IBM Multi-Cloud Data Encryption

Encrypt sensitive data in cloud and hybrid environments with policy-based access controls, built-in key management, and audit logging.

Highlights

- Manage encryption and policy enforcement across your entire enterprise from a single point
- Easily design and administer data access policies with customer-defined roles at the user, group and process level
- Protect sensitive data with sophisticated cryptographic splitting technology
- Leverage integrated, transparent key management that conforms to industry regulatory requirements and provides simplified and centralized key management
- Be audit ready with user access and activity logs that seamlessly integrate into existing Security Information and Event Management (SIEM) systems

Security and privacy concerns continue to be the biggest barriers to cloud adoption. In fact, an overwhelming majority of 91% of organizations are very or moderately concerned about public cloud security[1]. Strong perimeter security is a good security step, but the sensitive data itself must also be protected for compliance and security purposes. Perimeter security has extremely limited data control, and creates a lack of security and privacy in cloud environments, making organizations hesitant to trust their data - particularly sensitive data - to third-party cloud providers. Additionally, with cyber security threats rapidly growing from external attacks as well as from insider threats, data has become ever more vulnerable to compromise.

Having a “cloud-first” strategy can provide organizations agility, operational efficiencies and competitive advantage. However, underlying concerns regarding data privacy, security, and unauthorized access to data that’s in the cloud, makes organizations cautious about migrating workloads to the cloud. Complicating a multi-cloud deployment is the challenge of implementing a singular data protection strategy across the enterprise while complying with continually increasing and costly regulatory mandates. Subsequently, organizations can no longer solely rely on the cloud provider for outsourcing security and compliance, because the responsibility and risk ultimately falls on the organization.

Data-centric protection must be deployed by the enterprise. Data-centric protection should not only encrypt data, but also provide robust access control and audit logging capabilities. Following these key requirements will help ensure that an enterprise’s data is accessed according to the organizational roles and processes they set. Enterprise controlled policy and key management should also be an integral part of any comprehensive solution. The solution must be easy to deploy, administer and manage across all environments: and scalable as the enterprise grows.

IBM® Multi-Cloud Data Encryption focuses on the critical data protection concerns that customers face when moving to the cloud, thereby reducing the risk of, and making it easy to adopt an essential cloud-first strategy with a data-centric approach. Multi-Cloud Data Encryption provides a broad range of features, including data access management, integrated key management, and sophisticated encryption that combine to deliver the scalability and flexibility to help protect the most sensitive workloads - across the enterprise.

ACHIEVE OPERATIONAL EFFICIENCY

The Multi-Cloud Data Encryption offering, which is part of the larger IBM Data Security and Protection portfolio, allows you to manage the data encryption process across private, public, and cloud environments -- from a single vantage point. Its easy-to-use, agent-based deployment model helps protect sensitive data on servers (physical or virtual), no matter where the data resides. Multi-Cloud Data Encryption is tightly integrated with other IBM Security products such as IBM QRadar Security and Information Event Manager (SIEM) and IBM Security Key Lifecycle Manager (SKLM).

Single-Pane-of-Glass Management

The Multi-Cloud Data Encryption centralized virtual management console provides a single location from which you can provision, deploy and manage all instances of the product's encryption agents across the enterprise. It is easily deployed as a virtual appliance into any virtualized environment across one or more data centers. From that server, the agents are deployable to any virtual or physical server running a supported Operating System (OS). You can host the management server wherever you choose, including on-premises. This approach enables you to keep your keys out of the cloud environment while managing data encryption remotely.

The Multi-Cloud Data Encryption console helps provide a holistic view of your data encryption and supports cryptographic control over policy enforcement and user data access across your data center environment. From this console, you also can define and manage access policies, create and manage keys, and aggregate access logs.

Scalable, agile and easy to use

Multi-Cloud Data Encryption can scale to protect large enterprise workloads and easily integrates into existing or new multi-cloud architectures. The management console can be made highly available in any environment to provide access to data when needed, and it can be distributed across data centers to support disaster recovery (DR) architectures. It supports IBM's Bluemix cloud, as well as other cloud and data center environments.

RESTful APIs for Enterprise-wide Integration and Deployment

Multi-Cloud Data Encryption uses a RESTful API so that automation can be easily applied. All management console functions are available via the API. Large-scale deployments can be managed using the API and basic scripting. This facilitates resource and cost savings and eliminates barriers to entry.

Transparent to the End User

Multi-Cloud Data Encryption agents operate at the OS level of the servers they are deployed on, performing efficiently at the kernel level. Data is protected transparently during the process of writing files to disk without end-user interaction and without a significant impact on performance.

MITIGATE RISK & MANAGE COMPLIANCE

IBM Multi-Cloud Data Encryption helps organizations reduce the risk of data exposure and meet compliance mandates, whether regulated or voluntary, as part of an overall information security process. You can easily manage the who, what, where, when and how of data access.

Role-Based Data Access Controls

Working with your existing directory services, Multi-Cloud Data Encryption's robust role-based access controls allow an administrator to define a second layer of data access control policies that are based upon roles and job functions. This additional policy is used to specify which filesystem functions are authorized (read/write/etc.) and the level of data access logging desired. By limiting access to only designated users, Multi-Cloud Data Encryption can help ensure sensitive data is secure and private.

These access policies start with the default concept of Least

Privileged Access (LPA) to control access rights for users, groups or processes. LPA denies access to users unless they have been specifically granted access permissions through a customer-defined policy. The product works in conjunction with a directory service (e.g. Lightweight Directory Access Protocol (LDAP), Active Directory2), and the user must be granted rights in both systems to access and view decrypted data.

Privileged Access Management (PAM) restrictions can be enforced via policy, which helps prevent system administrators and root users from seeing clear text data. This allows privileged users to do their job without accessing or stealing private data, giving you vital control over data privacy and confidentiality, even when entrusting data to a cloud service provider.

Distinct Separation of Administrative Duties

By default, Multi-Cloud Data Encryption creates two distinct roles – the Product Administrator and the Security Administrator. The Product Administrator deploys the software and monitors the general health of the Multi-Cloud Data Encryption system and agents through system event logs. This role has no visibility into policy definitions, agent configurations, deployments or policy logs. The Security Administrators determine and approve data access rights, manage keys, define policies, deploy agents, set logging parameters, enable multi-factor authentication, and create the multi-Security Administrator approval process. The required number of Security Administrator approvals can be set based upon business needs.

Always on Data Protection, Powered by SPx™

Multi-Cloud Data Encryption provides cryptographic splitting technology that helps assure confidentiality, data privacy, and protection against brute force attacks. The SPx™ core combines AES-256 certified encryption, cryptographic splitting, and internal key management, and it has received a National Institute of Standards and Technology (NIST) FIPS 140-2 validation. Multi-Cloud Data Encryption also takes full advantage of the AES-NI4 hardware acceleration available in most current processors for optimal performance. Multi-Cloud Data Encryption allows customers to deploy agents that encrypt data at the volume-level and/or at file/directory level for additional granularity.

IBM Multi-Cloud Data Encryption delivers enterprise-grade data encryption for your data with minimal operational impact. Its easy-to-use, highly scalable technology makes implementing a “protect everything” approach to data security.

Integrated and Transparent Key Management

With its unique integrated and transparent built-in key management, all phases of key lifecycle management stay in your control, streamlining the key management process: Key creation, rotation, and revocation conform to industry compliance requirements.

Keys can be securely stored locally by the Multi-Cloud Data Encryption management console, or be exported - using the key management interoperability protocol (KMIP)5 - to a compliant external keystore, such as IBM’s SKLM. This approach provides you with flexible options so that you can control where your keys are stored, while also preventing cloud vendor access.

See Who is Accessing Your Critical Business Data

Multi-Cloud Data Encryption can easily record all data access requests as “approved” or “denied” per users or groups with real-time logging. The reliable event capture feature flags data access information that can be forwarded to event management systems, such as IBM’s QRadar SIEM, for analysis. The product supports several standard output formats, such as Log Event Extended Format (LEEF), Common Event Format (CEF), and Cloud Auditing Data Federation (CADF), for easy integration with existing products. By using Multi-Cloud Data Encryption and SIEM capabilities together, it’s possible to shorten the detection cycle on nefarious activities, helping reduce the risk of data compromise.

DATA ASSET PROTECTION

The average total organizational cost of a data breach is estimated at $7.1M, and the cost has been steadily climbing year over year. Lost business costs also continue to increase with recent estimates associated with a reported incident at $3.97M[2]. These staggering figures and the impact to your brand reputation can considerably alter your organization's future. By utilizing Multi-Cloud Data Encryption's robust capabilities, you can have confidence that your most valuable asset – your sensitive data – is secure and protected.

WHY IBM SECURITY SOLUTIONS?

IBM Security solutions, including encryption solutions for heterogeneous environments, are trusted by organizations worldwide for advanced data protection. Proven IBM Security technologies enable organizations to safeguard their most critical resources. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions.

IBM offers decades of leadership with encryption as part of an overall security environment, and with this technology can help protect your intellectual property. The IBM Data Security portfolio can help prevent cybercriminals from accessing and abusing your sensitive data, reduce the chances that compromised data can cause material harm, help your organization achieve compliance with regulatory mandates, and provide a modular approach for dealing with changes to the regulatory environment.

IBM has worldwide security expertise in some of the most highly regulated industries, including government, healthcare, transportation, energy production and financial services. IBM is trusted by companies of all sizes to secure today's data environments as well as plan for the future.

As a strategic partner, IBM empowers organizations to reduce security vulnerabilities and manage risk across the most complex IT environments. With proven, standards-based technologies, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions.

[1] *2016 Cloud Security Spotlight Report", Cloud Passage*

[2] *"2016 Cost of Data Breach Study: Global Analysis," Ponemon Institute*

For more information

To learn more about this offering contact your IBM representative or IBM Business Partner, or visit: ibm.com

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

♲ Please Recycle