IBLADES WHITEPAPER · FINANCIAL SERVICES & BANKING

Quantum-Safe Banking Infrastructure

Protecting core banking, payments, the ATM and branch edge, third-party vendor access, and the data pipelines feeding AI and fraud models against quantum and AI-era threats — without disrupting live banking operations.

← Financial Services & Banking

In this paper

1. Executive summary

Banks and financial institutions are pivoting from basic automation to production-grade AI, embedding autonomous agents across compliance, operations, and core payment and trade workflows, while integrating the overwhelming majority of their structured data into modern cloud platforms. This hyper-connected ecosystem of open banking APIs, multi-cloud platforms, and AI agents vastly increases systemic risk — even as ATMs, branches, and other legacy infrastructure remain difficult to patch without disrupting operations.

iBlades secures this environment with a single, hardware-anchored, post-quantum security fabric that overlays existing systems. It protects data in transit against future quantum decryption, isolates the ATM and branch edge from physical and logical attack, closes the gap created by vendor sprawl, and counters AI-driven attacks by shrinking the

exposed software surface — all without changing core banking applications or production-critical payment systems.

---

2. The 2026 threat landscape

AI-accelerated attacks

AI-powered attacks run at machine speed — discovering vulnerabilities in minutes, probing thousands of APIs and services at once, generating evasive malware, and mapping trust relationships to move laterally after a foothold. Against AI-driven fraud detection and credit models, **data poisoning** — the deliberate corruption of the data streams models are trained and scored on — becomes a direct financial and reputational risk, not just a data-security concern.

> **The real target is complexity.** AI attacks feed on exposed APIs, admin consoles, agents, and remote-access paths. Reducing that software surface does more to stop them than adding another software layer.

Harvest Now, Decrypt Later

Adversaries capture encrypted banking traffic today with the intent to decrypt it once quantum computers mature. Financial services are acutely exposed because so much of their data has a long shelf life: loans, wealth and treasury records, and transaction histories often need to remain confidential for a decade or more, well within the window in which today's encryption could be broken retroactively.

Ransomware, vendor risk, and a massive attack surface

A bank's attack surface spans core banking and database systems, payment rails and interbank messaging, millions of mobile and web sessions, ATM fleets, branch networks, and a sprawling ecosystem of external vendors, FinTech partners, and cloud providers. Multi-stage ransomware increasingly targets core ledgers and cloud backup clusters to paralyze operations, while attackers routinely exploit weaker, lesser-secured vendor and partner systems as a backdoor into otherwise well-defended internal networks. Managing consistent security policy, key rotation, and audit evidence across this scale of decentralized infrastructure — with a persistent shortage of specialized cryptography

and AI-security talent — is now one of the hardest operational problems financial institutions face.

---

3. The iBlades architecture

One hardware-anchored, quantum-ready fabric, built on NIST-standardized post-quantum cryptography (ML-KEM for key exchange, ML-DSA/Dilithium for signatures; FIPS 203/204) with keys generated locally and rotated autonomously.

- **NetTron™** — software-defined, peer-to-peer quantum-safe mesh; encrypts core banking, payment, and interbank messaging traffic and cryptographically signs data flowing into AI and fraud-model pipelines to prevent poisoning.
- **GuardTron™** — plug-and-play hardware edge node that isolates the ATM and branch edge, data-center and cloud ingress points, and third-party vendor connections; agentless and warranty-safe.
- **ManoTron™** — hardware-secured mobile communications for privileged administrators, executives, and incident-response teams on any network.

AI-resilient by design

- **Reduced attack surface** — fewer exposed interfaces and agents for AI to probe.
- **Hardware-anchored trust** — trust rooted in dedicated hardware that can't be scanned or manipulated like software.
- **Cryptographic isolation** — blocks AI-driven lateral movement even after a compromise.
- **Works alongside your stack** — inline and transparent; complements existing firewalls, SIEM/SOAR, EDR/XDR, IAM, and GRC tools.

---

4. Regulatory & compliance mapping

Framework	Requirement	How iBlades enables it
NIST PQC (FIPS 203/204)	Migration to quantum-safe algorithms	Native ML-KEM / ML-DSA across the fabric

Framework	Requirement	How iBlades enables it
PCI-DSS	Strong cryptographic protection and continuous tracking of cardholder data environments	Hardware-anchored encrypted wrapper around cardholder data flows with real-time access tracking
ISO 27001	Information security management	Zero-trust access, immutable audit trails
DORA	Digital operational resilience, including third-party and ICT risk management	Zero-trust vendor tunnels, segmentation, and automated resilience reporting
Central-bank cybersecurity framework	Secure architecture, encryption, identity access management, and third-party risk control	Automated network segmentation, identity filtering, vendor containment, and audit-ready evidence

---

5. A low-risk pilot path

- **Select** a non-critical starting point — a controlled third-party vendor access path or a single branch-to-data-center communication link.
- **Deploy** the edge node inline — a fast install with no changes to applications, network architecture, or user workflow.
- **Validate** isolation and performance with a red-team exercise; legitimate traffic passes with acceptable latency, attacks are blocked.
- **Demonstrate** post-quantum key rotation and audit-ready evidence; the deployment is reversible with zero operational impact if desired.

Ready to secure your banking operations?

Request a briefing to see how a low-risk pilot would work in your environment.

Request a briefing

⬇ Download PDF

Back to overview

Prefer email? Reach us at hello@iblades.ai

---

iblades.ai™

Safe, effective, secure.

Next-generation cyber architecture making cybersecurity simple, reliable, and accessible for everyone.

hello@iblades.ai

Products

- NetTron™
- GuardTron™
- ManoTron™
- Pricing

Solutions

- Financial Institutions
- Healthcare
- Infrastructure
- Government & Military

Company

- About Us
- Partners
- Documentation
- Contact

Compliance

- NIST Approved
- SOC 2 Type II
- HIPAA Compliant
- ISO 27001
- FedRAMP Ready

HEADQUARTERS

127 Spring Street, Suite 120

R&D CENTER

795 24th Street

Pleasanton, CA 94566 Ogden, UT 84401