Complete Guide to **Ethernet Services**

Powered by

summit BROADBAND

Powered by ciena

Security Is Driving Network Enhancements

New security strategies are driving network enhancements and upgrades to legacy architectures.

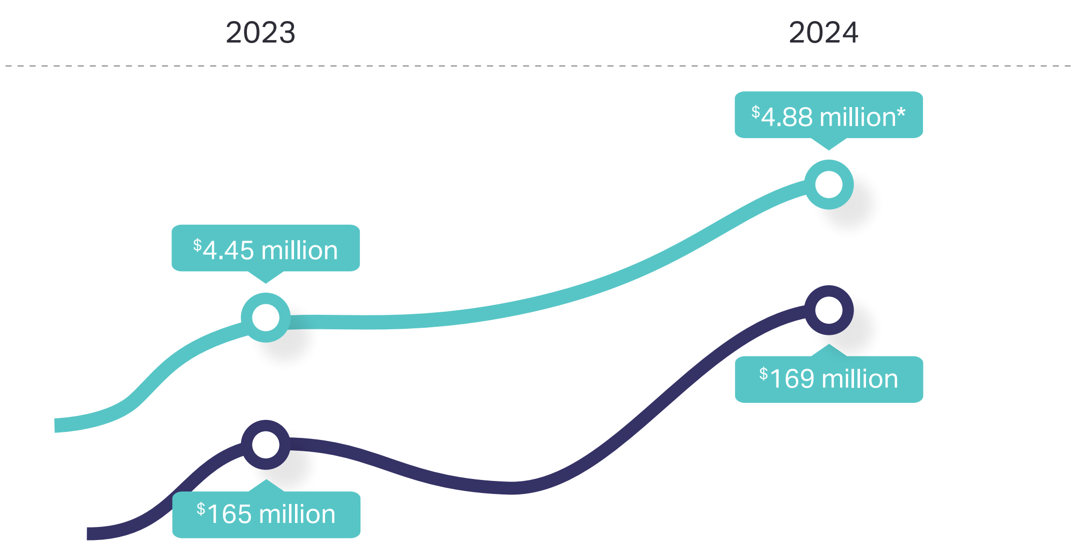
Why Now?

Risks and vulnerabilities are only getting worse, which is driving the convergence of network and security — and why network planners must take a proactive look at their network strategy.

○ Average Data Breach Cost[1]

● Cost Per Breached Record[2]

*$6.08 million for financial institutions[1]



Why Is Security Changing?

35% of breaches involved shadow data[1]

$5.17 M cost of data breaches solely involving public clouds[1]

11% rise in cost for lost business and post-breach response over the previous year[1]

16% compromised credentials[1]

$1.88 Million

average breach cost savings for organizations using AI and automation[1]

Secure Service Edge (SSE) Is **The New Normal**

Zero Trust Network Access (ZTNA)

Cloud Access Security Broker (CASB)

Secure Web Gateway (SWG)

Disproportionate **Impact** on Financial Services

2nd
Financial services is second only to healthcare for average breach cost.

$6.08 million
Average cost of a data breach in 2024 for financial services.[1]

258 Days
The mean time it takes defenders to identify and contain a breach.[4]

46%
Nearly half of all breaches involved customer personal identifiable information (PII).[1]

How Does Network Technology Affect **Security Posture and SSE?**

Choosing network technology (Ethernet, waves, dark fiber) that reduces east-west data paths in network can help limit scope of breaches versus mesh architectures and internet.

Software-based orchestration offers more control over Zero-Trust, containment and analytics without sacrificing performance.

Device-based architectures are increasingly targeted for vulnerabilities in hardware.

Increasing number and complexity of applications and cloud services requires underlying connections, especially to branch offices, to be robust.

summit BROADBAND.

Powered by
ciena

summitbb.com

summit BROADBAND

Powered by ciena

Finserv and the 5 Network Killers

Today's financial services (finserv) institutions are **juggling numerous digital demands** — from managing a hybrid workforce to an ever-increasing demand for digital apps.

We see **5 main trends** driving new finance sector network strategies.

1 The Shift to Hybrid Work

As hybrid work redefines workplace dynamics, corporate networks face mounting challenges. Many organizations are finding their networks struggling to keep pace with the high-speed residential internet connections employees have become accustomed to while working remotely. When hybrid employees converge on peak in-office days, network demands spike, leading to degraded performance or reliance on overbuilt architectures to handle the load. To address these challenges, businesses are exploring bandwidth-on-demand models and adaptive architecture.

2 Digital App Explosion

Evolutions in technology for financial services (fintech) continue to drive performance needs across multiple financial sectors. For instance, banking customers are accustomed to fully digital banking and payment players like Zelle, Chime or Venmo. The digital wallet industry alone is expected rise from $9 trillion in 2023 to $16 trillion in 2028, a growth of 77%.[3]

Consumer expectations for digital, mobile and self-service options coupled with security and reliability demands are pushing higher performance network options into the core strategy of financial institutions. The explosion of latency-sensitive middle and back office applications, now more than ever hosted in the cloud, compound the bandwidth-thirsty financial industry's network needs. Both leaders and laggards in finserv are being driven to consider core network upgrades to support wider and deeper app deployments.

3 Multi-Cloud Architectures and Cloud On-Ramps

Public, private and hybrid multi-cloud have become the de facto standard for balancing cost with finserv requirements for reliability, security, performance and scalability. As such, cloud on-ramps for mission critical services are becoming an integral piece of both application performance and cloud-based security as more applications are either cloud-enabled or fully hosted in multi-cloud environments.

Traditional mesh architectures, designed for legacy branch-to-branch connectivity, often have a bottleneck accessing cloud services, degrading the original performance of these architectures. Cloud direct connects or on-ramps coupled with SD-WAN over DIA and Ethernet could be an easy way to catch up to demand while future-proofing your architecture.

4 Cybersecurity and SASE

Cybersecurity is consistently among the largest concerns for CIOs and CISOs regardless of industry, but typically tops the list for finserv. SASE, and more specifically SSE which includes zero trust architecture (ZTA), is quickly becoming the new table stakes for security. With Executive Order 14208 mandating many of the SSE tenets for federal agencies, more regulations mandating similar measures for finserv are expected in short order.

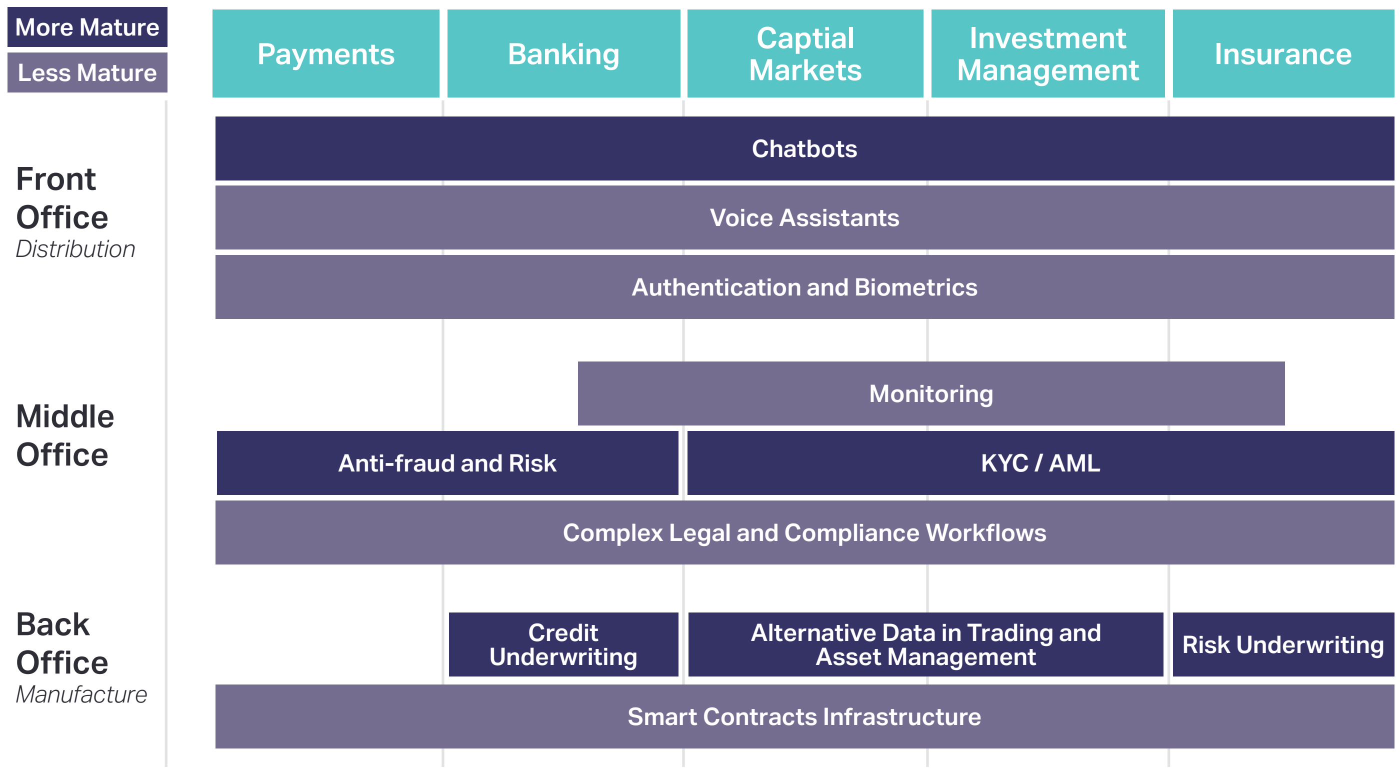
Regulatory mandates aside, the business impact of breaches for enterprises and customers are massive in the finserv segment. Coupling Layer 2 security features in an updated network with Virtual Firewall seems an obvious move given the increasing global threat vectors and growing attack surfaces.

5 Evolving Tech Demands Modern Infrastructure

Evolving technologies like AI are driving ever-increasing network demands. AI, now a cornerstone of financial services, is continually expanding its role — from enhancing risk management and credit underwriting to bolstering anti-fraud measures and optimizing customer interactions through advanced chatbots and IVR systems. These advancements, paired with sophisticated trading models, push the limits of existing infrastructures.

Moreover, new technologies are enabling additional finserv products and services like real-time payments, automated compliance and API-based regulatory integrations, but only for those with the underlying infrastructure to support those loads. We expect to see escalating clashes between legacy banking/trading institutions and new digital-first competitors for market share which will drive laggards toward network enhancements.

Fintech AI Use-cases



Source: Autonomous NEXT Report on Augmented Finance and Machine Intelligence

As finserv contemplates these evolving factors in its market segment, the leaders are already driving network demand for competitive advantages today and future-proofing for tomorrow. China is ahead of the game on the global stage leaving a competitive gap the United States is playing catch up to fill. Slow adopters will see the leaders prove out the technology strategies but will miss out on the gains, and the laggards or late adopters may get left behind as digital-first and tech-heavy players start to dominate the space.

Where do you fit in this spectrum? If you need to benchmark your network against other finserv enterprises, connect with our evaluation team.

[1] IBM, http://www.ibm.com/reports/data-breach
[2] Statista, http://www.statista.com/statistics/799396/worldwide-cost-effects-data-record-breaches/#:~:text=As%20of%20 2024%2C%20the%20average,was%204.88%20million%20U.S.%20dollars.
[3] Payments Cards & Mobile,http://www.paymentscardsandmobile.com/digital-wallets-transaction-value-to-surpass-16-trillion-globally/?utm_source=chatgpt.com
[4] IBM, http://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec