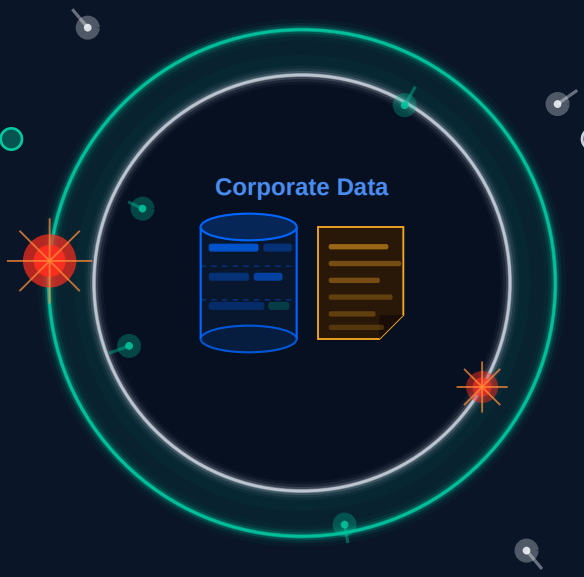
CYBERSECURITY PERIMETER DEFENSE

Ransomware-Proof and Quantum-Secure.

Breakthru Technologies™ delivers quantum-secure execution and data protection built on entropy—not decryption difficulty—to defend the enterprise perimeter against ransomware, AI-driven threats, and future compute-scale adversaries.

Execution Control Layer
Intercepts proposed actions before execution, evaluates against defined invariants, and applies a cryptographic gate — unauthorized actions are never expressed.



Data Protection Layer
Fractalized data, ephemeral keys, and protected reconstruction blueprints ensure that even exfiltrated fragments are unusable without the required authorization conditions.

THE CHALLENGE

The threat landscape has changed.

WITHOUT BREAKTHRU, YOU FACE:

- Encryption rendered obsolete by quantum computing advances
- Ransomware attacks that hold your data hostage
- AI systems acting outside approved operational constraints
- Expanding attack surfaces as data volumes and endpoints grow
- No immutable audit trail to prove data integrity after a breach
- Legacy security architectures that cannot adapt to emerging threats

WITH BREAKTHRU, YOU GET:

- Quantum-secure encryption based on the laws of physics — not math
- Ransomware-proof architecture with restructured storage and replication
- AI governance that prevents unsanctioned actions and misuse
- Zero-trust trusted channels for all data transmission and key exchange
- Immutable data lineage with cryptographic chain of custody
- Crypto-agile architecture that evolves with the threat landscape

CORE CAPABILITIES

Unbreakable by design. Future-proof.

Quantum-Secure Encryption
Deploy unconditionally secure, non-obsolescent encryption based on information-theoretic principles — protecting data against any computationally unbounded adversary.

Quantum Key Management
Generate and manage encryption keys across multiple endpoints without key transmission using quantum key distribution and perfect forward secrecy.

Ransomware Protection
Restructure and replicate data across multiple storage and retrieval points, ensuring ransomware cannot encrypt or hold your data hostage even after a perimeter breach.

AI Security & Governance
Prevent AI models and autonomous systems from acting outside approved constraints. Protect against prompt injection, unsanctioned actions, and AI-driven threat vectors.

Quantum Messaging & Zero Trust
Transmit data through quantum-secure zero-trust trusted channels. Eliminate interception risks across all communications and cryptographic operations.

Immutable Data Lineage
Maintain a cryptographically secured, tamper-proof chain of custody for every data record — audit-ready on demand.

HOW IT WORKS

From vulnerability assessment to unconditional security.

01 — Assess

Map your encryption posture, attack surfaces, and quantum vulnerability exposure across all data systems, endpoints, and communication channels.

02 — Architect

Design a quantum-secure, ransomware-proof defense architecture tailored to your environment — on-premises, cloud-hosted, or hybrid.

03 — Deploy

Implement quantum key generation, secure data restructuring, AI governance controls, and zero-trust channels with full integration support.

04 — Monitor

Continuously monitor for emerging threats, maintain crypto-agility as standards evolve, and ensure your security posture remains unconditionally secure.

USE CASES

Where perimeter defense delivers immediate and long-term value.

Quantum Threat Preparedness

Quantum computers will render RSA and ECC obsolete. Organizations must migrate now to avoid retroactive decryption of encrypted archives.

- → Assess quantum vulnerability exposure across all systems
- → Migrate to information-theoretically secure encryption standards
- → Deploy crypto-agile architecture that evolves with computing advances

Ransomware Resilience

Ransomware is the most costly threat facing enterprises, with average recovery costs exceeding $4M per incident.

- → Restructure storage to eliminate single points of encryption failure
- → Replicate data across multiple retrieval points automatically
- → Recover operations without paying ransom or losing data

Defense & National Security

Mission-critical operations require security architectures that defend against advanced nation-state adversaries.

- → Deploy post-quantum encryption exceeding national security mandates
- → Protect communications, records, and AI-driven situational awareness
- → Ensure long-term resilience without reliance on classified technologies

AI Safety & Trusted Autonomy

As AI systems are deployed in high-stakes environments, preventing unsanctioned actions is a critical governance requirement.

- → Implement AI governance controls at the system architecture level
- → Prevent prompt injection, model manipulation, and unsanctioned actions
- → Maintain decision integrity and execution trust across AI pipelines

STANDARDS & FRAMEWORKS

Built for the most demanding security mandates.

Aligned to the strictest national and international cybersecurity standards.

NIST PQC | FIPS 140-4 | Zero Trust | FedRAMP High | CMMC | ITAR | HIPAA

Ready to build an unconditionally secure perimeter?

Talk to a Breakthru specialist and find the right cybersecurity solution for your enterprise.

Contact us at info@breakthrutech.ai

Schedule a Demo