DATA SHEET

Securing Banking, Financial Services, and Insurance Digital Infrastructure with Terniion™

The Problem: High-Value Targets, Fragile Exposure

Banks, insurers, and capital markets firms sit at the center of the cybercrime economy. Financially motivated actors, sophisticated fraud rings, and state-aligned groups all treat your infrastructure as a prime target.

Edge devices, internet-facing applications, exposed APIs, and third-party connections have become common initial access paths—often through stolen credentials or unpatched vulnerabilities. Traditional ZTNA and VPN models still leave apps reachable at the network layer and scatter policy across multiple tools.

Terniion eliminates the attack surface for critical Banking, Financial Services, and Insurance (BFSI) systems, without forcing you to rip and replace your existing stack.

Business Outcomes for BFSI

Reduced Financial and Third-Party Risk

Shrink the blast radius of a breach by making core banking, payment, and trading systems non-routable, even if a vendor, edge device, or user endpoint is compromised.

Reduced Architectural Complexity

Replace VPN sprawl, exposed jump hosts, and brittle firewall rules with a single process-level overlay that spans branches, data centers, and cloud environments.

Lower Cost of Control and Compliance

Fewer point solutions to run, simplified network policy, and clear evidence of closed inbound ports and process-level isolation reduce both tooling cost and audit fatigue.

© 2026 Xiid Corporation. All rights reserved.

Faster, Safer Modernization

Bring legacy cores and new digital channels under the same protection model without re-platforming or breaking your investments in identity, SIEM, and observability.

5 Best Practices for Securing BFSI Infrastructure

Best Practice	Key Actions	Xiid Terniion Solution
Eliminate Exposed Channels and Endpoints	Reduce direct internet exposure for online banking, payment gateways, trading platforms, and back-office apps.	Terniion makes critical BFSI systems non-routable: no public IPs, no open inbound ports, only outbound, process-to-process tunnels via SealedTunnel.
Kill Credential Abuse as a Primary Vector	Move away from passwords, long-lived API keys, and shared accounts tied to high-value systems.	Aclave provides credential-less authentication for users and services, making stolen credentials and infostealer logs far less useful to attackers.
Contain Third-Party and Vendor Access	Limit how far a compromised vendor, contractor, or partner can move in your environment.	Vendors receive process-scoped, outbound-only access into specific systems instead of broad VPN or network-level reach, drastically constraining lateral movement.
Harden Branch, ATM, and Edge Connectivity	Secure branch apps, ATMs, kiosks, and edge services without complex per-site firewall gymnastics.	Terniion overlays existing WAN/SASE: branches and ATMs use outbound-only tunnels to reach central systems, removing exposed edge surfaces.
Future-Proof Sensitive Transactions and Data Flows	Assume adversaries are harvesting encrypted payment and transaction data today to decrypt later.	Triple-layer, post-quantum encryption protects payment traffic, interbank messaging, and sensitive workloads from harvest-now-decrypt-later campaigns.

© 2026 Xiid Corporation. All rights reserved.

How Terniion Secures BFSI Environments

Terniion is a secure network access control platform that sits as an overlay across your existing identity, networking, and monitoring stack.

Core Banking and Payments

- Core banking, card processing, and interbank systems operate with all inbound ports closed.
- Only authenticated, policy-approved processes can reach them through outbound-only, process-to-process tunnels.
- Even if an attacker lands on an edge system, there is no path into the core other than through a SealedTunnel.

Digital Channels (Web and Mobile)

- Existing application security, fraud analytics, and customer IAM stay in place.
- Terniion removes direct network reachability to the back-end services powering those channels.
- Attackers probing APIs and web apps cannot use the network layer to pivot into internal systems.

Branches, ATMs, and Remote Offices

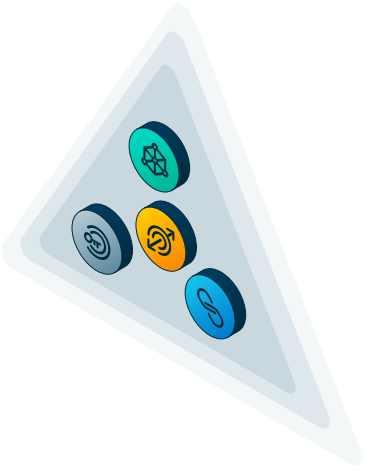
- Branch applications, ATMs, and local services connect out via SealedTunnel instead of site-to-site VPNs.
- You avoid per-branch firewall rule sprawl while keeping critical services non-addressable from the internet.
- Edge device exploits and misconfigurations no longer expose your internal networks.

Third-Party, SOC, and Service Provider Access

- Vendors, SOC partners, and auditors access only the specific applications and processes they need, never entire subnets or VLANs.
- Each relationship gets its own tightly scoped, auditable access pattern, reducing the risk that one compromised partner becomes a systemic incident.

Key Components

- **SealedTunnel**
  Executed via STLink— a lightweight software agent on either end, these are outbound-only, triple-encrypted, process-to-process tunnels that perform reliably even over unstable networks, ideal for distributed clinical sites.
- **Commander**
  The control brain coordinating secure connections across cloud, on-prem, and hybrid environments. It centralizes policy so “who can talk to what” becomes maintainable rules instead of 10,000 firewall exceptions.
- **Connector**
  Joins two outbound-only communication halves without ever decrypting traffic. It serves as a secure rendezvous where quantum-encrypted messages are dropped off and picked up by authorized STLinks, keeping critical infrastructure undiscoverable.
- **Aclave**
  Credential-less authentication that lets staff and partners access systems without usernames, passwords or long-lived credentials.



© 2026 Xiid Corporation. All rights reserved.

High-Value BFSI Use Cases

- **Secure Vendor and Third-Party Access**
  Replace broad VPN access with process-level, time-bounded connectivity into key systems (e.g., core banking, payment platforms, trading infrastructure). A single compromised vendor account can no longer see or traverse your internal network.
- **Protect Payment and Trading Platforms from Edge Exploits**
  As attackers increasingly target edge devices and internet-facing services, Terniion ensures underlying payment and trading systems remain out-of-range and isolated, even when vulnerabilities emerge.
- **Modern Remote Work for High-Risk Staff**
  Traders, treasury, finance, and privileged IT roles connect from anywhere over outbound-only tunnels that scope access to specific applications and processes—removing the need for broad VPN access to internal networks.
- **Segment Acquisitions and Legacy Environments Quickly**
  Newly acquired banks, insurers, or legacy platforms can be isolated behind Terniion while integration proceeds, reducing exposure during high-risk transition periods.

FAQS

Will Terniion replace our SSE or sit alongside it?

Terniion is designed as an overlay. It can coexist with existing SSE/ZTNA platforms, hardening private and high-value applications where traditional tools stop at user-to-app visibility and leave network reachability in place.

How does this affect audit and regulatory conversations?

By closing inbound ports, enforcing process-level isolation, and applying strong encryption, Terniion directly supports risk-based narratives around exposure reduction, lateral movement prevention, and resilience that regulators and auditors expect in financial services.

What's the time-to-value for a first deployment?

Most organizations start with a small set of critical applications—like payments, trading, or core banking portals—and see protection in weeks, not years. Terniion overlays your existing stack and avoids large re-architecture projects.

The Bottom Line

Financial institutions cannot afford to treat core systems as just another set of apps behind a perimeter.

Terniion gives you a way to:

- Cut financial and third-party risk by making critical systems genuinely unreachable.
- Simplify a complex access and network security stack.
- Reduce long-term control cost while improving compliance posture.
- Protect legacy and modern BFSI infrastructure under one future-ready model.

Secure the infrastructure your balance sheet depends on without starting from scratch.

Ready to see what unreachable BFSI infrastructure looks like in practice?
Read more about Terniion | Get a live demo

© 2026 Xiid Corporation. All rights reserved.