Hewlett Packard Enterprise

Data Security Protection for HPE Helion

HPE ESKM and HPE SecureData for HPE Helion hybrid cloud

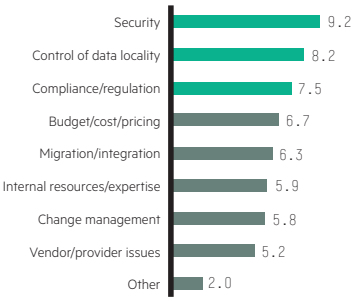
HPE Enterprise Secure Key Manager (ESKM) and HPE SecureData along with HPE Helion enable enterprises to extend data to the cloud computing solutions with a high level of security assurance.

About HPE Security—Data Security
HPE Security—Data Security brings leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise, we protect the world's largest brands and neutralize breach impact by securing sensitive data-at-rest, in-use, and in-motion. Our solutions provide advanced encryption, tokenization, and secure key management that protect sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission-critical transactions, storage, and Big Data platforms. HPE Security—Data Security solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases.

A hybrid cloud architecture

Improved economics, performance, capacity, and demand
Today's enterprises are turning to hybrid cloud computing architectures for improved economics, scalable performance and capacity, high availability, and on-demand IT tuned to the needs of individual workloads. However this means conquering the challenges of protecting data from security breaches, fulfilling data residency requirements, avoiding adverse legal actions, and minimizing the impact of operational negligence as sensitive information is exposed to new risks within multi-tenant, multi-cloud environments. HPE Enterprise Secure Key Manager (ESKM) and HPE SecureData along with HPE Helion enable enterprises to extend data to the cloud-computing infrastructure with a high level of security assurance. Controls over sensitive information are maintained using data-centric encryption and tokenization, full-disk encryption, and enterprise secure key management lifecycle support for HPE Helion OpenStack® cloud computing deployments.

IT leaders recognize transformation risks
Security and compliance remains a priority for cloud adoption



Source: 451 Research, Voice of the Enterprise: Cloud Computing, Q3 2015

Embrace cloud—knowing your data is secure.
HPE Security solutions for cloud deployments:

HPE Enterprise Secure Key Manager (ESKM)
Secure server, storage, and cloud data against losses, mishandling, and administrative and operational attacks, with seamless application interoperability and proven HPE Secure Encryption.

HPE SecureData
Secure sensitive data and maintain data residency and compliance while enabling existing business process and workflows with NIST Standardized (SP800-38G) HPE Format-Preserving Encryption (FPE); while enabling analytics on sensitive data in multi or hybrid cloud environments.

HPE Helion OpenStack
Provides end-to-end security for hybrid environments. Successful enterprises of every industry and size partner with HPE Helion to drive business outcomes.

Data protection at-rest, in-motion, and in-use

HPE Security—Data Security solutions and HPE Helion OpenStack hybrid cloud
Enterprises are now attaining the operational agility, IT scalability, and cost savings benefits enabled by cloud-deployed applications and workloads. However, the challenges of protecting data and maintaining regulatory compliance remain top concerns often inhibiting broader cloud technology adoption. Unique concerns include maintaining separation among multi-tenant environments, managing cloud administrator access risks, mitigating security gaps between connected multi-cloud environments, and addressing data residency requirements in the context of a physically distributed cloud infrastructure. With an enterprise's sensitive information at risk of exposure to loss and improper access in hybrid environments, security must be considered an integral part of an evolving IT strategy to avoid data being compromised.

HPE Security—Data Security, in partnership with HPE Helion OpenStack hybrid cloud, enables enterprises to achieve the benefits of hybrid cloud IT deployment by securing sensitive data throughout its entire lifecycle—at-rest, in-motion, and in-use—with continuous protection across the cloud, on premise, in transit, and through mobile-accessed environments.

Many enterprises use the cloud for economic data storage. HPE ESKM appliances offer high-assurance hardware security for keys and centralized management over archived, encrypted data-at-rest. ESKM integrates with HPE Secure Encryption to protect data at the server platform level within HPE Helion Cloud deployments, and uses built-in OpenStack encryption, leveraging Barbican, for project multi-tenant solutions. The approach enables authorized access to data and high availability using redundant key management servers for maintaining long-term business continuity.

By safeguarding keys in a tamper-evident key management appliance—externalized from the sensitive data in an HPE Helion OpenStack deployment—ESKM provides the necessary separation of encrypted data from the keys, a security best practice. ESKM's centralized controls across tenants for projects and full disk encryption (FDE) provide a single-pane-of-glass view into encryption key policy enforcement and auditing for attesting to regulatory controls in place.

HPE SecureData for Cloud is a unique, proven data-centric approach to protection—where the access policy travels with the data itself—by permitting data encryption and tokenization without changes to data format or integrity, and eliminating the cost and complexity of issuing and managing certificates and symmetric keys. As data is moving through traditional infrastructure and hybrid cloud IT, HPE SecureData for Cloud enables enterprises to protect data before it exits traditional IT infrastructure, as it transits public networks and is used within the cloud, while still enabling day-to-day business processes and analytics on protected data. HPE SecureData for Cloud delivers a data-centric framework that comprehensively protects all enterprise data across applications and storage, enabling secure movement and use of data within the cloud. Data is encrypted at capture and protected throughout the entire data lifecycle, wherever it resides and wherever it moves. HPE SecureData for Cloud protects information in compliance with PCI DSS, HIPAA, GLBA, state and national data privacy regulation as well as the European Commission's General Data Protection Regulation (applicable in all EU member states).

Security protection

OpenStack and Data Security protection
By using technologies from both HPE Helion OpenStack services and HPE Security—Data Security products, security protection is achieved in a multi-layered approach that enables customers to protect their data through its lifecycle, at-rest, in-use, or in-motion. To summarize, security protection is achieved via the following:

- **Data protection using hardware platform-based full disk encryption (FDE)**

  Full disk encryption (FDE) at the platform level is implemented for HPE Helion OpenStack using HPE ProLiant Gen8 or Gen9 servers with Smart Array controllers running HPE Secure Encryption, along with HPE ESKM for centralized secure key management. This capability has been tested for compatibility with HPE Helion OpenStack v3.0 and is integration-ready and qualified, out-of-the-box.

- **Data protection using tenant (project)-based encryption**

  Tenant-based encryption is achieved for sensitive data-at-rest on a per-tenant project basis, while storing and managing keys externally and centrally using HPE ESKM. This capability requires the OpenStack Barbican API and an OASIS Key Management Interoperability Protocol (KMIP) plugin for integration, and supports encryption of Cinder block storage with HPE Helion OpenStack v3.0.

- **Data protection using data-centric security (multi-cloud environments)**

  Data-centric security protects data through encryption and tokenization, enabling the secure movement of data across IT environments, and end-to-end defense spanning cloud and traditional infrastructure. HPE SecureData for Cloud protects sensitive data through HPE Format-Preserving Encryption (FPE), HPE Secure Stateless Tokenization (SST), and HPE Stateless Key Management—enabling a unified architecture for compliance, audit scope reduction, and cross-cloud analytics on protected data. HPE SecureData is compatible with HPE Helion OpenStack v3.0.

Cloud best practices

Complete Helion cloud deployment protection
Data-centric encryption and tokenization, server platform-level encryption, and integrated secure key management can help customers meet their data protection requirements for secure hybrid cloud computing deployments. HPE ESKM and HPE SecureData, together with HPE Helion OpenStack Hybrid Cloud, provide a best-practice multi-layered security approach to maximize protection of sensitive data. Customers can rest assured that their data is safe whether at-rest, in-motion, or in-use—on premise and in the cloud.

Learn more at
hpe.com/software/DataSecurity
voltage.com

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-5241ENW, May 2016