Hewlett Packard Enterprise

Delivering transparent data encryption while centrally managing keys

HPE Enterprise Secure Key Manager for Bloombase StoreSafe

Highlights of HPE ESKM

HPE Enterprise Secure Key Manager (ESKM) provides a centralized key management solution for unifying and automating an organization's encryption controls by creating, protecting, serving, and auditing access to encryption keys. HPE ESKM helps protect sensitive information such as payment cardholder data, customer and employee records, electronic health records, intellectual property, cloud-hosted data, and classified information with encryption key lifecycle management that provides high security assurance. HPE ESKM supports the Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP) enabling the broadest range of applications and solutions from Hewlett Packard Enterprise and partners to protect data reliably and securely.

- A large ecosystem of storage and server applications from Hewlett Packard Enterprise and partners that interoperate seamlessly with HPE ESKM for a unified key management approach
- Key operations automated to simplify administration and reduce the risk of manual errors for long-term reliable performance
- HPE ESKM, a FIPS 140-2 Level 2-validated appliance, with Level 3 hardware option
- Reliable, field-tested hardware appliance that offers high availability key generation and recovery by clustering up to eight nodes and scalability to manage up to 25,000 endpoints and two million encryption keys

The challenge

Risks to data security make the protection of enterprise data more important than ever. With each new breach of sensitive information, companies are increasingly concerned about sensitive data that is exposed across IT infrastructures. Many enterprises rely upon legacy server and storage systems that either cannot natively support encryption or can only support proprietary options, which require hardware retrofitting or expensive upgrades to protect sensitive data. It is a challenge to protect data comprehensively and without sacrificing the performance that daily application operations require.

While encryption is a critical first step to protecting data, authorized use and business transparency are expected, when controlling access to encryption keys, over encrypted data for a trusted solution. Protecting data alone is not sufficient in the case of a security breach or attack since encryption is only effective if your keys are safeguarded from misuse.

Moreover, auditors expect that security policy is in compliance only when reliable controls and proper administrative procedures are in place to govern encryption keys. The increased use of encryption across IT applications within an enterprise creates operational silos, which in turn can lead to inconsistent controls, higher overhead from managing redundant key management systems, and unclear separation of duties. This creates an increased level of risk and leads to time-consuming audits.

The solution

Bloombase StoreSafe and HPE ESKM provide a complete solution for encryption of sensitive data and centralized key management, offering enterprises comprehensive protection for data-at-rest security and business continuity. StoreSafe offers a network-based encryption solution across global, heterogeneous storage environments that enable applications to secure structured and unstructured data using proven Advanced Encryption Standard (AES) cryptographic mechanisms with minimal application and infrastructure change. HPE ESKM delivers industry-validated, trusted key management for StoreSafe and a wide range of infrastructure applications.

IT environments that do not have data encryption built natively into storage and server systems no longer need to retrofit a disk array with self-encrypting drives or upgrade tape drives, for example. Proprietary systems that lack encryption and key management interoperability, or legacy storage systems, can simply deploy StoreSafe as a proxy between enterprise applications and storage systems on the network to encrypt and decrypt the data in-line as it is stored and accessed.

Once data is encrypted, HPE ESKM centrally manages encryption keys and automates key lifecycle operations by interoperating with StoreSafe using industry-standard OASIS KMIP, enabling extensibility and reuse for future storage and server solutions. HPE ESKM delivers one of the most secure and scalable enterprise key management solutions on the market today, supporting 1000s of encryption clients.

Highlights of Bloombase StoreSafe

Bloombase StoreSafe is an all-in-one storage security protection software appliance that provides turnkey, nondisruptive, application-transparent encryption security of data-at-rest including data in physical and virtual data center deployments as well as traditional IT storage, Big Data, and cloud applications. Bloombase StoreSafe protects heterogeneous storage systems transparently and with minimum application and infrastructure changes.

- Transparent in-line network-based encryption while providing flexible and secure access control
- Virtual appliance for hardware, operating system, and filesystem-independent deployment
- Flexible and secure access control provided by fine-grain read/write access control and host- and user-based access control serving all enterprise needs
- High-availability software appliances running in cluster for failover in mission-critical systems and load-balancing for high-throughput storage applications

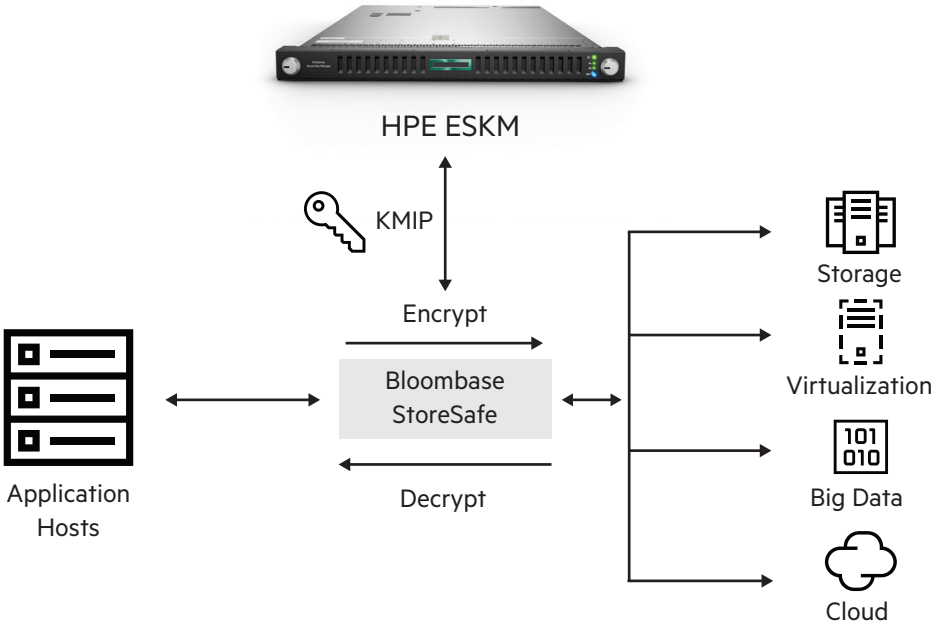

Figure 1. HPE ESKM and Bloombase StoreSafe protect sensitive data-at-rest from loss and help enable compliance with data privacy regulations

HPE ESKM and Bloombase StoreSafe benefits

- Encrypts data across heterogeneous systems by interoperating with current, legacy, and proprietary storage systems for key management
- Protects sensitive data-at-rest, and helps enable compliance with data privacy and security regulations with clear audit visibility
- Centralizes key management by separating keys from encrypted data to improve security, reliability, and availability at a global enterprise scale
- Provides scalable and flexible deployment of encryption over volumes of data from on-premises to cloud-based storage with a unified approach to hybrid IT
- Automates key operations—including lifecycle controls, key replication, and audit logging—to help simplify administration and lower the risk of a security breach

For more information about Bloombase StoreSafe and HPE ESKM interoperability, visit **protect724.hpe.com/docs/DOC-14697** and **bloombase.com/go/hpe**

Learn more at

voltage.com/eskm

hpe.com/software/datasecurity

Bloombase

bloombase.com

bloombase.com/go/storesafe

Sign up for updates

Hewlett Packard Enterprise

4AA6-9017ENW, January 2017