PRODUCT INFORMATION

qSecure-FS™

File Storage Encryption

www.quintessencelabs.com

File Encryption Capabilities

- Implement transparent and automated file encryption for physical, virtual, and cloud environments.
- Define and enforce granular access control policies.
- Manage encryption keys centrally and securely in qCrypt protected by FIPS 140-2 validated hardware.
- Achieve compliance: ensure separation of duties, track user access to protected data and keys.

Highly Secure

- Central management of cryptographic objects with full lifecycle management, usage policy and object policy controls.
- Encrypted keystore with Trusted Platform Module (TPM) root of trust; FIPS 140-2 Level 3 cryptographic module available.
- Administrator separation of duties.
- Client access control and optional dual control (double wrapping).

Fully Interoperable

- Seamless integration into legacy infrastructure.
- Interoperable: SMB, NFS, AWS S3, and WebDAV for clients and storage.

Flexibility and Performance

- Can be deployed as a VM instance or physical appliance.
- Caching of keys and data files for improved performance.
- Data splitting option for added security and availability.

Protecting Data through Encryption

Need for Encryption

Perimeter-based security does not provide sufficient protection for the growing volume of sensitive data stored locally on servers or in a public or private cloud. To protect information against security breaches, the data needs to be securely encrypted, while remaining readily available and accessible to approved users.

Encryption protects information from breaches, whether internal or external, malicious or accidental. It is also needed to comply with many industry mandates and regulations. Encryption protects organizations from the financial loss, operational impact on customers and damage to reputation of security breaches.

qSecure-FS

QuintessenceLabs qSecure-FS delivers flexible and secure encryption services for file storage, and can be used both for network file server and cloud storage services. qSecure-FS operates as a cryptographic gateway between clients and storage, and handles all the necessary operations to cryptographically protect files, store the encrypted content on file servers or cloud storage services, and manage access control to the stored data.

The solution encrypts sensitive data on servers, such as credit card numbers, personal information, logs, passwords, configurations, and more, protecting them in the event of a breach and other potential threats.

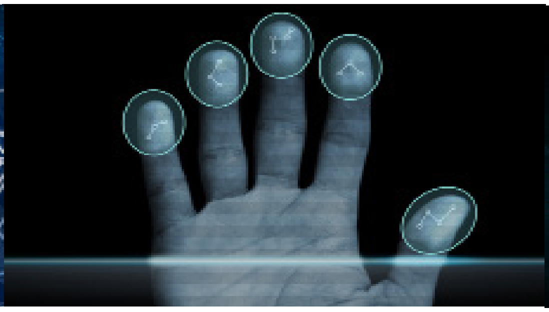
qSecure-FS allows you to encrypt your sensitive data before storage in any file system or the cloud while maintaining local secure control and ownership of your encryption/decryption keys.

qSecure-FS integrates seamlessly with QuintessenceLabs’ flexible key and policy management with granular user and object policy controls, delivered by the QuintessenceLabs’ TSF™ key management product suite, a FIPS 140-2 Level 3 enterprise solution.

For more information on the TSF and on QuintessenceLabs’ Encryption Modules, refer to the Trusted Security Foundation and Encryption Module Solution Guides.

SPECIFICATIONS

qCrypt and qCrypt-xStream



Management functionality

- Accessible via command line, Web UI, and REST API.
- Management functions include system management, administrator management, log management, storage configuration, key manager configuration.
- Neither clients of qSecure-FS nor storage back-ends used by qSecure-FS will require modification or installation of agents.

Interfaces

- Server interfaces for client connection: SMB/CIFS, NFS, AWS S3 and WebDAV.
- Storage interfaces for local file system: SMB/CIFS, NFS, AWS S3 and WebDAV.
- Platform Management delivered through SSH command line, Web UI over HTTPS and REST interface over HTTPS.
- qSecure-FS can direct client data between dissimilar interfaces.

Cryptographic Functions

- qSecure-FS encrypts and adds integrity check values to data passing from a client to storage, and decrypts and checks integrity for data passing from storage to a client.
- Cryptographic operations protecting data passing between clients and storage interfaces have a security strength of 256 bits.
- Protection mechanisms ensure confidentiality and integrity of client data. Access controls are applied to stored files and objects, as well as cryptographic keys and other security parameters.
- qSecure-FS uses Suite B cryptographic algorithms, and can perform cryptographic functions with a FIPS 140-2 Level 3 cryptographic module.

Key Management

- Each file protected by qSecure-FS is encrypted and integrity protected by unique keys. These keys can be wrapped with key encryption keys. Optional double-wrapping of file protection keys can be implemented to support dual control, as well as flexible caching capabilities.
- qSecure-FS is deployed in tandem with QuintessenceLabs qCrypt, a FIPS 140-2 up to Level 3 enterprise key manager with the option of integrated high speed full entropy random.

Solutions Portfolio

The QuintessenceLabs Cyber Security Product family comprises a Trusted Security Foundation™ (TSF™) consisting of Random Number Generation (qStream), key management (qCrypt, qCrypt-xStream, and qCrypt-VM) and trusted cryptographic hardware, and a suite of QuintessenceLabs Encryption Modules (QEM) delivering cryptographic applications, including the qProtect and qSecure product ranges.

QuintessenceLabs Encryption Modules deliver targeted cryptographic applications for a wide range of security needs.
The qSecure product range provides cryptographic services for file storage and database management systems, while qProtect delivers the highest security for mobile assets in uncontrolled environments.

QuintessenceLabs – the Global Leader in Quantum Security

QuintessenceLabs' portfolio of modular products addresses the most difficult security challenges, helping implement robust security strategies to protect data today and in the future.