A10

AI-ready Hybrid Cloud

eBook

Future-proofing Financial Services in an AI-Driven, Hybrid Cloud World

TABLE OF CONTENTS

Introduction

In today's dynamic financial landscape, institutions are navigating a minefield of digital demands, regulatory pressures, and operational complexity. Hybrid cloud adoption, open banking APIs, and AI innovation promise transformation, but also introduce sprawling infrastructure, technical debt, and fragmented security. As financial organizations evolve, they inherit legacy systems and disconnected tools that hinder agility and visibility.

This eBook from A10 Networks explores how financial institutions must tackle infrastructure complexity, tool sprawl, and AI integration. It outlines how A10 can help to secure hybrid cloud environments and boost operational performance and control. It also looks at how decision makers can reduce risk as they modernize legacy systems, and build resilient, high-performance services in an increasingly complex financial ecosystem.

Financial institutions inherit legacy systems and disconnected tools that hinder agility and visibility

As AI adoption continues to grow, many institutions lack the infrastructure to support its demands.

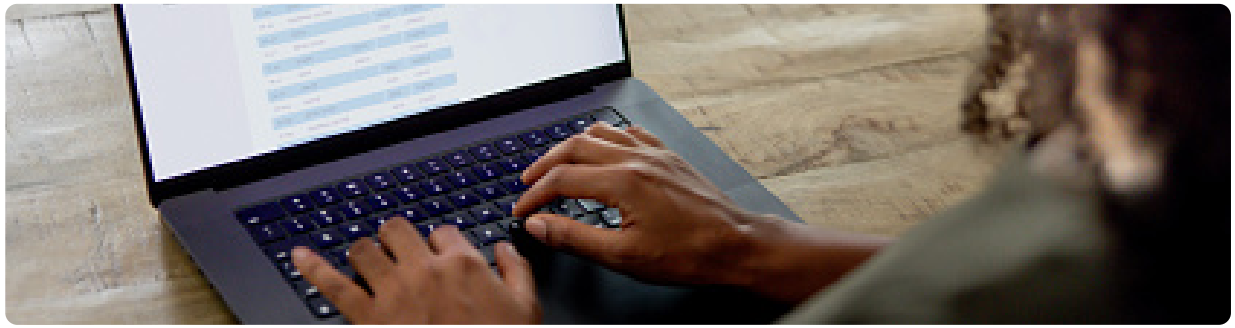
How a Black Swan Event Reshaped Banking and Exposed Infrastructure Risk

Over the past five years, banking systems have undergone a profound transformation, shaped by rapid technological advancement, shifting customer expectations, and disruptive global events.

The COVID-19 pandemic was a true black swan moment, accelerating the decline of bricks-and-mortar banking and propelling customers almost overnight toward digital channels and services offered by challenger banks. Mobile banking apps, online platforms, and contactless payments quickly became the norm, fundamentally reshaping how people interact with financial institutions.

In response, fintech innovation surged. Platforms like PayPal, Zelle, and Venmo entered the mainstream, prompting banks to expand their digital offerings and enhance mobile capabilities. Artificial intelligence and machine learning gained traction, powering fraud detection, customer service chatbots, and personalized financial insights. Customer service evolved into a 24/7 experience, often supported by AI-powered tools.

Meanwhile, rising cyber threats and stricter data privacy regulations forced institutions to rethink their security and compliance strategies.



Fast forward to 2025, and financial institutions operate in a high-stakes environment where delivering secure, high-performance digital experiences is no longer optional, it's a strategic imperative.

With the rise of hybrid cloud architecture, open banking APIs, and AI-driven services — alongside global regulatory frameworks like PCI DSS and PSD2 — banks face enormous operational and technological complexity.

Beneath the surface of digital transformation lies a growing burden: inherited technical debt and sprawling infrastructure that threatens agility, visibility, and security. As AI adoption continues to grow, many institutions lack the infrastructure to support its demands. Security, performance, scalability, and visibility remain major obstacles to effective AI deployment.

Additionally, corporate expansion — primarily through mergers and acquisitions — has had an effect. After the deals have closed, financial organizations often inherit a patchwork of legacy systems, siloed IT departments and data, disconnected tools, and fragmented cloud estates. This leads to inevitable cloud and tool sprawl, creating operational drag and complicating modernization efforts. Most institutions now operate with assets spread across multiple cloud providers and on-premises systems.

Managing this sprawl is a technical minefield. Institutions must find ways to consolidate, streamline, and secure their infrastructure to remain competitive, resilient, and trusted in an increasingly complex financial landscape.

Financial organizations often inherit a patchwork of legacy systems, which inevitably complicates modernization efforts.

Hybrid Complexity and Technical Debt: The Hidden Cost of Digital Transformation

Like APIs, bot attacks have been around for a long time and are becoming more sophisticated.

Today, financial institutions rarely operate within a single cloud, nor do they maintain a fully on-premises infrastructure. According to the LSEG Global Cloud Survey (2025), 82 percent of financial services firms now operate with either a hybrid or multi-cloud strategy.

Furthermore, in A10's recent survey, The State of AI Infrastructure Report 2025, 42 percent of enterprises said hybrid cloud is their preferred model for AI workloads, balancing scalability with control.

While hybrid cloud may have become the norm, with it comes a tangled web of complexity. IT teams manage sprawling IT estates that span multiple public cloud providers — often five or more — alongside private clouds and deeply entrenched legacy systems. This fragmented architecture is frequently less about deliberate choice, and more the result of mergers, acquisitions, and years of incremental technology investments, each adding another layer of tools, platforms, and processes.

The result is a lack of visibility, control, and orchestration across environments. IT teams struggle to monitor performance, enforce consistent security policies, and respond quickly to incidents. Legacy systems, while still mission-critical, often lack the flexibility and scalability needed to support modern workloads, especially those driven by AI and real-time analytics. This patchwork of infrastructure hinders operations and contributes to mounting technical debt and hidden inefficiencies that slow innovation and increase risk.

AI Everywhere, Security a Barrier: From Cloud to On-premises

Financial institutions are now adopting artificial intelligence as an essential part of their operations. No longer a peripheral tool, AI is central to how banks deliver services, build applications, and maintain competitive advantage.

From fraud detection and customer service to back-office automation and regulatory compliance, AI is transforming the financial services landscape. Its integration is particularly impactful in hybrid cloud environments, where agility and scalability are essential.

The State of AI Infrastructure report underscores this shift. An impressive 76 percent of enterprise organizations are already using generative AI applications, signaling widespread adoption. However, the study also reveals a critical gap where infrastructure is struggling to keep pace. While 79 percent of organizations plan to modernize their infrastructure within the next 18 months, only 19 percent have automated scaling in place to support AI workloads.

This disconnect highlights the urgency for financial institutions to align their infrastructure with their AI ambitions. In the financial sector specifically, the research highlighted that 71 percent of firms are leveraging AI for predictive analytics, a clear reflection of the industry's focus on data-driven decision-making and proactive risk management.

Yet, integrating these advanced technologies into environments burdened by technical debt remains a formidable challenge. Among the many hurdles reported by the IT and networking professionals surveyed, security emerged as the most significant constraint and biggest concern.

This was especially true of data leakage, with ‘the potential for AI to access sensitive systems or data’ and the ‘inability of current security tools to understand AI traffic patterns emerging as common responses cited by participants. Nearly half (49%) say security is the primary barrier preventing their infrastructure from fully supporting AI workloads.

76%

of enterprise organizations are already using generative AI applications, signaling widespread adoption

79%

of organizations plan to modernize their infrastructure within the next 18 months, but only

19%

have automated scaling in place to support AI workloads

Most legacy systems were never designed to support the scale, speed, and exposure of today's digital services.

SOC-centric Security: A Smarter Approach to Threat Defense

CISOs and security teams are equipped with an overwhelming array of disconnected tools, each designed to solve a narrow problem but collectively contributing to confusion, inefficiency, and dangerous blind spots.

These tools often operate in silos, lacking interoperability and centralized oversight, making it nearly impossible to build a cohesive, attacker-centric defense strategy. As cyber criminals and nation-state actors grow more sophisticated, exploiting gaps in visibility and coordination, security teams are left reacting to threats rather than proactively neutralizing them.

The issue isn't a lack of investment or focus; many organizations have poured significant resources into cybersecurity. The problem lies in the inability to correlate data and orchestrate responses across fragmented systems. Many institutions remain unaware of the depth of their technical debt, which undermines their security posture and operational agility. This debt manifests in outdated infrastructure, redundant tools, and inconsistent policies that hinder threat detection and response.

These challenges are especially acute when securing modern web applications and APIs, which are increasingly complex, distributed, and performance-sensitive. Most legacy systems were never designed to support the scale, speed, and exposure of today's digital services. APIs, in particular, have become the connective tissue of digital ecosystems, serving as interfaces to data and services — and increasingly as the primary interface to access AI solutions.

As organizations embed AI into customer-facing applications, APIs become the critical conduit through which models are accessed, integrated, and exploited.

This makes them a high-value target for attackers. As a result, when visibility gaps widen, compute limitations become more pronounced, and the absence of mature monitoring and governance frameworks leaves institutions vulnerable. Without unified control and intelligent automation, these weaknesses are amplified rather than resolved.

In this environment, a security operations center (SOC)-centric approach offers a critical shift from reactive defense to proactive threat management. By centralising telemetry, behavioral analytics, and incident response within a unified operational framework, SOC-driven security enables teams to correlate data across silos, detect patterns of malicious activity, and respond with speed and precision. This integrated visibility is essential for defending web applications and APIs against evolving threats — especially those that serve as AI interfaces — and for maintaining resilience in the face of constant change.

A security operations center (SOC)-centric approach offers a critical shift from reactive defense to proactive threat management.

Financial services organizations must 'control the controls' they can

Why Low Latency, Uptime and Performance Matter in Trading

In high-frequency trading environments where algorithms execute thousands of trades in fractions of a second, latency isn't just a technical metric, it's a financial liability.

Microseconds matter and can determine whether a trade is profitable or a missed opportunity, making speed and precision critical. Institutions operating in this space require full control over performance-critical assets, from network infrastructure to application delivery, to ensure consistent, low-latency execution.

However, the rise of cloud-based resources introduces a layer of unpredictability. While cloud platforms offer scalability and flexibility, they also come with variable latency, shared infrastructure, and limited transparency into underlying systems.

For financial institutions this lack of control can translate into financial and operational risk. The challenge becomes how to maintain deterministic performance in an environment built for elasticity, not precision. To mitigate this, organizations must "control the controls" they can.

Additionally, visibility is paramount. Real-time telemetry, centralized monitoring, and automated policy enforcement help eliminate blind spots and ensure consistent performance across cloud and on-premises assets. Institutions must also invest in infrastructure that supports edge computing and localized decision-making, reducing reliance on distant data centers and minimizing round-trip delays.

Ultimately, reducing risk in high-frequency trading isn't about eliminating the cloud, it's about architecting around its limitations. With the right tools and strategies, financial institutions can maintain the speed, control, and reliability needed to compete in one of the most demanding digital arenas.

Empowering Financial Institutions with Resilient, Scalable, and Secure Infrastructure Solutions

A10 Networks can help financial institutions by:

- **Simplifying hybrid environments:** A10 solutions help financial institutions streamline complex hybrid cloud and on-premises infrastructures, reducing operational overhead and improving manageability.
- **Controlling data flows with precision:** Intelligent traffic management enables granular control over data movement across environments, ensuring consistent performance and reducing latency in mission-critical applications.
- **Ensuring high availability and performance:** Advanced load balancing and traffic optimization maintain uptime and responsiveness, even under peak demand or in latency-sensitive trading scenarios.
- **Securing data without sacrificing speed:** Built-in encryption and decryption services protect sensitive financial data while preserving throughput and scalability across distributed systems.
- **Reducing technical debt and boosting agility:** Consolidating legacy systems and automating traffic workflows allows institutions to deploy new services faster and respond more effectively to market and regulatory changes.
- **Strengthening threat detection and response:** A10's SOC-driven approach with integrated security analytics and automated mitigation tools provide deep visibility into attacker behavior, enabling faster, more confident responses to emerging cyber threats.

A10 Networks has delivered scalable and secure applications for Travelex, reducing downtime and operational costs. A10 has also deployed its Thunder ADC solution within a global investment firm, ensuring high availability and reliable performance for its mission-critical trading and investment applications.

Travelex

Global Investment Firm

Mastering hybrid cloud complexity and tackling technical debt, while harnessing AI, is no longer optional, it's critical for banking operations.

Next Steps

Today, mastering hybrid cloud complexity and tackling technical debt is no longer optional, it's critical for any bank or financial services operation.

Institutions must adopt integrated solutions that streamline infrastructure, reduce legacy burdens, and enable secure, scalable service delivery. Whether modernizing core systems or enhancing digital agility, the ability to simplify operations while maintaining resilience is essential for long-term success in a rapidly evolving financial landscape.

As AI, cloud technology, and rising customer expectations continue to reshape banking, institutions with secure, agile infrastructure will be best positioned to innovate, build trust, and lead in a digital-first world. To fully harness AI's potential, financial organizations must modernize their systems, consolidating fragmented tools, eliminating inefficiencies, and adopting solutions that deliver end-to-end visibility and control.

This transformation enables a shift from reactive defense to proactive resilience, empowering banks to protect data, deliver personalized experiences, and thrive in a fast-moving financial landscape where adaptability, intelligence, and customer-centricity define long-term success.

To understand more about A10 Networks comprehensive application delivery, integrated security, traffic management, and cloud optimization solutions please click here.

Appendix

Data Privacy and Cybersecurity Regulations: Affecting UK and USA Financial Institutions

Regulation	Country	Description
UK GDPR	UK	The UK's version of the General Data Protection Regulation, retained post-Brexit. It governs how personal data is collected, processed, and stored, with strict requirements around consent, data subject rights, and breach notification.
NIS2 Directive	UK (EU origin)	A European directive aimed at improving cybersecurity across essential and digital services. In the UK, it influences operators of essential services (OES) and digital service providers (DSPs), requiring incident reporting and risk management.
PSD2 (Revised Payment Services Directive)	UK (EU origin)	Promotes innovation and competition in payments. Mandates strong customer authentication (SCA) and secure APIs for third-party access to banking data.
DORA (Digital Operational Resilience Act)	UK (EU origin)	Focuses on financial institutions' ability to withstand and recover from ICT-related disruptions. It mandates risk assessments, incident reporting, and third-party oversight. While EU-based, UK firms operating in Europe may need to comply.
PECR (Privacy and Electronic Communications Regulations)	UK	Complements UK GDPR by regulating electronic marketing, cookies, and communications privacy. Recently updated under the Data Use and Access Act 2025.
PCI DSS (Payment Card Industry Data Security Standard)	UK & USA	A global standard for organizations handling cardholder data. It sets technical and operational requirements to protect payment data, including encryption, access control, and regular testing.
US State Privacy Laws - CCPA, CPRA	USA	State-level laws like California's CCPA and CPRA regulate how businesses collect, use, and share personal data. They grant rights to consumers and impose obligations on businesses, including opt-out mechanisms and data access requests.
GLBA (Gramm-Leach-Bliley Act)	USA	Requires financial institutions to explain their data-sharing practices and protect sensitive consumer information. It includes the Safeguards Rule, which mandates security plans to protect customer data.
NIST Cybersecurity Framework	USA	Voluntary but widely adopted framework for managing cybersecurity risk. Used by financial institutions to align with regulatory expectations and industry best practices.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides security and infrastructure solutions for on-premises, hybrid cloud, and edge-cloud environments. Our 7000+ customers span global large enterprises and communications, cloud and web service providers who must provide business-critical applications and networks that are secure, available, and efficient.

Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit **A10Networks.com** and follow us **@A10Networks**.

Learn More

About A10 Networks

Contact Us

A10Networks.com/contact

Part Number: A10-EB-14179-EN-01 December 2025