Cloud applications pose a challenge to organizations seeking GDPR compliance. Gemalto and Vaultive work together to keep data safe and help achieve GDPR compliance.

**Safeguard Cloud Data with Encryption and Key Management:** Strong encryption is an essential way to establish data confidentiality and privacy. It can also exempt an organization from GDPR’s 72-hour data breach notification requirement. For software as a service (SaaS) applications running in the public cloud, it’s important to enforce best-practice segregation of duties between the service provider administering the cloud environment and corporate IT managing data protection policies and encryption keys. This separation of controls removes major barriers to cloud adoption by ensuring service providers have access to neither plain text data nor the customer’s encryption keys — ultimately, keeping customers in control as they securely share their data.

**Control Access:** Frequently, it is weak static credentials that are exploited to gain unauthorized access to sensitive resources or perpetuate a full-blown data breach. A robust Identity and Access Management (IAM) solution continuously monitors user activity throughout a SaaS application session to force step-up authentication for sensitive actions. Continuous contextual authentication is critical to ensuring only authorized users are accessing sensitive data and PII in the public cloud.

Gemalto-Vaultive Cloud Data Protection Solution

- Includes: SafeNet KeySecure + Vaultive Cloud Security Platform + SafeNet Authentication Service (SAS)
- Vaultive acts as a cloud encryption complement to SafeNet’s Data Protection Platform
- Identity protection + cloud data encryption with key management = strong data protection to help meet GDPR guidelines

**GDPR and Encryption**

- Experts predict that confirming that encryption measures are in place to secure and control data will be among the first steps regulators will take when investigating potential GDPR violations.
- Organizations using strong encryption and access control can demonstrate they are taking appropriate steps to mitigate risk.
- Under no circumstance is personal data allowed to leave the EU in response to a foreign government’s subpoena or data request without a prior international agreement in place. Gemalto and Vaultive enable organizations to maintain best-practice segregation of duties to help address this challenge.
- Exemptions from having to announce a breach not only saves resources/money but also prevents damage to brand reputation.

**Vaultive Cloud Security Platform**

The Vaultive Cloud Security Platform is a unified security and governance solution that protects sensitive data and user activity across an organization’s cloud security footprint through a powerful combination of context-aware policy controls, feature-preserving encryption, and auditing and alerting. The Vaultive platform integrates rapidly with both mainstream SaaS applications and custom web applications to protect data and promote secure, compliant application usage.
Gemalto SafeNet KeySecure

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.

Cloud Data Encryption Features

- Maintain data privacy and security in the public cloud by encrypting data before cloud exposure and retaining sole control of the encryption keys.
- Provide a seamless user experience with patented feature-preserving encryption, so that data can be indexed, searched, and sorted while remaining encrypted in the cloud.
- Enforce best-practice segregation of duties between the service provider administering the cloud environment and the organization’s sensitive data.
- Provide a centralized platform that secures multiple data types across a range of cloud applications. Supports multiple encryption keys per application and simplifies compliance with data residency and privacy.
- Meet FIPS 140-2 Level 1, 2, or 3 depending on the specific HSM configuration in the SafeNet KeySecure.

Identity and Authentication Features

- Leverage SafeNet Authentication Service (SAS) to enforce robust multi-factor authentication for user login to popular SaaS applications.
- Provide continuous authentication post-login when users perform potentially risky behaviors or access sensitive SaaS application features – the Vaultive platform can detect this and invoke SAS to re-authenticate or step-up authentication.

About Gemalto’s SafeNet Identity and Data Protection Solutions

Gemalto’s portfolio of Identity and Data Protection solutions 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 SafeNet Identity and Data Protection solutions enable 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/contact-us

Follow Us: blog.gemalto.com/security