Hewlett Packard Enterprise

Centralize key lifecycle management for reliable storage encryption

HPE ESKM for NetApp Storage Encryption

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
- Automated key operations 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 to protect data-at-rest, reduce management costs, and increase overall compliance with industry and government regulations

Sensitive data is under constant threat of attack. Risks to data security such as industrial espionage, hacking, or even employee negligence make protection of enterprise data more important than ever. Enterprises are especially concerned about data-at-rest that resides in storage infrastructure as a primary vulnerable target. Additionally, enterprises have to be concerned with industry and government regulations that require reliable security controls in place, or suffer the consequences of fines and remediation penalties. In response to these threats and requirements, enterprises have turned to encryption as a well-proven method to achieve data security and meet regulatory compliance.

While encryption is needed to protect the increasing volume of sensitive data that is often used for analytics and business application purposes, protecting data within a storage infrastructure becomes a complex challenge when you are repurposing drives, disposing of defective drives, or upgrading systems. Implementing storage encryption can also be ineffective if performance is impacted and enterprises are still left with unreliable protection. There needs to be an easy and cost-effective way to secure enterprise data consistently, without affecting business operations.

Moreover, enterprises deploying encryption may quickly realize that although encryption is critical, it is not sufficient to provide a comprehensive security solution. Enterprises must also control access to the encryption keys across all encrypted data without interruption. As more data is encrypted, more keys need to be effectively controlled to ensure data can be decrypted when authorized.

Over time, a variety of key management schemes may evolve across encryption applications that can prevent the ability to securely and effectively manage encryption. Lack of a centralized policy to assure unified controls, unreliable manual procedures that do not enforce best practices for key lifecycle operations, low scalability to support new applications, no separation between applications and administrators, and similar hurdles increase complexity when deploying and maintaining several key management systems.

Security and regulatory compliance auditors realize that security is effective only when access controls and proper procedures are in place to manage encryption keys. The increased use of encryption across IT applications within an enterprise creates operational silos, which in turn lead to inconsistent controls, higher overhead from managing redundant key management systems, and unclear separation between applications. This can increase the level of risk and lead to time-consuming failed audits.

A systematic and centrally automated key management approach is a best practice method to maintain control over access to keys and to help ensure appropriate administrate rights are in place to manage keys. The bottom line: if you lose access to your keys, you lose access to your data!

Highlights of NSE
NSE is NetApp's implementation of full-disk encryption (FDE) using self-encrypting drives from leading vendors. NSE is a nondisruptive encryption implementation that provides comprehensive, cost-effective, hardware-based security that is simple to use. This single-source solution can increase overall compliance with industry and government regulations without compromising storage efficiency. With HPE ESKM and NSE, enterprises have a global solution for data protection by using a flexible approach that is extensible to future applications.

- Full disk encryption
- Complete transparency
- Mandatory data encryption

HPE ESKM and NSE benefits

- Accelerates security deployment through prequalification with NSE
- Lowers risk of data security breaches using reliable high-assurance, high-availability hardware
- Automates key lifecycle management for NSE across global environments
- Centralizes policy administration from the top down with a single system to access, maintain, and audit
- Reduces overhead by integrating and extending key management with other enterprise encryption applications

NetApp

netapp.com

netapp.com/us/products/storage-security-systems/netapp-storage-encryption.aspx

Learn more at
voltage.com/eskm
hpe.com/software/datasecurity

Sign up for updates

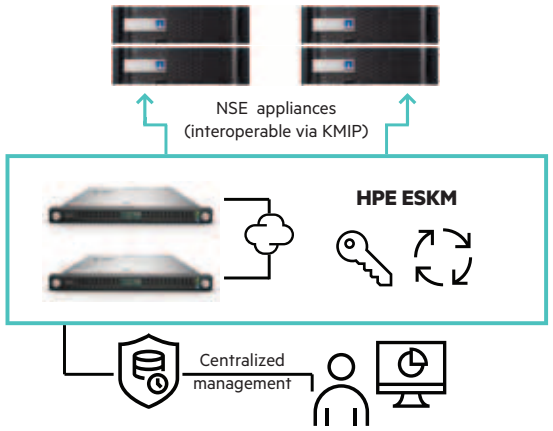

Figure 1: The HPE ESKM and NetApp NSE appliances help to protect sensitive data-at-rest from loss and facilitate compliance with data privacy and security regulations.

The solution

NetApp Storage Encryption (NSE) to protect data-at-rest and HPE ESKM to manage keys together offer a comprehensive security solution. NetApp NSE provides single source encryption without compromising storage efficiency and HPE ESKM offers a centralized management solution for unifying and automating an organization's encryption controls across IT. When deployed together, the solution helps businesses more quickly comply with regulatory mandates, simplify audits, and attest to controls in place that extend globally. Enterprises have a solution which achieves the following:

Accelerates security deployment through prequalification with NSE—HPE ESKM is prequalified for NSE appliances with support for KMIP interoperability. HPE ESKM and NSE make encryption easy to deploy to quickly meet security compliance goals. Storage teams minimize disruption using a turnkey approach that scales with data protection needs.

Helps lower risk of security breaches with high-assurance, reliable hardware—Long-term data retention requires reliable, continuous access to keys for recovery of encrypted data. The HPE ESKM appliance is designed for high availability, including redundant components, and automated key replication and backups for enterprises that require the highest levels of assurance for key recovery.

Automates key lifecycle management for NSE across global environments—Policy-based security controls are centrally administered and automated to help reduce management overhead and manual errors during each phase of a key lifecycle. Administrative rights avoid compromising applications with segregation between different applications, devices, and keys.

Centralizes security policy with a single system to access and audit—NSE may be segregated by geography and ownership while coexisting with other applications managed by HPE ESKM. Group separation provides unified visibility for multitenant environments. HPE ESKM makes auditing of encryption easy, quick, and reliable by reducing application silos, so security and compliance teams can now enforce policy that is consistent across a global environment.

Increases ROI by integrating with other encryption applications—HPE ESKM and NSE support OASIS KMIP for compatibility with other standards-based key management applications. The extensible approach enables consistent management when adopting future enterprise-encryption applications to deliver the same level of high assurance security.

Hewlett Packard Enterprise

a00000477ENW, January 2017