illumio

INDUSTRY BRIEF

Breach Containment for Small and Midsize Banks

How Illumio helps community and regional institutions stop a single incident from becoming an enterprise-wide crisis

About 13,000 small and midsize banks and financial institutions across the U.S. and Europe carry a large share of the responsibility for local economic life. In many communities, they are the only face-to-face banking option.

They also serve sectors the largest banks tend to overlook: outstanding agricultural loans at U.S. community banks reached $162.6 billion at the end of Q1 2026.[1] In Europe, 2,400 cooperative banks serve 228 million people,[2] or about half of all Europeans. Their weight in the financial system far exceeds their asset size. So does the risk they now carry.

And they're growing. U.S. branch networks expanded for two straight quarters through Q1 2026, and community and regional banks posted record net income through Q2 2026. That growth is good news. It also means more branches, more vendors, and more integration points to defend, right as small IT and security teams are asked to protect all of it.

For a bank this size, the question is no longer whether an attacker gets in. It's how far they can move once they do — and that's something you can decide in advance.

The challenges

Smaller banks face the same threats as the world's largest. But they're aimed at teams a fraction of the size, defending flatter, more hybrid, and more vendor-dependent environments.

They run on small teams

Security and IT are often the same few people, and they're competing for scarce cybersecurity talent.

The vendor base has consolidated

Most institutions rely on a web of core providers, managed

1 Krista Williams (Federal Reserve Bank of St. Louis). "Banking Analytics: Agricultural Lending by Community Banks Remained Strong in Q1." July 2026.
2 European Association of Co-operative Banks. "Europe's Cooperative Banks Thrive: 2,400 Banks Serving 228 Million Clients and 91 Million Members." October 2025.

Key benefits

Illumio Segmentation was built for the challenges small and midsize banks face every day.

Quantifiable ROI

Forrester Total Economic Impact (TEI) found 111% ROI and $10.2 million in benefits over three years, with payback in six months.

Smaller blast radius

66% reduction in a cyberattack's blast radius by restricting lateral movement — a direct answer to the flat-network problem.

Faster containment

Illumio customers contain ransomware nearly 4 times faster with segmentation than with detection and response alone.

Lower operational cost

$3.8 million saved by limiting downtime and $3 million from tool and firewall consolidation (Forrester TEI).

A recognized leader

A Leader and Customer Favorite in The Forrester Wave: Microsegmentation Solutions and a 2026 Gartner Peer Insights Customers' Choice.

Sized for this market

The Illumio Starter Bundle — 100 Segmentation and 100 Insights workloads, delivered as SaaS — gets a small team to a defensible core in weeks.

To explore practical ways to protect critical services and contain cyber disruptions, contact your Illumio or partner representative.

service providers (MSPs), and fintech integrations they don't fully control. One compromised provider can reach dozens of institutions at once — and the duty to notify customers and regulators still lands on the bank.

The security model is broken

The gap between disclosure and exploitation has narrowed to almost nothing. Most intrusions now use stolen credentials and legitimate tools rather than malware. A signature or a patch has nothing to catch when the attacker looks like an authorized user.

Ransomware is escalating

Attacks on financial institutions are climbing again, encryption rates are rising, and median demands in the sector are at record highs.

Bank networks are flat

In most small and midsize banks — VMware-heavy, partly cloud, built up over years — teller workstations, branch servers, and core connections share one trust zone. Little stands in the way when an attacker gets inside.

Regulators have moved to enforcement

The Digital Operational Resilience Act (DORA) is in active enforcement across the EU, the NIS2 directive has widened the net, and U.S. examiners are applying the same scrutiny.

What banks need

Those constraints don't change what a bank has to deliver. Across conversations with these institutions and their examiners, the goals come down to four outcomes:

- **Operational resilience.** Critical services keep running during an attack, not just after it.
- **A smaller attack surface.** Fewer paths from anywhere in the environment to anything that matters.
- **Ransomware containment.** Assume a breach will get through, and limit how far the threat travels.
- **Visibility across the hybrid environment**. One live picture of legacy, virtualized, cloud, and vendor connections.

The reality is simple: you can't stop every breach, but you can decide in advance how far it spreads. That comes down to two capabilities working together — visibility into what's talking to what, and enforced segmentation that ringfences what must stay protected.

What Illumio offers

Illumio is built for the realities of small and midsize banks: small teams, hybrid environments, and a growing set of connections that must be understood, not just trusted.

Value Proposition	What is does for the bank
Minimum Viable Bank	Identify the smallest set of systems your bank has to keep running — core ledger, payments, and customer data — and build resilience around that core first. It's a realistic starting point for a five-person team, instead of an all-or-nothing project.
Ransomware Containment	Enforce boundaries so one compromised workstation or branch server can't reach the core. That helps turn a potential enterprise-wide outage into a contained, recoverable incident.
Critical Asset Ringfencing	Put always-on boundaries around the core platform, payment rails (FedNow/FedLine, SWIFT, CHAPS/BACS, SEPA/TARGET2), and customer data — whether or not detection catches the intrusion in time.
Compliance	Turn enforced segmentation into the evidence examiners already ask for: a technology risk control for DORA, an environment aligned to the SWIFT Customer Security Controls Framework (CSCF), and documented boundary control for NIS2 and PCI DSS 4.0.1.
Visibility	Map connectivity between all systems and workloads to identify potential risks, exposure, and weak points in the system. This identifies where policy will be required to increase resilience.

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 and Customer Favorite in The Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.