Trellix

Navigating the Shift to Post-Quantum Cryptography

Secure Your Data by Implementing Quantum Resistance

By Tim Schooley and Laurie Robb

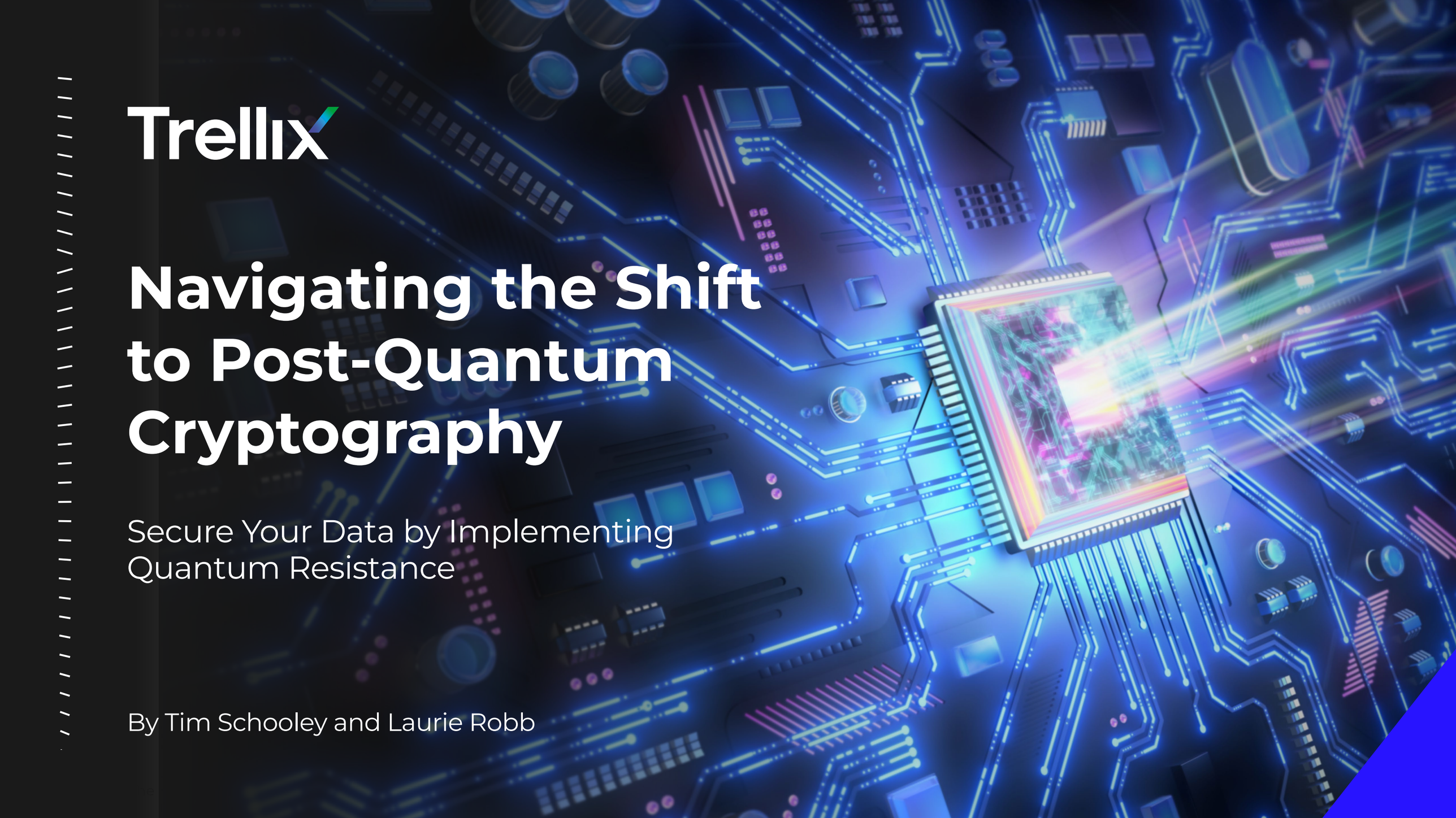


Table of Contents

The digital age is on the verge of a profound change driven by advances in quantum computing. While this will lead to many promising breakthroughs, these machines also pose a threat to the encryption that protects our data from threats. To address these risks, understanding and preparing for Post-Quantum Cryptography (PQC) is vital. Let's examine the fundamentals of PQC, why it's urgent to act now, how organizations can start preparing today, and the support that Trellix® experts and technology solutions can offer for your transition.

Q-Day: The Uncertain Horizon and Your Sensitive Data

Quantum computers, using qubits that leverage quantum mechanics like superposition and entanglement, can perform calculations far exceeding classical capabilities, thereby threatening current cryptographic standards. You may have heard the term "Q-Day," which has emerged recently among security professionals. Q-Day marks the day when a quantum computer could break today's standard encryption.

Q-Day's exact timing is unknown. It could be several years, more or less. Yet the risk to your data is present now. Adversaries might be engaging in "harvest now, decrypt later" (HNDL) attacks, collecting your encrypted sensitive data, such as customer PII, financial records, or intellectual property, today, to decrypt it once powerful quantum computers emerge. While the viability of this threat depends on the long-term value of the harvested data, some of the most valuable information today will retain its value far into the future. Information that remains critical for decades, such as national security secrets or foundational intellectual property, is at a higher risk than other data, including names, addresses, and phone numbers that might change.

Adversaries might be engaging in "harvest now, decrypt later" attacks.

60%

of security professionals surveyed believe Q-day will happen within a decade[1]

65%

Around two-thirds of organizations are concerned about the rise of "harvest-now, decrypt-later" attacks[2]

[1] TechRadar, 2025
[2] Ibid

The potential for future breaches of currently secure confidential or restricted data makes the move to PQC urgent for data with enduring sensitivity. It also reinforces that organizations must place a continued emphasis on current data protection programs that prevent exfiltration and monitor for potential leakage in real time.

How Quantum Algorithms Threaten Our Encryption

Two main quantum algorithms challenge our current cryptography:

1. **Shor's Algorithm targets asymmetric cryptography like RSA and Elliptic Curve Cryptography (ECC).**

Shor's algorithm directly threatens asymmetric algorithms (RSA, ECC, Diffie-Hellman). It can efficiently solve the mathematical problems they rely on, rendering them insecure against a sufficiently powerful quantum computer. Both RSA and ECC, despite their different mathematical underpinnings, will require replacement.

2. **Grover's Algorithm affects symmetric cryptography like Advanced Encryption Standard (AES).**

Symmetric algorithms such as AES are at risk from Grover's Algorithm. Unlike Shor's Algorithm, which targets specific mathematical problems, Grover's Algorithm is a generic quantum search algorithm. Imagine you're searching through a vast, unsorted list—like all the possible encryption keys for AES—to find the one correct key. Traditionally, you'd have to check items one by one, on average, getting through half the list. Grover's Algorithm offers a significant quadratic speedup. It can find the correct item in roughly the square root of the total number of items. For a key with "n" number of bits, there are 2^n (squared) possible keys. Grover's reduces the search effort to approximately 2^n divided by 2 quantum operations, effectively cutting the strength of the symmetric key in half.

$4.88 million

The average global cost of a data breach reached $4.88 million in 2024, a 10% increase over the previous year[3]

[3] IBM Cost of a Data Breach 2024 report

Let’s look at two examples:

- AES-128 security is reduced to 64-bit strength by Grover’s. This would be ineffective protection against quantum adversaries in the long term.
- AES-256 offers a more robust option. Even reduced to 128-bit strength by Grover’s, it remains formidable and offers strong security against known quantum attacks. It is the current standard for quantum-era symmetric encryption.

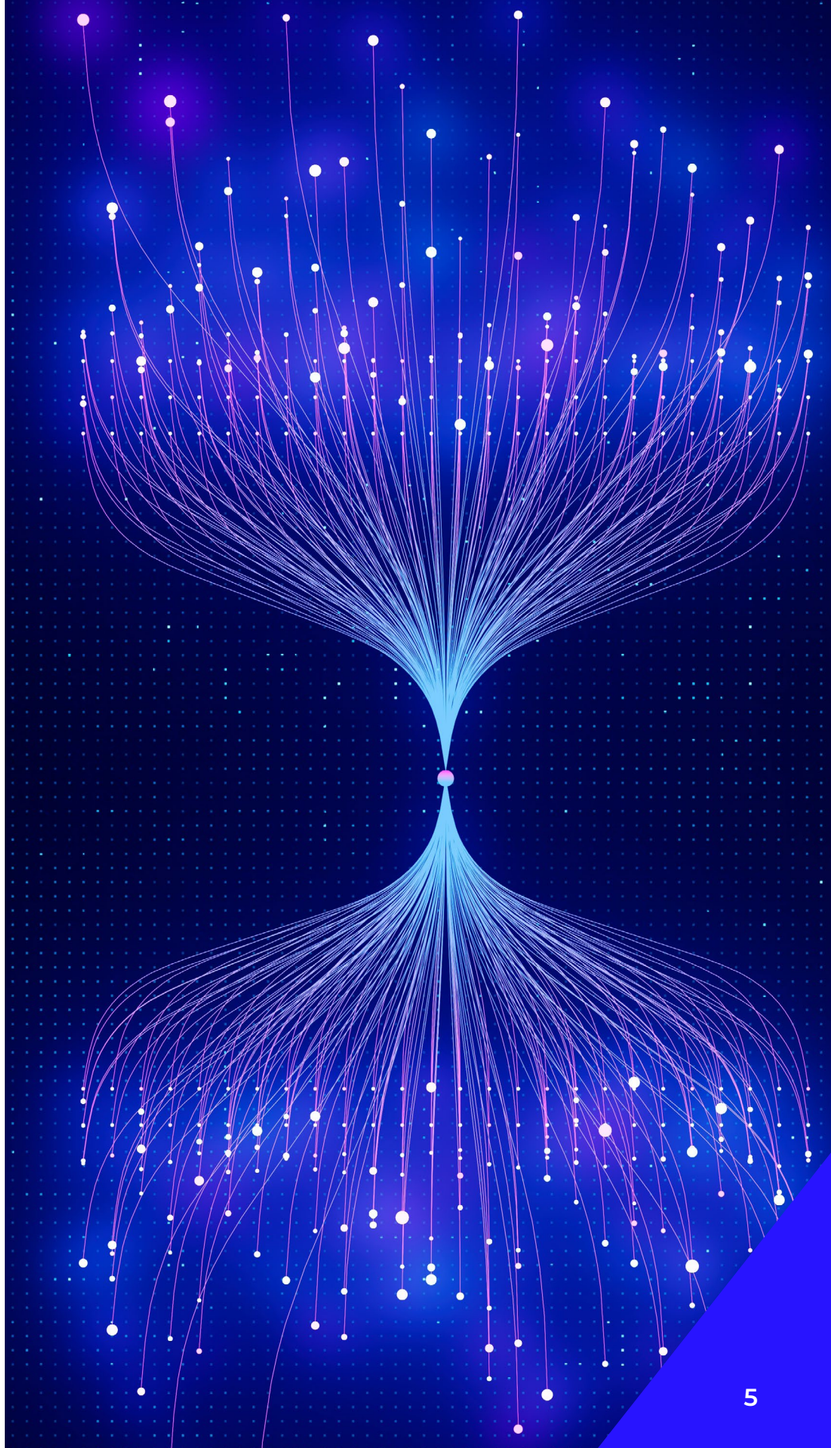
Building Quantum-Resistant Asymmetric Cryptography

Our current, widely used asymmetric cryptography solutions, such as RSA and ECC, rely on mathematical problems, such as factoring large numbers or solving the elliptic curve discrete logarithm problem. For decades, these problems have been considered too difficult for classical computers to solve within a reasonable timeframe, forming the bedrock of our digital security.

For decades, these problems have been considered too difficult for classical computers to solve.

Shor’s Algorithm changes this landscape by demonstrating that quantum computers can efficiently solve these specific problems. This capability effectively breaks the security of RSA and ECC in a post-quantum world.

PQC necessitates a shift to entirely different families of mathematical problems, ones believed to be hard for both classical and quantum computers to solve. A leading approach in this new era is “lattice-based cryptography.” New standards, like CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures, incorporate this new technique.



Instead of the problems that RSA and ECC use, these new algorithms derive their security from the presumed difficulty of certain complex tasks within high-dimensional geometric structures called lattices. These new mathematical foundations were chosen because they do not appear to possess the kind of structure that Shor's algorithm can exploit, making them strong candidates for building quantum-resistant security.

Crypto Agility: Adapting to an Evolving Landscape

Cryptographic agility (also known as crypto agility) is the ability to efficiently update cryptographic algorithms without significant disruptions to processes or operations, which is crucial as PQC standards mature. Implementing this capability involves more than just swapping algorithms. It starts with a thorough cryptographic inventory and strategic research to understand the landscape of vulnerable algorithms and the most effective transition to adequate protection.

Together, Trellix and wolfSSL are actively working toward FIPS 140-3 validation.

Trellix's Data Encryption team embarked on an in-depth inventory of our applied cryptography in mid-2023. This foundational work evolved into an exciting collaboration with wolfSSL to integrate cutting-edge PQC into our data encryption product line, including both our Drive Encryption and File & Removable Media Protection products. Renowned for its lightweight, portable, and high-performance cryptographic library, wolfSSL offers broad support for emerging PQC algorithms. Together, Trellix and wolfSSL are actively working toward validation for FIPS 140-3 for wolfSSL's cryptographic module, specifically for the Unified Extensible Firmware Interface (UEFI) environment. FIPS is one of the most widely accepted standards for cryptography compliance, especially in the public sector, supply chain, and other regulated industries. Through this initiative, we plan to bring robust, certified PQC security to the foundation of Trellix Drive Encryption, where authentication occurs at the time of system boot.

Agility means your key management systems (KMS) will need to support new PQC key types, and protocols must integrate new PQC cipher suites. Ensuring compatibility with hardware, such as smartcards, will also be expected. Since PQC is still developing, agility provides an insurance policy against future threats and allows you to adopt the best-performing PQC algorithms as needs evolve. Organizations can take necessary steps now, including designing systems with cryptographic abstraction layers and collaborating with encryption vendors on their PQC roadmaps.

PQC Standards Take Shape, But Evolution Continues

The U.S. National Institute of Standards and Technology (NIST) is leading PQC standardization. Through rigorous evaluation rounds, NIST has selected key algorithms to form the backbone of this new cryptographic era. Algorithms selected in its initial rounds include the lattice-based CRYSTALS-Kyber (ML-KEM) for key establishment and CRYSTALS-Dilithium (ML-DSA) for digital signatures, alongside the hash-based SPHINCS+ (SLH-DSA) for digital signatures as well.

Awareness of these initial standards is key for future planning. It is also important to recognize that the PQC landscape will continue to evolve, potentially with further standardization efforts or updates as research progresses and real-world deployment experience grows.

<50%

Less than half of organizations are actively preparing for the post-quantum threat, with over one-third lacking the necessary scale or technology to transition to PQC[4]

30%

Only 30% of organizations currently allocate budget specifically for PQC readiness[5]

[4] Entrust Cybersecurity Institute, 2024
[5] DigiCert Global Study, 2023

Planning for a Quantum-Resistant Future

We anticipate a phased transition to PQC for most organizations over the next five years. This methodical approach is essential to minimize disruption and manage risk. A measured strategy also allows new PQC algorithms to gain valuable “soak time” in real-world deployments and for security organizations to gain crucial buy-in from stakeholders needed to support the transition. This time will also ensure that security professionals can identify and address unforeseen implementation issues before legacy systems are fully retired.

Trellix Data Encryption experts will help our customers identify their most critical data, assess cryptographic dependencies, and strategically integrate PQC solutions into existing infrastructure. Customers can expect crypto-agile solutions coupled with expertise to make their transitions both smooth and secure.

We also plan to phase out legacy asymmetric cryptography vulnerable to quantum attacks in Trellix solutions in the next 10 years. In that time, we anticipate that the new PQC standards will be mature, and implementations will be well-tested. Symmetric encryption, such as AES-256, will likely remain a fundamental component of secure systems. Our objective is a fully quantum-resistant security posture, and customers can count on us for ongoing vigilance and to adapt to new standards as needed.

Final Thoughts on the Shift to Post-Quantum

The shift to Post-Quantum Cryptography is a significant undertaking and a necessary one. Trellix experts are ready to help customers navigate this transition, ensuring their most sensitive data remains secure against today’s threats and the quantum challenges of tomorrow. Contact us for more information on Trellix Data Encryption or to be connected with one of our solution experts to begin planning for your transition to a quantum-resistant future.

About the Authors

Tim Schooley
Technical Product Manager
Trellix Data Encryption

Tim Schooley has dedicated his entire 18-year career to the mission of keeping customer data safe, consistently contributing to and driving innovation within what is now Trellix's Data Encryption portfolio. With a background in computer science, he leverages his deep knowledge of building secure systems to guide product evolution as a Technical Product Manager. He navigates the complexities of modern cryptography, like post-quantum standards, and adapts to dynamic regulatory environments. Tim frequently bridges the technical and business realms, ensuring solutions are both forward-looking and grounded in real-world operational requirements.

Laurie Robb
Director, Product Marketing
Trellix Data Security

Laurie has more than 25 years of experience in marketing communications across a variety of industries including cybersecurity, SaaS, technology management, and healthcare. At Trellix, she leads Product Marketing for Data Security, translating complex technical concepts into clear, compelling stories that fuel engagement and growth. She frequently writes about and presents on data security industry topics, delivering high-impact messaging and content that bridges the gap between technical and business audiences. She is passionate about simplifying complexity, helping cybersecurity companies stand out, and understanding customer challenges. Laurie is also a proud member of the leadership team for Women in Cybersecurity Northeast Ohio affiliate.

Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's comprehensive, open and native cybersecurity platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through artificial intelligence, automation, and analytics to empower over 50,000 business and government customers with responsibly architected security.

More at *www.trellix.com*
Follow Trellix on *LinkedIn* and *X*.