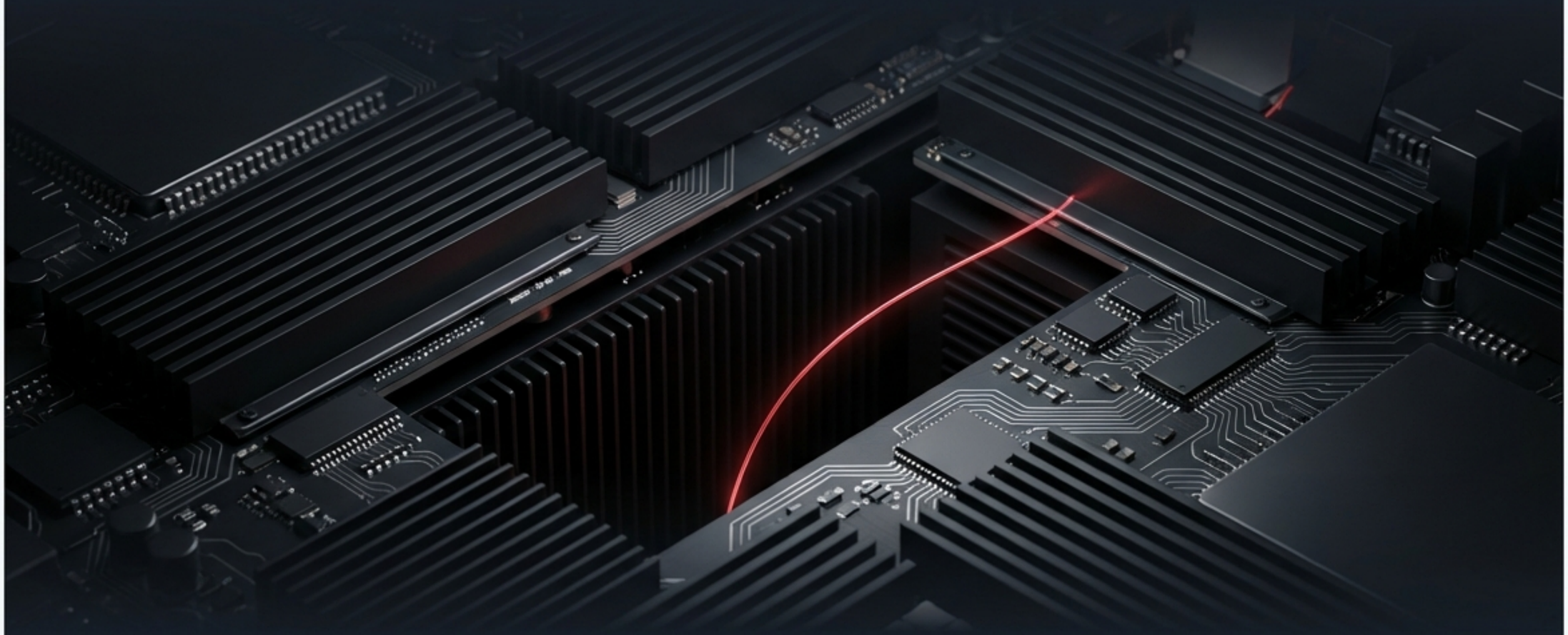
The Unseen War for American Innovation

Protecting Our Most Valuable Asset in an Era of State-Sponsored IP Theft.



Q-InfoSecur™ | Q-SecurKey™

The Threat is Real, and the Numbers are Staggering.

$225–$600 BILLION

The annual cost to the U.S. economy from Chinese IP theft.

1 IN 5

U.S. companies report having their IP stolen by China within the last year.

“The greatest transfer of wealth in history.”

—NSA Director

EVERY 12 HOURS

The frequency at which the FBI opens a new China-related counterintelligence investigation.

This is not random cybercrime. It is a coordinated state-sponsored strategy to leapfrog American technology by stealing our IP.

The Anatomy of a $1 Billion Corporate Devastation

The Theft from American Superconductor (AMSC)

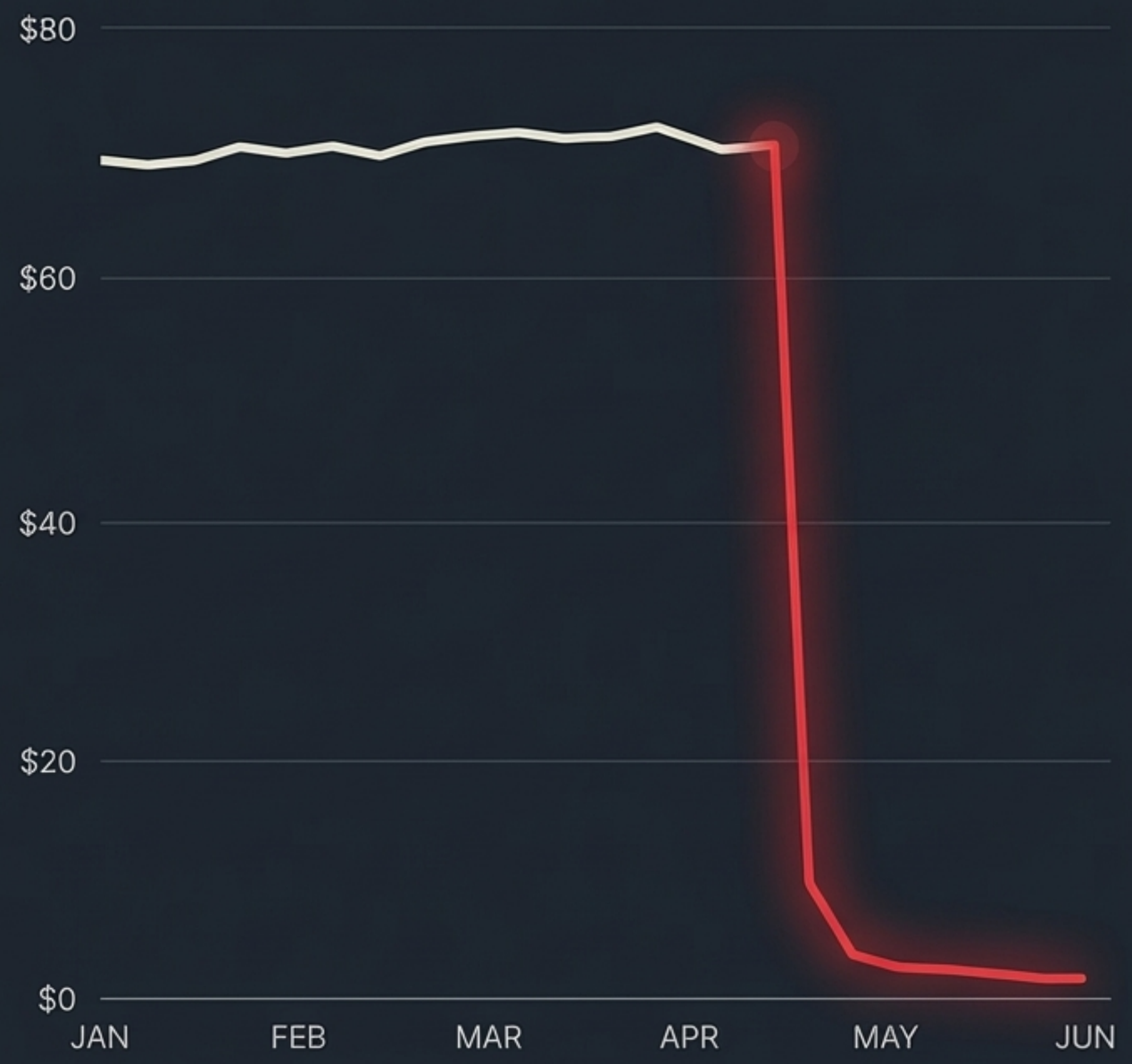
THE VICTIM:
AMSC, a leading wind turbine technology company.

THE THEFT:
A state-backed competitor, Sinovel, stole proprietary proprietary control software with help from an insider.

THE DAMAGE:

- Stock price collapsed **84%** in a single day.
- Over **$1 Billion** in market value erased.
- **700+** American jobs eliminated.

Sinovel became the world's #2 wind turbine manufacturer using stolen AMSC technology.



The Attack Surface is Every Pillar of American Industry.

Core router source code stolen, enabling a state-backed competitor to become a $95B giant.

Proprietary chemical process secrets stolen, erasing a decades-long competitive advantage.

Autonomous vehicle trade secrets stolen by engineers defecting to a Chinese startup.

Personal data of 147 million Americans and critical database trade secrets stolen by the PLA.

OPERATION CUCKOOBEES

Trillions in multi-industry IP (fighter jet blueprints, pharma formulas) stolen by state actor APT 41.

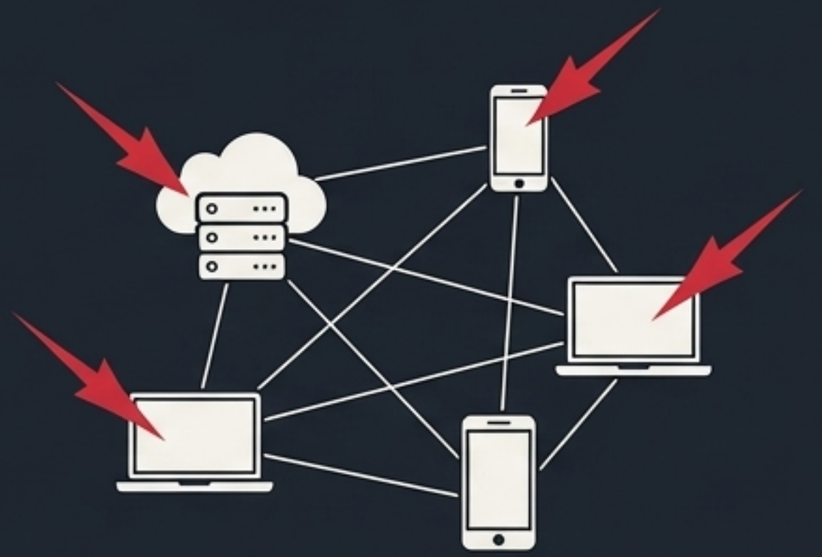
Yesterday's Defenses are Obsolete

The "Castle and Moat" security model is fundamentally broken.

THE OLD MODEL: TRUSTED PERIMETER

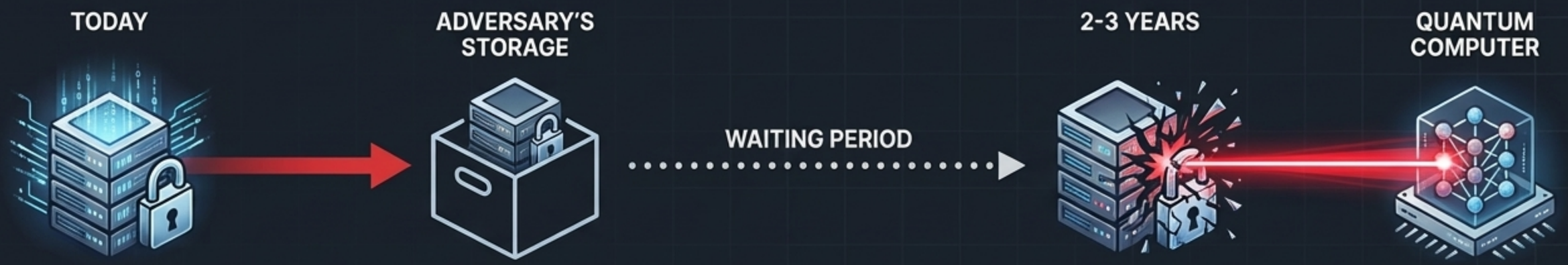
Strong walls on the outside, but once an attacker is in, they have free rein to move laterally and exfiltrate data.

THE NEW REALITY: NO PERIMETER



1. **Data Lives Everywhere:** In the cloud, on devices, across borders—there is no single perimeter.
2. **Sophisticated Attackers:** State actors and AI-powered threats easily bypass walls.
3. **The Insider Threat:** It assumes everyone inside is trustworthy (as seen in the Apple & AMSC cases).

The Future Threat is Already Here: “Harvest Now, Decrypt Later”



The Threat: Adversaries are stealing encrypted data *today* with the explicit goal of decrypting it once quantum computers are available.

The Impact:

- Trade Secrets & Patents
- Source Code & Blueprints
- Long-Term Financial Records
- Healthcare and Genetic Information

A quantum catastrophe is actively being set into motion right now.

A New Architecture for a New Reality

We need an entirely new kind of vault—impervious to today's attacks and tomorrow's quantum threats.

Our Solution: Q-InfoSecur™, built on two integrated, game-changing technologies.

Pillar 1: Post-Quantum Cryptography (PQC)

The Unbreakable Material

Pillar 2: Zero Trust Architecture (ZTA)

The Intelligent Access Protocol

Pillar 1: Post-Quantum Cryptography (PQC)

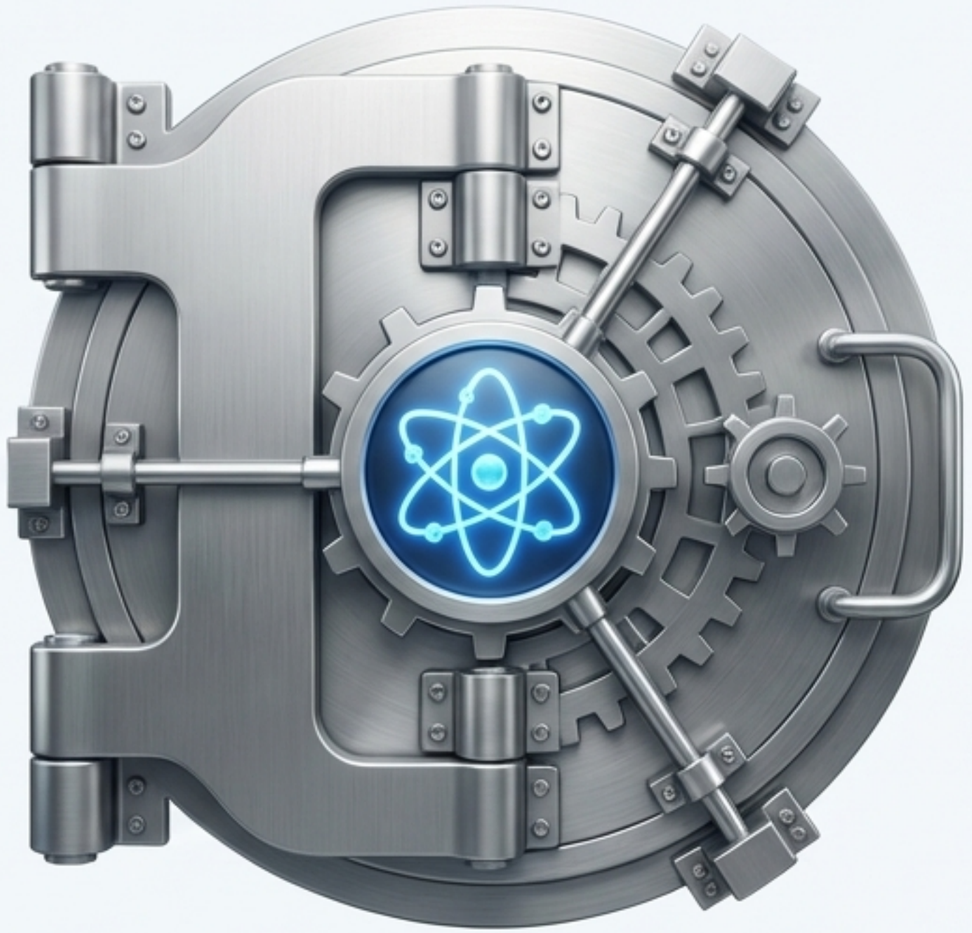
Securing Data Today that Stays Secure Forever.

Technology: Powered by Q-SecurKey™, our PQC uses advanced mathematical algorithms designed to withstand attacks from both classical and quantum computers.

Business Value:

- ✓ **Long-Term Data Security**: Information encrypted today remains secure for decades.
- ✓ **Future-Proofs Compliance**: Stay ahead of emerging security regulations.
- ✓ **Permanent IP Protection**: Your trade secrets, formulas, and source code remain yours—forever.

Key Takeaway: Even if an attacker steals your encrypted data today, it will remain completely unreadable when they get access to a quantum computer.

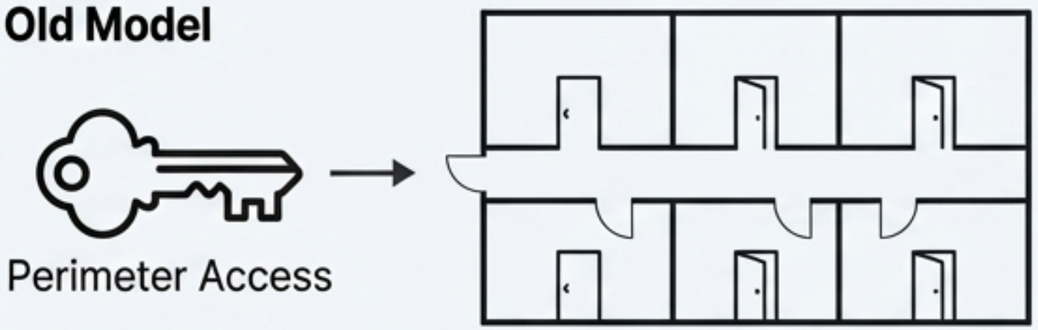


Pillar 2: Zero Trust Architecture (ZTA)

Never Trust, Always Verify

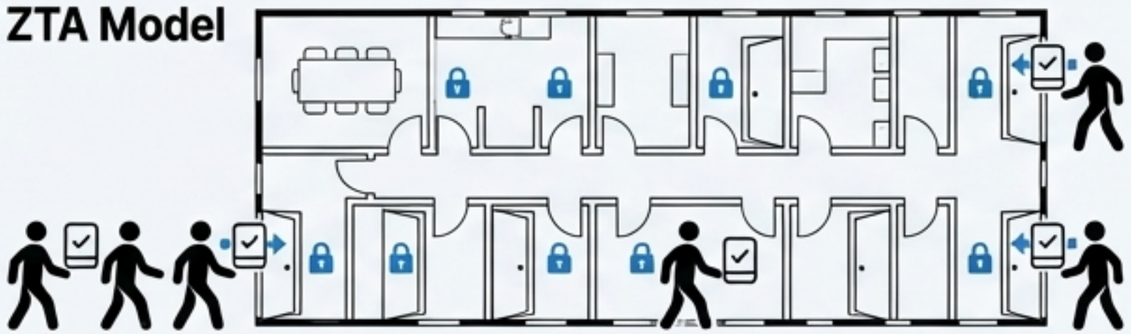
Imagine a modern facility where everyone needs to show ID and authorization at ***every single door***, even if they're already inside. ZTA applies this principle to your data network.

Old Model



Perimeter Access

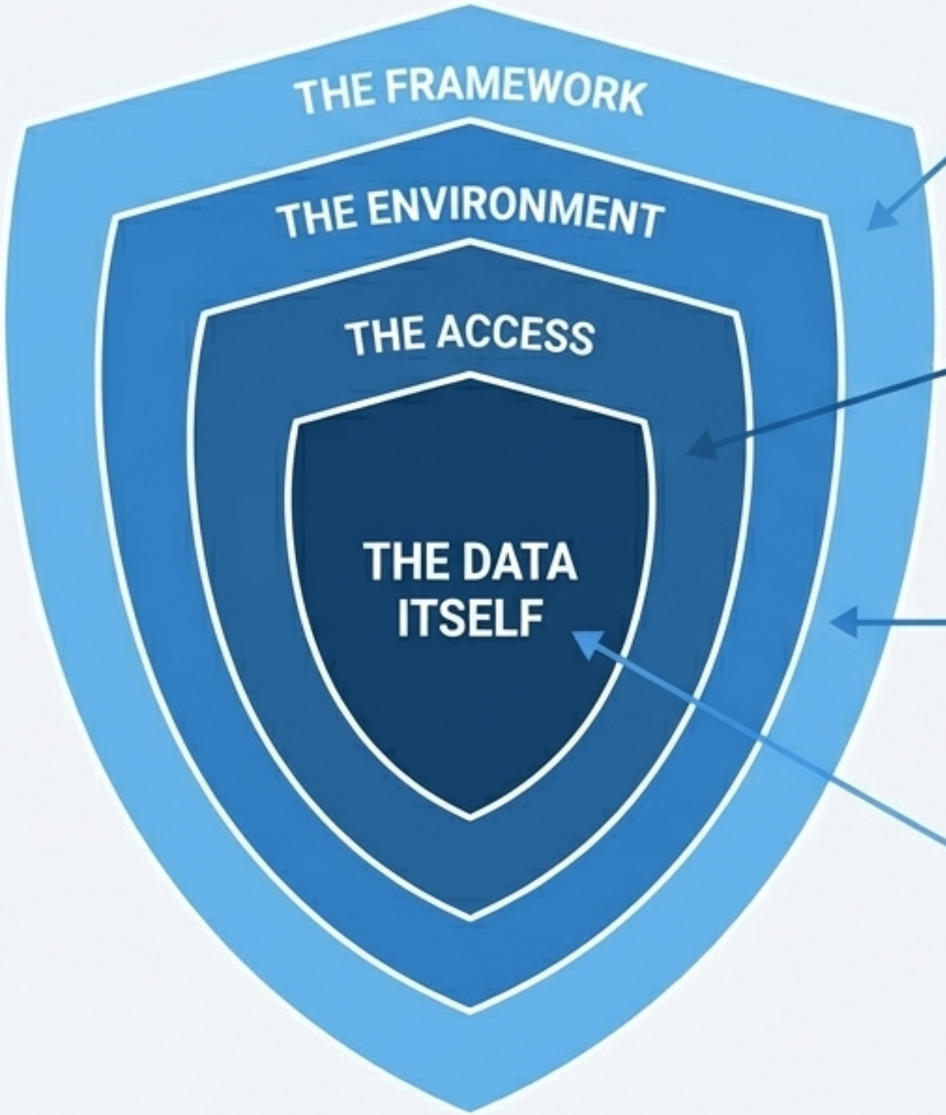
ZTA Model



The 5 Key Principles

1. **Explicit Verification:** Authenticate every access request in real-time.
2. **Least Privilege Access:** Grant access only to what's needed, nothing more.
3. **Microsegmentation:** Isolate network zones to contain any potential breach.
4. **End-to-End Encryption:** Data is protected at rest, in transit, and in use.
5. **Continuous Monitoring:** Log and analyze all activity to detect threats instantly.

The Power of Integration: Why PQC + ZTA is the Ideal Solution.



Q-SecurKey™ PQC

Even if data is stolen, it's unreadable now and forever.

This defeats 'Harvest Now, Decrypt Later'.

Q-InfoSecur™ ZTA

Prevents unauthorized access and data theft in the first place.

This defeats insider threats and lateral movement.

Continuous Monitoring

Detects and responds to threats before damage occurs.

This provides real-time threat intelligence.

Comprehensive Audit Trails

Built-in controls satisfy regulatory requirements automatically.

This ensures compliance.

Transforming Unbreakable Defense into Strategic Business Advantage.

1. Comprehensive Regulatory Compliance, Simplified

- Inherently satisfies requirements for GDPR, HIPAA, PCI DSS, SOX, and more.
- Provides tamper-proof audit trails.
- Reduces compliance costs by an estimated 40-60%.

2. Dramatic Risk Reduction for Data Breaches

- The average cost of a data breach is over $4.45 million.
- End-to-end encryption and breach containment render stolen data unreadable.
- Reduces potential breach damage by over 90%.

3. Financial Fraud Prevention and Trust

- Real-time transaction monitoring for AML compliance.
- Phishing-resistant authentication eliminates password vulnerabilities.
- Builds customer trust through verifiable data protection.

An Elegant Solution: It's Architectural, Not a Complete Rebuild.

Our 100% software solution works as a layer on top of your existing infrastructure.

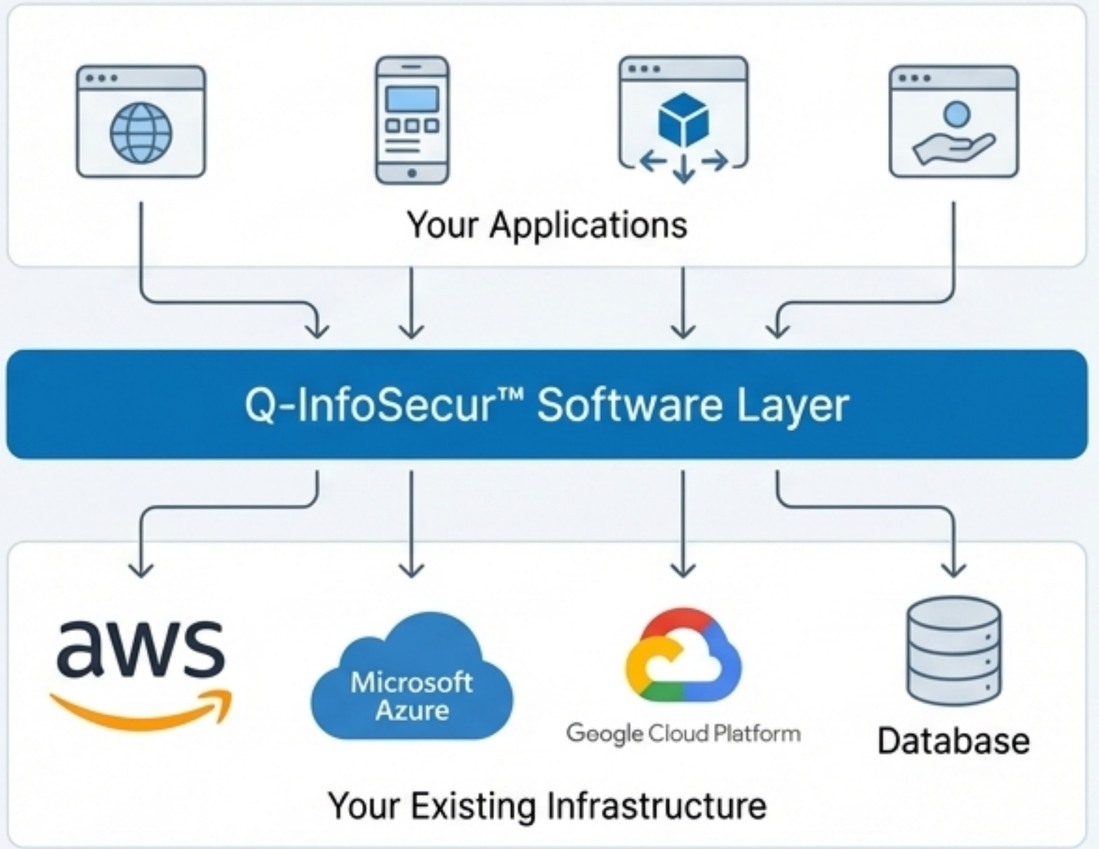
Technical Highlights

- **Cloud-Native:** Built for AWS, Azure, and GCP from the ground up.
- **API-Driven:** Modern REST APIs for seamless integration.
- **Transparent to Applications:** Applies field-level encryption without changing database structure or application code.

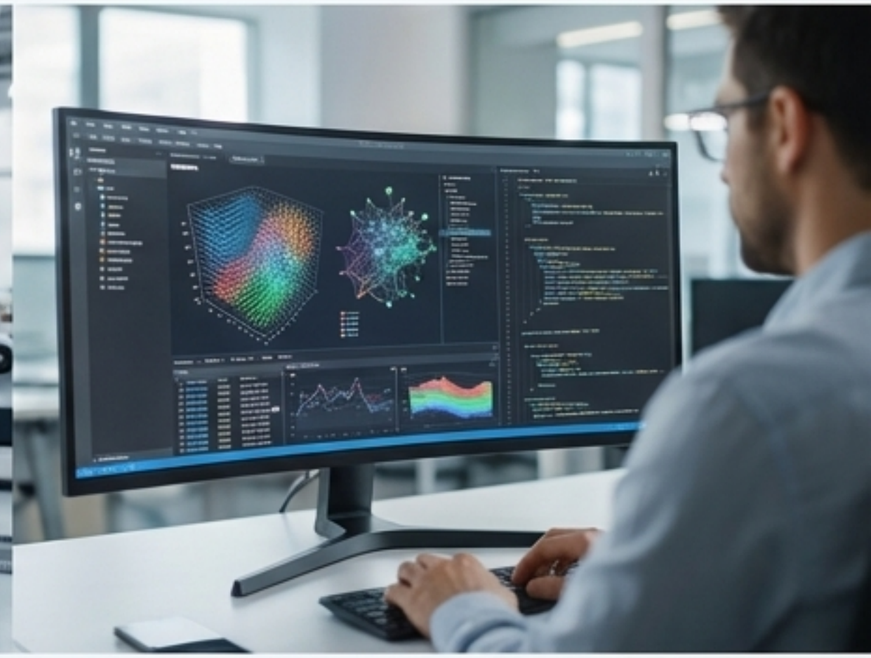
Rapid Implementation Timeline

Policy-based configuration allows for fast deployment.

Example: AWS S3 bucket protection in hours, not weeks. A complete enterprise rollout in weeks, not months or years.



Protecting Your Company is Protecting American Innovation.



Economic Security

- Preserving R&D investments and market leadership.
- Securing critical supply chains.

National Security

- Preventing theft of dual-use technologies.
- Securing infrastructure against nation-state attacks.

Job Protection

- Protecting innovation protects the high-paying jobs it creates.

  (Recall: The AMSC theft eliminated 700 American jobs.)

The Choice Is Clear. The Time Is Now.

The Status Quo is a Clear and Present Danger

State actors are systematically targeting your industry.

Quantum computers will render current encryption useless.

The cost of inaction is measured in millions, if not billions.

The Opportunity is a Demonstrable Advantage

Gain a competitive edge through security leadership.

Win customer trust with proven, quantum-resistant protection.

Enable secure digital transformation and accelerate innovation.

Every day without quantum-resistant protection is another day adversaries can harvest your encrypted data.
Every day without Zero Trust is another day your business is vulnerable.

Secure the Future of Your Business.

For Business Owners (CEOs)

- Video TechTalk (7 min)
- Audio TechTalks (12 & 40 min)
- Articles (7 & 11 pg)

For Technology Leaders (CTOs, CIOs)

- Video TechTalk (8 min)
- Audio TechTalks (12 & 35 min)
- Articles (12 & 26 pg)
- FAQ (48 pg)

Info@TransformativIP.com
www.transformativip.com/protect

The future of American innovation depends on the right choice today.
Q-InfoSecur™ and Q-SecurKey™ provide the shield.