CIGENT
AlwaysPROTECTED™

Quantum Attack Protection

Beyond Tomorrow: The Urgent Reality of Quantum Computing Risks

Quantum computing isn't a distant future threat to your encryption. It is an imminent threat, if not tomorrow or next week or even next year, but soon enough and sooner than you think.

Some have created a countdown clock, a "years to quantum" or Y2Q clock, currently set for April 14, 2030. The specificity of that date is deceiving. No one knows the month, date, year, or even decade when that milestone will be met. The fact is that quantum computing, which can break today's most sophisticated algorithms, is coming soon.

Thankfully, you can protect your data here and now.

Whether from adversarial nation-states or well-funded criminal operations—or a combination of the two—the quantum threat is very real. Threat actors are capturing as much encrypted data as they can today in hopes that in the future—possibly the very near future—they will have the cryptanalytically relevant quantum computers (CRQCs) and the ability to break the encryption keys and gain access to them.

Understanding Basic Quantum Computing Concepts

To understand the quantum threat to encrypted data, it helps to have a basic understanding of quantum technology in the computing field.

Quantum computing takes a vastly different approach to defining and manipulating information compared to traditional computing.

- Quantum computing does not code data in a binary on or off, one or zero "bit" of information. Instead, it uses a "qubit," which can be either on or off or both at the same time—or in various in-between states.
- The state of a qubit at any moment is a probability, not a fact. It is a phenomenon known as "superposition."
- Add in the idea of "entanglement." Qubits are interconnected. That means the state of any one of them cannot be described without considering the state of the others.

These innovations are how quantum computers achieve speeds and efficiencies that classic binary machines cannot begin to match. Breaking current cryptosystems is conceptually easy work for a quantum computer. Peter W. Shor, a professor of applied mathematics at the Massachusetts Institute of Technology, published a paper in 1997 outlining the theoretical method, now called Shor's algorithm, that quantum computers could use to break any code.

From the first quantum computer made in 1980 to the first algorithm to break RSA encryption to the experimental machines in government and private labs, quantum computing science is making quantum leaps forward. Advances are coming faster and faster. It is only a matter of time before encryption as we know it today becomes useless.

How Quantum Computing Affects Encryption

Quantum computers make the "harvest now, decrypt later" strategy feasible. It is a bet that is quite likely to pay off sooner rather than later. Exfiltration cyberattacks, where encrypted data is scooped up and stolen in volume, are increasingly common as a result.

Encryption is the practice of turning data into random and unreadable strings of characters or code, turning plaintext into ciphertext. Current encryption methods use complex mathematical formulas to transform data and encrypt it so that it is unreadable. To then decrypt the ciphertext and transform it back into readable plaintext, you need a decryption key.

The complexity of the mathematical formulas used to encrypt and decrypt data is what has traditionally protected data. The idea is that no one has the computing power to take on that complexity in a practical or timely manner.

Quantum computers eat complexity for lunch.

It would take hundreds of trillions of years for a traditional computer to break the 2,048-bit Rivest-Shamir-Adleman (RSA) system, which is based on two large prime numbers. In theory, a quantum computer could break that key in seconds. Even the newer Advanced Encryption Standard (AES) encryption key that uses a series of linked mathematical operations and is now the U.S. government standard is susceptible to quantum computers.

Responding to the Quantum Computing Threat

The U.S. government is taking quantum computing seriously. The National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems outlines the key steps agencies should take to maintain U.S. leadership in quantum information science, mitigating encryption risks, protecting U.S. technology, and more.

The U.S. National Institute of Standards and Technology (NIST) is also developing post-quantum cryptography (PQC) protocols and standards now. Your organization should similarly take steps now for the post-quantum future. You don't need to wait for tomorrow's technology to adopt a strong protective stance today.

Lines of Defenses and Layers of Protection

The first line of defense in protecting your data from quantum cypher breakers is to keep data out of their hands in the first place.

Threat actors are attacking federal agencies and defense organization systems all day and every day.

Attacks can target everything, from large data centers to devices on the edge, including PCs, laptops, servers, and removable media, a multitude of other device types, including IOT, OT, manned, and unmanned vehicles. Devices operating on the edge, in insecure environments, are particularly at risk as they are vulnerable to adversaries gaining physical control and rely heavily on encryption to protect data at rest.

The layers of protection from Cigent keep threat actors from accessing your data on these devices. Using several technologies together dramatically reduces the risk to your data. These include:

- **Pre-boot authentication (PBA) mechanisms.** Any device is vulnerable to attack in the window between power-on and when the boot loader begins initialization. Requiring pre-boot user authentication in the BIOS, UEFI, or the device boot loader creates a secure environment that is external to the device operating system. It closes this vulnerability by requiring a user to enter a password or PIN, security token, or biometric data before the device decrypts the disk and the operating system proceeds to load.

- **Multifactor authentication (MFA).** Deploying MFA protections verifies the identity of a user with technologies that go beyond a simple username and password combination. The more secure MFA methods to verify identity and keep threat actors from accessing data include:
  - **Hardware tokens:** Employ physical devices that generate a one-time password (OTP) or code to verify identity and unlock a device.
  - **Biometric user authentication:** A physical attribute of an authorized user, such as an iris scan, fingerprint, or facial recognition, which can reliably verify identity.
  - **Push notifications:** Sending a prompt to a registered device that a user employs to approve or deny an entry attempt is a user-friendly MFA method.
  - **Public key infrastructure (PKI):** A cryptographic key that is stored on a smart card that a user inserts along with a pin is commonly used.

- **Secure hidden partitions.** Store sensitive data in a hidden partition, generating enclaves that an adversary cannot discover—and that makes it impossible for the adversary to even know the data exists. The hidden partitions are unreadable at the sector level. Even if an adversary gets direct physical or remote access to a device and is able to log in, the partition and the data in it are not discoverable unless unlocked using further step-up authentication.

- **Secure SSD Plus AI software and non-recoverable keys.** Protect data on any operating system with patented software that offers full disk encryption, verified full drive erasure, real-time threat detection and response, and secure logs that capture all insider threat activity. The SSD software's proven methodology creates and stores encryption keys and then uses advanced algorithms to deconstruct and distribute the keys throughout the drive. Embedded AI protection monitors data access patterns and can automatically activate protective measures when tampering is detected.

- **Tamper-resistant measures.** These technologies provide physical data protection. When tampering is detected, such as when sensors detect voltage or temperature changes, or when movement is detected, data is zeroized. Physical destruction of data and devices is also possible.

- **Advanced threat protection**. Cigent takes a comprehensive security solution designed to detect, prevent, and respond to sophisticated cyber threats. Our ATP approach employs multi-layered tactics that use behavioral analysis, machine learning, and real-time threat intelligence to protect your systems and data from advanced malware, ransomware, and phishing attacks.

- **Verified data erasure**: The only way to unequivocally ensure that an adversary cannot access sensitive data is to eliminate the data. The impact of quantum computing is not entirely known. Adopting a rigorous data sanitization approach ensures that regardless of future technical capabilities the data is not retrievable.

- Studies have consistently demonstrated that standard industry best practices do not effectively ensure the erasure of all data. Cigent provides patented capability to verify data erasure with block-by-block analysis. Block-level inspection ensures that all data has been properly sanitized. Cigent verified data erasure provides an alternative to physical drive destruction with a simple, efficient approach that can be applied in emergency situations or where physical destruction is not an option. With the confirmation of data sanitization, the risk of compromise is eliminated, and drives may be re-purposed or recycled.

The Importance of Compliance

Complying with the various standards and mandates is not about jumping through bureaucratic hoops. Adopting solutions that have been rigorously tested and validated is the only way to ensure that any solution works as promised. When it comes to protecting your data, good enough is nowhere near good enough.

Cigent solutions comply with requirements from NSA, DISA, NIST, MITRE, NIAP, the Air Force, Cyber Resilience of Weapon Systems, and the UK's NSSIF, among others. They also meet FIPS 140-2 and 140-3 standards and address EO 14028 encryption mandates.

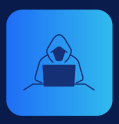
Call us for more info

CIGENT
AlwaysPROTECTED™

Leading the Way on Quantum-Resistant Cryptography

While preventing data access is the first line of defense and adopting a layered approach that relies on multiple protections, both tilt the odds in your favor, the reality is that we need to stay a step ahead of our adversaries. That is especially true when adversaries can harness the speed and power of quantum computing.

That is why Cigent invests in post-quantum cryptography. We are hard at work on cutting-edge technologies for securing vital systems, data, and communications in a quantum computing future.



Staying Ahead of Threat Actors

While it is easy to look at quantum computing as a threat, it is also an opportunity. Quantum computing empowers new methods and strategies for protecting data and systems.

Cigent is a leader in securing data across platforms because we pursue opportunities for innovation with as much vigor as we work to protect your data. Indeed, we are revolutionizing data protection with unique security solutions that guard against sophisticated cyber threats and data capture.

Our team of advanced data recovery, storage, and cybersecurity experts are already working on “next-gen” and proactive approaches to keep your organization, data, systems, communications and equipment as safe as possible.

Prepare Now for the Quantum Future

While many experts see quantum-based cryptography and quantum encryption cracking as being many years in the future, a breakthrough can occur at any moment and in any place—perhaps at the hands of adversaries.

Adopting effective layers of data protection and working with providers who are driving quantum-resistant and quantum-proof approaches to cryptography are two of the best ways to prepare today for the quantum future. We invite you to schedule a conversation today.