Advancing Segmentation to Strengthen Security and Compliance in Financial Services

Protecting critical infrastructure, containing ransomware, and simplifying compliance.

Financial institutions are prime targets, and the stakes are rising

Financial services firms have long been favored targets for cybercriminals. From multinational banks and retail brokerages to fintech startups and credit unions, organizations across the sector store, process, and transmit highly sensitive financial and personal data. According to the IBM X-Force Threat Intelligence Index[1], the financial sector was the second-most attacked industry globally, accounting for 22.4% of all incidents, behind only manufacturing.

Ransomware remains the most common and costly type of attack, accounting for 36% of incidents in the financial services sector. Meanwhile, IBM's Cost of a Data Breach Report 2025[2] found that financial institutions face an average data breach cost of $5.56 million, significantly higher than the global average of $4.44 million.

Despite heavy investments in security, today's financial institutions are grappling with increasing threats due to increasingly complex hybrid environments, legacy systems, distributed workforces, and growing third-party ecosystems. These factors all contribute to an expanding attack surface and reduce visibility into east-west traffic, making it easier for attackers to move laterally within networks once they gain access.

Security is not just a technology problem, it is a regulatory imperative

Cyber resilience in financial services is not only about stopping attacks. It is also about satisfying a growing list of regional and global cybersecurity regulations that demand proactive defense measures and proof of compliance.

Key regulatory frameworks include:

- **DORA (Digital Operational Resilience Act – EU/EEA):** Requires financial institutions to implement resilience measures across Information and Communication Technology (ICT) systems, including breach reporting, testing, and third-party risk management.
- **MAS TRM (Monetary Authority of Singapore – Asia-Pacific):** Emphasizes Zero Trust, strong access controls, and third-party vendor risk management.
- **SWIFT Customer Security Program (Global):** Requires banks and financial institutions connected to the SWIFT network to enforce segmentation and safeguard transaction systems.
- **PCI-DSS (Global, Payment Industry):** Mandates strict control over systems that store, process, or transmit credit card data, including network segmentation to reduce audit scope and limit the spread of attacks.
- **FISMA (Federal Information Security Modernization Act – U.S.):** Requires U.S. financial agencies and their contractors to implement comprehensive security programs based on the NIST Cybersecurity Framework.
- **NYDFS Cybersecurity Regulation (U.S.):** Requires financial institutions operating in New York to implement a risk-based cybersecurity program.

Noncompliance can result in significant penalties, lawsuits, customer churn, and reputational damage. For example, Capital One's $190 million class-action settlement in 2021 for a breach that exposed 100 million customer records demonstrates the financial and operational consequences of inadequate protection.[3]

Compliance is critical, but complex to achieve

While these frameworks offer essential guidance, aligning with them is a significant challenge for CISOs and risk officers across different regions. Common difficulties include:

- **Fragmented infrastructure:** Hybrid and multi-cloud architectures make it difficult to enforce consistent policies and track compliance across systems.
- **Legacy environments:** Older systems may not natively support modern controls like Zero Trust or host-based segmentation.
- **Resource constraints:** Mid-sized institutions often lack the personnel or expertise to interpret and implement abstract compliance requirements.
- **Audit fatigue:** Repeated, manual efforts to prepare for audits can drain time and resources away from active threat mitigation.

Implementing Zero Trust is not a checkbox exercise. It is a strategic, multi-phase journey. Illumio and IBM offer the tools and expertise to streamline that journey and deliver security outcomes that matter.

Segmentation as the foundation for security and compliance

Illumio's Breach Containment Platform enables financial institutions to control communication between assets and workloads. It prevents lateral movement, contains threats, and supports least-privilege access controls. Illumio works across hybrid and global environments without requiring changes to network architecture.

Combined with IBM Consulting's global governance, risk, and compliance expertise, the solution aligns with regional mandates and improves overall cyber resilience.

Compliance requirement	How Illumio + IBM help meet it
DORA (EI/EEA)	IBM supports ICT risk frameworks; Illumio enforces segmentation to meet resilience testing and third-party controls.
MAS TRM (APAC)	Illumio supports Zero Trust and least-privilege enforcement; IBM integrates controls into risk frameworks.
SWIFT CSP (Global)	Illumio enforces boundaries around SWIFT-connected systems; IBM validates compliance and reporting.
PCI-DSS v4.0 (Global)	Illumio reduces audit scope by segmenting cardholder data environments; IBM validates compliance.
FISMA/GLBA/NYDFS/ NIST CSF (U.S)	IBM identifies regulated systems; Illumio delivers segmentation and containment across environments.

Why choose Illumio and IBM

This partnership brings together Illumio's leading Breach Containment platform with IBM's global cybersecurity and regulatory compliance expertise.

Illumio

- Named a Leader in *The Forrester Wave™: Microsegmentation Solutions, Q3 2024*
- Visibility and segmentation across any environment, including legacy systems
- Host-based, scalable enforcement without infrastructure changes

IBM

- More than 8,000 cybersecurity experts worldwide and 130-plus SOCs
- Deep financial services experience across U.S., EU, and APAC regulatory regimes
- Comprehensive support for DORA, MAS, SWIFT CSP, PCI-DSS, FISMA, NIST CSF, and more

Real-world success: Global bank meets SWIFT and PCI requirements

A Global 250 bank struggled to achieve compliance with SWIFT and PCI-DSS using legacy firewalls. By implementing Illumio Segmentation, the bank gained real-time visibility into application dependencies and was able to define and enforce segmentation policies across cloud, on-premises, and virtual infrastructure.

> "Microsegmentation with Illumio is more scalable, more agile, and quicker to implement than other solutions. Illumio has ensured consistent security across our environments."

VP of Enterprise Systems
Global 250 Bank

Build resilience. Demonstrate compliance. Maintain trust.

With ransomware threats rising and compliance requirements expanding across all regions, financial services institutions need more than just firewalls. They need visibility, control, and proven operational tools to reduce risk and improve response.

Illumio and IBM provide a trusted, scalable solution that empowers financial services organizations worldwide to secure their operations, maintain compliance, and preserve customer trust.

Learn more about how IBM + Illumio can your organization stay secure and compliant.

Contact Illumio today to take the next step.

illumio.com/support/contact

[1] IBM X-Force Threat Intelligence Index 2022
[2] IBM cost of a Data Breach Report 2025
[3] Cybersecurity Dive, "*Fed ends Capital One breach-related enforcement action*," July 2023

About Illumio

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments – stopping the spread of attacks before they become disasters. Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.