

IBM Multi-Cloud Data Encryption

Highlights

- Centrally manage data-at-rest encryption & policy enforcement
 - Easily design & administer data access policies with user-defined roles
 - Sophisticated cryptographic splitting technology
 - Patented object store encryption
 - File and volume agent native backup and restore capabilities
 - Leverage integrated, transparent key management
 - User access and activity logs seamlessly integrate into SIEM systems
-

Protect data on-prem and in the cloud with policy-based access controls, built-in key management, audit logging, encryption and key rotation.

In the age of digital transformation, more and more organizations are moving to hybrid and multi-cloud environments for agility, operational efficiencies and competitive advantage. However, underlying concerns regarding data privacy, security, and unauthorized access to the applications and data spread across these complex environments makes organizations cautious about migrating workloads there. In fact, an overwhelming majority – 91% – of organizations are very or moderately concerned about public cloud security¹.

Organizations can not solely rely on the cloud service provider (CSP) for outsourcing security and compliance, because the responsibility and risk ultimately falls on the organization itself. At its simplest, there is a shared responsibility where the CSP may be responsible for the security “of” the cloud (primarily the compute, storage database, and networking), while the customer is responsible for security “in” the cloud (primarily the data itself). Further complicating an on-premise, hybrid or 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. While each security layer from the perimeter to the host can narrow the opportunity for unauthorized access and the use of your data, we

should not stop there. The sensitive data itself must be protected, while still allowing authorized users to perform their job functions.

Data-centric protection is the critical, last-line-of-defense in a layered security model. This 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. IBM® Multi-Cloud Data Encryption focuses on the critical data protection concerns that organizations face when moving to the cloud or between clouds, thereby reducing risk and making it easier to adopt an essential cloud-first strategy with a data-centric approach that can also extend into hybrid environments. 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—regardless of where the data resides

ACHIEVE OPERATIONAL EFFICIENCY

Multi-Cloud Data Encryption, which is part of the larger IBM Security Data Protection portfolio, fully supports multiple languages, allowing you to manage your global data encryption process across private-, public-, and hybrid-cloud environments—all from a single vantage point. Its easy-to-use, agent-based deployment model helps protect

sensitive data wherever it resides—server managed storage, network file systems or sent via API to object storage. Multi-Cloud Data Encryption is tightly integrated with other IBM Security products such as IBM QRadar Security and Information Event Manager (SIEM), IBM Data Risk Manager 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 Linux, Windows or AIX 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 environment. From this console, you also can define and manage access policies, create, rotate, and manage encryption 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 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 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 file system functions are authorized (read/write/etc.) and the level of data access logging desired. By limiting access to only designated users and specific applications or processes, 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, or "LDAP") and Active Directory, 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.

Always on Data Protection, Powered by SPxCore™

Multi-Cloud Data Encryption provides

cryptographic splitting technology that helps assure confidentiality, data privacy, and protection against brute force attacks. SPxCore™, the patented software module powering Multi-Cloud Data Encryption's core functionalities, combines quantum-resilient AES-256 encryption, bit level splitting, and internal key management and it has received a National Institute of Standards and Technology (NIST) FIPS 140-2 validation².

Encrypt your Files, Folders, and Object Stores

Multi-Cloud Data Encryption allows customers to deploy agents that encrypt data at the volume-level and/or at the file/directory level for additional granularity. The file and volume agents include native backup and restore capabilities for creating full or differential copies of the encrypted data. This can support local backups as well as moving data from server to server, or even CSP to CSP, without ever decrypting the data, helping to facilitate hybrid multi-cloud architecture models.

Multi-Cloud Data Encryption also allows customers to securely leverage object storage with client-side encryption key management and access control. The object store agent leverages cryptographic splitting to send shares of encrypted data to multiple object store locations or multiple CSPs. This is called M-of-N, where N is the total number of shares, but only M shares are needed to restore the data. This helps with data resiliency and recovery, and can also help customers avoid service provider lock in; given that 94% of enterprises today have multiple clouds – mixing public, private, dedicated and countless SaaS applications – the ability to manage risk across them in a

flexible way is a critical success factor³.

Integrated and Transparent Key Management

With its unique integrated and transparent built-in key management, Multi-Cloud Data Encryption helps keep all phases of key lifecycle management in your control, streamlining the key management process. Furthermore, 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)—to a compliant external keystore, such as IBM's SKLM or Gemalto's LunaSA HSM. 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.

Multi-Cloud Data Encryption can also help you comply with current regulations like the General Data Protection Regulation (GDPR) by performing cryptographic erasure of all sensitive data housed in cloud environments, helping to destroy private data and render it unreadable when needed.

DATA ASSET PROTECTION

The average total organizational cost of a data breach is estimated at \$7.391M in the United States. Lost business costs account for a significant portion of these damages, with recent estimates associated with a

reported incident at \$4.2M⁴. 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, wherever it resides.

¹“2018 Cloud Security Spotlight Report,” Cybersecurity Insiders

²“Report on Post-Quantum Cryptography,” NISTIR 8105

³“Cloud adoption to accelerate IT modernization,” McKinsey & Company, April 2018

⁴“2018 Cost of Data Breach Study: Global Analysis,” Ponemon Institute

Why IBM?

IBM Security solutions, including encryption solutions for hybrid multi-cloud environments, are trusted by organizations worldwide for smarter 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.

Next steps

→ [Learn more about Data Protection solutions from IBM Security](#)

→ [For more information, please contact an IBM Representative](#)

For more information

To learn more about this offering, contact your IBM representative or IBM Business Partner, or visit the resources linked above.

© Copyright IBM Corporation 2019.

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:
NA



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