Data Security Protection for Helion

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

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, multicloud environments. Enterprise Secure Key Manager (ESKM) and SecureData along with 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 Helion OpenStack cloud computing deployments.

Data Protection At-Rest, In-Motion, and In-Use
Micro Focus Data Security Solutions and 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.

Micro Focus Data Security, in partnership with 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-premises, in transit, and through mobile-accessed environments.

Many enterprises use the cloud for economic data storage. ESKM appliances offer high-assurance hardware security for keys and centralized management over archived, encrypted data-at-rest. ESKM integrates with Secure...
Encryption to protect data at the server platform level within 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 a 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 of encryption key policy enforcement and auditing for attesting to regulatory controls in place.

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, 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. 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. 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 Helion OpenStack services and Micro Focus 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 Helion OpenStack using HPE ProLiant Gen8 or Gen9 servers with Smart Array controllers running Secure Encryption, along with ESKM for centralized secure key management. This capability has been tested for compatibility with 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 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. SecureData for Cloud protects sensitive data through Hyper Format-Preserving Encryption (FPE),
Voltage Secure Stateless Tokenization (SST), and Voltage Stateless Key Management—enabling a unified architecture for compliance, audit scope reduction, and cross-cloud analytics on protected data. SecureData is compatible with HPE Helion OpenStack v3.0. Cloud Best Practices.

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. ESKM and 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-premises and in the cloud.

Learn more at www.microfocus.com/securedata