Transformativ IP

PQC+

The Executive Backgrounder

Q-InfoSecur™ + Q-SecurKey™ + Proactive 50-State Regulatory Compliance

What Every CEO, CTO, and CISO Needs to Know

About the Quantum + AI Threat — and the Architecture Built to Stop It

Why You're Reading This

Let's be direct. Two things are happening at the same time, and together they create a problem no enterprise security stack built before 2024 was designed to handle.

- **First,** AI has industrialized cyberattacks. Attackers no longer probe one weakness at a time — they scan, learn, and adapt at machine speed.
- **Second,** quantum computing is approaching the point where it can break the encryption protecting almost every system you operate today. Expert consensus puts that moment 2–3 years out, possibly sooner.

Adversaries already know this. They're stealing your encrypted data right now — not to read it today, but to decrypt it the moment a powerful enough quantum computer comes online. The industry calls this "Harvest Now, Decrypt Later," or HNDL. China's IP theft alone is estimated at $225–600 billion per year against U.S. companies. Average breach cost: $4.45 million per incident. Those are today's numbers, before Q-day arrives.

Meanwhile, the regulatory ground is shifting under you. The DOJ Data Security Program took effect in 2025, treating sensitive data protection as a national security matter. Add 19+ other federal statutes — HIPAA, GLBA, SOX, FERPA, FISMA, FASCSA — plus a patchwork of state-level rules, and "checklist compliance" simply doesn't work anymore.

What PQC+ Is

PQC+ is the Transformative IP solution combining **Q-InfoSecur™** (a quantum-resistant data security layer), **Q-SecurKey™** (dynamic, ephemeral key generation that eliminates the static key target), and **proactive regulatory compliance** automated across all 50 states and 20+ federal statutes.

It is engineered to solve the post-quantum, AI-accelerated, regulation-saturated security problem in one architecture — not as bolt-on point products.

This backgrounder is designed for one purpose: to walk you through what the threat actually looks like, why most "PQC upgrades" on the market won't actually protect you, what PQC+ does differently, and what a sensible buying decision looks like. No academic jargon. No fear-mongering. Just the picture you need to make a confident decision.

What's Inside

1. The Two Threats Converging On You Right Now

It helps to think of modern cyber risk as a two-stage attack — because that's exactly how sophisticated adversaries are running it.

Stage One: AI Does the Breaking In

AI didn't just speed up old attack methods. It changed the economics. A well-resourced attacker can now do, in hours, what used to take a team of humans weeks.

Three ways AI is already breaching systems today

- **Pattern matching.** AI scans massive, distributed environments looking for the weak spot — a misconfigured cloud bucket, an outdated TLS library, a forgotten endpoint. It doesn't attack the strongest wall. It finds the unlocked window.
- **Automated, adaptive attacks.** Credential-stuffing and phishing campaigns now learn in real time. Block one attempt and the next one is already adjusted.
- **Attack-path prediction.** AI maps lateral movement across cloud, IoT, and ICS environments faster than your blue team can investigate the first alert.

Stage Two: Quantum Decrypts What AI Stole

Quantum computing has moved from theory to commercial reality. Twelve major manufacturers — IBM, Google, Amazon Braket, Microsoft Azure Quantum, and others — are now producing quantum machines or providing cloud access to them. Caltech demonstrated a 6,100-qubit array. Google's Willow chip showed self-correction at scale. Engineering hurdles are falling faster than predicted.

Once a sufficiently powerful quantum computer is operational, Shor's algorithm reduces RSA and ECC decryption from "the age of the universe" to minutes. Every certificate, every TLS handshake, every encrypted backup currently relying on RSA-2048 or ECDSA — transparent.

> ⚠ **Harvest Now, Decrypt Later (HNDL)**
>
> Adversaries don't need to wait for quantum to be useful. They're already exfiltrating your encrypted data and stockpiling it. The day a working cryptographically-relevant quantum computer exists, all of that stockpiled data becomes readable. Patents. M&A files. Trade secrets. PHI. Financial records. Source code. Everything they've siphoned for the last decade.

The Combined Picture

AI provides the "harvest now" at unprecedented scale. Quantum delivers the "decrypt later." Together, they expose any architecture that depends on static keys, perimeter defense, or long-lived certificates — which is essentially every architecture in production today.2. Why a Simple "Algorithm Swap" Won't Save You

There's a comforting story being sold across the industry: "Just swap RSA for a NIST-approved post-quantum algorithm and you're done." It's not true. The math gets stronger; the architecture stays broken.

Here's why an algorithm-only PQC upgrade leaves you exposed:

The Architectural Flaw	What It Means for You
Centralized key vaults (KMS/HSM)	Your KMS or HSM is a high-value single point of failure. One successful compromise — by an external attacker or an insider — unlocks vast amounts of your data. Upgrading the algorithm doesn't change this.
Static, long-lived keys	A key that protects data for years becomes the lynchpin of HNDL. Attackers only need one successful strike to unlock years of stockpiled data. Static keys are the prize.
Massive retrofit cost	Many PQC algorithms create "data bloat" — larger keys, larger ciphertext — that strain bandwidth and add latency. Retrofitting them into legacy OT, ICS, or mainframe systems is months of work, often with downtime you can't afford.

The Architectural Flaw	What It Means for You
Access control gap	Encryption keeps data secret. It doesn't enforce who gets to read it. Today's authorization lives in external ACLs at the app or network layer — useless the moment data is exfiltrated or the perimeter is breached.

The takeaway is uncomfortable but important: replacing the math without redesigning the architecture is like buying a stronger lock for a door that's left wide open. To actually be safe, four things have to change at once.

1. **Eliminate the static key.** If there's no key sitting at rest, there's nothing for HNDL to harvest.
2. **Bind authorization to the data itself.** Security rules must travel with the data, not live in an external system.
3. **Remove the static patterns AI learns from.** Dynamic, per-session secrets defeat AI's strongest weapon.
4. **Make deployment non-disruptive.** If the solution requires you to rip out legacy systems, it won't get deployed in time.

PQC+ was engineered specifically against this list.

3. The PQC+ Architecture, Plainly Explained

PQC+ is the combination of two technical pillars and one operational pillar. Together, they replace perimeter security with security that lives inside the data itself.

Pillar 1: Q-SecurKey™ — Keys That Don't Exist Until They're Needed

This is the most important architectural shift to understand. Traditional systems generate a key, store it somewhere, and reuse it for months or years. Q-SecurKey™ does the opposite: it generates keys on demand, uses them once, and never stores them.

How it works (the four-step view)

1. A user requests access to an encrypted data object.
2. The system pulls that user's verified attributes — identity, clearance level, device, location, time, zero-trust policy token — from a trusted policy engine.
3. Those attributes, plus secret seeds and public parameters tied to the data, flow into a Key Derivation Function (KDF).
4. The KDF deterministically generates a unique, session-only decryption key. The key exists for the length of the transaction, then is gone.

Why this defeats Harvest Now, Decrypt Later

There is no static key for the attacker to harvest. There is no central vault to breach. Even if an adversary steals everything in your environment — every server, every backup — they cannot reconstruct the keys,

because the keys were never written down. They only ever existed for a moment, derived from attributes the attacker doesn't have.

Pillar 2: Q-InfoSecur™ — The Rules Live Inside the Data

Q-InfoSecur™ embeds the Access Control List directly into the encrypted data payload. The data and the rules governing its access are cryptographically bound together. We call this a self-enforcing crypto object.

What that gives you

- **Provenance maintenance.** Move the data, copy it, exfiltrate it — it doesn't matter. The rules go with it. The data protects itself.
- **Rapid Response Capability (RRC).** Revoke access instantly without bulk re-encryption. Update one policy in the Zero Trust engine and the next derivation attempt fails. No more weekend re-encryption marathons.
- **Single-copy multi-classification storage.** Top Secret, Confidential, and Unclassified data can sit on one infrastructure. The embedded ACL ensures each user sees only what they're authorized to see. Dramatic infrastructure simplification.

Pillar 3: The "+" — Proactive Compliance Across All 50 States

This is what makes the offering PQC+ rather than just PQC. The architecture isn't only quantum-resistant — it's engineered to satisfy U.S. regulatory requirements automatically, not as a separate workstream.

The compliance layer ships with three integrated components:

- **Q-InfoSecur™ PFS** (Perfect Forward Secrecy) for data-in-motion — DOD/DISA-certified, ephemeral session keys, ~10–50ms latency overhead.
- **Q-InfoSecur™ DLT™** for data-at-rest — a "double-blind" sharded storage architecture distributed across a Byzantine fault-tolerant network. Stolen fragments are computationally infeasible to reassemble.
- **Q-InfoSecur™ COMPLIANCE™** for policy and consent — real-time data masking, multi-jurisdictional rules, native support for FHIR (healthcare) and FDX/FIBO (finance) ontologies.

The architectural one-liner worth remembering

4. Where PQC+ Beats the Alternatives

You're going to be pitched several approaches over the next 18 months. Here's how PQC+ compares head-to-head.

Capability	Traditional PQC Algorithm Swap	KMS / HSM Upgrade	PQC+ (Q-InfoSecur™ + Q-SecurKey™)
Quantum-resistant math	Yes	Partial (algorithm-dependent)	Yes — NIST-approved PQC
Eliminates the static key target	No	No — still a centralized vault	Yes — keys never stored
Defeats Harvest Now, Decrypt Later	Forward only — stolen data still at risk	No	Yes — no key to harvest
Embedded authorization in the data	No	No	Yes — self-enforcing crypto object
AI-attack resistance	No — static patterns remain	No — vault is a known target	Yes — dynamic, attribute-based
Works on legacy OT/ICS/mainframe without code changes	Rarely	No	Yes — transport-layer overlay
50-state regulatory alignment	Out of scope	Out of scope	Built in — DOJ DSP, HIPAA, GLBA, SOX, GDPR, FISMA, more
Instant access revocation (no re-encryption)	No	Limited	Yes — Rapid Response Capability

The pattern is consistent. Other approaches solve one piece of the puzzle. PQC+ solves all four — the quantum problem, the AI problem, the legacy-deployment problem, and the compliance problem — in a single architecture.

5. Compliance Without the Spreadsheets

If your compliance team is currently maintaining a spreadsheet that maps controls to HIPAA, GLBA, SOX, FERPA, GDPR, PCI-DSS, and now the DOJ DSP — you already know the problem. Every new regulation adds another row, another control, another audit cycle.

PQC+ collapses that work into architecture. The same cryptographic enforcement that protects the data also produces the audit evidence regulators want to see.

The DOJ Data Security Program: The Catalyst

The DOJ DSP is the single most important regulatory development for U.S. enterprises in a decade. Here's what makes it different:

DSP Element	What It Means
Status	Active and enforceable
Stated goal	Prevent foreign adversaries from accessing sensitive U.S. data
Named countries of concern	China, Russia, Iran, Cuba, Venezuela, North Korea
Covered data categories	Human "omic"/biospecimen, biometric, precise geolocation, personal health, personal financial, covered personal identifiers
Bulk thresholds	Low — e.g., health data on 10,000 people, or genomic data on just 100 people
User consent as a defense?	No. DSP is a national security rule — consent is not an exemption
Scope	Not limited to data brokers; any organization meeting the thresholds is in scope

The Broader Compliance Web PQC+ Addresses

The DSP is one of 20+ federal statutes governing your data, layered on top of state-level requirements. PQC+'s architecture maps directly to the controls these laws require:

Sector	Key Statutes & Mandates Addressed by PQC+
Healthcare	HIPAA, HITECH, FFDCA, 21 CFR Parts 800–1299, FTC HBNR
Financial data	GLBA, FCRA, FACTA, EFTA
Financial reporting	SOX, Securities Exchange Act of 1934

Sector	Key Statutes & Mandates Addressed by PQC+
Education	FERPA, COPPA
Supply chain	FASCSA, Section 889 NDAA
Cybersecurity	FISMA, CISA, NIST CSF
IoT	IoT Cybersecurity Improvement Act, NIST device standards
Energy	NERC CIP, Energy Policy Act
Telecommunications	Communications Act, TCPA, Broadband DATA Act
Government	Privacy Act of 1974, Federal Records Act, FOIA, E-Government Act
Industry mandates	PCI DSS (card processing), FDX (financial data exchange)

Why this matters at the CFO level

Penalties for non-compliance are not theoretical. DSP violations can trigger operational shutdowns. HIPAA fines run $100 to $50,000 per violation. GDPR fines can reach 4% of global revenue. PQC+ doesn't just reduce breach risk — it converts compliance from a recurring cost center into an automated, audit-ready control.

6. What Implementation Actually Looks Like

This is the part most security upgrades fail. The architecture is solid; the deployment is a nightmare. PQC+ was specifically engineered to avoid that. There are two deployment paths, and you can use both at the same time.

Method 1: Transport Layer Protection — The Quick Win for Legacy Systems

This is how you get immediate protection on the systems that are hardest to change — OT, ICS, mainframes, brittle line-of-business apps. A gateway or proxy is deployed in front of the existing system, and it transparently PQC-encrypts the entire data stream before it enters the network.

What this means in practice

- **Zero application code changes.**
- **Zero downtime.**
- **Zero re-engineering of legacy systems.**
- The legacy app has no idea anything has changed. It just keeps working — except now it's quantum-resistant.

Method 2: SDK Integration — The Deep Strategy for New Systems

For greenfield applications and systems under active development, the Q-InfoSecur™ and Q-SecurKey™ SDKs let developers embed the protection directly into application code. This is the long-term path that gives you maximum control.

What you get

- Field-level encryption (down to a single VARCHAR column in a database).
- Per-microservice ACLs.
- Cryptographic operations tied directly to business logic.
- Native support for AWS, Azure, GCP, Kubernetes, Android, iOS, Windows, Linux.

The Pragmatic Three-Step Rollout (Aligned with CISA Guidance)

5. **Inventory.** Build a cryptographic asset inventory. Identify the "crown jewel" data — the long-lifespan sensitive information that an HNDL adversary most wants.
6. **Secure legacy systems first.** Deploy Method 2 (Transport Layer Protection) for immediate risk reduction on the systems hardest to modify. This delivers protection in days, not quarters.
7. **Integrate with new systems.** Use the breathing room from step 2 to plan strategic SDK integration for greenfield applications. Bake security in at design time.

Performance You Can Actually Live With

Characteristic	What to Expect
PFS session setup latency	~10–50 ms over a standard TLS handshake — negligible for nearly all enterprise workloads
Storage overhead (DLT™)	1.3x to 2.0x depending on k-of-n availability ratio
Resilience	Byzantine fault tolerance — multiple node failures without data loss or service interruption
Scale	Designed for high-volume transaction systems via Q-InfoSecur™ MESSAGE™
Cloud readiness	Kubernetes-based deployment across AWS, Azure, GCP
Network layer	Operates at Layer 3 — transparent to applications and storage

7. The Business Case — ROI in Plain Numbers

Strip away the security theater for a moment. Here's the actual financial argument.

Cost Avoidance

Risk Category	Cost Range	PQC+ Mitigation
Average data breach (IBM 2024)	$4.45M per incident	Architecture prevents both interception and bulk exfiltration
HIPAA fines	$100 to $50,000 per violation	Embedded ACLs and audit trail produce compliance-ready evidence
GDPR fines	Up to 4% of global revenue	Real-time policy enforcement, cross-jurisdictional
DOJ DSP violations	Including potential operational shutdown	Native DSP-aligned controls
IP theft (China alone, U.S. annual)	$225–600 billion economy-wide	Self-enforcing crypto objects survive exfiltration

Operational Efficiency

- **Reduced TCO.** PQC+ replaces 5–10 disparate point solutions — encryption gateways, KMS, DLP add-ons, compliance tooling, audit prep software. Fewer licenses, fewer integrations, fewer vendors.
- **Automated governance.** An estimated 70–80% reduction in manual compliance and audit prep workload through policy-driven controls and automated consent management.
- **No bulk re-encryption events.** Rapid Response Capability eliminates the weekend-long re-encryption cycles your team currently runs when permissions change at scale.

Competitive Differentiation

This is the part most executives miss. A security architecture that's good enough to be auditable in real time becomes a sales asset. You can:

- Enter regulated markets faster — native FHIR and FDX/FIBO support shortens healthcare and financial integration cycles.
- Sign data-sharing partnerships your competitors can't — because the data carries its own enforcement, not a contract you hope the partner honors.
- Run AI initiatives on sensitive data that competitors won't touch — because granular ACLs let you expose exactly what's permissible, nothing more.
- Move from "we contractually commit to security" to "we can technically prove it" — which is the language enterprise procurement now wants.

The strategic reframe

Most security spending is defensive — it reduces a loss number. PQC+ does that, but it also enables revenue activities that aren't possible without it: AI on sensitive data, multi-party data sharing, regulated-market entry, cross-border transactions under DSP. The ROI is in both columns.

8. How to Decide — A CEO/CTO/CISO Decision Checklist

You don't need to be a cryptographer to make this call. You need to answer eight honest questions. If any of these worry you, PQC+ is the conversation worth having.

The Eight Questions

1. **How long does our most sensitive data need to remain secret?** If the answer is "more than two or three years," HNDL is your problem right now.
2. **Where do our encryption keys live, and who can reach them?** If the answer involves a single KMS or HSM, that's your single point of failure.
3. **Could we revoke access to a specific dataset in the next ten minutes?** If revocation means "run a re-encryption job over the weekend," access control is theoretical, not real.
4. **How many separate tools do we run for encryption, key management, DLP, and compliance?** Five or more is a smell. PQC+ is built to consolidate that stack.
5. **Are we in DOJ DSP scope?** If you hold health, biometric, geolocation, financial, or omic/biospecimen data at the thresholds named in the rule, the answer is yes. Consent will not save you.
6. **How long would a full PQC migration of our legacy OT/ICS/mainframe environment take with our current vendors?** If the honest answer is "years," Method 1 (Transport Layer Protection) is the way you bridge the gap in weeks.
7. **What's our exposure to AI-accelerated attacks today — not Q-day, today?** If your defenses depend on static patterns, you're already losing this fight.
8. **If we were breached tomorrow, could we prove technical compliance — not just "we had policies" — to a regulator?** PQC+ produces that evidence automatically.

Recommended Next Steps

These aren't commitments — they're a sensible discovery path.

1. **Run a DSP scope assessment.** A short data inventory tells you what's actually in scope under the DOJ rule. Most organizations are surprised.
2. **Map your compliance gaps.** A side-by-side of current controls against DSP plus your top three sector statutes (e.g., HIPAA + SOX + FISMA) usually surfaces 60–80% of the urgent work.
3. **Pilot Q-InfoSecur™ PFS on one high-risk data flow.** This is a small, contained deployment that produces real evidence — not a slide deck — about the latency, the integration cost, and the operational fit.
4. **Formalize a phased roadmap.** Method 1 for legacy. Method 2 for greenfield. Sequenced to hit DSP requirements first and the broader regulatory web second.

The Bottom Line

Quantum is no longer a distant threat. AI has already industrialized the attack side. The DOJ Data Security Program has redefined compliance as a national security obligation. The combination is real, urgent, and unforgiving of organizations that wait.

PQC+ — the integration of Q-InfoSecur™, Q-SecurKey™, and proactive 50-state regulatory compliance — is the architecture engineered to address all three at once. Quantum-resistant encryption. Keys that don't exist until they're needed. Authorization that lives inside the data. Compliance that produces its own audit evidence.

The question isn't whether you'll need this architecture. ***The question is whether you'll deploy it on your timeline — or your regulator's.***

Continue the Conversation

This backgrounder is the entry point. Transformative IP offers deeper material tailored to each role on your executive team:

Audience	Available Materials
Business Owners / CEOs	7-min Video TechTalk • 12-min and 40-min Audio TechTalks • 7-page and 11-page Articles
CTO / CIO / CISO	8-min Video TechTalk • 12-min and 35-min Audio TechTalks • 12-page and 26-page Articles • 48-page Technical FAQ

To request the materials above, schedule a DSP scope assessment, or initiate a Q-InfoSecur™ PFS pilot on one of your high-risk data flows, contact: