



Symmetrics™

The New Trust Layer for the **Post-Quantum Internet.**

Symmetrics' breakthrough has solved the problem that eluded cryptographers for 75 years:

One-Time Pad symmetric key encryption — now deployable at Internet scale.

**Known as the most secure form of encryption ever invented, in a post-quantum world
Symmetrics secures every transmission, transaction, and communication on the internet,
every data file, health record, email, text, phone call, video call, cloud, and network — making
it the foundational Trust Layer for the global digital economy.
No rip-and-replace needed. Attack *prevention*, not detection.**

The Once-in-a-Generation Opportunity

Every generation produces one or two foundational technology shifts so profound that they reshape entire industries and create enduring franchise value for those who move first. Cloud computing was one. The internet was another. Quantum-secure cryptographic infrastructure is next — and unlike those prior shifts, this one comes with a hard deadline.

The threat of quantum computing to today's encryption is not theoretical. The Cybersecurity and Infrastructure Security Agency (CISA) has mandated that federal agencies begin procuring quantum-resistant technologies, with compliance deadlines beginning January 1, 2027, for New National Security Systems. Every bank, every cloud provider, every government, every enterprise that transmits or stores sensitive data faces the same reckoning. The question is not whether to act — it is who will provide the solution at scale.

The Technology: Why Symmetrics Stands Alone

In 1949, Claude Shannon proved that One-Time Pad (OTP) encryption provides perfect secrecy — the ciphertext reveals no information about the original message, and *it is computationally impossible to break*. Used for decades by the NSA and Department of Defense, OTP had one insurmountable limitation: encryption keys had to be physically hand-delivered. The limitation was never mathematical. It was logistical.

Symmetrics has eliminated that limitation entirely. Through a patented Key Distribution Center (KDC) architecture, Symmetrics generates true random keys and delivers them securely over the internet to authenticated devices and validated users in real time — making One-Time Pad Symmetric Key (OTPSK) encryption practical at internet scale for the first time in history. Virtually all encryption systems in use today rely on *mathematical algorithms* that quantum computers will eventually break. Symmetrics' system has no mathematical structure to attack. **It is immune to brute force, AI, and quantum computing by design.**

Recent engagement with the National Institute of Standards and Technology (NIST) indicates that Symmetrics' technology is being prioritized for accelerated evaluation and certification — a development that could

materially accelerate deployment across federal agencies, critical infrastructure, and regulated enterprises worldwide.

What the World's Leading Cybersecurity Voices Are Saying

"The quantum threat storm is arriving: CISA mandates quantum-resistant technology for new national security systems by January 1, 2027. Post-quantum cryptography is only a bandage that may be broken tomorrow. Only Claude Shannon's 1949 one-time pad (OTP) symmetric encryption achieves information-theoretic security independent of computational assumptions, making it highly resistant against any adversary, quantum or otherwise. Symmatrics eliminates OTP's ancient Achilles' heel — physical delivery — with its revolutionary split-key method and quantum-generated Paired Keys provided not-over-the-air, allowing OTP-grade symmetric keys to be distributed securely over the internet right now.

Symmatrics is not a choice for governments or businesses confronting existential quantum and AI concerns — it is a must-have."

— Chuck Brooks, President, Brooks Consulting International | Adjunct Faculty, Georgetown University | #2 Global Cybersecurity Influencer (IFSEC) | Former Presidential Appointee, Dept. of Homeland Security | Symmatrics Advisory Board Member

"Symmatrics provides a clear, mathematically unbreakable path to quantum-secure communications. This is the right answer at the right time, just as algorithmic and architectural breakthroughs accelerate the threat of Q-Day, making RSA-2048 obsolete. Because so much of modern society relies on secure internet communications, this makes the Symmatrics protocol one of the most significant IT innovations in decades."

— Joe Eaton, Ph.D. in Computational and Applied Mathematics | Distinguished Systems Engineer, NVIDIA | Symmatrics Advisory Board Member

The Leadership Team

Symmatrics was founded by two former NSA professionals with 53 years of combined service, whose prior company, Matrics, was acquired for \$230 million by Symbol Technologies. In 2016, the founders focused on bringing One-Time-Pad Symmetric Key Encryption to the supply chain. In 2022, Walter Raquet met the founders and immediately recognized that they had the solution for cybercrime. He joined as Chairman and convinced the founders to pivot to being a cybersecurity company, and was appointed CEO in October 2025. Raquet co-founded Knight Capital Group, which grew from \$17 million and 60 employees to 1,400 employees, approximately \$300 million of EBITDA, and a public market capitalization of roughly \$8 billion in four years.

Our broader leadership team has led innovation across some of the world's most influential institutions, including the CIA, the White House, Goldman Sachs, and NIST.

Encryption as Infrastructure

Symmatrics is building a cryptographic infrastructure platform — not another cybersecurity product. The platform's three components work together to enable secure symmetric key distribution over the internet without relying on vulnerable public-key infrastructure:

Key Distribution Centers (KDCs)	Generate and distribute cryptographic keys to authorized users.
Secure Access Portal (SAP)	Authenticates devices and verified users before issuing keys for OTP encryption.
Developer SDK	Allows applications to integrate secure symmetric key delivery into their architecture.

Just as Amazon Web Services transformed computing by providing scalable cloud infrastructure, Symmetrics provides scalable cryptographic symmetric key delivery infrastructure for the internet — a trusted encryption layer that any organization can integrate directly into its systems. Applications include secure enterprise networks, identity and access management, encrypted messaging platforms, data center protection, and blockchain and digital asset security.

Why Infrastructure Platforms Become the Most Valuable Companies

Infrastructure platforms — Amazon Web Services, Cloudflare, Okta — become some of the most valuable companies in technology because they operate beneath entire ecosystems. Thousands of companies build on top of them. Symmetrics is building a similar layer, this time for encryption and secure key distribution that enables the most secure encryption system ever invented.

Identity Without Passwords: Traditional identity systems rely on passwords, user IDs, and long-lived credentials that can be stolen or compromised. **Symmetrics eliminates these vulnerabilities** by issuing true, ephemeral symmetric keys tied to authenticated devices with verified users — **removing the need for usernames, passwords, and trust certificates** entirely and making access control cryptographically enforced.

The Inevitable Future of Encryption: Quantum will break all Public Key Infrastructure

Three major forces are reshaping how digital systems must be secured:

Exploding Cybercrime	Global cybercrime losses are expected to reach \$23 trillion annually by 2027 (Kroll).
Quantum Computing Threats	CISA now requires federal agencies to procure quantum-resistant technologies, with compliance deadlines beginning January 1, 2027, for New National Security Systems.
Expansion of the Digital Economy	AI, cloud infrastructure, digital assets, and machine-to-machine communication are dramatically increasing the volume of sensitive data traversing networks — driving demand for permanent cryptographic protection.

Our Product Suite

Key Distribution Center (KDC):

At the core of our platform, the KDC generates and delivers symmetric keys to user devices running our Secure Access Portal (SAP) software. Rather than relying on hackable public-key infrastructure (PKI), the KDC provides keys based on true random numbers, deployable for less than \$50,000. IBM's 2025 Cost of a Data Breach Report found the average breach cost \$4.8 million — meaning a \$1 million annual investment that prevents just one breach saves \$3 million on average. The U.S. alone has 3,778 data centers, with nearly 3,000 more under construction.

Key Distribution Center (KDC) becomes critically important as Public Key Infrastructure (PKI) collapses in the quantum era. RSA, ECDSA certificates, TLS handshakes, and SSH keys will be 100% vulnerable. The Key Distribution Center relies entirely on symmetric keys, secure channels, controlled authentication, ephemeral session keys, and a centralized trust authority — and sidesteps the entire PKI ecosystem. It is not “patching” PKI — we are replacing it with a simpler, quantum-safe trust layer. The KDC will become the default quantum-proof cryptographic engine for VPN, Messaging, File Transfer, Access Control (passkey), Quantum-Safe Wallet Infrastructure, and more.

Quantum Protected VPN (QPN™):

VPN compromise is a critical and growing issue — over 2 million VPN passwords were stolen by malware in a single year, with 56% of organizations experiencing VPN-related attacks. The Symmetrics VPN eliminates this liability by protecting employee access to the enterprise cloud, ensuring strong device identity, and providing quantum-secure encryption of data in transit. Industry revenue is projected to grow from \$108 billion in 2026 to \$534 billion in 2034.

Our VPN solution - the Quantum Protected Network (QPN) - is built on Symmetrics' quantum-proof encryption, giving organizations a communication channel that remains secure even against future quantum attacks. Unlike traditional VPNs that rely on RSA, ECDH, and elliptic-curve handshakes vulnerable to Shor's algorithm, our architecture uses symmetric, read-once key exchange with no exposed public keys — eliminating the “harvest-now, decrypt-later” threat. Session keys are ephemeral, high-entropy, and never reused, meaning intercepted traffic cannot be decrypted today or decades from now. The result is a fundamentally more secure VPN: faster to establish, resistant to quantum cryptanalysis, immune to certificate compromise, and perfectly suited for zero-trust environments and critical infrastructure where long-term confidentiality really matters.

AuthAM – Authentication and Access Management:

AuthAM eliminates passwords and user IDs entirely — issuing, rotating, and enforcing ephemeral symmetric credentials for users and machines via a central identity and key management service. Access control becomes cryptographically enforced, dramatically reducing credential theft risk. Target markets include financial institutions, credit card companies, and any customer-facing business seeking to secure transactions from hacking.

Symmetrics' secure access platform brings quantum-proof protection to identity systems such as Microsoft Active Directory, passkeys, privileged accounts, and zero-trust authentication workflows. Traditional identity protocols depend on public-key cryptography: Kerberos tickets, certificates, and passkey signatures — which are all vulnerable to future quantum attacks and susceptible to “harvest-now, forge-later” threats. Our symmetric, read-once authentication eliminates this risk by replacing public keys with ephemeral, quantum-immune credentials that cannot be replayed or reconstructed. Each authentication event uses high-entropy, one-time verifiers issued by our KDC, providing unforgeable identity assurance for admins, servers, and endpoints.

Data-at-Rest Encryption:

Data-at-Rest ensures stored data never remains in decryptable form without active authorization. Keys are never co-located with data, client-side encryption uses ephemeral keys stored in a separate secure KDC, and even if storage is compromised the ciphertext remains useless. This eliminates centralized key repositories and mitigates “harvest now — decrypt later” attacks.

Symmetrics Cloud:

Symmetrics Cloud will bring the entire platform together into a single managed infrastructure layer that runs Symmetrics encryption everywhere — protecting data in transit and data at rest across an organization’s full environment. Access to the infrastructure is gated by the Symmetrics Quantum-Protected VPN, so every connection in and every session within is secured end-to-end with quantum-proof symmetric encryption, closing the door on harvest-now, decrypt-later attacks. Instead of integrating encryption service by service, organizations deploy their workloads directly onto Symmetrics Cloud and gain quantum-secure protection by default — the same trusted key-distribution layer that powers the rest of the platform, delivered as infrastructure. Built to meet the certification standards that regulated enterprises and federal agencies require, Symmetrics Cloud will give institutions a direct deployment path for their post-quantum migration ahead of the federal deadlines.

Intellectual Property: Independently Valued at Up to \$1.7 Billion

In September 2026, Symmetrics’ IP portfolio was independently valued by AiPi Solutions (www.aipisolutions.com), a specialist patent valuation and litigation firm, at between \$868 million (conservative scenario) and \$1,775M (bull case) — driven in large part by the acceleration of the quantum computing threat, which renders Symmetrics’ OTPSK technology uniquely positioned. The full 136-page IP report from AiPi is available upon request.

“It would be highly unlikely that Symmetrics’ patents would be sold for less than \$868 million.”

— Eric Morehouse, Founder & Managing Director, AiPi Solutions

Contact Us

Jim Garrity, SVP, Growth — Jim.Garrity@symmetrics.com
Michael Portera, SVP, Investor Relations — Michael.Portera@symmetrics.com
Drew Davis, SVP, Strategy & PR — Drew.Davis@symmetrics.com

[Symmetrics.com](https://symmetrics.com)