

SOLUTION BRIEF



Encrypting Data in the Cloud:

Skyhigh Cloud Security Platform and Gemalto SafeNet

Cloud-based services are helping organizations operate more easily and more efficiently than ever before. Moving to the cloud also means lower costs, faster time-to-value, and increased employee productivity. While advantageous for many reasons, moving all or portions of an enterprise's operations to the cloud introduces a certain level of risk. With data traveling offsite, how does an organization ensure the security and privacy of its sensitive data?

The Solution

Skyhigh Networks and Gemalto combine to securely enable the adoption of cloud services. Skyhigh Cloud Security Platform transparently encrypts data stored in cloud services according to defined security, privacy, and regulatory policies. SafeNet KeySecure manages the encryption keys used by Skyhigh Cloud Security Platform from a central location so that security administrators can simplify their security deployment. When deployed together, organizations can confidently take advantage of cloud services knowing their data is secure at all times.

Skyhigh Cloud Security Platform

Skyhigh Cloud Security Platform is a security service – available in the cloud, on-premise, or as a hybrid deployment – that encrypts both structured and unstructured data in cloud services. Skyhigh delivers standards-based AES and function-preserving encryption modes that support searching, sorting, and formatting capabilities even when data is encrypted. Administrators can set specific policies to determine which fields should be encrypted or tokenized in order to ensure automatic, uniform security across the cloud deployment.

SafeNet KeySecure

SafeNet KeySecure is a key management server (available as a physical or virtual security appliance) that centralizes the administration (e.g. key generation, rotation, recovery,

Executive Summary

Organizations can maintain exclusive control over the keys encrypting their sensitive data headed to the cloud while also preserving cloud application functionality. The solution can be hosted via the cloud, on-premises, or as a hybrid deployment to help optimize resources.

Key Benefits

- > **Access the cloud from mobile devices without traffic backhaul:** Skyhigh Cloud Security Manager allows mobile devices to access cloud resources without requiring an agent or VPN connection.
- > **Efficiently manage encryption:** Central platforms for both cloud encryption and key management reduce the cost and effort of securing multiple cloud services and managing the keys for disparate security solutions.
- > **Detailed audit trails:** Skyhigh records detailed application usage data such as views, updates, and downloads. SafeNet KeySecure records all key state changes for full transparency in key management.
- > **Regulatory compliance made easy:** Skyhigh's encryption renders data unreadable to unauthorized users (including third-party administrators managing the cloud infrastructure), satisfying many industry and government regulations.
- > **Nullify notification requirements:** In the event of a breach, security teams can nullify HIPAA and HITECH notification requirements by rendering the data forever useless through deleting its encryption key.

escrow, etc.) of cryptographic materials from across an organization's encryption infrastructure. KeySecure's support of the OASIS Key Management Interoperability Protocol (KMIP) allows customers to manage keys and certificates for a broad ecosystem of encryption solutions, in addition to the keys for Skyhigh Cloud Security Platform.

SafeNet Luna SA

Luna SA HSMs are robust, high-availability, high-performance appliances that maximize the integrity and security of cryptographic operations. These tamper-proof key storage appliances have been certified FIPS 140-2 Level 3 compliant. Luna SA protects encryption keys in a hardware appliance away from the reach of unauthorized users. Highly specific, tailored rights administration enhances the security surrounding the keys further mitigating any risk to valuable cryptographic materials.

Skyhigh Cloud Security Platform and CloudHSM

For organizations using AWS CloudHSM, Skyhigh functions as a key brokering and distribution provider, enabling secure deployment and retrieval of keys across multiple cloud service providers. This enhances performance for key exchanges, which can also be used to support application layer encryption vs. "gateway only" deployment models.

Key Features

Encryption that preserves the user experience

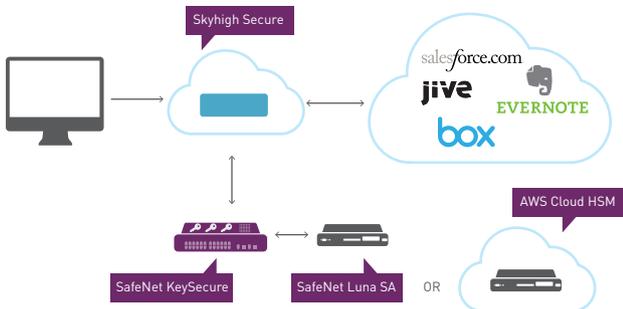
Skyhigh Cloud Security Platform transparently encrypts data, yet preserves sort, search, and format functionalities. No agent, third-party application, or mobile-device VPN is required to securely access cloud based data.

Quick and easy setup

Using the KMIP standard for its integration, SafeNet KeySecure deploys easily to manage Skyhigh Cloud Security Platform's encryption keys. Since, KeySecure is capable of managing the cryptographic material of any solution that employs the KMIP standard, additional security solutions can get up and running quickly while preserving the integrity of the keys at the root of the offering.

One gateway, one key manager

Skyhigh Cloud Security Platform serves as a central point of contact for the cloud services it protects. By connecting KeySecure to manage the infrastructure's encryption keys, administrators can employ encryption for any number of cloud-based services connected to Skyhigh. This streamlined solution makes uniform encryption and policy management easier for large organizations that may leverage multiple cloud services.



Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: data-protection.safenet-inc.com

 GEMALTO.COM

Use Cases

- > **Cloud encryption** - secure data as it is stored in cloud environments.
- > **Key Management** - centralize key management from across departments and disparate encryption solutions.
- > **Logging and auditing** - record all key state changes to monitor security administrator activity.
- > **Key availability** - ensure that encryption keys are always available to decrypt secured data.
- > **Manage multiple key types** - centrally manages symmetric, asymmetric, secret data, and X.509 certificates

Customer: Top 10 Global Insurance Firm

Key Drivers: Protect personally identifiable information (PII) uploaded to Salesforce.com and customer-facing applications on Force.com. Encrypt and decrypt data for all traffic to and from Salesforce.

Solution: Leverage AWS CloudHSM and SafeNet HSM appliances by Gemalto with Skyhigh acting as the key broker.

Key Benefits:

- > Protected sensitive data uploaded to Salesforce.
- > Nullified any breach notification requirements.
- > Experienced no network backhaul due to a 100% cloud-based solution.

Visit www.skyhighnetworks.com and www.safenet-inc.com to learn more.

About Gemalto's SafeNet Identity and Data Protection Solutions

Gemalto's portfolio of SafeNet Identity and Data Protection solutions enables enterprises, financial institutions and governments to protect data, digital identities, payments and transactions—from the edge to the core. Our solutions take a data-centric approach to security with innovative encryption methods, best-in-class crypto management, and strong authentication and identity management to help customers protect what matters, where it matters.


security to be free