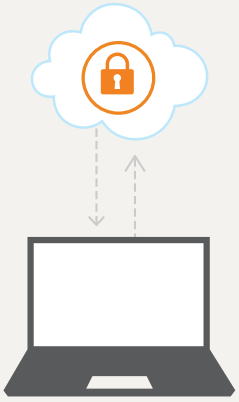


SOLUTION BRIEF

Maintain Data Privacy and Security as You Migrate to the Cloud

Together, Vaultive and Gemalto allow complete protection, ownership and control of your ever-expanding data and cryptographic keys—on either virtual machines or dedicated physical devices hosted on-premises, or in the cloud.

Introduction

Today, organizations are leveraging multiple SaaS providers in order to deliver business-critical cloud-based applications, such as Office 365 and other enterprise cloud services. While these relationships can limit duplication of efforts and enable flexibility and cost savings, they can also raise management and security concerns. Maintaining independence and control over your organization's data while leveraging a third-party environment can be a challenge.

In the case where the cloud service provider performs the encryption, they can gain access to your unencrypted data. Even with native security features like bring your own key (BYOK), the service provider still requires access to your keys in order to preserve application functionality. This ability for a third party to access plain text data, particularly email and files, can lead to privacy and compliance issues associated with data sovereignty and residency requirements, leaving many organizations hesitant to adopt this business model.

Fortunately, Vaultive and Gemalto provide a solution to fill those gaps, affording the security and control increasingly required by organizations to fearlessly take advantage of cloud services and their inherent benefits.

Organizations can also deploy the SafeNet Authentication Service alongside Vaultive's Cloud Data Security Platform to provide both strong identity and data protection, addressing a broader set of threats aimed at unauthorized access to data in the cloud.

Solution

Gemalto and Vaultive join forces to secure your data in the cloud

The Vaultive Cloud Data Security Platform encrypts SaaS application data for the entire duration of its lifecycle in the cloud while preserving SaaS user functionality, and SafeNet KeySecure offers secure and centralized key management. Integrating these two solutions allows for best-practice separation of controls between an administrator managing the cloud environment and an organization's security professionals managing the data protection and encryption keys. This separation of controls removes major barriers to cloud adoption by ensuring that service providers do not have access to plain text data nor encryption keys. This in turn supports adherence to complex data residency and privacy regulations as well as to industry-specific compliance requirements when moving to the cloud—ultimately giving your organization the protection you need to move data to the cloud.

Key Features

- **Quick adoption of cloud services:** The powerful rule-based policy engine built into Vaultive's Cloud Data Security Platform enables rapid integration with your web-based SaaS applications. Best-practice methods ensure data is encrypted at the boundary of an organization's protected network, and IT teams retain exclusive control of encryption keys.
- **Easy management and consolidation:** An integrated solution 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.
- **Multiple deployment approaches:** Manage and deploy keys in physical, virtual, and public cloud environments.
- **Flawless user experience:** Patented processes preserve characteristics of the data so that it can be indexed, searched, and sorted while remaining encrypted, with no end user training or action required.
- **Exclusive ownership and custody of the encryption keys:** Using the Key Management Interoperability Protocol (KMIP) standard, SafeNet KeySecure can centrally manage the data owner's keys. Since SafeNet KeySecure is capable of managing the cryptographic material of any solution that employs the KMIP standard, additional solutions can be integrated quickly while preserving the integrity of the data encryption keys at the root of the offering.

The Vaultive Cloud Data Security Platform

The Vaultive gateway operates as a stateless network-level software encryption proxy, which can support any web-based application. The Vaultive Cloud Data Security Platform provides a flexible means of configuring any web-based SaaS application based on a set of generic policy-based rules that can be easily customized to meet your data security requirements.

The Vaultive gateway is implemented as a redundant, high availability cluster of virtual appliances that resides in the pathway between the organization's network and the cloud service provider. As data flows between the organization and the cloud, the Vaultive gateway intercepts and automatically encrypts data in transit to and from the cloud, ensures that data at rest in the cloud is encrypted, and keeps the data encrypted while in use in the cloud. The Vaultive Cloud Data Security Platform can be deployed behind the firewall, in the DMZ or at a trusted third party.

SafeNet KeySecure from Gemalto

SafeNet KeySecure from Gemalto is the industry's leading centralized key management platform, and is available as a hardware appliance or hardened virtual security appliance. By utilizing SafeNet KeySecure, organizations benefit from its flexible options for secure and centralized key management—deployed in physical, virtualized infrastructure, and public cloud environments.

Only Gemalto can deliver key management tamperproof, FIPS-validated appliances supporting a hardware root of trust using SafeNet Hardware Security Modules or Amazon Cloud HSM service.

Key Benefits

Simple, Instant Enablement of Control & Ownership of Data

Separating encryption and key ownership from the duties of the Cloud Service Provider (CSP) administrator and security professionals offers you unmatched control of and access to the data you store in the cloud. Vaultive encrypts cloud data throughout the entire lifecycle, while organizations retain control and ownership of keys. SafeNet KeySecure provides centralized key management for multiple key types from across departments and disparate encryption solutions.

Privacy & Confidentiality of Data

Cloud service providers are required by law to comply with subpoenas and other requests by the government to turn over customer data, including data subject to attorney-client privilege. In some instances, the cloud provider may even be expressly prohibited from notifying its customers. With Vaultive, because the keys are managed by the data owner using SafeNet's KeySecure, any data provided by third-party organizations is encrypted.

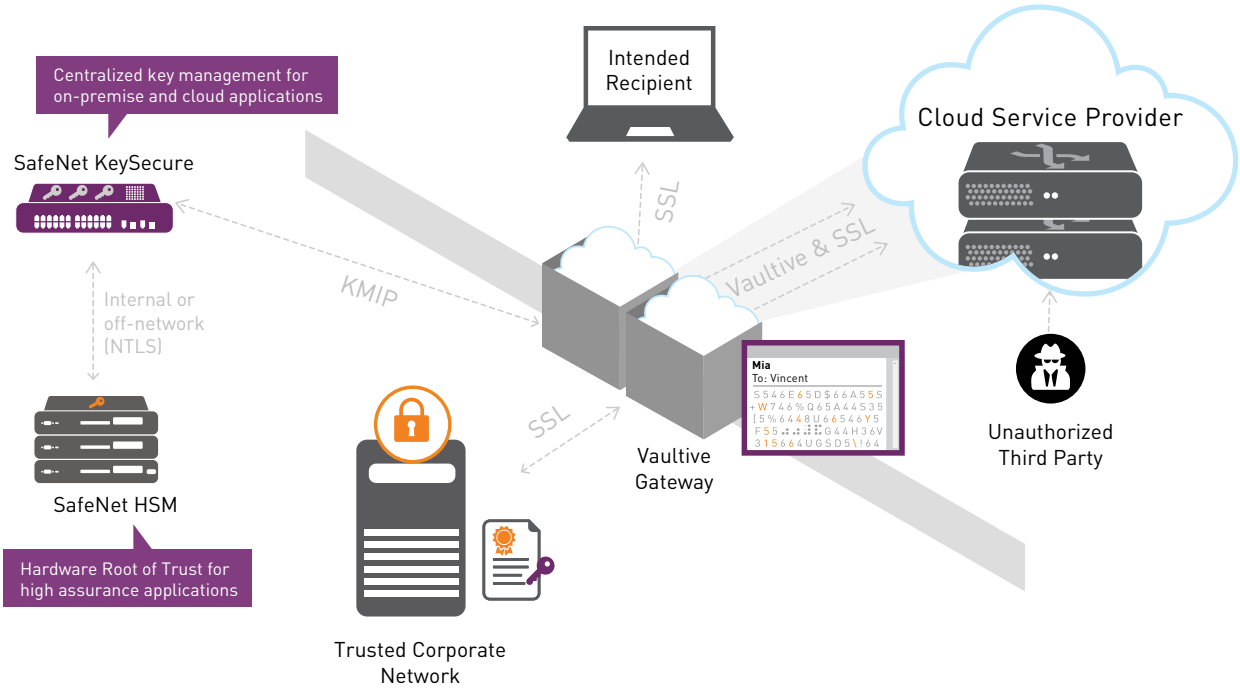
Addressing Data Residency Regulations, as seen with EU GDPR

Multi-national organizations face the challenge of complying with evolving privacy and data residency regulations. Vaultive encrypts data in each jurisdiction per the requirements and regulations of the territory, and the encryption keys are held within that territory.

Regulatory Compliance Made Easy

Vaultive helps customers in regulated industries fulfill mandates, such as FDIC, HIPAA-HITECH, GLBA and PCI-DSS, which include requirements for data protection technical safeguards. Vaultive ensures all data is encrypted per organizational policies before leaving the trusted network, while SafeNet KeySecure records all key state changes for full transparency and detailed audit trails.

Vaultive-SafeNet Joint Solution



About Vaultive's Cloud Data Protection Platform

Vaultive, a cloud data security company, enables organizations to move securely to Office 365 and other leading cloud platforms. The Vaultive Cloud Data Security Platform automatically encrypts data before it goes to the cloud and gives sole custody of the encryption keys to the customer. This approach gives organizations complete control and ownership of their data wherever it resides while delivering a seamless, native experience to software-as-a-service end users.

About Gemalto's SafeNet Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions—from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

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

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free