CLOUDFLARE

EBOOK

Beyond single points of failure

A financial services playbook for simplifying regulatory resilience

Table of contents

A financial services resilience paradox

Financial services institutions (FSIs), historically early technology adopters, face a paradoxical path to modernization. While they have quickly embraced advancements from the cloud to AI, expanded digital footprints also inadvertently threaten operational resilience.

For instance:

- **Cloud/network migrations:** Aging infrastructure alongside modern applications introduces performance gaps; improper configurations, poor access controls, and insecure APIs also add risk.
- **GenAI adoption:** While AI could add up to $340 billion in value to the banking sector alone,[1] AI also powers more evasive attacks.
- **Hybrid work:** Distributed work has disintegrated traditional approaches to access control.
- **Third-party integrations:** Interconnectedness with fintechs and other partners amplifies supply chain risks.

In other words, the technologies needed for firms to grow also challenge their resilience. They also strain regulatory adherence to the European Union's (EU) Digital Operational Resilience Act (DORA), the Dodd-Frank Act, and other mandates.

AI adds to the complexity. In February 2025, new EU AI Act rules — such as requiring financial institutions to comply with AI literacy requirements — went into effect. But a few months later, US President Donald Trump's One Big Beautiful Bill (OBBB) Act proposed a 10-year halt on state and local AI regulations altogether, including for financial services.

It is clear that regulatory resilience is not an option — it is now fundamental to sustaining market stability.

This guide offers strategies to strengthen regulatory resilience by modernizing the approach to these core areas:

- **Applications:** Financial services (finserv) applications (including AI-powered applications and APIs) must be accessible, without interruptions, to millions of concurrent users at any given time.
- **Security:** Institutions must modernize and unify security everywhere in order to scale cloud and AI initiatives.

The repercussions of weakened resiliency

UK banks and financial institutions logged **800+ hours of unplanned tech and systems outages** between January 2023 and February 2025.[2]

Most EU CISOs **(79%) say meeting DORA/ Paperwork Reduction Act (PRA) regulations has impacted their mental health.3**

By some estimates, the total direct and indirect costs of cyber attacks impacting the industry since before the COVID-19 pandemic represents up **to 10% of global GDP.**[4]

Payment fraud-related losses for FSIs have **tripled to $8.8 billion** since 2020.[5]

64% of finserv leaders cite **regulatory compliance as a significant obstacle** to managing data in the cloud.[6]

Only 25% of US finserv leaders feel “highly” or “very” prepared for **GenAI risk and governance.**[7]

Key compliance frameworks that demand resilience

The financial sector faces unprecedented challenges as cyber threats grow in sophistication and scale and threaten market stability. FSIs must maintain seamless service delivery to adhere with end-to-end resilience requirements:

1. **Network resilience:** In the event of a systemic failure, infrastructure must fail over seamlessly and reroute traffic dynamically. For example, the **Securities and Exchange Commission (SEC) Regulation Systems Compliance and Integrity (Regulation SCI) requirements, DORA's Information and Communication Technology (ICT) risk management framework, and business continuity plans set by the European Banking Authority (EBA)** require networks to maintain operational continuity regardless of where a failure occurs.

2. **Security resilience:** True resilience also requires consistent defense against malicious attacks like distributed denial-of-service (DDoS), credential abuse, and web application exploits. This satisfies requirements from **DORA, the Financial Industry Regulatory Authority (FINRA), the US Office of the Comptroller of the Currency (OCC)**, and others.

3. **Data resilience:** Balancing data utilization and privacy requires robust governance mechanisms. Robust cloud backups for data sovereignty and recovery time — along with protections against data breaches and ransomware — align with the **EU's General Data Protection Regulation (GDPR), DORA's incident reporting and information sharing requirements, SEC Rule 17a-4 for electronic records retention, and other measures**.

Regional mandates, such as those from the UK's Bank of England, Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA), also cover a broad spectrum of resilience and risk management requirements.

Staying up to date with evolving compliance has become more challenging than ever. But having a flexible, resilient architecture streamlines compliance — and enables secure digital innovation.

Banking management teams reported spending

42%

of their time in 2023 on regulatory and supervisory compliance, instead of traditional management functions.[8]

Bolstering application security and delivery

The challenge: Going beyond technology redundancy

Financial services firms are under regulatory pressure to ensure operational resilience, especially after high-profile outages affecting major banks and payment networks. They must guarantee consistent, reliable service — regardless of infrastructure failures or cyber attacks.

To prevent such failures, regulators, such as the **US Federal Reserve, European Central Bank, and the UK's FCA**, demand dual-vendor resilience strategies. To meet such requirements, financial institutions have traditionally leaned on redundant tooling, for instance, deploying individual "best-of-breed" content delivery networks (CDNs), web application firewalls (WAFs), and other stitched-together services.

While this approach addresses isolated risks, it often creates fragmented architectures that struggle under pressure. For example, when organizations run the same traffic through each vendor in a linear fashion, it can lead to:

- **Unnecessary costs and performance tradeoffs**, since traffic must pass through two networks — each with their own processing and connection overhead — before going back to the origin(s)
- **Loss of full traffic visibility**, which, in turn, **impedes threat intelligence-powered services** such as DDoS mitigation, bot management, and rate limiting

Furthermore, if they use only one cloud provider (as is the case for 78% of financial institutions[9]), a single vendor/component failure has the potential to cascade into a widespread outage.

Hundreds of Indian banks suffered payment systems disruption from a ransomware attack in 2024. The attack occurred through a **misconfigured open-source automation tool** that allows developers to build, test, and deploy software.[10]

What is needed: A cohesive architecture with a unified control plane

To address core requirements for operational resilience, financial institutions must engineer their architecture for efficiency, not excess. **Focus on establishing a globally distributed yet cohesive network architecture, with one unified control plane.**

Building a cohesive architecture starts with ensuring that application services, cloud, and network providers meet the following criteria:

- **Globally distributed routing** (such as Anycast), to absorb large-scale attacks, like DDoS, while maintaining availability across diverse environments
- **Automatic routing** of all traffic to the nearest data center with enough capacity to process all requests efficiently
- **Accelerated routing** where they actively monitor the fastest paths over the Internet, ensuring the most optimal routes to origin(s)
- **One unified dashboard** where services (such as CDN, DNS, and application services) can be accessed from a single pane of glass, with a simple UI
- **Edge-based protection and failover**, to mitigate attacks at scale and reduce dependency on centralized data centers

Together, these approaches deliver more adaptive continuity, where financial systems can recover intelligently and prioritize the services that matter most in a crisis: payment processing, real-time trading, fraud detection, and digital banking experiences.

> **"No matter what the markets are doing or how high transaction request volumes get, we strive to provide our clients with a secure, seamless, and low-friction trading experience. We achieve that by maintaining the best infrastructure and security systems technically possible … Cloudflare offered a comprehensive solution that addressed all of our needs."**
>
> **Liu Li**
> Chief Technology Officer, Sparrow Exchange, Amber Group

Bolstering security resilience

The challenge: Tool sprawl leaving security gaps

Financial services is the most attacked industry globally,[11] facing threats similar to those targeting critical infrastructure and nation-states. Many firms use the traditional approach of stacking “best-of-breed” tools designed for specific threats at a specific layer: WAFs for web protection, separate fraud analytics engines, independent DDoS services, standalone Zero Trust access controls, and so on.

However, this results in **siloed tools**, **fragmented visibility**, and (as described in the previous section), **inconsistent failover behavior**.

Additionally, business logic — such as WAF rules, identity/device access policies, or fraud controls — are commonly hardcoded into vendor-specific stacks. **This makes policy change too slow, brittle, and high-risk given today’s evolving geopolitical, threat, and regulatory environments.**

Imagine a bank spots and blocks a phishing email sent to a remote developer, Bob. That should trigger tighter access controls, but was it an isolated incident? Have any of Bob’s account credentials been compromised already? Are attackers also targeting one of the bank’s websites or digital properties? With excessive tool sprawl and a siloed approach, there is no clear answer — nor a unified response.

In December 2024, a state-sponsored advanced persistent threat (APT) group exploited an API flaw in a remote support vendor’s platform to access documents in US Treasury system workstations.[12]

What is needed: Layered protection across the stack

Financial services firms are under regulatory pressure to ensure operational resilience. Resilience is not achieved at a single layer; it must span the full technology stack. For true defense-in-depth, firms should consider at least one security platform that delivers layered protection across the stack.

Focus on the vendor's ability to deliver:

- **Comprehensive protections from the network to application layer**, "bi-directionally" — across inbound and outbound traffic
- **A unified control plane for all services**, agnostic to the underlying cloud or network providers, to enable real-time observability and integrated logic across all layers
- **A "rules-as-a-service" approach**, where security rules are managed through a flexible policy layer rather than tools, to empower faster response and consistent enforcement

In this way, FSIs can simplify how they deliver consistent defense-in-depth when faced with critical incidents. In addition, they more efficiently manage a broader spectrum of threats, with automated responses and rapid mitigation:

- **Network risks** such as DDoS attacks, unauthorized remote access, and malware/ransomware propagation
- **Application risks** such as denial of service, API abuse, online payment fraud, zero-day exploits, cross-site scripting, account takeovers, and bot attacks
- **Cloud risks** such as misconfigurations in SaaS applications and cloud storage, data loss/exfiltration risks, and data sovereignty non-compliance
- **AI risks** such as unauthorized GenAI tool use, proprietary code exposure, AI bots and scrapers, and AI-powered attacks
- **Workforce risks** such as multi-channel phishing, visits to risky websites, and unauthorized data access

> **The ability to oversee all of our infrastructure in one place is incredibly valuable. Multiple teams can monitor security from a single dashboard, and management has a single source of truth for future investment and development decisions … Being prepared and proactive with Cloudflare will save us a lot of time and money in the long term."**
>
> **Dev Pathi**
> Chief Technology Officer, Credit Saison India

Ensure regulatory resilience with Cloudflare

Financial services institutions trust Cloudflare's architecture for unmatched operational resilience (beyond 99.99% SLA)

Architectural independence

Cloudflare's vast global network (PoPs across 330+ cities, with 388 Tbps now (as of May 1) operates as a distributed edge platform that sits between your users and your infrastructure.

This provides independence from any single cloud provider, and enables:

- Multicloud failover without vendor lock-in
- Dynamic traffic routing across different backend providers
- Protection against single points of failure in your core infrastructure

Resiliency beyond redundancy

Network protections:

- Global Anycast routing to automatically absorb DDoS attacks and distribute traffic
- Border Gateway Protocol (BGP) and DNS resilience delivered through a distributed infrastructure
- Automatic failover during infrastructure outages

Intelligent routing and caching:

- Reduces data egress costs by serving content from edge locations
- Eliminates cold start latency through always-on edge services
- Provides cost-effective resilience without overprovisioning standby resources

Cohesive architecture

Our unified control plane consolidates:

- DNS, CDN, security, and performance services in one platform
- Consistent policy enforcement across all traffic
- Single-pane-of-glass visibility

Decoupled policy from infrastructure:

- WAF rules and security policies are managed independently of backend infrastructure
- Version-controlled configuration can be tested and deployed safely
- Portable policies work consistently across different cloud environments

Unified security. Network to cloud. Apps to AI.

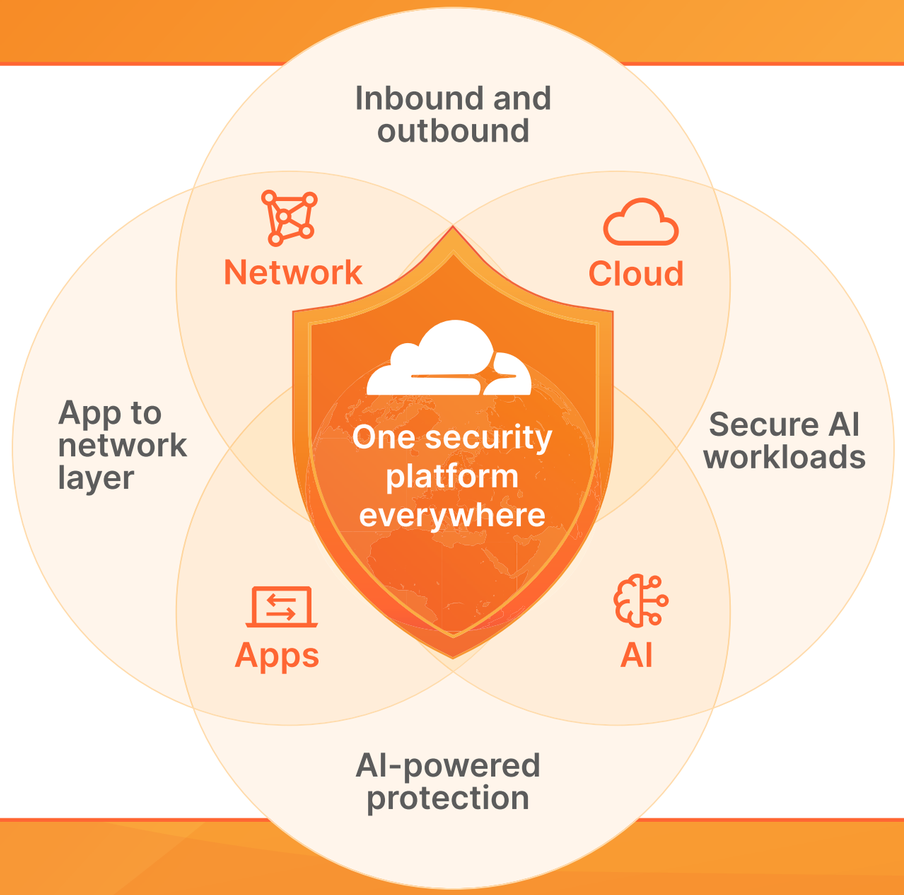
Cloudflare's one security platform also scales seamlessly from network to cloud and protects all users and data across applications and AI. It leverages an intelligent and programmable global cloud network to unify a range of diverse technologies, AI-powered threat intelligence to deliver low-touch, high-efficacy protection, and AI-powered data loss prevention detections to distributed organizations of all sizes.

App to network layer

- Web app and API protection (WAAP)
- Security service edge (SSE)
- DDoS protection
- ...and more

AI-powered protection

- Email security
- Bot management
- Platform simplified with AI agents
- ...and more



Inbound and outbound

- Secure access service edge (SASE)
- Network-as-a-Service (NaaS) and multicloud
- Network interconnect
- ...and more

Secure AI workloads

- AI gateway Firewall for AI
- Critical infastructure trusted to run AI
- ...and more

Analyst-recognized services spanning applications, security, and networks

Named in Gartner® Magic Quadrant™ reports for **Single-Vendor SASE**, **Security Service Edge (SSE)**, **Email Security Platforms**, **Cloud Application Platforms**, and **Cloud Web Application and API Protection (WAAP)**

Named in Forrester Wave™ reports for **Security Service Edge (SSE)**, **Zero Trust Platforms**, **Enterprise Email Security**, **Web Application Firewall (WAF) Solutions**, **Serverless Development Platforms**, and **Edge Development Platforms**

Named in IDC MarketScape reports for **Zero Trust Network Access (ZTNA)**, **Network Edge Security as a Service**, and **Worldwide Edge Delivery Services**

Get started with Cloudflare's connectivity cloud

Financial services institutions need a comprehensive platform that delivers comprehensive visibility and security controls on a resilient global infrastructure.

Cloudflare's connectivity cloud — a unified, intelligent digital platform that enhances how organizations connect, protect, and build their digital environments — delivers on that promise.

With Cloudflare's connectivity cloud, financial services institutions can more efficiently ensure regulatory resilience and compliance, transforming the complex landscape of digital modernization into a pathway for sustainable growth, with proven operational resilience.

Visit www.cloudflare.com/banking-and-financial-services/ to learn more.

> **The threat landscape evolves at breakneck speed, and macro-level visibility into emerging threat trends is critical to protecting the global financial system. Through our intelligence-sharing collaboration with Cloudflare, we're creating a powerful feedback loop — allowing our members to accelerate response times and strengthen defenses across the entire financial sector."**
>
> **Teresa Walsh**
> Chief Intelligence Officer and Managing Director, EMEA FS-ISAC

References

1. “BPI Addresses Rising Compliance Responsibilities for Banks in EGRPRA Response.” Bank Policy Institute, March 11, 2025, https://bpi.com/bpi-addresses-rising-compliance-responsibilities-for-banks-in-egrpra-response/.
2. “More than one month’s worth of IT failures at major banks and building societies in the last two years.” UK Parliament, Treasury Committee, March 6, 2025, https://committees.parliament.uk/committee/158/treasury-committee/news/205611/more-than-one-months-worth-of-it-failures-at-major-banks-and-building-societies-in-the-last-two-years/.
3. Maundrill, Beth. “DORA Compliance Costs Soar Past €1m for Many UK and EU Businesses.” Infosecurity Magazine, January, 16 2025, https://www.egnyte.com/press-releases/the-cloudcurity-magazine.com/news/dora-compliance-costs-soar/.
4. Tuominen, Anneli. “Enhancing banks’ resilience against cyber threats – a key priority for the ECB.” European Central Bank, The Supervision Blog, July 26, 2024, https://www. bankingsupervision.europa.eu/press/blog/2024/html/ssm.blog240726~7bfb4e2267.en.html.
5. Global Financial Crime Report 2024, “BIS Financial Stability Report 2024.” FATF Trends and Typologies Study 2024.
6. “The Cloud, AI, and Data Security in Focus: Insights from Egnyte’s 2024 Financial Services Report.” Egnyte, October 8, 2024, https://www.egnyte.com/press-releases/the-cloud-ai-and-data-security-in-focus-insights-from-egnytes-2024-financial-services-report.
7. “New Deloitte survey finds expectations for Gen AI remain high, but many are feeling pressure to quickly realize value while managing risks.” Deloitte, January 15, 2024, https://www.deloitte.com/global/en/about/press-room/gen-ai-survey.html.
8. “Capturing the full value of generative AI in banking.” McKinsey & Company, December 5, 2023, https://www.mckinsey.com/industries/financial-services/our-insights/capturing-the-full-value-of-generative-ai-in-banking.
9. Bandhakavi, Swagath. “Over 78% of financial institutions rely on single-cloud providers, study finds.” Tech Monitor, December 11, 2024, https://www.techmonitor.ai/hardware/cloud/financial-institutions-single-cloud-provider-study.
10. Kalra, Jaspreet. “Ransomware attack forces hundreds of small Indian banks offline, sources say.” Reuters, July 31, 2024, https://www.reuters.com/technology/cybersecurity/ransomware-attack-forces-hundreds-small-indian-banks-offline-sources-say-2024-07-31/.
11. “Identity Theft Resource Center’s 2024 Annual Data Breach Report Reveals Near-Record Number of Compromises and Victim Notices.” Identity Theft Resource Center, January 28, 2025, https://www.idtheftcenter.org/post/2024-annual-data-breach-report-near-record-compromises/.
12. Lakshmanan, Ravie. “Chinese APT Exploits BeyondTrust API Key to Access U.S. Treasury Systems and Documents.” The Hacker News, December 31, 2024, https://thehackernews.com/2024/12/chinese-apt-exploits-beyondtrust-api.html.

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-7126.2025JUL28