Compliance, Breach Containment, and Cyber Resilience for the Banking Sector

Expose attack paths. Contain breaches fast. Keep critical banking systems running and compliant.

Financial institutions sit at the center of the global economy, making them prime targets for cyberattacks. Recent events show how fast a single issue can escalate. The ICBC ransomware attack halted U.S. Treasury settlements. A faulty CrowdStrike update halted endpoint visibility. Recent AWS outages disrupted banking services worldwide.

And, as banks expand their use of cloud, digital services, and third-party providers, their attack surface grows. Blind spots appear, and attackers use weak credentials and unpatched systems to move laterally toward high-value assets. Rising geopolitical tension and state-sponsored threats make these risks even more serious.

Regulators are raising the bar

Regulators are responding with tougher rules to improve resilience across the sector. The EU's DORA framework sets strict standards for ICT risk management, continuity, and recovery. It also requires firms to understand the complex dependencies behind their operations.

In the U.S., regulators such as the Federal Reserve, OCC, FDIC, and Treasury emphasize real-time visibility and strong containment to help reduce systemic risk. Cyber disclosure rules from the SEC make this need even more urgent. Australia and Singapore classify financial services as critical infrastructure and mandate Zero Trust controls, including segmentation. The message is clear: resilience must be demonstrated, not assumed.

> "With Illumio, we have made a significant leap to maximize security and minimize the risk of operational disruptions."
>
> **Steffen Nagel**
>
> Head of IT
> Frankfurter Volksbank

Pressures facing today's CISOs

CISOs must protect complex, fast-changing environments while threats grow in speed and reach. These pressures make resilience difficult:

- **Visibility is fragmented.** Hybrid environments create blind spots that slow response and leave endpoints exposed.
- **Alert fatigue is dangerous.** SOC teams drown in false alarms, which delays decisions and increases the chance of missing real threats.

• **Lateral movement is hard to stop.** Attackers pivot across networks using common tools, with attacks spreading quickly before teams can contain them.

• **Compliance keeps shifting.** New rules require continuous resilience, and failures bring serious legal and reputational costs.

• **Endpoints are the new battleground.** Detection tools struggle to keep up with zero-days, and attacks continue even with protection in place.

• **Accountability is rising.** Cyber risk is a board-level issue, and CISOs must show measurable improvements with limited resources.

Illumio: built for breach containment and resilience

Illumio is designed to stop breaches from spreading across hybrid environments. Its platform delivers fast, scalable containment across cloud, data center, and endpoint systems. Teams gain a shared, real-time view of how workloads communicate, making it easier to reduce risk.

Illumio Segmentation: the core of Zero Trust

Illumio Segmentation enforces microsegmentation at the host level, not through static firewalls or VLANs. Policies follow workloads wherever they run. Dynamic, label-based controls let teams define intent in simple business terms and adapt as environments change.

Illumio Insights: visibility that drives action

Illumio Insights uses an AI-driven security graph to map live application traffic and highlight paths an attacker could exploit. Integrations with Microsoft Sentinel and Security Copilot help analysts cut through alert noise, focus on real risks, and isolate workloads quickly. By turning raw traffic data into actionable intelligence, Insights improves resilience and helps meet rising regulatory expectations.

Proven value for financial institutions

Illumio is trusted by leading financial organizations. Six of the top 10 global banks and more than 20% of the Fortune 100 use Illumio to protect hundreds of thousands of workloads.

Forrester's Total Economic Impact Study found that customers save an average of $3 million on data center firewalls and reduce operational costs by 90%.

Cyber threats to banks are constant, but their impact can be contained. The Illumio Platform helps institutions see how systems connect, stop the spread of attacks, and respond faster when incidents occur.

Improve cyber resilience

Learn more on how Illumio helps the banking sector protect critical systems.

Visit:

illumio.com/solutions/banking-and-financial-services

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.