

# VeriQloud: Protecting data in the quantum era, today and tomorrow

*What happens when quantum computers break public key encryption? VeriQloud, a leader in data security, can help keep our data secure—now & in the future.*

CALGARY, AB, CANADA, June 23, 2026 /EINPresswire.com/ -- In today's digital age, nearly all our personal information is transmitted and kept online in some form of electronic format. Names, addresses and birth dates, medical histories, bank accounts, even intellectual property-sensitive data that is mainly secured through public key encryption methods, such as Rivest-Shamir-Adleman (RSA).

As quantum technologies advance, today's encryption methods based on complex mathematical algorithms are at risk of obsolescence, and there is growing urgency to find new tools to keep our information safe. Recent developments in quantum technologies suggest that the first quantum computers could be just five to ten years away from being realized; when this happens, data becomes easily accessible by a quantum computer capable of breaking current classical and encryption methods in a matter of seconds.


Enter [VeriQloud](#), a cybersecurity company founded in 2017 in Paris, France, and has since expanded to offices in North America (Canada). VeriQloud provides timely solutions to secure digital information and communication in a quantum world, where quantum computers are powerful enough to break existing encryption methods.

Didier Guignard, VeriQloud's head of business and research development in North America, predicts that, "Rather than a household item, quantum computers will be high powerful



**3 Types of Data Security**  
VeriQloud's Quantum-Safe Approach

- Data at Rest**  
Qasmat  
Splits data into shares stored across multiple locations. No encryption keys needed — rebuilding requires a minimum number of shares defined by you.
- Data in Transit**  
Qline  
Secures data traveling between systems using Quantum Key Distribution (QKD). Fully open, flexible, and customizable to each client's infrastructure.
- Data in Use**  
QEnclave  
Protects data during computation — even from the computer itself. Based on blind quantum computation protocols for secure quantum cloud computing.

 VeriQloud

VeriQloud's encryption solutions for post-quantum data security

processing units accessible via clouds. When we are sending data to the cloud, we want to make sure that it is secure from any unintended recipients and from the quantum computer itself.”

VeriQcloud is a leader in the data security space, starting with quantum-safe solutions that can be deployed on today’s classical digital infrastructure.

There are three main categories of data to consider when it comes to data security solutions: data at rest, data in transit, and data in use.

#### Data at rest

VeriQcloud takes a unique approach for data at rest, meaning data sitting in storage. The solution they offer, named Qasmat, consists of splitting the data into pieces or shares, and then after applying a classical encryption protocol, push them to several locations such as data storage servers or clouds.

Didier Guignard explains: “When a third party wants to get to your original data, it doesn’t exist as a whole anymore as it has been split into shares that are stored in multiple locations. They need to know where the shares are, and need to have access to at least a minimum number of shares to be able to rebuild your original data. This minimum number of shares can be fully definable by you, the client, as an end user. The more you want to protect your data, the more shares you generate to prevent the rebuilding of your original data.”

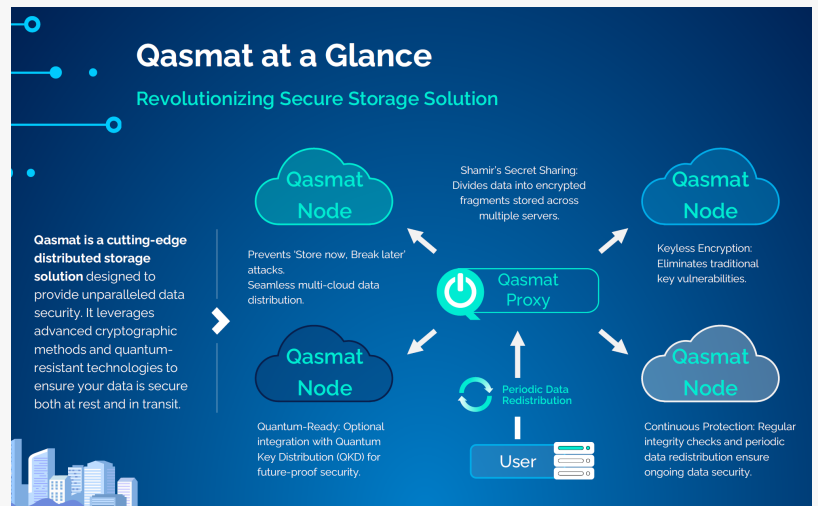
Splitting up shares of data gives time to detect unwanted access to the first server location and put action in place to stop the third party before the other shares can be located.

**“Rather than a household item, quantum computers will be high powerful processing units accessible via clouds.”**

➤ **Didier Guignard**  
Head of Business and Research Development in North America  
VeriQcloud

VeriQcloud

VeriQcloud - a leader in post-quantum data security.



VeriQcloud's Qasmat data security solution for encrypting data at rest.

Qasmat's solution offers the key advantage of not relying either on encrypted keys—often difficult to securely manage and maintain—or on classical, complex mathematical techniques that may be vulnerable to future quantum attacks.

#### Data in transit

Data in transit refers to data that is actively traveling between systems or devices. VeriQloud keeps such data protected by secure communication through Qline, which offers the highest level of cryptographic protection through Quantum Key Distribution (QKD).

Qline is unique as a fully open and flexible system. Its components can be customized, allowing optical, electronic or software elements to be replaced or adjusted to suit each client's specific needs and use cases. "The power of customization has been proven in action," says Didier Guignard. "VeriQloud implemented a solution to work seamlessly with Deutsche Telekom's wavelength-division multiplexing (WDM) system, integrating QKD into an operational metropolitan fiber-optic network without overhauling infrastructure."

#### Data in use

Finally, there is data in use, meaning data fed to or resulting from performing computations. Securing data in use protects the information from the computer itself. VeriQloud is actively researching this area, recently introducing QEnclave, a practical solution for secure quantum cloud computing based on blind quantum computation protocols.

VeriQloud is a pioneer in that area since CEO and co-founder, Dr. Elham Kashefi, in collaboration with Anne Broadbent and Joseph Fitzsimons, invented the first ever [Universal blind quantum computation](#) (UBQC) protocol which allows a client to have a server carry out a quantum computation for them such that the client's inputs, outputs and computation remain perfectly private.

"QEnclave, a solution inspired by UBQC, creates a trusted environment where the user's data and algorithm are not accessible to anyone, or to any system, including the server that is being used to compute the user's data," explains Didier Guignard. "While still in its infancy, we are excited about QEnclave and this promising area of research."

#### What now: The importance of data security

It's critical to secure sensitive data now, before quantum technologies advance to the point where classical encryption is easily breakable. Currently encrypted data can be "sniffed" or stolen from a server, and although a third party may not be able to access the information now, they have it on file and will be able to break the encryption in the future once they have the ability to do that using quantum technologies ("[Harvest Now, Decrypt Later](#)").

The fact that data can be stolen and stored now and broken into later is an eye-opening reality that requires immediate action to prevent it from happening. So, what's next?

Didier Guignard recommends that the first step for an organization to ensure the security of their data is to conduct a full data inventory, including hardware and software infrastructure, to gain a complete picture of what sensitive data there is, how it is stored, transmitted and used. Next, a plan for protecting the data can be put in place—one that will use existing and future technology and be prepared for the quantum future.

With advancing technologies and the evolving quantum landscape, VeriQloud can support this process and propose solutions to protect data in the quantum era, today and tomorrow.

Katanya Kuntz

Qubo Consulting Corp.

katanya@quboquantum.com

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/921613714>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.