifies data, automates insight generation, and scales innovation across the full technology stack. It transforms traditional AIOps and automation programs into AI-driven ecosystems capable of continuous optimization and contextual response. Integrated with Cisco's AI Canvas, Topaz helps to ensure that network intelligence flows through business operations, linking infrastructure performance to measurable business value.



Cisco and Infosys: Accelerating the era of agentic operations

Cisco contributes deep domain intelligence and trusted telemetry through its AI-native platforms. Infosys, through its Cloud & Infrastructure Services organization and Topaz AI-First framework, assumes responsibility for transforming that intelligence into autonomous operations across the enterprise.

Infosys leads the orchestration, lifecycle governance, and continuous evolution of agentic workflows across hybrid infrastructure environments. By integrating Cisco's network intelligence with cloud, edge, security, and business service operations, Infosys establishes a unified AI-driven operating model where networks function as a managed and continuously optimized domain within a broader autonomous enterprise fabric.

Together, they establish an ecosystem for Agentic Operations — where Cisco powers domain intelligence and Infosys delivers and governs the AI-First operational framework at scale.

The partnership bridges the divide between network data and business outcomes. Cisco's network-level insights integrate with Infosys's AI frameworks, where contextual reasoning links infrastructure performance to customer experience, financial efficiency, and sustainability. This integration helps organizations detect and resolve issues faster, improve service predictability, and optimize resources across the digital stack. Network, security, and operations teams operate from a shared intelligence layer that adapts to change.

Through joint architectures, Cisco platforms such as Meraki, ThousandEyes, and Cisco Intersight® interoperate seamlessly with Infosys automation and analytics solutions. This integration reduces deployment risk, shortens time to value, and provides a clear path toward AI maturity.

The collaboration grounds every step in responsible use of AI without re-creating governance overhead. Cisco focuses on data security, privacy, and transparency within the AI Canvas environment, and Infosys provides enterprise-grade guardrails and monitoring. Together, recommendations and automated actions operate within enterprise governance and compliance frameworks.

Enterprises adopting the Cisco–Infosys solution can expect measurable benefits such as faster mean time to resolution, improved security posture, optimized performance, and lower operational cost. Most importantly, they gain the agility to innovate confidently, knowing that their digital infrastructure can learn, adapt, and scale with them.

Cisco and Infosys are not simply integrating platforms. They are redefining how intelligence flows across the enterprise. By combining Cisco's network insight with Infosys's operational execution, they create a connected intelligence fabric that turns data into action and automation into autonomy.

Predictive Network Assurance

AI that sees, reasons, and resolves issues before users notice.

Cisco AI Canvas continuously interprets live telemetry from switches, routers, and applications to detect emerging anomalies. Integrated with Infosys Topaz, those insights trigger agentic workflows that diagnose root causes and execute pre-approved remediations, often without human intervention. The result is a self-healing network that predicts incidents, tunes performance in real time, and frees engineers to focus on innovation instead of firefighting.

Autonomous Cloud Edge Provisioning

Networks that deploy, secure, and optimize themselves.

When a new branch or edge site comes online, Cisco AI Canvas defines intent and validates policy compliance across domains, while Infosys Topaz automates the infrastructure build using pre-trained AI models and reusable playbooks. AI agents configure SD-WAN, enforce zero-trust security, and balance workloads across hybrid clouds. The outcome: self-provisioning, self-optimizing edge networks that scale instantly with business demand.

Conclusion

Choose autonomous networks with Cisco and Infosys

Cisco's AI Canvas and Infosys Topaz — delivered and governed through Infosys Cloud & Infrastructure Services (CIS) — provide an AI-First foundation that connects deep network insight with enterprise-wide operational execution.

Through CIS, Infosys serves as the accountable enterprise delivery and operations partner for AI-First infrastructure and autonomous network management. Infosys designs the operating model, embeds responsible AI governance, manages AI agent lifecycles, and continuously optimizes cross-domain workflows to ensure that network intelligence translates into sustained business value.

This combined approach turns data into actionable intelligence, enabling systems to anticipate issues and act with contextual awareness. By bringing together Cisco's domain expertise and Infosys CIS' leadership in responsible AI and scalability, enterprises gain a trusted path to resilient, self-managing digital infrastructure that enhances agility, efficiency, and continuous innovation.

Take the next step toward autonomous networking

Modernize how your organization manages and secures its digital infrastructure. Cisco and Infosys can help you transition from rule-based automation to intelligent, self-managing networks that continuously learn, reason, and adapt.

Learn more:

- CISCO AI canvas - [AI Canvas - Cisco](#)
- Infosys Topaz - [Infosys Topaz: An AI-first offering to accelerate business value](#)
- For solution guidance or to request a joint Cisco and Infosys assessment, contact the Cisco account team at CISNetwork_Communication@infosys.com.

For more information, contact askus@infosys.com



© 2026 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.