Financial services in the age of AI:

The network built for millisecond-level performance

Analysis of findings from financial services respondents in
“No time to wait: The accelerating impact of AI on campus and branch networks”

Introduction

AI is reshaping financial services, from customer engagement and fraud detection to operations, compliance, and decision-making. In campus and branch environments, this creates new traffic types, new attack vectors, and new demands on performance, bandwidth, and resilience.

For financial services firms, the challenge is immediate. A new Cisco survey of more than 3400 senior IT and network leaders (513 in the financial services sector) shows that financial services firms recognize the operational and business risk. The research found that 78% of financial services respondents are more confident in their AI strategy than in their network's ability to support it. At the same time, 47% of respondents are already upgrading their networks to stay ahead of the competition, the third highest rate across all industries surveyed.

So how can financial institutions bridge the gap between ambition and execution?

The network is now a business risk issue

In financial services, downtime isn't just an IT issue. It can quickly become a customer experience problem, a compliance issue, and a reputational risk. That pressure is growing as AI expands.

Unlike legacy applications, AI workloads are often highly interdependent; a minor network hiccup doesn't just slow one process—it can trigger a cascade of failures across automated decision-making and real-time fraud detection systems.

When these systems falter, the impact is immediately visible to the end user, whether through a delayed transaction, a failed authentication, or an inaccurate AI-driven recommendation. In an era where customers demand instant, personalized service, any friction in the underlying network directly undermines the brand promise and erodes long-term loyalty.

75% of financial services respondents say failure to support AI-capable networks could compromise their ability to meet customer expectations.

For companies competing in the arena of digital responsiveness, secure service delivery, and personalized customer experiences, the AI readiness of campus and branch networks is now a core business requirement.

Strategic takeaway

Prioritize campus and branch modernization as a business initiative, not just a refresh cycle. Evaluate which environments are tied to revenue, service, and compliance. Identify where transaction reliability is most critical and where compliance exposure is most at risk.

AI traffic is pushing infrastructure harder

Generative AI is shifting traffic patterns from predictable requests to bursty interactions that demand significant bandwidth. Agentic AI introduces even greater complexity. These agents initiate frequent, high-velocity, machine-to-machine communications that require consistent, low-latency paths across distributed campus and branch environments to function without interruption.

In the survey, 42% of financial services respondents cite increased latency sensitivity for AI workloads as a major network challenge. Real-time fraud detection, algorithmic trading, and instant payments are central to modern financial services. Because they rely on millisecond-level performance, even minor network variability can erode customer trust and trigger compliance failures.

"Networks have evolved from a cost center to an innovation platform. Due to new demands from AI, we are now thinking more deeply about how to modernize and make the network platform more capable to offer the capabilities business is asking for. It has become more of an innovation platform now, and we are investing more."
—Senior director of enterprise networks in the financial services industry, APAC

As AI inference moves closer to the point of transaction, tolerance for network variability approaches zero.

Strategic takeaway

IT leaders in the financial services sector should start planning for AI-specific traffic behavior now. Start by identifying workflows where latency directly affects customer experience, fraud response, or transaction speed. Map where AI-driven traffic spikes are most likely to stress branch, campus, or WAN capacity. Then, prioritize sites where AI demand, compliance exposure, and user impact intersect.

A phased strategy that improves visibility, performance, segmentation, and resilience in priority environments can deliver near-term gains as financial institutions build a controlled modernization path.

AI is expanding the attack surface

Firms are fast-tracking AI adoption, which means security is rapidly becoming more complex. In fact, 79% of financial services respondents say AI has expanded their network attack surface, and 81% believe security risks will increase as AI moves beyond generative use cases." Agentic AI introduces a category of risk that current network security architectures are not equipped to manage. It operates with a level of autonomy that traditional perimeter-based security cannot detect, creating new opportunities for unauthorized lateral movement and API exploitation.

For financial institutions operating under frameworks like DORA, Basel IV, and an expanding net of global AI regulation, the implications are as much about compliance as they are about security. As AI systems evolve, firms must demonstrate not only that their networks are secure, but that their AI-driven processes remain transparent, resilient, and fully compliant with evolving data-sovereignty requirements.

87% of financial services respondents have already implemented additional security controls for AI workloads.

For firms operating under strict regulatory scrutiny, security architecture must go beyond protection to deliver consistency, visibility, and policy enforcement across distributed environments.

Strategic takeaway

Start by evaluating whether current network and security tools are equipped for AI-generated traffic patterns. AI workloads often rely heavily on token-based authentication, API exchanges, and autonomous interactions—these are harder for conventional security tools to interpret.

IT leaders in the financial services sector should focus on embedding security closer to the edge; enforcing consistent policy across branch, campus, and cloud; and reducing silos between networking and security operations. Make it a priority to create a simpler, more unified security posture that can scale as AI usage expands.

The time is now

If an AI-readiness gap persists, financial institutions could be in for higher remediation costs, delayed initiatives, inconsistent customer experiences, and avoidable business risk.

The data suggests delay is more expensive than action:

76% of respondents agree that delaying network modernization could lead to higher long-term costs through reactive upgrades and remediation.

67% say network infrastructure could limit their ability to fully capitalize on AI innovation.

The goal is to avoid the cost and disruption of reactive upgrades while improving the network's ability to support growth. By doing so, CIOs and IT leaders will put themselves in a better position to support the business with confidence as AI expectations continue to rise.

While the urgency is clear, the path forward doesn't require a "rip-and-replace" strategy. Instead, it requires a phased modernization that targets the most critical bottlenecks first. For financial services companies, this challenge is more complex, regulated, and consequential than in any other sector.

There's no time to wait.

See how Cisco AI-ready secure network architecture is built to help financial services firms thrive in the AI era.

Explore Cisco solutions

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**