INFOGRAPHIC

The State of Networking, Security & AI in Financial Services

Insights from 322 **IT leaders, risk leaders, and C-level executives** across banking, insurance, payments, capital markets, and fintech.

THE BIG PICTURE

Financial networks are being asked to deliver more, without adding risk, cost, or complexity.

57.1% experience disruption affecting customers, trading, or digital banking monthly or more often.

79.5% cannot automatically detect and quarantine breaches in real time.

72.4% are open to considering a secure Network-as-a-Service model.

The issue is not a lack of awareness or intent. It is the difficulty of turning enforcing both across a distributed, third-party-connected estate.

THE PRESSURE: COST AND RISK HAVE CONVERGED

Security and economics are now the same network conversation.

24.2% cybersecurity threats and regulatory risk

22.4% rising operational costs

Security, cost, staffing, performance, and complexity are tightly balanced. Point fixes won't solve the broader operating problem.

When given a clean slate, respondents prioritize:

25.2% lower total cost of ownership

24.2% stronger built-in security, Zero Trust, and isolation

20.8% simplified operations and automation

Cost, built-in security, and simplification account for 70.2% of redesign priorities.

THE SECURITY SEAM PROBLEM

Most institutions are advanced somewhere - and exposed somewhere else.

21.1% have fully segmented third parties with enforced policy controls.

20.5% have automated detection and real-time quarantine.

21.4% have continuous real-time visibility across the estate.

18.6% have Zero Trust that is fully aligned and enforced.

18.9% have automated audit reporting and policy enforcement.

Only **1.9%** report the advanced state on five or more of seven measured capabilities.

Detection, visibility, or segmentation alone still leave gaps for lateral movement, disruption, and audit exposure.

WHERE THE SEAMS SHOW UP

Containment gap

Detection is not the same as stopping the incident.

- **44.4%** require manual quarantine or have delayed detection and manual remediation.
- Manual response moves at human speed; attacks move at machine speed.

Implication: Move enforcement and isolation into the network accelerating containment.

Third-party exposure

The soft edge is outside the traditional perimeter.

- **78.9%** do not report enforced segmentation between third parties and core systems.
- **46.6%** find secure, isolated guest or partner access difficult or very difficult.

Implication: Make guest, contractor, and partner access the first segment to enforce.

Visibility and compliance

You cannot enforce what you cannot see.

- **78.6%** lack continuous real-time visibility across connected devices, users, and things.
- **59.3%** carry a moderate to significant manual burden to maintain audit readiness.

Implication: Establish a continuous view of assets, traffic, posture, and policy before adding tools.

THE OPERATING IMPACT PANEL

The binding constraint is the operating model - not just headcount.

28.3% are understaffed and stretched thin.

23.9% are fully staffed but constantly firefighting.

47.8% of fully staffed teams still report constant firefighting.

Hiring alone won't overcome complexity. Simplification, automation, and consolidation create real capacity.

THE CONVERSATION IS SHIFTING

The sector is moving from interest to action - but adoption must be governed.

AI in network operations and security

46.6% are already deploying AI or planning to within 12–18 months.

66.8% are engaged when those exploring AI are included.

The conversation has shifted from whether to use AI to how to govern, explain, and audit it.

Secure Network-as-a-Service

39.1% would consider adopting a secure NaaS model.

33.2% want to learn more.

27.6% would not consider it.

Trust, control, data sovereignty, integration, and accountability must be addressed with evidence.

WHAT LEADERS SHOULD DO NEXT

Close the seams before adding more layers.

01 **Establish visibility first**
Create a continuous, unified view of every connected device, user, partner, and traffic path.

02 **Enforce containment and segmentation**
Prioritize automated quarantine and third-party isolation from core systems.

03 **Simplify the operating model**
Replace manual configuration, fragmented tooling, with policy-driven automation.

04 **Modernize with proof**
Evaluate AI and secure NaaS through clear governance, breach simulation, and measurable operational outcomes.

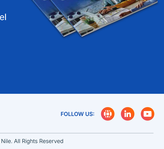
Final takeaway

Modernization isn't another isolated control - it's an architecture aligning security, compliance, reliability, and cost

These insights are not isolated, they represent a fundamental shift in financial services networking. Get your copy of the Leadership Survey Report to explore the full analysis.

The State of Networking, Security & AI in Financial Services

Insights from IT leaders and C-level executives in Financial Services



Download report

FOLLOW US: