OPSWAT.

OPSWAT FOR FINANCIAL SERVICES

# Post-Quantum Readiness: Securing Data Flows That Keep Finance Running

Quantum computing is an emerging technology that poses an active risk to financial organizations. Adversaries are already executing Harvest Now, Decrypt Later (HNDL) attacks, stockpiling your encrypted transactions and key material today to decrypt once quantum capability arrives. OPSWAT's hardware-enforced isolation and software supply chain controls secure every data boundary, so your most sensitive infrastructure stays structurally unreachable.

## The Challenges

**Harvest Now, Decrypt Later (HNDL):**
Adversaries are already stealing your encrypted transactions and key material today to decrypt once quantum arrives. Every day you delay puts more data at future risk.

**The Inbound Vector:** Every bidirectional port opened for SOC monitoring is a new attack surface, and a potential DORA, GDPR, or NYDFS violation.

**Cloud Bleed:** Bidirectional DevSecOps pipelines let compromised dependencies bleed back into source code and core infrastructure.

**Takeaway:**
As long as your architecture relies on bidirectional software policies, you have an inbound vector.
The solution requires a shift to hardware-enforced physics where the return path is physically impossible to traverse.

## The OPSWAT Value

**Hardware-Level Isolation (MetaDefender Optical Diode™):** Keys enter the vault; nothing exits. Hardware-enforced unidirectional flow isolates management planes and key vaults at the physics level.
*Physics, not policy. Zero-trust enforcement that no software exploit can bypass.*

**One-Way Telemetry**: Stream Splunk, syslog, SNMP, and HTTPS feeds from trading platforms, core banking, and OT systems to your SOC/SIEM with zero inbound exposure.
*Operational visibility without compromising network integrity.*

**Cloud & Supply Chain Darkening**: MetaDefender Optical Diode enforces one-way breaks at every cloud and DevSecOps boundary with IP headers stripped and no reverse path. MetaDefender Software Supply Chain™ scans every package, container, and dependency before it crosses.
*Your internal architecture stays invisible to the cloud.*

TRUST
**Deep CDR™ Technology & Sandbox**
Neutralizes prompt injection and poisoned models before they reach your infrastructure.

PRIVACY
**Proactive DLP™**
Secures sensitive data to align with DORA, NYDFS, NIST AI RMF, and more.

DEFENSE
**MetaDefender Optical Diode™ and MetaDefender Software Supply Chain™**
Physical immunity against HNDL attacks and C2 backdoors, guaranteed by physics. Scan every package for secrets, vulnerabilities, and poisoned AI models.

OPSWAT.
Protecting the World's Critical Infrastructure

Ready to build a quantum-resilient security architecture? Connect with one of our experts: opswat.com/get-started