illumio

INDUSTRY BRIEF

Illumio: Protecting the Banking Sector

Banks and other financial institutions are turning to Zero Trust Segmentation to guard against ransomware and breaches

Why is the sector at risk?

Banks, investment houses, retail brokerages, lenders, fintech startups, and other financial services institutions are the proverbial "big game" for cybercriminals. The reason is simple: That's where the money is.

Financial services was the top industry targeted by cybercriminals for the five consecutive years of 2016-2020, according to an IBM report. In 2021, financial services accounted for 22.4 percent of attacks, in second place just behind manufacturing – but still very much a prime target for ransomware and other cyberstrikes.

Of attack types, ransomware was far and away the most prevalent in financial services, accounting for 36 percent of attacks across all industries, IBM reported.

Risk of a security breach is heightened as banks and other institutions undergo digital transformation, introduce new cloud systems, and expand partnerships with third-party products and service providers. Brisk M&A activity, continued use of legacy IT and cybersecurity systems, and a shift to remote work can also erode an institution's security posture.

Those technological and business changes broaden the attack surface and pose new challenges to visibility. Detecting and identifying a breach is becoming more difficult across complex and interconnected networks. If a breach does occur, a bank can suffer sizable financial losses and negative publicity that undermine confidence among commercial and retail customers, business partners, counterparties, investors, and regulators.

Guarding against ransomware and other kinds of breaches has become more than just a cybersecurity problem – it's now a business resilience challenge at the highest levels.

How Illumio helps

Protect customer data

Understand access to systems, implement security policies to limit access, and report and analyze all traffic that doesn't match rules.

Achieve regulatory compliance

Scope vulnerabilities across the full environment, map application dependencies, apply granular segmentation policies, and monitor connectivity for compliance violations.

Enable digital transformation

Use visibility into relationships between data center and cloud components to secure both on-premises and cloud applications consistently, and integrate with DevOps processes to automate security at scale.

"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

Applying Zero Trust Segmentation to banking

Illumio's Zero Trust Segmentation technology enhances traditional perimeter and firewall defenses to embed security at a far more granular level into the interior of networks and data centers. Instead of a single firewall protecting hundreds of applications and devices, security is applied at each asset individually.

Illumio follows the Zero Trust principle that no application, device, or user can be trusted without verification and must therefore only have least privilege access. As a result, financial institutions can protect critical assets and stop malicious actors from reaching critical systems and data, guarding against loss of customer and market data or a major operational failure.

Illumio's core capabilities equip banks and other financial institutions to:

- Secure critical assets and services, even in the event of a breach.
- Stop the spread of ransomware across networks, data center servers and applications.
- Realize comprehensive visibility across applications, devices, and networks.

Secure critical assets and services

Illumio Zero Trust Segmentation ensures that access to any asset or application is secure and authenticated. It eliminates paths that allow lateral movement and enforces and maintains policy within large, rapidly changing environments.

- Easily segment assets, environments, users and groups.
- Enforce policies dynamically to consistently secure evolving applications, devices, and networks.

Stop the spread of ransomware

Illumio immediately shrinks your attack surface by automating workflows — like policy discovery, authoring, distribution, and enforcement — that block communications on any high-risk port in your network, limiting vectors commonly leveraged by ransomware.

- Pinpoint your critical sources of ransomware risk.
- Proactively close and monitor high-risk pathways.
- Create a reactive containment switch to stop in-progress incidents.

Realize comprehensive visibility

Illumio provides actionable insights by mapping all communications between assets, including applications, clouds, containers, data centers, and endpoint devices. And it does this without touching or changing your network.

- Share a unified view of your communications for your teams and your SIEM/SOAR tools.
- Lower operational risk by identifying unnecessary connections.

Illumio enables banks to prevent ransomware and breaches from causing a major business failure by protecting critical applications.

Improve cyber resilience

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

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

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.