Guardium for Cloud Key Management

Many Infrastructure-, Platform-, and Software-as-a-Service providers offer data-at-rest encryption capabilities with encryption keys managed by the service provider. Meanwhile, many industry guidelines, internal data protection mandates, and industry best practices recommend that keys be stored and managed separately from the cloud service provider and the associated encryption operations. Providers can help their customers fulfill these requirements by offering "Bring Your Own Key" (BYOK) services to enable customer control of the keys used to encrypt their data. Customer key control allows for the separation, creation, ownership, and revocation of encryption keys or tenant secrets used to create them.

Leveraging cloud providers' BYOK APIs, *Guardium for Cloud Key Management* reduces key management complexity and operational costs by giving customers lifecycle control of encryption keys with centralized management and visibility.

Highlights

- Full lifecycle cloud encryption key management
- Leverage the value of "Bring Your Own Key"
- Centralized key management across cloud environments
- Automated key rotation and key expiration management

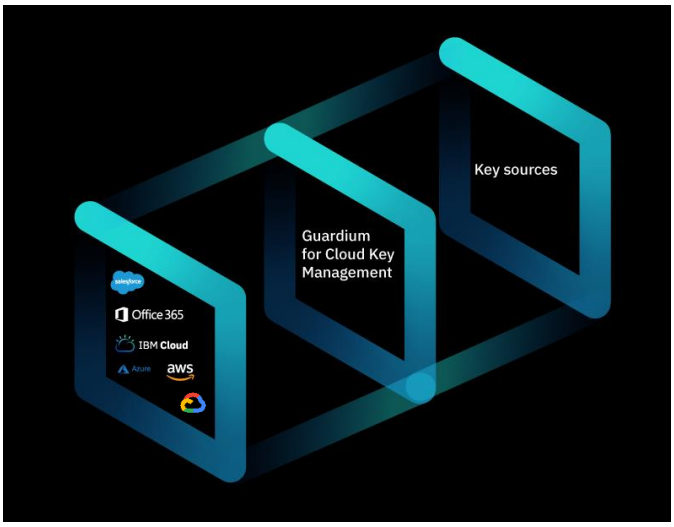
The key control imperative

The requirement to protect sensitive data across Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) has resulted in broader cloud provider encryption offerings. Meanwhile, industry experts such as those from the Cloud Security Alliance recommend that encryption keys be held by customers. As the quantity of encryption keys needing to be secured and managed across multiple clouds increases, so too does challenge of holding keys. There is also the imperative of knowing how, when and by whom encryption keys are used. *Guardium for Cloud Key Management* provides comprehensive key lifecycle

management to fulfill requirements for safe, comprehensive key management across multiple clouds.

Supported clouds include:

- Microsoft Azure
- Microsoft Office365
- Microsoft Azure Stack
- Microsoft Azure China and Germany National Clouds
- Amazon Web Services
- IBM Cloud
- Google Cloud
- Salesforce.com
- Salesforce Sandbox



Enhanced IT efficiency

Guardium for Cloud Key Management offers multiple capabilities in support of enhanced IT efficiency:

- Centralized key management gives you access to your cloud providers from a single browser window, across multiple accounts or subscriptions
- Automated key rotation offers IT efficiency and enhanced data security

- Cloud service logins are authenticated and authorized by the service provider—no login database, AD or LDAP configuration is required
- For workloads that require it, *Guardium for Cloud Key Management* can request creation of native cloud provider keys and provide full lifecycle management for them
- With varying key technologies and terminology, *Guardium for Cloud Key Management* presents key operations in the semantics of the cloud provider
- Already created thousands of keys at your cloud provider? *Guardium for Cloud Key Management* can synchronize its database with keys created at the cloud provider

Strong encryption key security

Customer key control presents requirements for secure key generation and storage. *Guardium for Cloud Key Management* leverages the security of the Data Security Manager and supported hardware security modules (HSMs) to create keys and store them with FIPS 140–2 Level 1 security. With the requirement for key security mechanisms such as safe storage of cloud backup keys, *Guardium for Cloud Key Management* acts as a key escrow for supported clouds and allows for full key metadata control both during upload and for keys in use.

The compliance tools you need

Guardium for Cloud Key Management's cloud-specific logs and prepackaged reports offer fast compliance reporting. Logs may also be directed to a syslog server or SIEM. The solution can be deployed rapidly on-premises to help address more stringent compliance requirements.

Guardium for Cloud Key Management simplifies the need to hold and manage encryption keys for cloud services, a critical solution for fulfilling industry and organizational data protection mandates.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security

---

© Copyright IBM Corporation 2020.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at https://www.ibm.com/legal/us/en/copytrade.shtml, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

Discover how IBM Security Guardium solutions can help you take a smarter, integrated approach to safeguarding critical data across your hybrid, multicloud environments. Visit ibm.com/security/data-security/guardium