Quintessence Labs

SOLUTION GUIDE

Complete Enterprise Data Protection with TSF® and Smartcrypt

The Trusted Security Foundation® (TSF®) key and policy manager appliance can enable data discovery, classification and encryption capabilities, through seamless integration of the PKWARE Smartcrypt solution.

Overview

Data security is the highest priority for any business that handles sensitive information. Organizations need to protect all their data, avoid silos and security gaps and do this without disrupting operations.

QuintessenceLabs' security solutions address these challenges. The Trusted Security Foundation® (TSF®) key and policy manager platform is a secure, centralized, and highly interoperable solution delivering critical key and policy management capabilities. It manages keys over their full life cycle, implements strong object and user policy management, offers in-built replication for up to 16 nodes for maximum availability, and more.

The TSF key and policy manager also comes with the option of embedded data discovery, classification and encryption capabilities, through seamless integration of the PKWARE Smartcrypt solution. This provides our customers with an efficient and safe end-to-end integrated security platform without the need for additional infrastructure.

What it Offers

Key Management with the TSF 400:

The Trusted Security Foundation is a comprehensive key and policy management appliance integrating three main components: a high-speed true random generator with a quantum entropy source, a FIPS 140-2 Level 3 HSM, and the TSF key and policy manager application. This TSF key and policy manager delivers extensive key and policy management capabilities with a full lifecycle management of cryptographic objects. Its random number generator enables the generation of the highest quality keys, secret objects and passwords. It is fully interoperable, KMIP compliant and supports PKCS#11.

Data Discovery:

To keep data safe, organizations must first find where sensitive information resides in their storage networks and user devices, and then take steps to protect that data. Traditional data discovery provides limited remediation options, leaving organizations searching for other solutions to protect the information. With the integrated Smartcrypt option, TSF key and policy manager customers have access to a software agent continuously monitoring storage locations for sensitive information. Each time a file is added or modified, Smartcrypt initiates a scan based on the organization's definition of sensitive data. If the data fits one of the defined patterns, the system can initiate classification and apply encryption, masking, or other forms of protection.

Classification:
Data classification is an essential component of enterprise data protection, allowing administrators and end users to identify files and messages that contain sensitive information. The TSF key and policy manager with the Smartcrypt option includes data classification in an automated workflow with data discovery and protection. When sensitive data is detected, customers will be able to leverage classification tagging and implement encryption, masking, or other protective measures in line with their security policies.

Encryption:
Persistent strong encryption is the most effective form of data protection, preventing unauthorized users from accessing sensitive information no matter where files are located. Unlike other forms of encryption, persistent encryption is applied to data itself, rather than to a storage location or transmission system. Information protected by persistent encryption remains secure throughout the entire data lifecycle, whether files are saved on servers, endpoint devices, removable storage, or in the cloud. Persistent encryption ensures that only authorized users can access data, even in the event that the data is lost or stolen.

How it Works

The Smartcrypt Enterprise Manager is deployed onto the TSF key and policy manager solution, and is set up to enable data protection policies to be defined and activity to be monitored across the organization. A Smartcrypt agent is installed on each user device or IT asset to protect data in accordance with the organization's policies. The software agent continuously monitors storage locations for sensitive information. Each time a file is added or modified, a scan is initiated. If the data fits a pre-defined pattern, the system can initiate classification and apply encryption, masking, or other forms of protection.

The solution can be configured to monitor network storage locations and employee devices like laptops and desktops. The discovery and remediation processes are transparent to end users, while ensuring that the organization maintains complete control over encryption activity.

Get in Touch

QuintessenceLabs' quantum-based encryption and key and policy management solutions have effectively strengthened data protection across entire organizations. We secure data so you can focus on what you do your best.

For more information, contact us at **info@quintessencelasb.com** or visit **quintessencelabs.com**.