



A kulcs kérdés – Kulcskérdés

Entrust KeyControl

Hajabács Balázs
System Engineer

2025. november 13.



More shocking numbers



24 Million passwords, API keys, and credentials were found in public GitHub repositories in 2024

70% of leaked secrets remain valid two years later

Source: GitGuardian – sprawl report 2025 - <https://www.gitguardian.com/state-of-secrets-sprawl-report-2025>

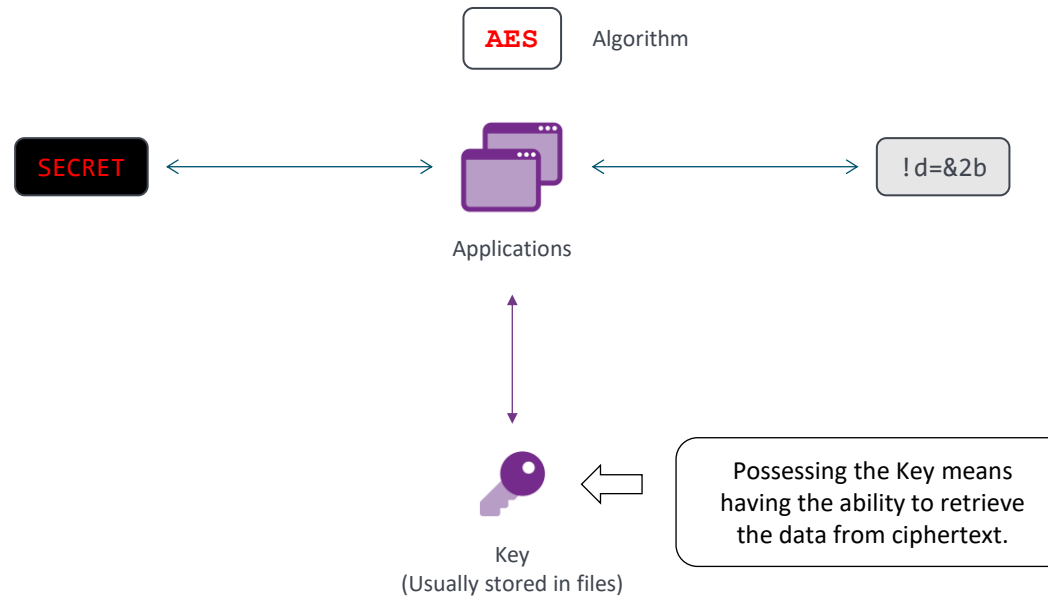


High-Impact Cloud Key & Token Incidents



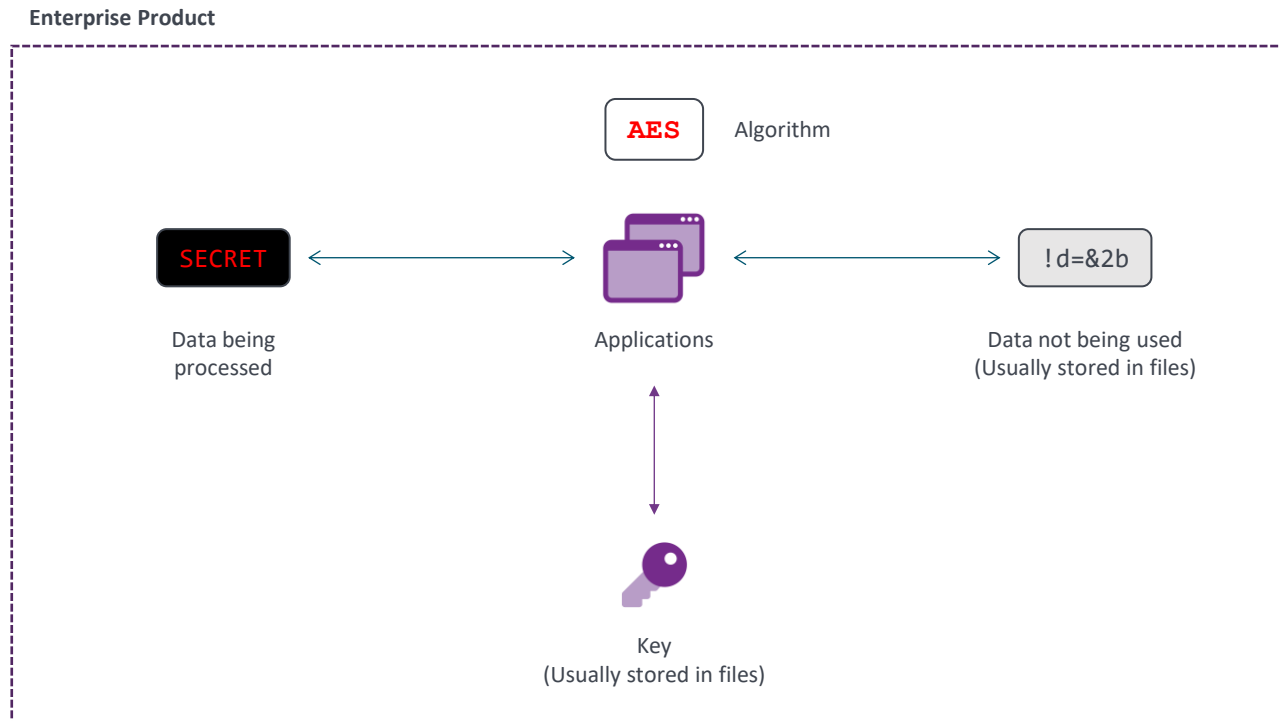
Year	Company	Exposed Secret	Cause	Impact
2022	Toyota	API keys & source code (T-Connect)	Public GitHub repo left open by subcontractor	~296,000 customers affected in Japan; location, email, VIN leaked; 5-year undetected exposure
2022	Uber	Hardcoded AWS & Duo credentials	Contractor's PowerShell script in private repo leaked via MFA bypass	Attackers accessed internal dashboards, GDrive, Slack, Bitbucket; lateral movement across systems
2023	Microsoft	SAS (Shared Access Signature) token - Azure	Key mistakenly included in Microsoft-hosted GitHub repo	Nation-state attackers forged tokens for email, Teams & SharePoint; undetected for over 2 years
2025	Salesforce	OAuth token via Drift chatbot	Token reused across tenants; attacker exploited token in Salesloft/Drift system	Data exfiltration across dozens of orgs ; support cases, customer records, embedded passwords

Encryption and Keys



Executed by **Applications**, encryption is a method protecting sensitive data by converting it into ciphertext, using an **algorithm** and a **random** key.

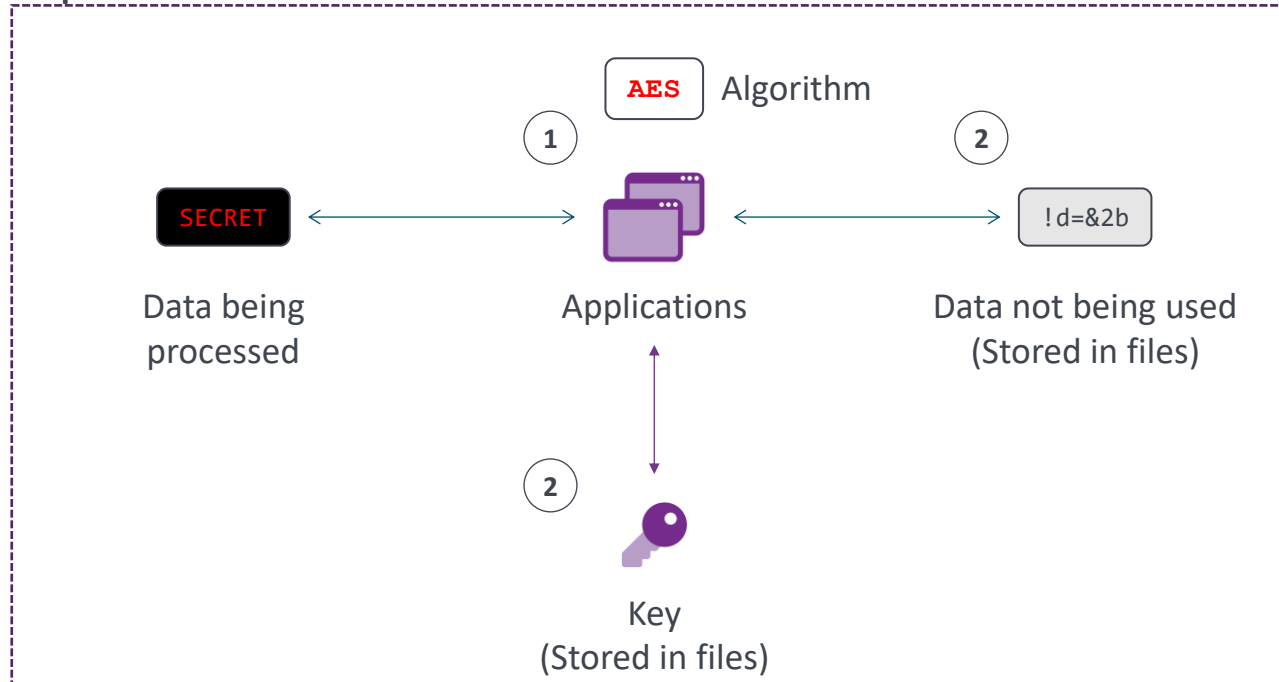
Encryption in Enterprise Products



Enterprise Products know you care about the data stored / processed inside. Therefore, they have usually been equipped with the ability to generate key and encrypt data.

Concerns Over the Encryption and Key

Enterprise Product

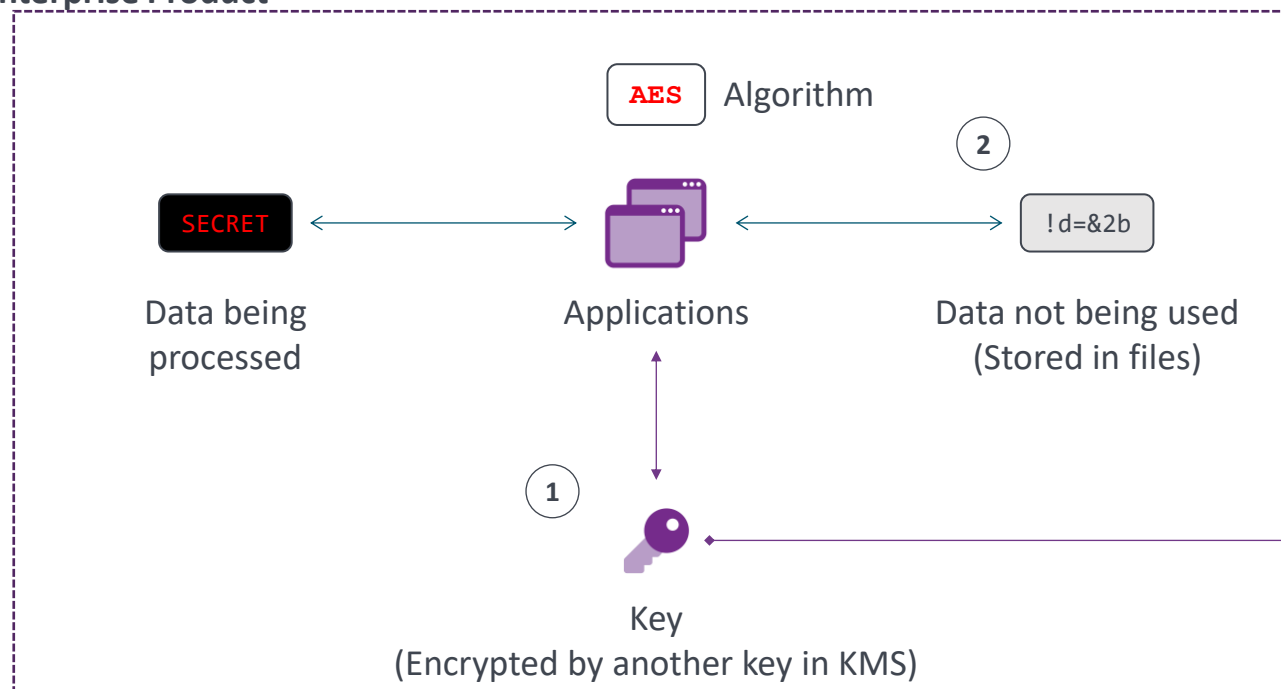


1 Rights to use the Key is usually tied to authentication / authorization policies of the products (Having certain accounts compromised could have the data decrypted as well)

2 Keys are stored with encrypted data in the same product


What Do You Need to Protect the Keys?

Enterprise Product



Therefore, most products having native encryption allows third-party key management, i.e. a **Key Management Server (KMS)**

3



ENTRUST Cryptographic Security Platform (CSP)
Key Management Server

1

Any key encrypting data (Data Encryption Key) should be encrypted by another key (Key Encryption Key)

2

KEK should not be stored with encrypted data

3

KEK Storage should be robust

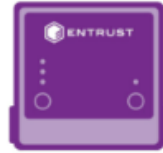
EXTERNAL KEY MANAGEMENT: KEY ADVANTAGES



Create keys on premises, and securely export to the cloud (AWS, Google Cloud, Microsoft Azure and Salesforce)



Confidence that keys have been generated securely using a strong entropy source



Confidence that the long-term storage of keys are protected by a FIPS and Common Criteria certified HSM



Not locked into cloud service provider – free to export to other providers on demand



Do you have a consistent encryption strategy in a hybrid or multi cloud environment?

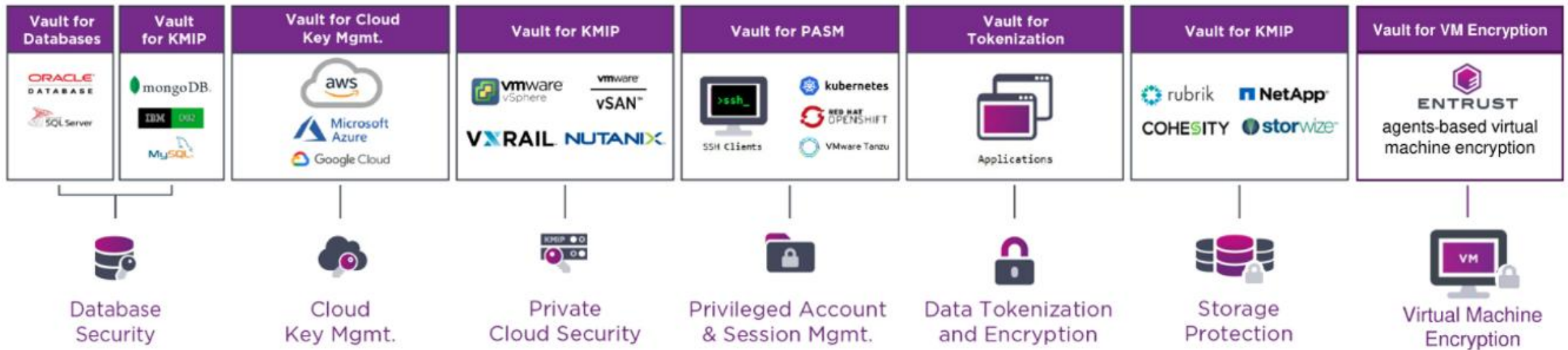


ENTRUST

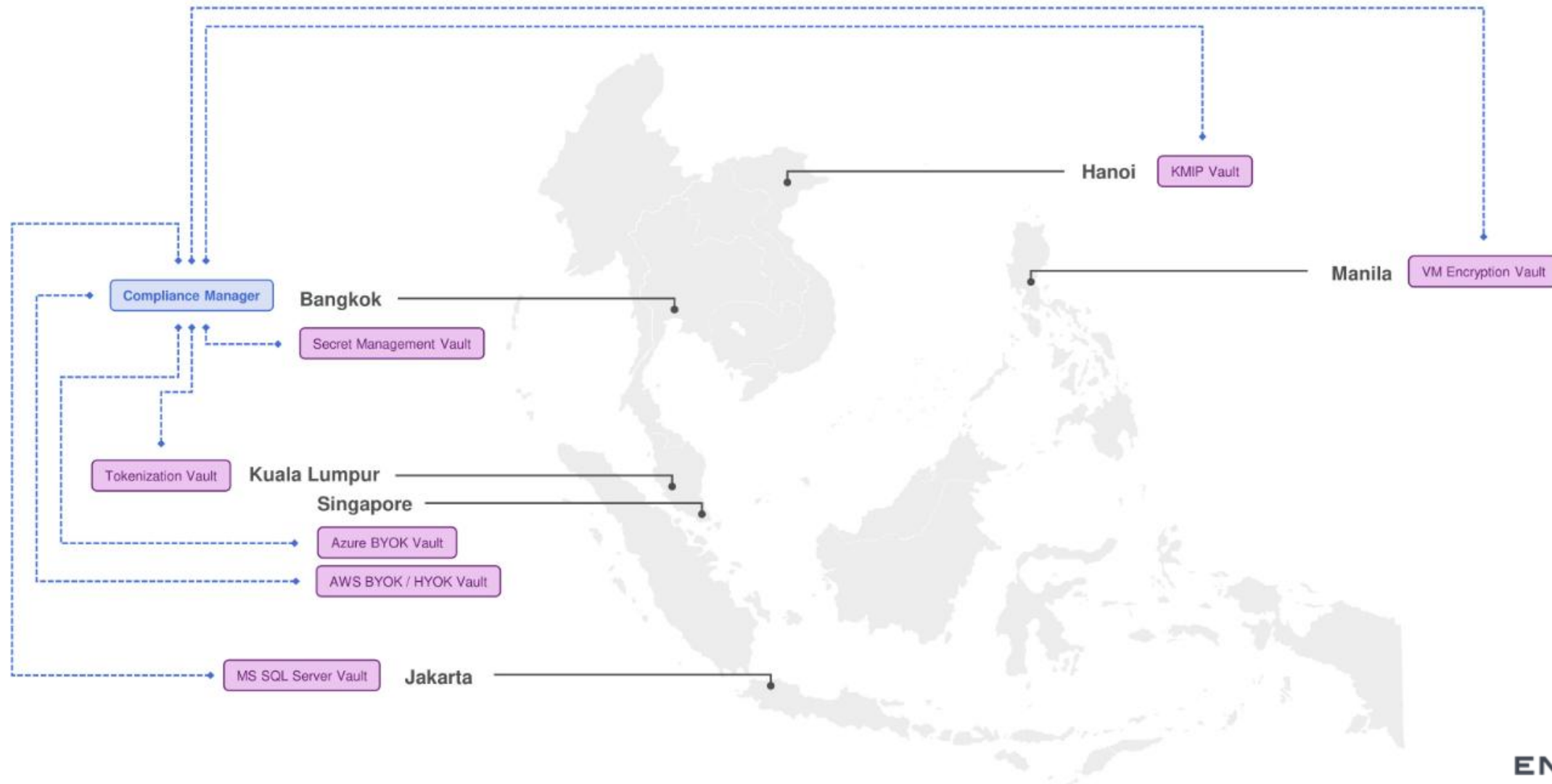
DECENTRALIZED VAULTS



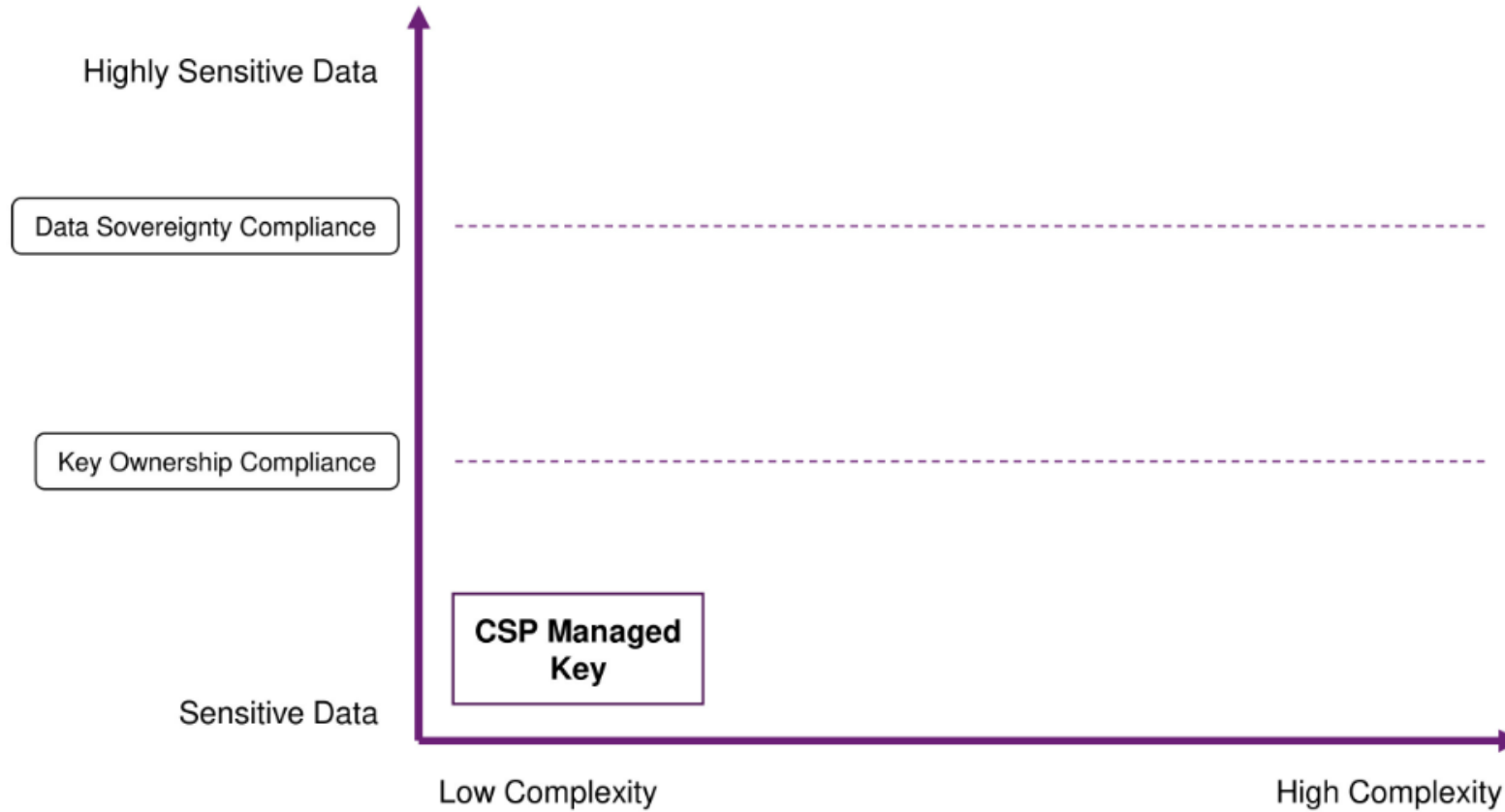
KEYCONTROL VAULTS & USE CASES



DECENTRALIZED KEY MANAGEMENT



KEY MANAGEMENT STRATEGIES



CUSTOMERS' CONCERNS ABOUT KEYS IN CLOUDS

KEY OWNERSHIP



Keys are generated by CSP which is stored in the same environment with encrypted data and customers are not allowed for copies of keys

KEY CONTROL



Customers cannot disallow CSP using the keys stored in the Cloud;
Keys in the Cloud cannot be revoked or deleted immediately when necessary

DATA SOVEREIGNTY



CSPs have to comply with the laws and regulations of the countries where they run the Clouds, that sometimes enable governments to access the data stored in the Clouds

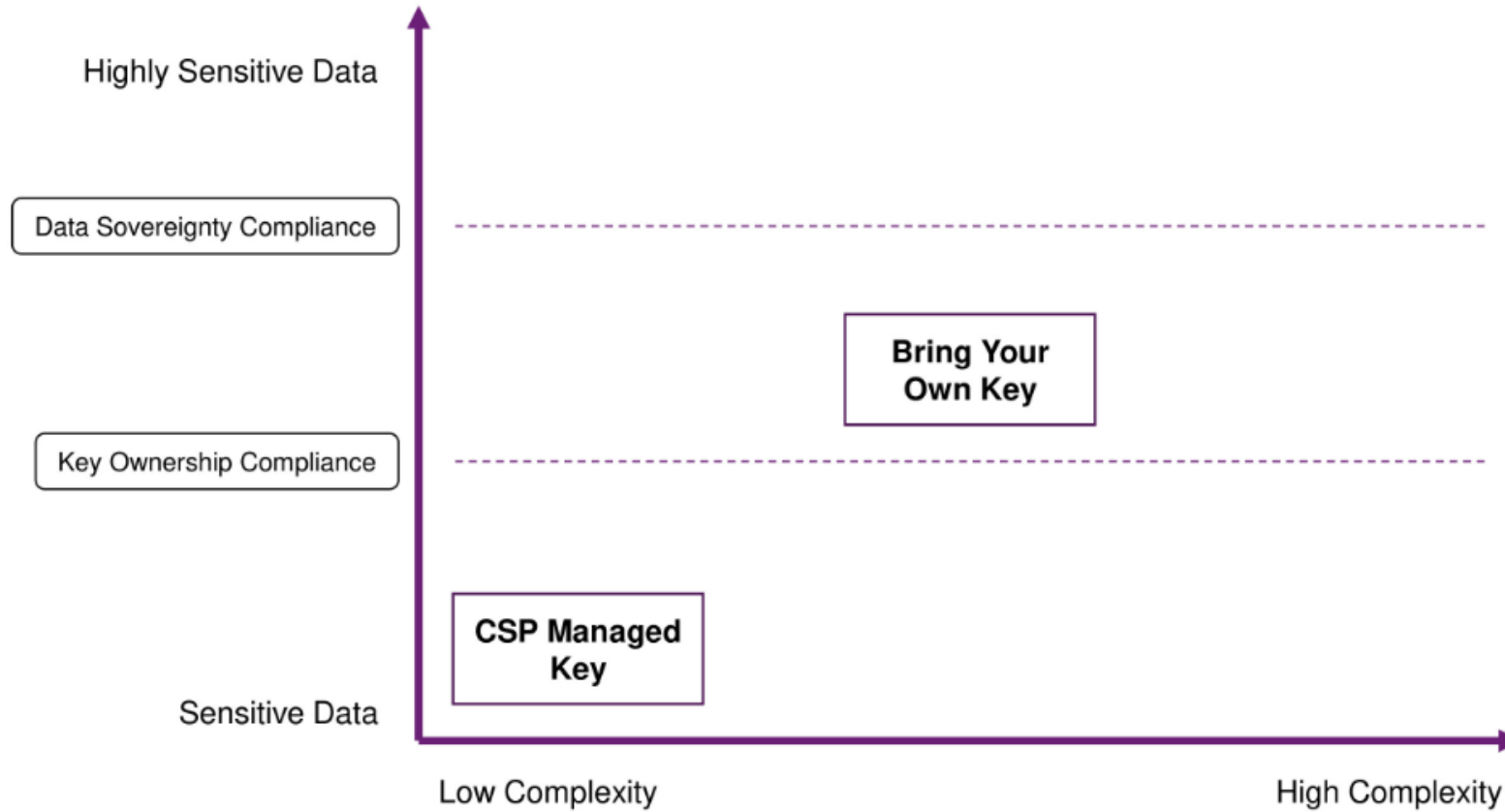
MULTI-CLOUD SECURITY



Keys are managed separately and differently across multiple Clouds;
Data must be decrypted before it could be transferred to other Clouds

* CSP: Cloud Service Provider

KEY MANAGEMENT STRATEGIES



BRING YOUR OWN KEY



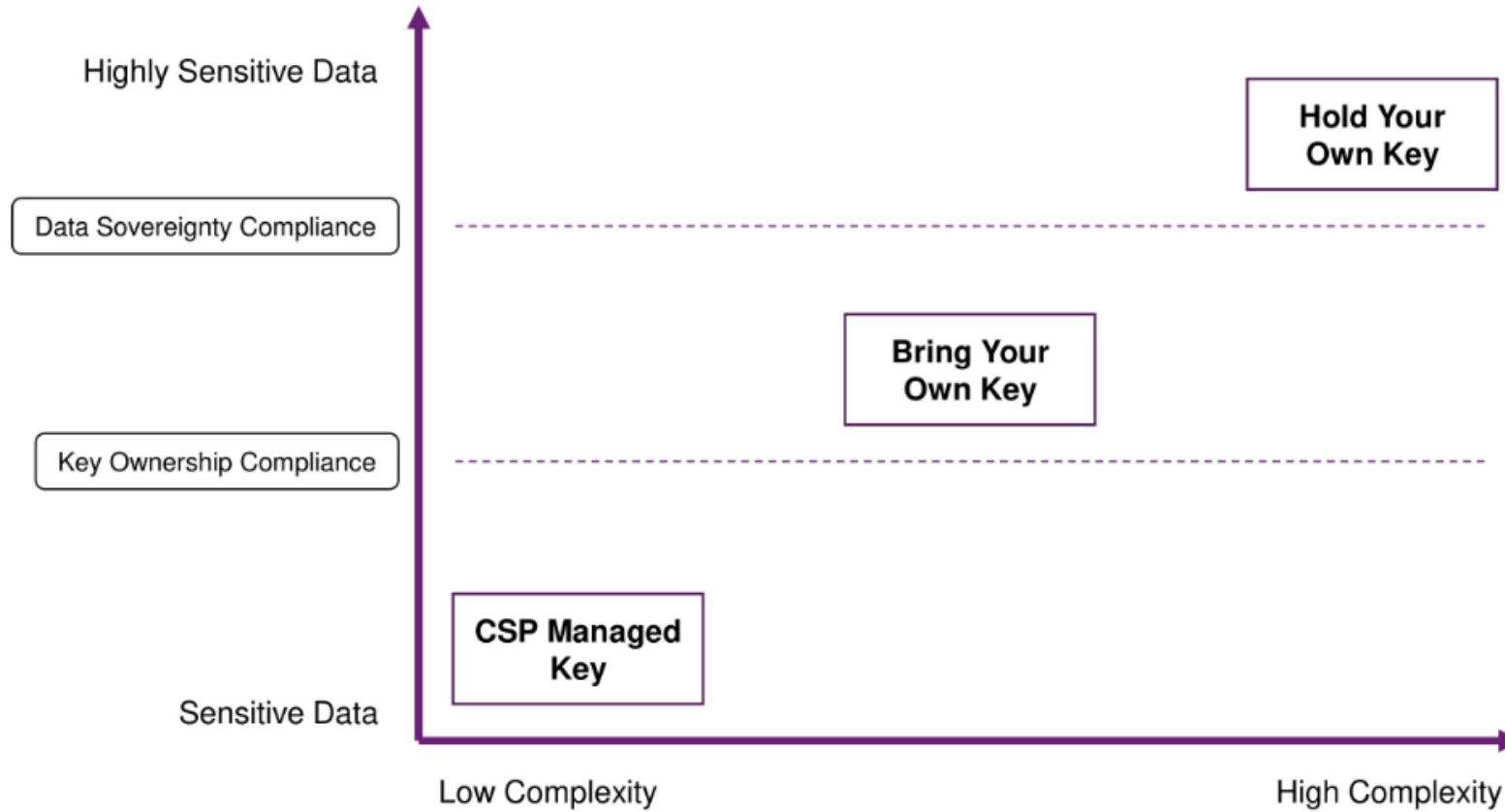
Pros

- › Suitable for fulfilling Key Management compliance
- › Available for most of the services running in the Cloud
- › Easy to deploy
- › Customer get a copy of the Keys in their own environment instantly

Cons

- › Keys still need to be delivered to CSP in order to decrypt the data
- › Keys brought to the Cloud stay there unless customer requests deletion
- › Customer does not have other choices if the application / service does not support BYOK

KEY MANAGEMENT STRATEGIES



HOLD YOUR OWN KEY

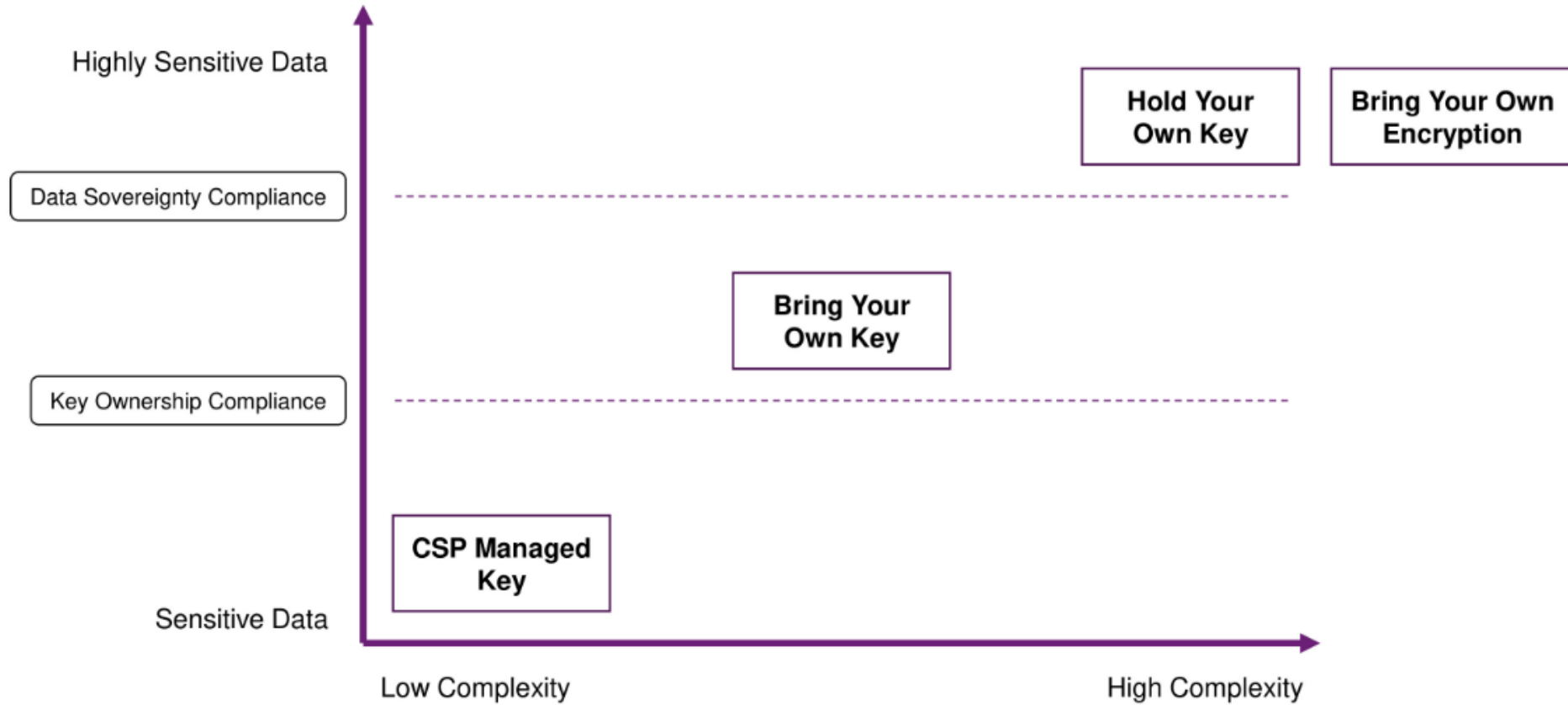
Pros

- › Ideal for protecting highly sensitive data and adhere to strict regulation and compliance policies
- › Customer retains ownership and control of their keys used by the applications in the Cloud at all times
- › Keys can be revoked immediately by disabling the services of KMS

Cons

- › It is limited to the services that are tailored for HYOK
- › KMS must be available whenever a sensitive data in the Cloud needs to be decrypted
- › The encryption may not be transparent to users

KEY MANAGEMENT STRATEGIES



BRING YOUR OWN ENCRYPTION

Pros

- › It is the only way to allow consistent encryption and key management policies in multi-cloud and hybrid-cloud environments
- › Sensitive data stays encrypted all the time, even when it is transferred between different Clouds
- › CSP has no right to decrypt or encrypt sensitive data even if the data is in the Cloud

Cons

- › Customer has to take the full responsibility to ensure the encryption applications / services can work in the Clouds
- › Most SaaS services do not allow BYOE
- › Troubleshooting could be difficult because CSP does not have obligation to ensure sensitive data is encrypted or decrypted appropriately

BYOE COMPARED WITH CLOUD KEY MANAGEMENT

No Encryption Ownership			Customer-owned Encryption
Cloud Service Provider (CSP) Managed Key <ul style="list-style-type: none">➤ Default option for data-at-rest encryption, such as storage service encryption➤ Keys are generated by CSP and stored in the "Key Vault" in the Cloud➤ Keys never leave the Cloud (no archiving, backup or export to anywhere outside the Cloud)➤ Customer does not have access to the keys	Bring Your Own Key (BYOK) <ul style="list-style-type: none">➤ This is also known as "Customer-managed Key"➤ Keys are generated by customer's own Key Management Server (KMS)➤ When needed a copy of keys are uploaded ("brought") to the "Key Vault" from the KMS➤ Customer owns the keys but CSP can access the keys being brought to the Cloud	Hold Your Own Key (HYOK) <ul style="list-style-type: none">➤ Default option for application encryption, such as productivity service encryption➤ Keys are generated by customer's own Key Management Server (KMS)➤ Keys never leave the KMS ("held" by KMS)➤ Customer has the full ownership and control on the keys	Bring Your Own Encryption (BYOE) <ul style="list-style-type: none">➤ Customer deploys their own encryption applications and services in the Cloud➤ Keys are generated by customer's own Key Management Server (KMS)➤ When needed Keys can be delivered to the encryption applications but not the CSP➤ Customer has the full ownership and control on the keys and encryption policies

CSP's Responsibility

Key Ownership and Control

Customer's Responsibility

WHICH ONE IS THE BEST FOR YOU?

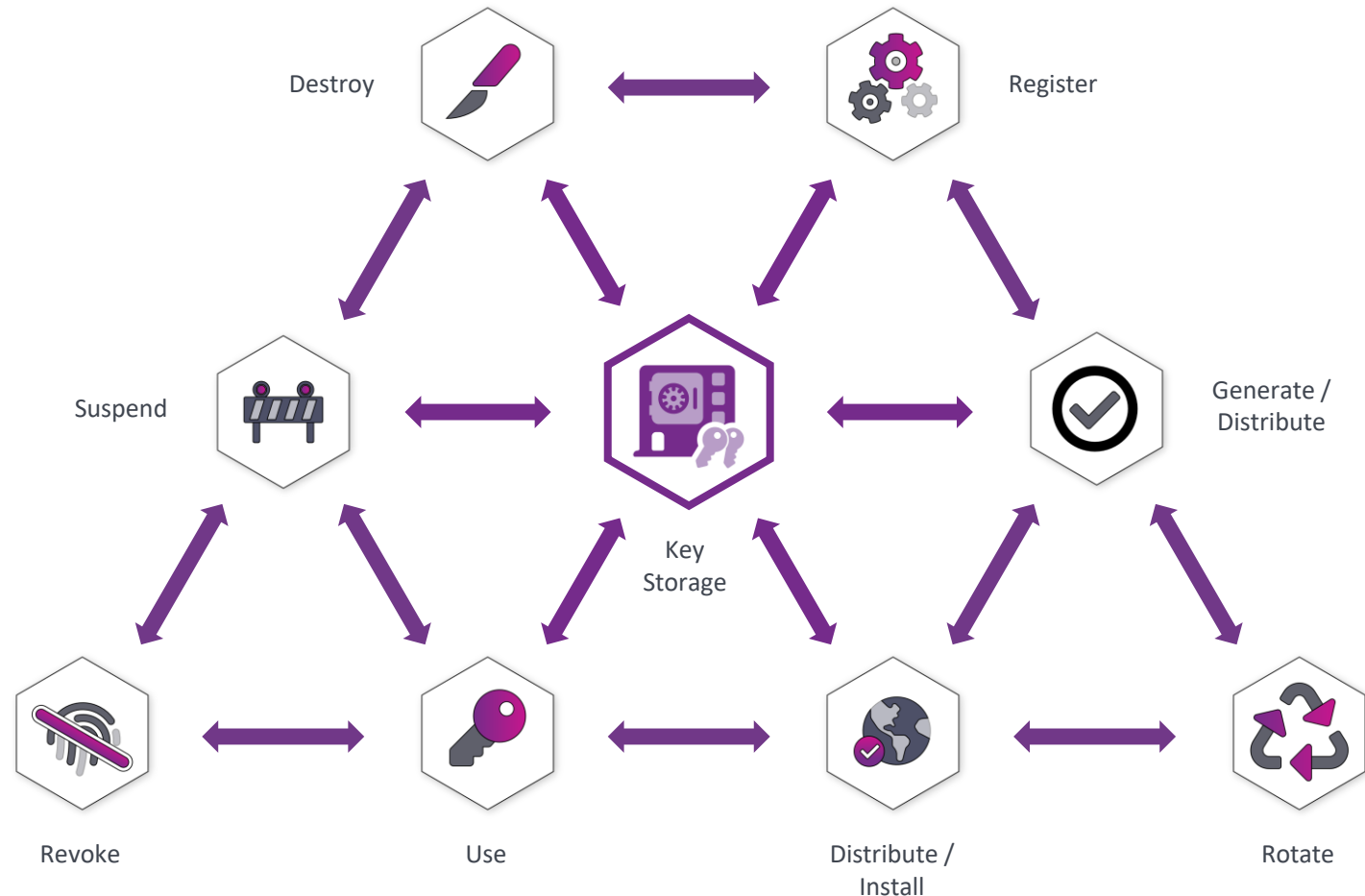


	CSP Managed Key	Bring Your Own Key (BYOK)	Hold Your Own Key (HYOK)	Bring Your Own Encryption (BYOE)
Data Encryption	✓	✓	✓	✓
Key Ownership	NIST SP 800-57	✓	✓	✓
Multi-cloud Key Management		✓	✓	✓
Full Control on Keys			✓	✓
Data Sovereignty	CLOUD Act		✓	✓
Full Control on Encryption Policy				✓
Multi-cloud Data Encryption				✓

Key Lifecycle Management

Delivers complete key lifecycle – from inception to retirement

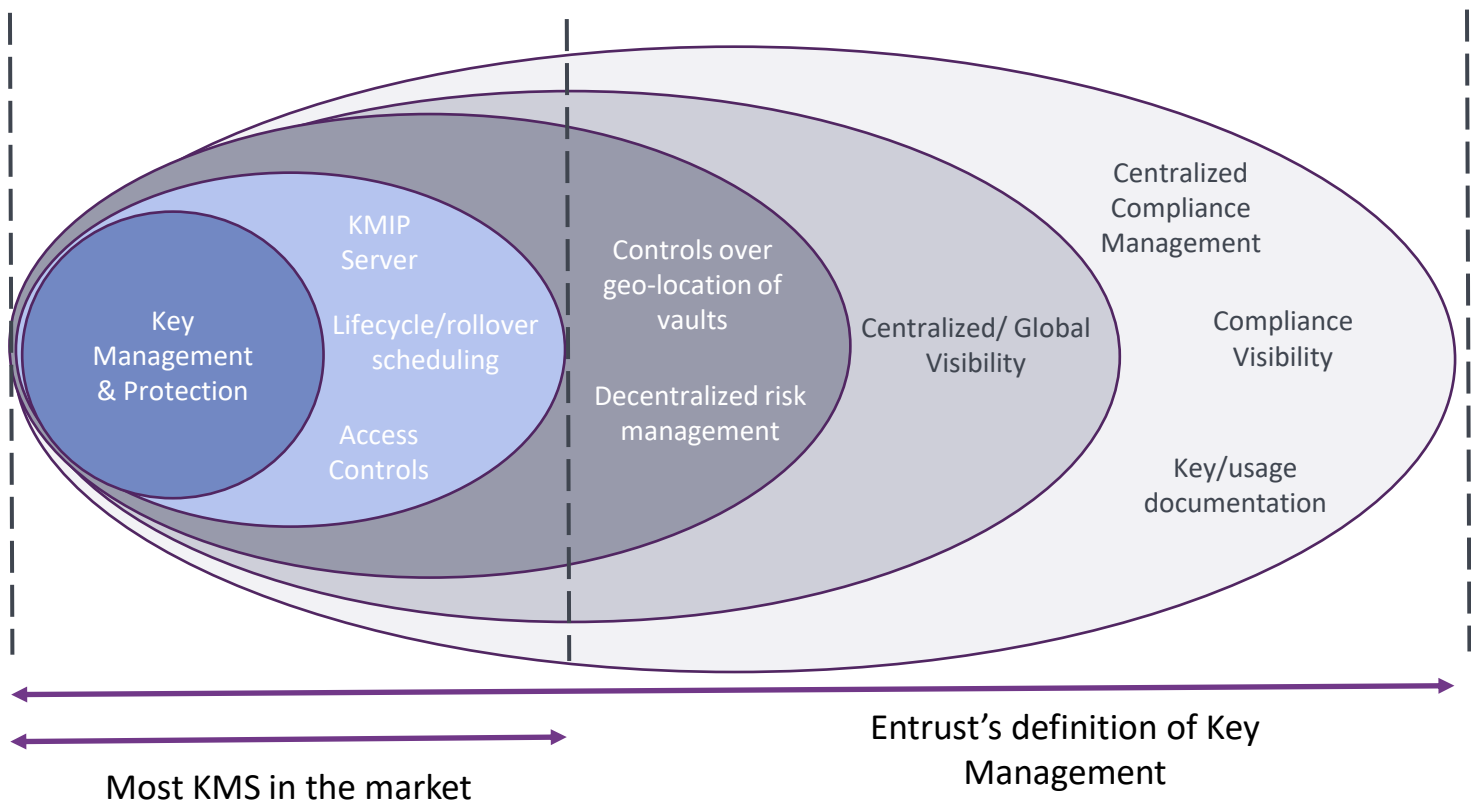
- Key generation
- Key rotation (manual and scheduled)
- Management of unlimited keys/key sets
- Ability to import existing keys
- Ability to suspend not just revoke keys



Entrust's Vision on Key Management



Redefining Key and Secrets Lifecycle Management



Traditional Lifecycle Management



Decentralized Vault-Based Architecture



Comprehensive Central Policy



Compliance Management Dashboard

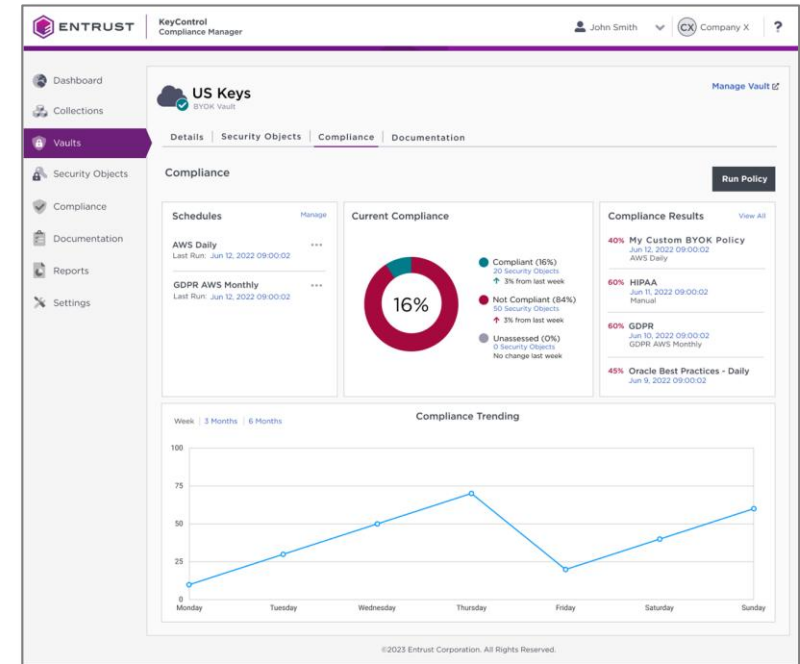
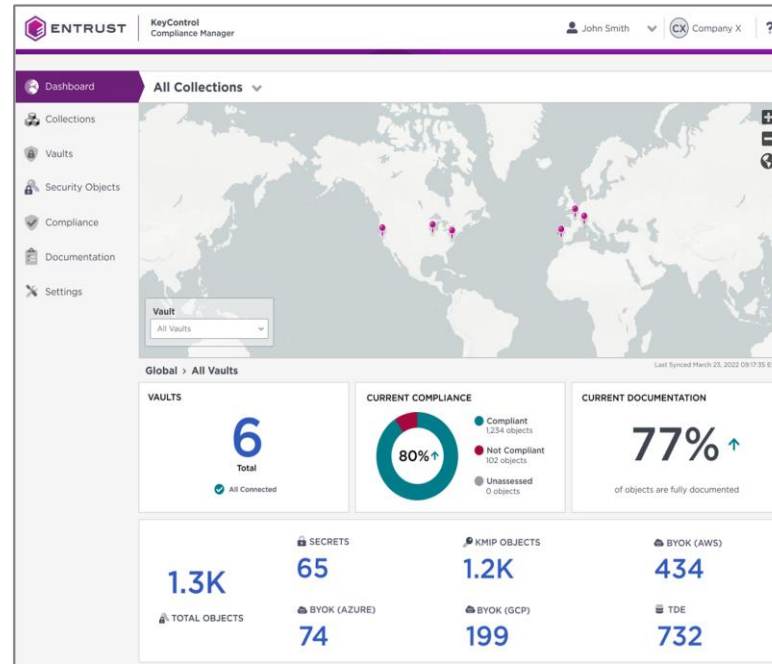


Centralized Policy and Compliance Management



Comprehensive dashboard provides:

- Visibility over globally distributed key vaults
- Details of keys stored at each location
- Degree to which stored keys comply to policy
- Extent to which your keys are properly documented



Calculate Risk Score for Cryptographic Objects



ENTRUST

CRYPTOGRAPHIC SECURITY PLATFORM
Compliance Manager

Joseph Ling

Default Tenant

?

Dashboard

Collections

Data Sources

Security Objects

Compliance

Documentation

Appliance Clusters

Settings

Security Objects
All objects within the data sources

Collection: All Data Source: All Type: All Risk: All Search Contains...

Download

Object Name	Collection	Data Source	Status	Documented	Compliance	Age	Risk
test.ceret.003-fa...	GG	CSP - CM		✓ Documented	❗ Not Compliant	0 Days	19 HIGH
AES_KEY_001	GG	GG_CryptoAPI_01	Available	✓ Documented	❗ Not Compliant	1 Month 19 Days	10 MED
CAGatewayTrans...	GG	CSP - CM		✓ Documented	❗ Not Compliant	0 Days	19 HIGH
e6a13b2a-194b-4...	SZ	SZ_KMIP	Active	✓ Documented	✓ Compliant	5 Days	4 LOW
codesign02.devo...	GG	CSP - CM		⚠ Not Documented	✓ Compliant	0 Days	21 HIGH
172.19.24.50-fact...	GG	CSP - CM		⚠ Not Documented	✓ Compliant	0 Days	21 HIGH
DESKTOP-597UR...	GG	CSP - CM		⚠ Not Documented	✓ Compliant	0 Days	21 HIGH
CertificateAuthor...	GG	CSP - CM		⚠ Not Documented	✓ Compliant	1 Day	21 HIGH

1 - 100 of 171

© 2025 Entrust Corporation. All rights reserved.

KeyControl

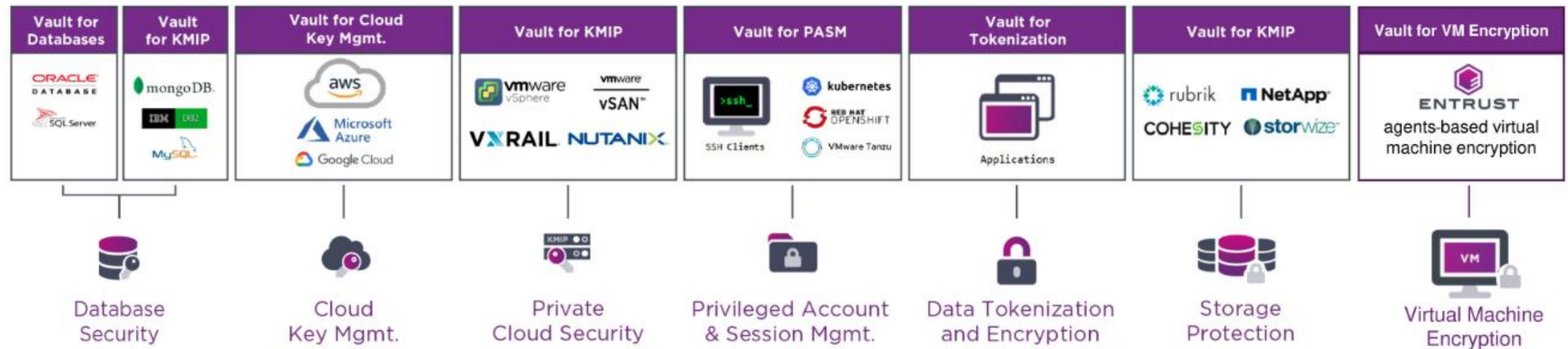
Enterprise Key Lifecycle Management & Compliance Platform



KeyControl Compliance Manager

Global Compliance Dashboard - Policy Enforcement - Granular Key Inventory - Audit/Risk

KEYCONTROL VAULTS & USE CASES





Köszönöm a figyelmet!

entrust@clico.hu

Hajabács Balázs
System Engineer

2025. november 13.

