Case study: Quantum-grade privacy for up to 3 million internet users

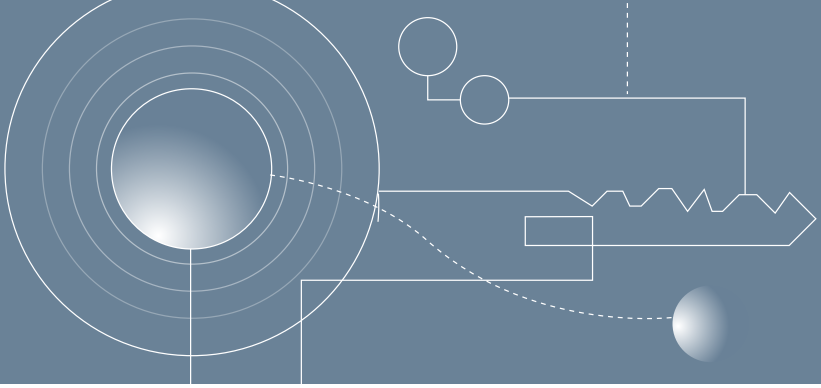
PureVPN and Quantinuum take first step towards quantum-resilient infrastructure

QUANTUM
ORIGIN

QUANTINUUM

PureVPN is a global virtual private network provider with customers in 78 countries. It places a premium on its users' privacy and data integrity. It had become increasingly concerned by cyber attacks and the threat to encryption posed by quantum computers. PureVPN wanted a way to take the cyber protection of its 3 million internet service users to the next level.

They identified Quantum Origin as the right first step towards quantum-resilient infrastructure.



The strongest encryption keys

The most valuable data demands the strongest protection. PureVPN considers its users' privacy and the integrity of their data to be of the utmost value. This led PureVPN to begin a search for technological solutions that could help them not only to offer the strongest cryptographic protection, but to build out a broader quantum-resilient infrastructure.

Quantum Origin is Quantinuum's cryptographic key generation platform. It generates the strongest encryption keys on the planet, keys which are not susceptible to being broken by quantum or any other future computing technology.

Act fast

PureVPN was focused on addressing its concerns as quickly as possible. It took only three weeks from the moment PureVPN first identified Quantum Origin as a candidate technology, to the time the solution was implemented.

Ultimately, the partnership enables PureVPN to continue growing in existing markets while differentiating itself from a technology standpoint relative to other companies in the network security industry.

The Challenge: Protecting digital privacy in a quantum future

PureVPN's mission is to provide secure, transparent, and cost-effective solutions for customers to browse the internet safely and anonymously across an array of systems and browsers. It transmits data for over three million users globally, using more than 6,500 servers across 78 countries.

PureVPN recognizes increasingly sophisticated cyberattacks put pressure on the encryption layer in any cybersecurity stack. In addition to this, quantum computing is beginning to fundamentally change the security landscape by threatening the secure transmission of information.

Bad actors are recording confidential and valuable data today to decrypt in the future. Some experts such as Sundar Pichai of Google and Michele Mosca of the University of Waterloo say quantum machines will be powerful enough to break current encryption standards this decade[1]. Once that happens, encryption algorithms such as RSA, ECDSA, DSA, and Diffie-Hellman will be exposed. They are vulnerable to this threat, often referred to as "hack now, decrypt later".

PureVPN needed a cryptographic technology that would provide the first step to strengthening their users' cyber protection today and in the future.

[1] *https://www.bcg.com/publications/2021/quantum-computing-encryption-security*

The Solution: Strengthening security using quantum-enhanced cryptographic keys

Quantinuum's cybersecurity product, Quantum Origin, draws on the operations of a quantum computer to generate the strongest encryption keys ever designed. These keys answer the immediate threat of weak encryption, which can be exploited by increasingly sophisticated cyber attackers. Ultimately, the cryptographic keys support PureVPN's longer-term objective to offer a quantum-resiliency solution while delivering best-in-class service to its customers.

Benefits:

- PureVPN generates encryption keys through a simple API call request
- The product seamlessly integrates with PureVPN's existing security infrastructure
- In roughly five weeks, Quantinuum and PureVPN were able to assess various aspects of the deployment such as:
    - the CPU load on end-devices
    - rise in handshake ratios
    - browsing experience deterioration
    - diverse network compatibility, prior to eventual implementation
- It is future-proof. Quantum Origin is ready for the post-quantum algorithms finalized by the US National Institute for Standards and Technology (NIST).

"By partnering with Quantinuum, our customers can browse the internet, confident their data is getting quantum-grade protection. Quantum Origin has been very well designed to plug into existing infrastructure, without requiring substantial investment in hardware, software or quantum computing knowledge. The platform is flexible, allowing us to reliably request the strongest cryptographic keys on the planet, even as we scale our offerings. Quantum Origin was a critical part in our move to quantum-resilient cybersecurity." *-Uzair Gadit, co-founder and CEO of PureVPN*

The Results:
Enhanced security for up to 3 million users and a 40% increase in sales enquiries

PureVPN has been able to maintain its service to enterprise and consumer customers, while bolting on a quantum-resilient security solution for its three million users. In addition, PureVPN has fortified its position as a powerful, stealthy, and speedy provider. Keys from Quantum Origin now protect PureVPN's customers in the US, UK, Australia, Canada, Germany, and the Netherlands across all supported platforms, operating systems, and devices.

"Since partnering with Quantinuum, we have rolled out Quantum Origin-derived cryptographic keys across 95% of our infrastructure with the remainder to be rolled out in the coming weeks. This new capability has directly translated to a 40% uptick in sales inquiries."

PureVPN's deployment of Quantum Origin sends an unambiguous signal about their commitment to digital privacy and data integrity. Since deployment in March, PureVPN has seen a rapid rise in user numbers on their Android platform. In fact, the total unique number of Android OpenVPN users grew by 67.5% between April and June.

Thanks to its plug-and-play design, Quantum Origin's deployment did not require substantial reskilling, hardware or software upgrades, or the need to establish any in-house quantum computing capability.

Gadit also remarked: "As one of the leading VPN service providers, we take the security of our users too seriously to rely just on mere speculation on when, not if, quantum technology will advance or completely destroy privacy. When quantum computers raise the stakes between codemakers and codebreakers, we want to be on the right side of history, or in this case, the future."

Technological deep-dive: The quantum threat to encryption

1 Quantum computers will break current encryption standards.

Many of the encryption systems we use today are based on a special family of mathematical problems which are easy to solve in one direction but intractable in the other. As an example, RSA is a popular algorithm for encrypting internet data and for digitally signing transactions. RSA relies on multiplying very large numbers. This is trivial for any ordinary computer. However, the reverse is effectively impossible because it would take an unreasonable amount of time to find the solution. We're not talking minutes here; we're talking thousands of years using even the world's fastest high-performance computers.

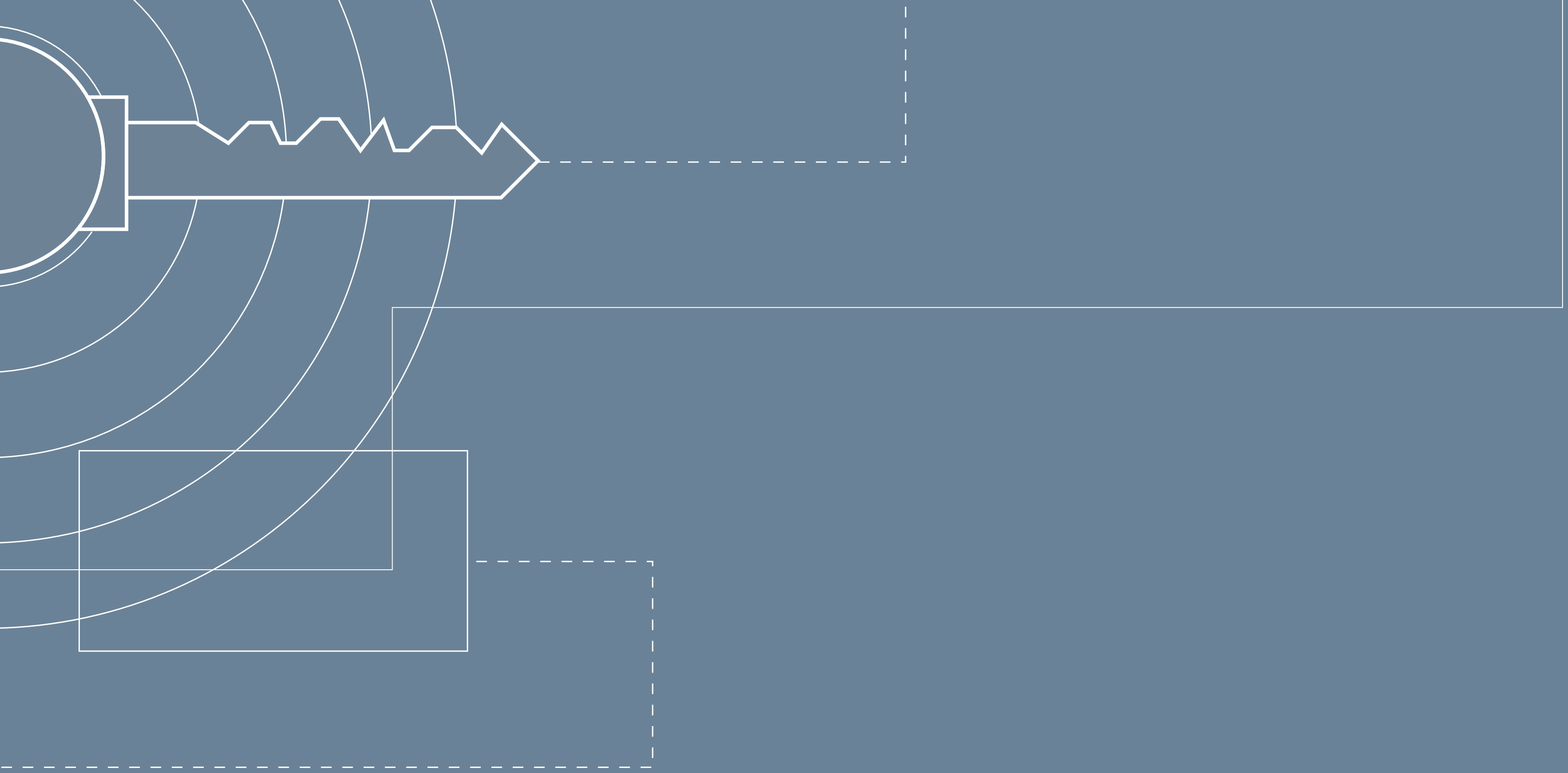
Quantum computers work differently. A powerful and stable quantum computer running an algorithm called Shor's Algorithm would be able to find the two numbers that were multiplied together in a reasonable amount of time. This means an attacker with a powerful quantum computer could read data encrypted using an RSA public key or forge transactions signed by an RSA private key. This completely breaks the bedrock of our cybersecurity systems. To defend against these threats, a competition has been underway for six years by NIST to find new post-quantum algorithms for which there are no known quantum attacks.

Today such a quantum computer does not exist, but they are expected to be developed within 5-10 years.

2 What is hack now, decrypt later?

"Hack now, decrypt later" describes an attack where adversaries record encrypted data as it passes through networks and store it for future decryption once powerful quantum computers become available. It is believed hack-now, decrypt-later attacks have already commenced. In fact, data that is continuously being transmitted around the world continues to rely upon quantum-vulnerable algorithms.

For any company who shares data like financial, health or social security information with a long sensitivity lifespan, this is a real concern. When an advanced quantum machine is available, organizations who have taken a proactive stance to employ quantum-resilient encryption and systems by being crypto-agile will be ahead of the security curve. Quantum Origin strengthens existing cybersecurity and supports NIST post-quantum algorithms when organizations are ready.



Quantum Origin generates the world's strongest encryption keys.

To learn more about strengthening your cybersecurity with Quantum Origin, please get in touch: origin@quantinuum.com

QUANTUM
ORIGIN

QUANTINUUM