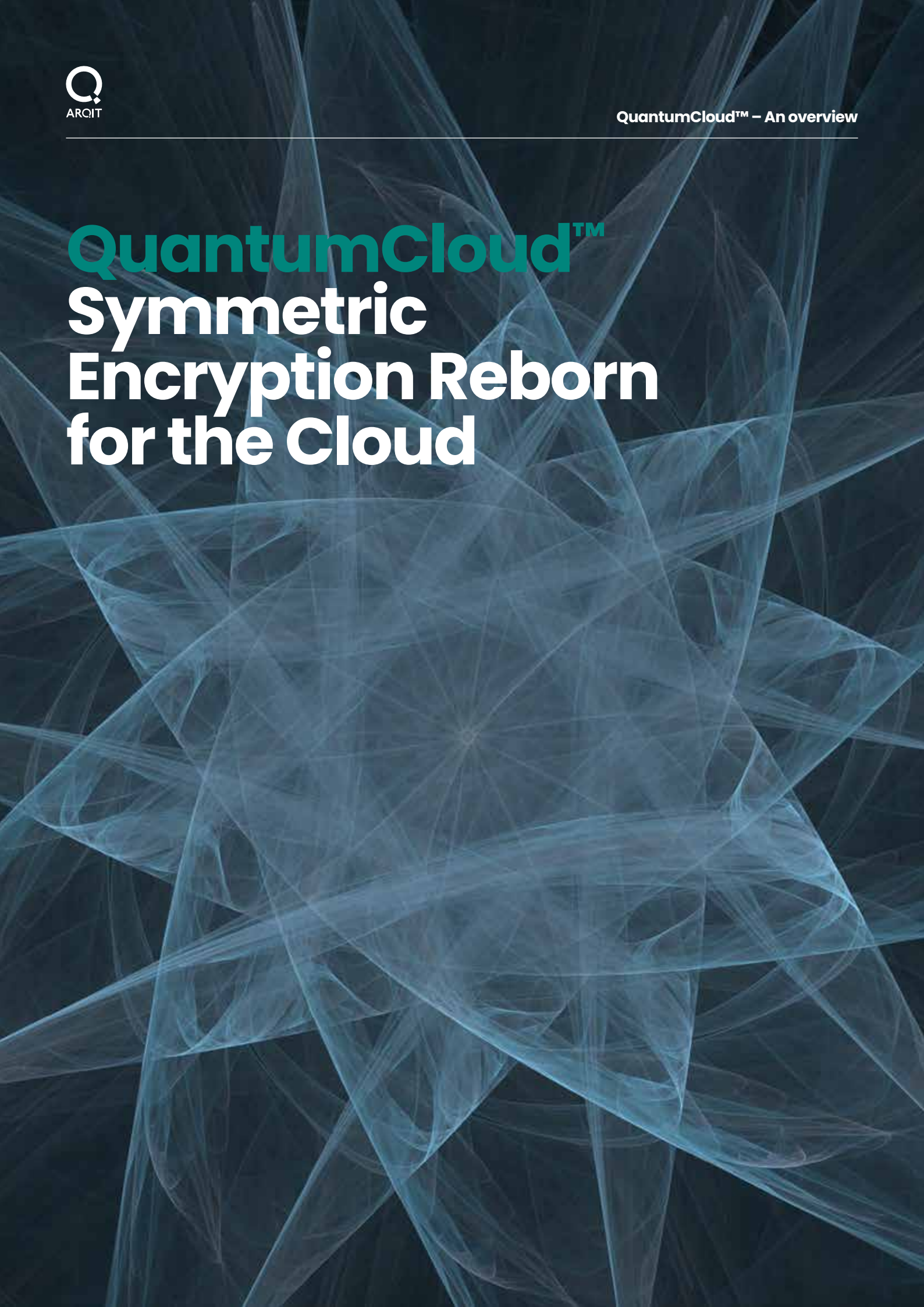
QuantumCloud™
Symmetric Encryption Reborn for the Cloud



QuantumCloud™
An overview

The security of all data, networks and assets is threatened by known and emerging vulnerabilities to legacy encryption that was not designed for the hyperconnected world.

The IT community is comfortable with the use of symmetric keys and knows them to be secure against all forms of attack. Until now there has not been a scalable and secure way to deliver them.

QuantumCloud™ does just that.

With a cloud self-service model, low computational burden, low cost and high interoperability, QuantumCloud™ delivers the trustless and computationally secure benefits of symmetric encryption keys to all and any connected device in the World. It is a scalable, policy-based service that is quick to deploy and requires no infrastructure.

There are three components to QuantumCloud™ which we'll examine in more detail:

1. A network of QuantumCloud™ nodes which enforce security policy, participate in key negotiation with devices, securely store digital signatures and data, and are a gateway to other services on the QuantumCloud™ network.

2. An SDK and software agent for installation onto endpoint devices that coordinates communication with QuantumCloud™.

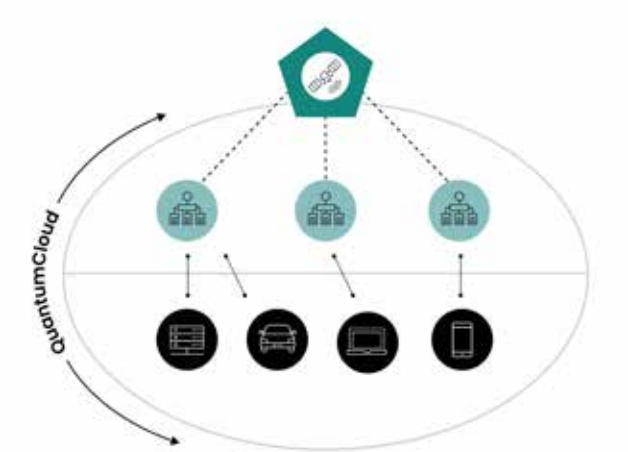
3. An administrative web portal for system administrators to access their QuantumCloud™ account, administer devices, and manage security policies.

Working together, these components provide a comprehensive security infrastructure for endpoint devices and devices at the edge, creating a seamless security fabric. QuantumCloud™ focuses on shared symmetric key establishment which enables efficient, high-security communication between devices. This has particular application in today's networks which are more distributed and varied than ever before. By combining the power of symmetric encryption with a cloud-based service, QuantumCloud™ delivers the security solution that the industry has been waiting for.

In this document, we'll look at the most important features of QuantumCloud™ and how they can improve security and reduce management burden in your enterprise. This document is aimed at security professionals, system administrators and IT specialists who deal with enterprise security and want to learn more about the features and benefits of QuantumCloud™.

A cloud-based SaaS solution for device security

QuantumCloud™ is a cloud-based solution available to any device that's connected over TCP /IP. It's composed of a group of nodes distributed globally, each of which acts as a local exchange for devices to authenticate and negotiate keys with other devices on the network. Communication with the node happens over API calls, either directly from the device or through the QuantumCloud™ SDK. Each node is connected with other nodes in the network using secure symmetric keys.



Those keys are created at the nodes through the use of quantum satellites which deploy a novel protocol called ARQ19. This has solved all of the known problems of Satellite Quantum Key Distribution. We'll discuss that in more detail further on.

When a device first registers with QuantumCloud™ it creates a new symmetric key shared using a proprietary method. Once devices are registered and authenticated with QuantumCloud™ they can access its services, such as creating a shared symmetric key with another device on the network or taking part in a group key session with many other devices. The network traffic between devices happens directly over TCP/IP, and the final keys agreed between the devices aren't known to QuantumCloud™.

Accounts are administrated through the web -based QuantumCloud™ portal, giving system administrators and IT professionals an overview of their account and a suite of tools to manage devices and policies.

Zero infrastructure

Being a cloud-based solution, QuantumCloud™ doesn't require specialist hardware installed on premise. This not only reduces capital expenditure, but also provides a reduced management overhead and infinite flexibility of operations. Devices run a lightweight SDK or make direct API calls to the QuantumCloud™ service.

Easily scalable and affordable

It's easy to add devices to the global QuantumCloud™ network, whether it's ten or ten thousand. And since billing is based on the usage of keys and the number of devices, customer only pay for what they use.

Crypto-agility out of the box

QuantumCloud™ is always running the latest version, making sure devices always have access to the best-in-class security on offer. Customers can seamlessly take advantage of any improvements as the network continues to grow, including new infrastructure such as fibre networks and satellite QKD technology.

Real-time security

In contrast to PKI, where certificates are managed using revocation lists that can become out of date, QuantumCloud™ enforces security policy in real-time. As soon as a device has its access revoked it is no longer able to participate in the network.

Quantum secure digital signing

The breakdown of PKI in a post-quantum world does not only undermine secure communications, it also leaves PKI based digital signatures vulnerable. QuantumCloud™ can sign transactions in the cloud with Quantum Keys created for multiple parties that guarantees security and provenance of a transaction. Signatures can be selectively shared with third parties such as regulators, compliance and audit teams if needed.

This is vitally important for the emerging technology of blockchain and distributed systems that are

gaining adoption and credibility, particularly in the Central Bank Digital Currency sector where Arqit has its first customer and wider use-cases as a unique asset class. However the adoption of these systems will always be hampered by the quantum threat and large attack surface of PKI. Arqit's QuantumCloud™ platform brings a definitive and secure solution for both Blockchain and Digital Wallets.

Managed Encryption of Data at Rest

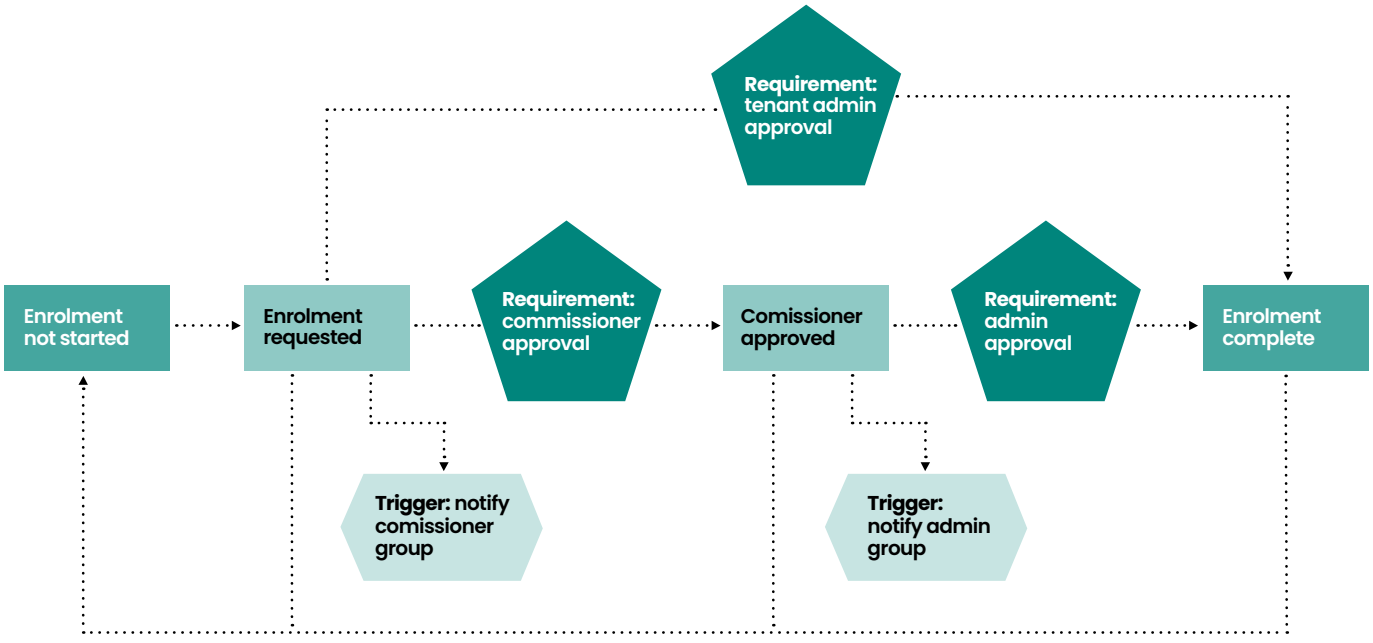
QuantumCloud™ provides a global network of quantum security, and the ability to use these Quantum Keys to encrypt data and store it across multiple cloud and on-premesis storage providers. This quantum encryption can be shared across multiple locations, and keys can be accessed and shared securely to any permissioned device globally. This is a major step forward in protecting data at rest.

Devices that communicate with QuantumCloud™ undergo a provisioning process in order to access all of its services. This process is initiated by the device delivering a "bootstrap" key over the air using a novel QuantumCloudTM process.

The bootstrap key is an ephemeral input into a key creation process which "ratchets" the key, deriving a new authentication key that's computable by both the QuantumCloud™ network and the device itself in parallel, but unknown to upstream actors. This process is called Autonomous Trustless Keyfill (ATK). These ATK authentication keys allow the device to create secure, authenticated sessions with QuantumCloud™ nodes, ensuring any communication between the device and the node is completely trusted and secure. This ATK authentication key cannot be known even if the bootstrap key is compromised.

The key ratcheting concept enables provisioning workflows as directed by the customer. All devices must pass through a provisioning workflow before gaining access to QuantumCloud™ services. When a device first registers, it starts on the first step of this workflow, and the device can then request to move to further steps. For example, a device's ATK authentication key might transition through 3 stages in its lifecycle: "bootstrap", "quarantine", and "production", at each stage using the ratchet process to derive the next authentication key in the chain.

Each step can trigger notifications to security staff and inform them about devices accessing the network, as well as require authorisation from device users or specified user groups before continuing. This allows organisation fully auditable, fine-grained control over the devices that gain access to QuantumCloud™ services.



Authentication key secrecy in supply chains

The ratcheting process provides implicit secrecy, meaning that mal-actors with access to earlier keys in the ATK authentication key chain are unable to derive information about the current key. In cases where a device passes through multiple steps in a supply chain, each manufacturer can use a different authentication key which upstream suppliers cannot know.

Fine-grained access control

Only devices that have passed through the provisioning workflow successfully are able to access QuantumCloud™ and participate in the network. System administrators can audit these workflows to see which devices have access and revoke it at any time through the QuantumCloud™ Portal.

Secure symmetric key negotiation

Once an endpoint is provisioned and registered in QuantumCloud™ it is able to access the DSCC (Distributed Symmetric Communication Cryptography) service which enables negotiation of secure keys between pairs or groups of devices. In contrast to traditional public-private key methods employed by systems using PKI, QuantumCloud™ enables endpoints to negotiate symmetric keys with other endpoints without the use of quantum-unsafe asymmetric algorithms. The agreed symmetric key, which cannot be known to QuantumCloud™, may be used with AES-256 as standard, although other key lengths are available.

This key negotiation uses a proprietary protocol which performs favourably against current key exchange and encrypted transport methods such as TLS.

Groups of devices can also create a group key, shared by all devices in the group but not known to QuantumCloud™ which acts as the coordinator. The key establishment is extremely efficient, with the number of handshakes growing linearly with the number of participants.

Once the symmetric key is generated it can be used to create a secure tunnel between the two (or more) devices.

For example, TLS 1.3 supports the use of pre-shared keys[1], and the agreed symmetric key could be used as this pre-shared key.

Global delivery and frequent rotation

Keys are deliverable at a global scale, meaning that the security of symmetric keys can be attained between devices without manual on-site key injection. Furthermore, keys can be renegotiated hourly, rather than monthly, or even yearly, as practiced in some organisations today.

Quantum secure

The threat of quantum computers and their ability to break existing asymmetric keys like RSA puts data at risk. Symmetric keys, if constructed properly and with sufficient entropy and length, are believed to be quantum secure[2] . The keys negotiated through QuantumCloud™ are therefore resistant to quantum attack, both now, and for the foreseeable future.

Limited trust

While other protocols exist that are able to distribute symmetric keys (perhaps most notably Kerberos), QuantumCloud™ has the advantage that the cloud nodes in the network are not able to discover the final key shared between endpoints. QuantumCloud™ acts as a broker in the network who aids in negotiation without knowing the outcome using a split-trust model.

No certificates

Devices on the QuantumCloud™ network are uniquely identified and authenticated by Quantum-Cloud™, removing the need for a central repository of certificates. Devices know and can prove their own identity to other devices in the network.

---

[1] Eronen, P., Tschofenig, H. (2005). RFC4729: Pre-Shared Key Ciphersuites for Transport Layer Security (TLS). The Internet Society. https://tools.ietf.org/html/rfc4279

[2] Quantum Safe Cryptography and Security. (2015). European Telecommunications Standards Institute. https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafe_Whitepaper.pdf

Key management as a service

The QuantumCloud™ Portal is an online administration tool for system administrators. Security outcomes are enforced through the use of policies which govern a range of attributes about how keys are used by QuantumCloud™, such as:

- How long a key can be reused before it is renewed
- Types and lengths of keys that can be generated (e.g. AES-256)
- Uses a key can have, e.g. whether it can be used to create secure tunnels between devices
- Whether to use key-wrapping
- Which users can revoke a key
- Automatic rules when, for example, a device has been inactive for a certain length of time

Aside from policy management, administrators can also manage users and access levels, view and manage devices, and create provisioning workflows to apply to devices and device groups. The portal is web-hosted and fully screen-responsive, with a simple intuitive user interface.

A dashboard provides a simple overview of the health of the system, allowing users to see issues at a glance. This single pane of glass combines information about devices on the network, recent active sessions, which policies are active, and highlights any issues that need user attention.

Focus on outcomes, not implementation

Wrapping rules and options into high-level policies allow administrators to focus on security outcomes, rather than the detail of the implementation. Much of the implementation is abstracted from the user, which also means that customers can take advantage of security improvements in the platform without rewriting code or updating devices.

Consolidated management of devices and policies

The portal dashboard provides a comprehensive overview of the health and usage of the system in one place. Comprehensive auditing and logging functionality makes it easy to diagnose issues.

Zero trust

PKI is deployed as a separate infrastructure layer and, due to the complexity of managing it, it is normally deployed in a very permissive fashion; the restrictions of who can talk to who are managed by the systems in layers above it. With the policy management of QuantumCloud™ customers can deliver fine-grained control over which devices can form encrypted tunnels with other devices, building a better zero trust network

Standards compliant

QuantumCloud™ is adopting the industry-standard KMIP interface and the latest standards from ETSI, making it easy to integrate with existing key management infrastructure.

The answer that the industry has been waiting for

QuantumCloud™ is the only security platform that offers a cloud-based service to create symmetric keys where and when they are needed at a global scale. It transforms the way the industry can approach cyber threats, putting the focus on enforcing security rather than managing it, and unlocking the power and simplicity of symmetric key encryption.

Customers can start realising the benefits of symmetric key infrastructure in their business by integrating with QuantumCloud™ today.
Solve today's problems now, with the assurance that you also removed the risk of quantum attack.

Get in touch today to find out how.