Quintessence Labs

SOLUTION GUIDE

Enterprise Storage Security

Today's enterprises have a broad spectrum of storage options for their data at rest — from traditional file storage to databases, storage for virtual machines, and cloud-based services. Regardless of the type of data storage, it is vital to keep it safe.

Data is driving growth. As companies scale, so do their storage needs for the full range of data types managed: email, documents, financial records, end-user profiles and more. Keeping customers' data safe is an important commitment, and if that commitment is broken, there are real costs and consequences in loyalty and retention. In addition, strong data protection is a requirement of industry regulations around the world — one example is Europe's General Data Protection Regulation. Meeting compliance can be challenging, both technically and organizationally, but it is essential to help keep the data of customers, users and employees safe.

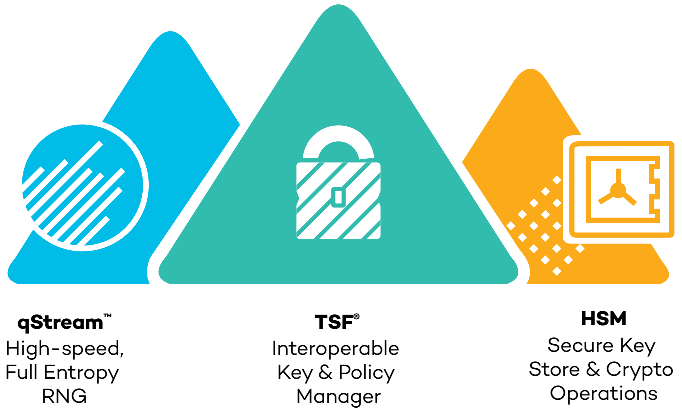
A sound data protection strategy for enterprise storage requires rigorous security procedures. All-round protection of storage via encryption or other proven security methods, is needed, with appropriate customer notification and protection steps should breaches or other forms of data loss occur. Encryption, when well-implemented, provides the strongest protection of data even in the event of a breach, but to be effective requires sophisticated key and policy management implemented over the data's full lifecycle.

The Trusted Security Foundation® Key and Policy Manager Enables Secure Storage

Encryption is the foundation of secure storage, but only if it's done well. Encryption keys must be managed over their full lifecycle and flexible policy management is needed to ensure strong data protection without impacting operations. Furthermore, poor quality encryption keys can significantly weaken data protection. Finally, many key managers are not interoperable with other devices or platforms, generate weak keys, or lack the proper policy control – resulting in siloed data protection, negative impacts on operations, and potentially weaker encryption.

An essential part of any encryption project is to implement a strong key and policy management capability. QuintessenceLabs' Trusted Security Foundation® (TSF)® key and policy manager helps the deployment of effective encryption by generating full entropy keys at the high rates required for enterprise needs, securing those keys in a FIPS 140-2 Level 3 conformant key store, and managing keys and policies with the rigor and granularity needed to secure your organization. Our TSF key and policy manager delivers full key lifecycle management and usage and policy controls enabling strong and comprehensive end-to-end encryption.

The TSF key and policy manager product suite is strengthened by a built-in quantum random number generator to ensure that the strongest keys are used to protect your data. The TSF key and policy manager is price competitive, and conforms to industry-wide standards to ensure high performance, smooth deployment and management. Fully interoperable, it seamlessly integrates with other devices in your architecture, and allows you to focus on your operations without security compromise, confident in the strength of your data protection.



QuintessenceLabs Key Management Solution

The OASIS Key Management Interoperability Protocol (KMIP) addresses interoperability with a standard instruction set that lets systems from different manufacturers efficiently talk to one another. QuintessenceLabs' TSF key and policy manager adheres to KMIP, delivering solutions that can be seamlessly integrated into legacy infrastructure with minimal disruption and delay.

The TSF key and policy manager is ideal for use for these and other common enterprise applications:

- Databases
- Disk and tape storage encryption
- VM and VSAN integration
- PGP and SSH key management

NetDocuments: A Proven Solution

NetDocuments is a leader in cloud-based document and email management, securing over 2 billion highly sensitive documents around the globe. The company needed to expand its data centers to meet steep customer growth while continuing to enhance the protection provided. As part of this effort, it wanted to implement best-in-class key management to generate and secure the master and document encryption keys for all its customers.

Our solution included multiple redundant and replicating TSF key and policy manager appliances deployed in NetDocuments' data centers around the world. Customer documents are encrypted with unique keys generated by the TSF key and policy manager, and "wrapped" using master keys to ensure isolation between customers, providing very high scalability that supports hundreds of millions of uniquely encrypted individual documents.

Quantum Resistance

Quantum computers are on the horizon and will enable unprecedented progress across many scientific and engineering fields. This exciting future has its dark side: the speed and power of a quantum computer, and its ability to solve the mathematically complex problems on which some of our security systems are based, mean that quantum computers will easily be able to defeat the defenses used to secure our data today.

While new quantum resistant algorithms are still in their early days, there is much that can be done to prepare storage architectures for this threat.

Symmetric encryption will remain secure in the face of quantum computers, as long as the key length is increased, and the keys used are truly random. This is where the use of high-speed quantum random number generators such as QuintessenceLabs' qStream™ quantum random number generator (QRNG), available as a stand-alone device or integrated into the TSF key and policy manager series, can really help protect stored data from the quantum threat.

The qStream QRNG uses a quantum entropy source that samples minute random fluctuations from electrons tunneling through an electrical barrier, generating "true random" at up to 1 Gbit/sec. From there, true random numbers can meet a wide array of security needs, lending unbeatable protection and flexible compatibility.

A secure key management capability requires the availability of replication nodes, additional servers with the ability to synchronously or asynchronously replicate copies of keys, should any one part of the system corrupt or lose keys, or otherwise go offline. The key material is extremely sensitive and must also be transferred between those nodes just as securely as it's stored. Today, most transfers happen over a mutually authenticated TLS connection, which will be vulnerable to quantum computer attacks. Symmetric key wrapping using a true random key provides a quantum resistant layer of extra protection for the TLS transfer. The Trusted Security Foundation® (TSF)® 300 and TSF® 400 key and policy managers include this symmetric key wrapping as part of their standard offering, protecting this in-network key exchange from current and future quantum threats.

Finally, for the most sensitive needs, advanced quantum key distribution (QKD) capabilities can be explored. QKD secures the exchange of keys between two locations using physics instead of math, and is hence not threatened by the development of quantum computers.

Get in Touch

QuintessenceLabs has formed proven partnerships with cloud infrastructure providers and other storage companies, where our quantum-enhanced solutions have effectively strengthened the data protection across entire organizations. We secure data so you can focus on what you do your best. Send us a message at quintessencelabs.com for more information or to request a demo.

Find product sheets and more informational papers on key management and more at **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: 3866