StorMagic

WHITE PAPER

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2021

StorMagic SvKMS

CONSOLIDATING ENCRYPTION KEY MANAGEMENT WITH SvKMS

INTRODUCTION

Data is spread out over the digital landscape. It may be archived in AWS S3 buckets, the Google Cloud Platform (GCP) used for web hosting, or perhaps distributed across multiple on-prem data stores. Organizations may have databases running in a private cloud, or possibly on virtual machines, such as VMware vSphere.

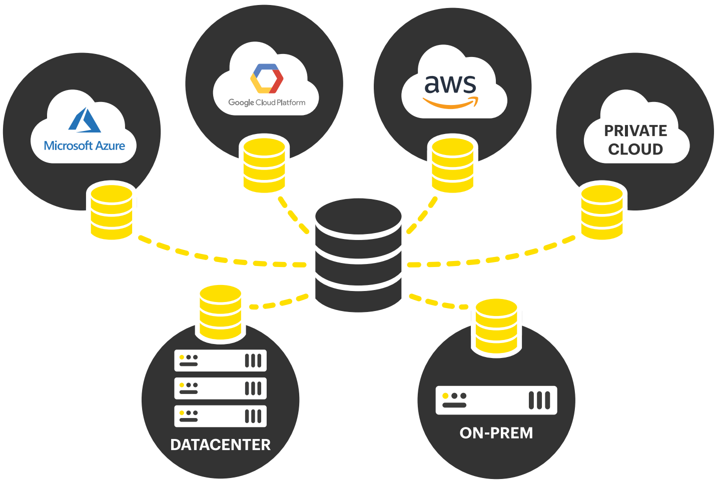

Fig 01: Disparate data stores across cloud, private cloud, on-prem and datacenters.

A lot of time, money and effort is spent by IT organizations around the world on cyber security - with the goal being to protect networks, devices, programs, and data from attack, damage, or unauthorized access. There is another aspect that is sometimes overlooked called "cyber resilience" - what happens to your data if a breach were to occur? As the volume of data created, managed and stored by organizations increases and diversifies, it becomes ever more important to have a cyber resiliency plan to protect and secure that data, and encryption is a tried-and-tested form of data protection.

Whatever the application, one of the challenges of effective data encryption across all of these services involves the security, storage and maintenance of the encryption keys. While encryption is now being built into many services to ensure data is protected, the handing of the keys is often a separate component, and more vital than the encryption itself.

> ***"60% of respondents find encryption key management painful"***
>
> 2020 Poneman Global Encryption Trends Study

For multi-cloud configurations, adopting each cloud provider's encryption and key manager results in duplication of key management functions for each service, as well as multiple interfaces. Additionally, using the key manager from each individual key management service requires keys and data to both be stored on the same cloud platform, which limits the ability to separate the lock (encryption) from the digital key.

Truly effective data protection requires a key management service that can provide a single pane of glass into the overall cryptographic environment, communicate with multiple cryptographic environments, scale up to meet increases in volume and data complexity, and provide separation between keys and the data they protect.

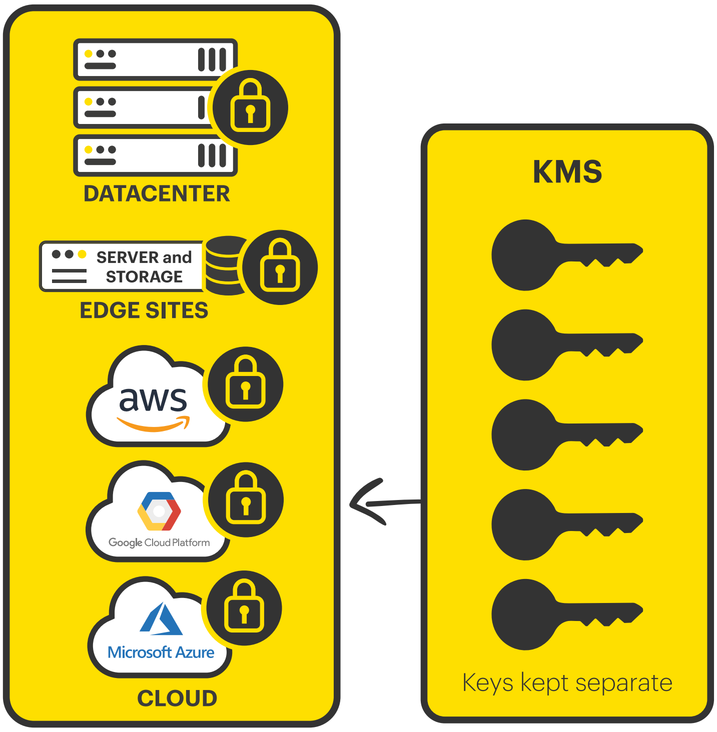

Fig 02: One centralized key manager for all environments.

This white paper provides an introduction to some of the issues around managing encryption keys and how StorMagic SvKMS overcomes these issues by effectively consolidating the key management functions for multiple services into one comprehensive key manager. It provides an overview of how SvKMS operates as a Cloud Service Provider's Key Management System and discusses how SvKMS uses modern standards, such as BYOK and KMIP, to interface with many different platforms and environments from on-prem, to cloud, hybrid-cloud and even multiple clouds.

CLOUD SERVICE ENCRYPTION

Forbes conducted a study back in 2018 that predicted 83% of enterprise workloads in some form (public, private, or hybrid) would be in the cloud by 2020. Nothing that has happened since would counter that view - organizations continue to embrace migration to the cloud. Yet moving data to a public cloud comes with risks around data protection and one of the tried and tested methods to ensure data is adequately protected has been encryption.

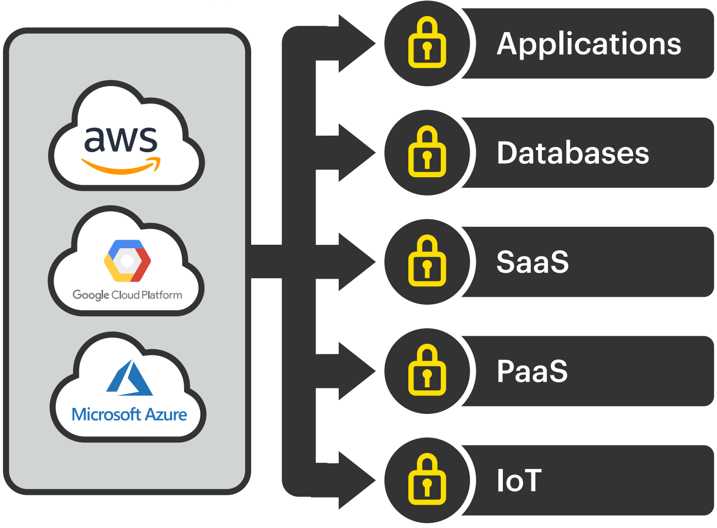

Fig 03: Data encrypted in the cloud.

All of the major cloud providers now allow their customers to employ server-side encryption and the ability to take advantage of built-in encryption key management. At face value, this makes the whole process of keeping data secure seem straightforward and streamlined within a single provider. But that isn't actually the case. Instead, it brings with it a series of issues and vulnerabilities - namely the fact that there is no separation of lock and key (a very basic security industry best practice).

COMMON ENCRYPTION KEY MANAGEMENT ISSUES

While the cloud continues to be popular for organizations as workloads are migrated out of their own datacenters, it brings with it a set of problems around security, even when leveraging the cloud provider's own encryption key management. These problems are often similar to those seen in other scenarios concerning key management.

For instance, a common practice is for organizations to rely on the internal key manager of each encryption service (such as the cloud provider) to handle its own key management. A single organization might have encrypted workloads in many different locations - in different clouds, in the datacenter, running on

MICROSOFT AZURE STORAGE

Azure Storage is a cloud computing service from Microsoft that provides scalable, durable, and highly available storage. Azure Storage encryption protects data and helps organizations meet security and compliance commitments by allowing them to manage their own encryption keys through a method called Bring Your Own Key (BYOK).

GOOGLE CLOUD PLATFORM

Google Cloud Storage is a service for storing objects in Google Cloud. Server-side encryption occurs after Cloud Storage receives data, but before the data is written to disk and stored. Customers can create and manage their own encryption keys for server-side encryption.

AMAZON SIMPLE STORAGE SERVICE (AWS S3)

Amazon Simple Storage Service from Amazon Web Services (AWS) is a data storage service that can be used in a variety of applications, such as storage, data archiving, and static web hosting. Amazon S3 supports native server-side encryption and Customer Provided Key options through BYOK.

different operating systems or VMs - all generating their own encrypted data with its own set of keys. This can create numerous problems, highlighted in the table opposite.

BRING YOUR OWN KEY (BYOK)

While most cloud platforms provide server-side encryption with all key management functions existing on the platform, many organizations prefer more control over their keys. They would prefer to move the keys away from the data storage location, while at the same time taking advantage of some of the encryption mechanisms provided by the storage provider. Just as with a physical lock and key, retaining ownership of the key ensures control of where the key is kept and how it is used.

The concept of Bring Your Own Key (BYOK) allows control of the keys to be retained by uncoupling the encryption keys from the location the data is stored.

ISSUE	SOLUTION
Storing both key and encrypted data within the same service, like a cloud provider, puts control of the keys in the hands of a third party.	A key management system that enables the separation of lock and key and allows complete control of all keys within an organization.
Duplication of work and resources when using multiple platforms and services. Keys in different environments must be managed separately.	Centralizing key management into a single location, that provides flexibility by integrating with many major cloud service providers and hybrid use cases.
Steep learning curve for understanding how to maintain each service provider's key manager. All key managers are specific to their respective cloud or service.	A simple yet powerful web portal that can be used to manage all keys for all services and applications.
Storing keys across multiple services creates the risk that an organization could use legal action to force a service provider to hand over keys.	Providing control of master keys to the owner of the data, instead of a third party service such as a public cloud.

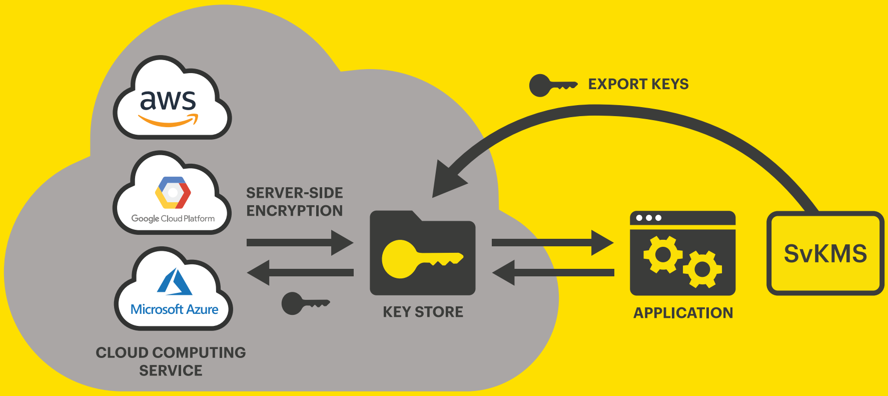

Fig 04: How BYOK (Bring Your Own Key) works

BYOK works through the use of a Key Encryption Key (KEK) which is created and stored in a KMS. The KEK encrypts and decrypts the Data Encryption Keys (DEK) used by the cloud service to encrypt data stored on the service. By wrapping the DEK with a KEK, stored and managed by an external KMS, the stored data has an additional level of security.

With BYOK, cloud service providers cannot access keys they don't have, and businesses are able to adhere to all established industry regulatory guidelines and data privacy laws regarding encryption key storage and management.

However, in order to implement a BYOK policy, and overcome the other common key management issues highlighted earlier in this paper, an organization must have access to a single, unified key manager with the enterprise-grade features necessary to enable secure, centralized key management. StorMagic SvKMS provides that capability.

WHAT IS SvKMS?

StorMagic SvKMS centralizes key management by generating, storing, and managing all encryption keys used across the entire organization.

SvKMS is a secure, highly available system that can be deployed within on-prem, cloud, multi-cloud, hybrid cloud, and edge configurations, and integrates with current hardware security module (HSM) deployments.

Regardless of where data is stored, it can be encrypted using keys generated and managed by SvKMS. What's more, SvKMS can even import and manage keys created outside the solution.

What sets SvKMS apart from other key management services is its flexibility of deployment in many different environments, its robust key features, and how simple its interface is to navigate and use, while still providing many enterprise-level features.

SvKMS provides many advanced key management features that are essential for administering a complex cryptographic ecosystem that include advanced integration capabilities, robust key management capabilities and powerful operational features.

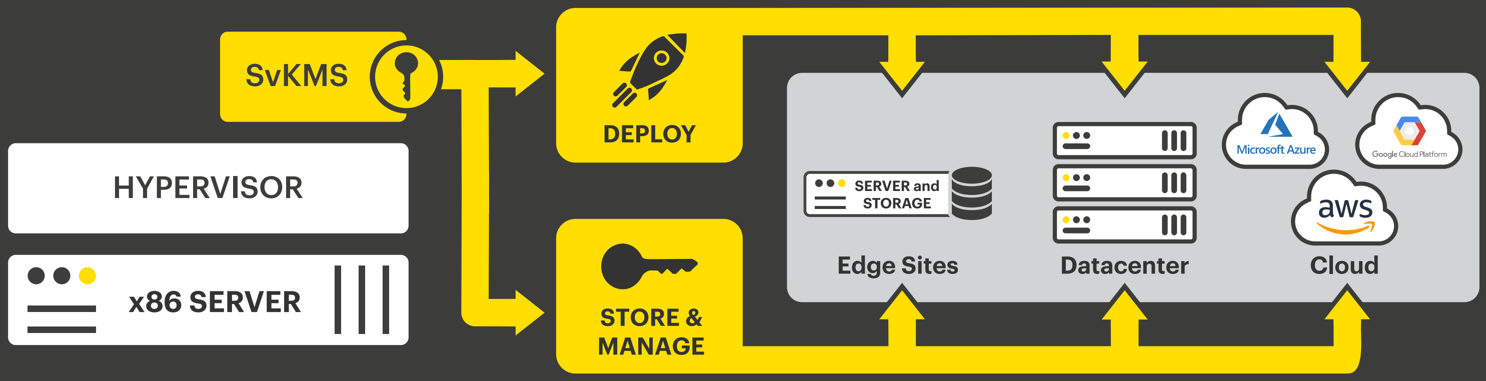

Fig 05: SvKMS can be deployed on-prem, in the datacenter or in the cloud.

ROBUST KEY MANAGEMENT CAPABILITIES:

Robust cryptographic operators	SvKMS supports many different key algorithms, including symmetric and asymmetric key types. These formats include the following: AES 128, 192, 256; RSA 2048, 3072, 4096; Elliptic curve (ECDSA) - support of 85 curve algorithms. By supporting many different key types, users of the system can choose the algorithm that fits their needs. For example, if latency is an issue, asymmetric keys like RSA and Elliptic Curve Cryptography (ECC) are much bigger, so this needs to be taken into account when designing an cryptographic environment.
Restrict authentication requests through IP whitelisting	IP whitelisting is a security mechanism that ensures only users that are coming from certain IPs are allowed to perform cryptographic functions. SvKMS enables administrators to whitelist IP addresses so that key management requests are restricted to specific IP addresses.
Advanced identify and access management through SAML 2.0	An identity provider is "a trusted provider that lets administrators use single sign-on (SSO) to access other websites." SSO enhances usability by reducing password fatigue. It also provides better security by decreasing the potential attack surface. SvKMS supports the Security Assertion Markup Language (SAML) standard, which is an open standard for authentication and authorization. SvKMS supports the latest version of the standard, 2.0. SvKMS can therefore support an identity provider that subscribes to the SAML standard. E.g. ADFS, OKTA, etc.
FIPS 140-2 certified	SvKMS meets the highest levels of compliance for a key management software product through FIPS certification. The United States Federal Information Processing Standard (FIPS) defines security and interoperability requirements for computer systems that are used by the U.S. federal government. The FIPS 140 standard defines approved cryptographic algorithms and sets forth requirements for key generation and for key management. The National Institute of Standards and Technology (NIST) uses the Cryptographic Module Validation Program (CMVP) to determine whether a particular implementation of a cryptographic algorithm is compliant with the FIPS 140 standard. An implementation of a cryptographic algorithm is considered FIPS 140-compliant only if it has been submitted for and has passed NIST validation.
Programmatic batch functions	Batch functions allow users of cryptographic systems to perform key management functions (create, delete, rotate, etc.) in bulk, meaning that huge operations may be performed at any given time to create efficiency. Through the use of programmatic functions, users may automate these functions to reduce administrative overhead.

ADVANCED INTEGRATION CAPABILITIES:

REST API makes integrations easy	REST defines a common interface for key management operations (get, fetch, rotate, create, delete, etc.), which may be automated through code. This also makes it easy for users to integrate with many different key management use cases, because the standard interface removes the requirements to have many different proprietary key management communication standards.
BYOK support	Bring Your Own Key (BYOK) allows organizations to encrypt their data and retain control and management of their encryption keys. SvKMS provides an easy and effective solution that ensures organizations always maintain control of their keys when employing encryption in IaaS, SaaS, and PaaS environments.
Leading edge KMIP adoption	The Organization for the Advancement of Structured Information Standards (OASIS), in partnership with various security companies, has developed the Key Management Interoperability Protocol (KMIP), a standardization method for encryption of stored data and cryptographic key management. By providing a common language that simplifies the use of encryption keys, many organizations can now adopt encryption as part of their data security policy. StorMagic SvKMS supports KMIP communication with cryptographic clients. As a KMIP server, SvKMS can create, store and manage keys that are used across a variety of cryptographic products and environments. It is this level of connectivity that propels SvKMS to the forefront of KMIP-supported Key Management Systems that supports the most popular encryption use-cases such as VM and Database encryption.
HSM extension	Many enterprise organizations still want to use hardware security modules (HSM) as the root of trust for cryptographic keys. That being said, HSMs can be difficult to use and don't support many actions. SvKMS can serve as an abstraction in front of an HSM where the keys are still stored and protected in the hardware but provisioned out through the key manager which can then perform many key management lifecycle functions and provide keys to modern encryption workflows such as cloud and edge deployments.

POWERFUL OPERATIONAL FEATURES:

Full key management lifecycle	The task of key management is the complete set of operations necessary to create, maintain, protect, and control the use of cryptographic keys. Keys have a lifecycle from inception to retirement. Encryption keys are not interminable, and the probability of a breach increases the longer that a key is in use, just like with the use of a password. SvKMS supports the full lifecycle for keys to ensure compliance and process mandates.
Centralized management	Many key managers of the past could only support one use case, often tied to a hardware appliance. Often these key managers supported many different interface protocols so there ended up being many different key managers. For example, a tape backup may support encryption, but the interface between it and the key manager was proprietary. The SvKMS key manager supports standard protocols, such as the key management interoperability protocol (KMIP) and a RESTful API, allowing administrators to manage all of their encryption use cases from one single, simple-to-use interface.
Backup and restore	To ensure redundancy of key material in case of an outage or system failure, SvKMS can backup the current encryption keys for future restoration. The backup and restore features provide a mechanism for setting on-demand and scheduled backups to an external location, then restoring these backups when required. The backup and restore features can be accessed through the user interface or through the SvKMS API.
Detailed auditing and logging	Auditing of key management functions is crucial to understand possible attack vectors and usage. Security Information and Event Management (SIEM) is a software solution that aggregates and analyzes activity from many different sources. SvKMS collects data through the use of the syslog format which can then be exported to external SIEM tools to analyze data.

CONCLUSION

Between BYOK, a RESTful API, and KMIP support, SvKMS provides a flexible framework for deploying encryption key management across virtually all platforms, services, and applications.

One of the greatest strengths of SvKMS is its ability to integrate quickly and easily to many different cloud platforms and applications.

StorMagic SvKMS provides a variety of enterprise-grade features in a single platform. Encryption keys are generated and managed safely and efficiently through a simple-to-navigate web portal.

Considering a centralized key management system? Take into account these questions:

WHEN DID YOUR ORGANIZATION LAST REVIEW ITS SECURITY POLICIES?

Business requirements can change quickly, especially when it comes to data and security. As the volume of data increases and the data storage location list continues to grow, it becomes even more important to have a key management system like SvKMS handling the day-to-day operations. SvKMS is scalable and can expand to integrate with more services and increase the number of managed keys in response to data volume.

DOES YOUR EXISTING SECURITY POLICY MEET ALL REGULATORY COMPLIANCE?

Failure to comply with regulatory requirements like PCI-DSS and GDPR can result in fines or even disruption of operations. What happens if you rely on each platform's built-in key manager? If one service is not compliant, will you have to migrate your data to one that does? Will you have to make changes on each service to maintain compliance? StorMagic SvKMS centralizes key management and enables businesses to consolidate all encryption keys, across all platforms, into a single, comprehensive compliance-driven key manager.

ARE YOU COMFORTABLE WITH THE KEYS PROTECTING YOUR DATA EXISTING OUTSIDE YOUR CONTROL?

Keeping keys and data on the same cloud service provider is like hiding the key to the front door under the mat; it's the first place someone would go looking. Managing your keys through SvKMS brings control over encryption keys back to where it belongs - in the hands of the key owner.

FURTHER READING

There are additional resources available covering StorMagic SvKMS's capabilities and features across the StorMagic website. Why not explore the **product data sheet** or read more about some of the software's **specific features**.

If you're ready to test SvKMS in your environment, you can do so free of charge, with no obligations. Simply download our **fully-functioning free trial of SvKMS** from the website.

If you still have questions, or you'd like a demo of SvKMS you can contact the StorMagic team directly by sending an email to **sales@stormagic.com**

StorMagic
The Quadrant
2430/2440
Aztec West
Almondsbury
Bristol
BS32 4AQ
United Kingdom

+44 (0) 117 952 7396
sales@stormagic.com

www.stormagic.com