Quintessence Labs

SOLUTION GUIDE

Cloud Storage Security

Enterprises and other large businesses that deal with massive volumes of digital information need to securely store this data — and today, many storage options reside in the cloud. While cloud storage is cost-effective and convenient, it's important to also ensure that the stored data is effectively protected.

Overview

Keeping large volumes of sensitive data calls for trustworthy data security that can handle changing business environments and ever-growing threats. One of the most important tools is to implement strong encryption. This poses multiple challenges: Are the encryption keys strong enough? Are they safely stored? Can different protocols be managed? Are practical policies available for effective operations? It's a large and complex challenge that demands sophisticated management capabilities.

It is also important — yet challenging — to ensure seamless end-to-end protection across an infrastructure, where the organization is made up of different business units with offices in various locations, often with security systems from multiple vendors in service for years, if not decades. Replacing long-standing systems can be hard, but so can integrating them organization-wide. Failures to integrate can lead to siloed data protection that makes the information between systems vulnerable.

> “Many cloud providers offer a variety of options for key management, including server side offerings that ultimately leave keys in the hands of the cloud provider's admins … Only by maintaining control over keys can organizations ensure their data is immune to blind subpoenas, as well as malicious insiders.”
>
> —Garrett Bekker
> Principal Security Analyst,
> 451 Research

As integration efforts are made, hosting data in the cloud has become a widespread practice for many good reasons; businesses appreciate the cost advantage and flexibility of relying on external providers to keep data stores accessible no matter where employees are located. Yet the advantages of cloud storage are tempered by the risks of a third party managing the company's infrastructure and data, which can threaten confidentiality, and with it, a client or customer's trust.

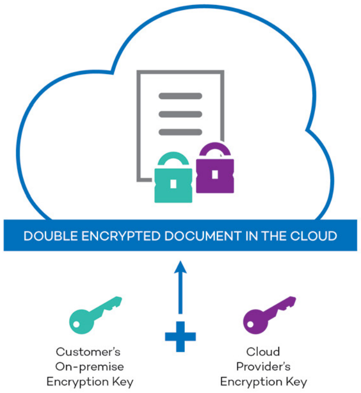
Key Wrapping: Minimizing Blind Subpoena Uncertainty

Part of those risks involves blind subpoenas, whereby a cloud storage provider can be obliged by law enforcement or another agency to provide data without being allowed to inform the data's owners. For example, in 2017, Google received nearly 100,000 data disclosure requests from government authorities, which were not necessarily disclosed to the data owners.

This is especially of concern, for instance, for a law firm that uses cloud storage, where the attorney-client privilege is normally a guarantee of protection. Even encrypted data is vulnerable if the cloud provider holds and is forced to reveal the encryption keys, exposing the supposedly secure confidential data. Considering that the owners of the data would be unaware of the handover, they would have no opportunity to challenge that request.

The best strategy to protect cloud-based data from blind subpoenas is to retain control of the encryption keys, while using the storage capabilities offered in the cloud. One way that has been successfully implemented by QuintessenceLabs is to encrypt or "wrap" the data encryption keys that in turn protect the data in the cloud.

Key wrapping is a powerful way to protect data stored in the cloud from unauthorized access. QuintessenceLabs' solution uses a true random number to make a wrapping key that is not available to the cloud provider, and that is used to add a second layer of encryption protection. Essentially, without this wrapping key, the data cannot be decrypted, removing the risk of a blind subpoena. Any data request by authorities would need to come directly to the data owners. If the law firm in our example has a wrapping key under their control, its staff and clients can be sure that their data is safe from unknown third parties.


DOUBLE ENCRYPTED DOCUMENT IN THE CLOUD
Customer's On-premise Encryption Key
Cloud Provider's Encryption Key

Key Wrapping

Fully Integrated Key Management

While enterprises struggle to evolve their security systems, vendors will often market integrated solutions to increase the appeal of their products. However, the definition of "integrated" can vary. Some products have key and policy management but lack HSM protection, and others have solutions designed only to protect specific platforms. Integration could also mean a simple bundle of devices from partnered vendors, each with their own contacts and responsibilities for their products should problems arise.

QuintessenceLabs' Trusted Security Foundation® (TSF®) key and policy manager is a truly integrated one-device solution, combining vendor-neutral key and policy management with HSM hardening, all backed by quantum-powered randomness to protect against the most advanced cyber-attacks, and includes a client SDK to enable development teams to easily harness the power and features of the platform.

End-to-End Cloud Data Protection

One great implementation of the TSF key and policy manager is with PKWARE, a trusted enterprise software company with over 30 years of history and one of QuintessenceLabs' biggest partners. The PKWARE Smartcrypt Enterprise Manager appliance provides persistent security for business data, with encryption management that is open standards-based and protects an entire infrastructure from mainframes to endpoints.

PKWARE's Smartcrypt Enterprise Manager seamlessly integrates with the TSF key and policy manager platform, allowing PKWARE's endpoint encryption capability to leverage the power of quantum random to generate master encryption keys and endpoint-based Smartkeys. Smartkeys are then distributed to encryption endpoints and integrated into devices or applications for a convenient and automatic security process.

The inherent advantages of the TSF key and policy manager help PKWARE deliver products that support encryption that stays with data wherever it's shared or stored (known as "persistent encryption") and be used by cloud storage providers who are mindful of the need to keep customers' data secure.

Protecting Data in the Public Cloud

Major cloud service providers (Google, Azure, Amazon, Salesforce, etc.) all support data-at-rest encryption, and it can be easy to delegate creation and management of encryption keys and operations to the provider. But this heightens the blind subpoena risk, and technically introduces service provider insider risk. To engender greater confidence to consumers, many providers introduce Bring Your Own Key (BYOK) and Host Your Own Key (HYOK) options.

BYOK usually means a user can import their own externally generated keys to the cloud service. Once imported, the keys are managed by the service provider, with the same potential vulnerabilities as keys generated and managed by the provider. HYOK lets users take full control of the encryption keys by hosting them on their own premises — when the service provider needs to perform a cryptographic operation, a call is made to the customer's system, which performs crypto operations locally without revealing keys to the service provider.

While appealing, HYOK introduces latency to transfers that may be operationally significant, and regardless, some service providers will require the customer deploy hardware and software supplied by the provider or a preselected vendor — though others publish an interface so that no proprietary implementation or specified vendors are forced upon the customer.

Migration of data and keys between cloud service vendors can be difficult if not impossible because of this fully-managed encryption or restrictive BYOK/HYOK services. It's important to understand whether or not a provider's customer has the flexibility to switch providers and take their keys and data with them, not to mention a general understanding of the security risks of vendors' encryption and key management services.

At QuintessenceLabs, the individual parts of the TSF key and policy manager platform lets us uniquely offer high-speed true random numbers and centralized key management for strengthening data protection. qStream™ is a true random number generator (TRNG) that uses quantum tunneling, a random effect that's measured and delivered through networks at up to 1 Gbit/sec, helping create strong encryption keys. Alongside is the TSF platform, QuintessenceLabs' key and policy manager solution which handles keys and key operations at high volumes, fully implementing stringent lifecycle management approaches (as specified by the NIST standard SP800-57 Part 1).

The TSF key and policy manager adherence to the OASIS Key Management Interoperability Protocol (KMIP), enables seamless integration with applications from vendors including Dell, Oracle, HP Enterprise, IBM, NetApp, CipherCloud, DataStax, Fujitsu, Quantum, Spectra, VMware, and many more. Learn more about the importance of true random numbers and best practices in key management in our informational papers on our website, **quintessencelabs.com**.

Get in Touch

QuintessenceLabs has proven partnerships with cloud infrastructure providers and other enterprises, where our quantum-based key management solutions have effectively strengthened data protection across entire organizations. We secure data, so you can focus on what you do best.

Contact us at **info@quintessencelabs.com** or visit **quintessencelabs.com**.

Quintessence Labs

AUSTRALIA
Unit 11, 18 Brindabella Circuit
Brindabella Business Park
Canberra Airport ACT 2609
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 3844