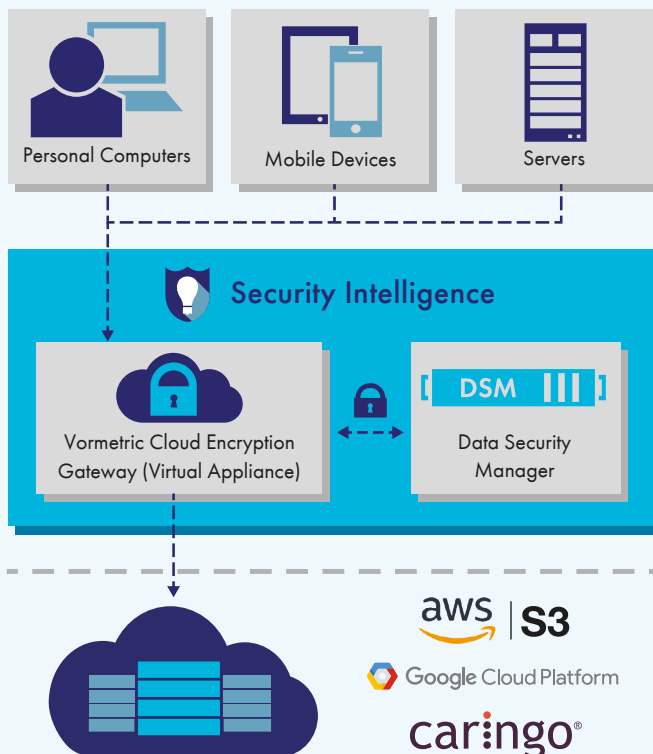# THALES

SECURE DATA IN CLOUD STORAGE

> Leverage cloud environments more broadly, while strengthening security and compliance controls

> Guard against unauthorized access from government subpoena and cloud provider's privileged user accounts

> Boost operational efficiency through expanding the Vormetric Data Security Platform to protect cloud storage

> Deploy quickly, without having to make changes to applications or user workflows

‹Thales eSecurity›

VORMETRIC CLOUD ENCRYPTION GATEWAY

Personal Computers

Mobile Devices

Servers

Security Intelligence

Vormetric Cloud Encryption Gateway (Virtual Appliance)

DSM

Data Security Manager

aws | S3

Google Cloud Platform

caringo®

The Vormetric Cloud Encryption Gateway offers capabilities for encrypting and controlling data in Amazon S3, Google Cloud Storage, and Caringo.

CONTENDING WITH CLOUD STORAGE RISKS

As organizations grow increasingly reliant upon cloud storage offerings like Amazon Simple Storage Service (Amazon S3), Google Cloud Storage and Caringo, the need to secure sensitive data in these environments grows increasingly urgent. However, given the externally hosted, multi-tenant nature of these services, it is proving difficult for security and compliance teams to gain the visibility and control they need.

How do businesses leverage these cloud services, while eliminating their specific risks? For example, how do they retain the controls they need to ensure that data remains protected, even if the cloud provider is subpoenaed or one of its administrator's credentials are compromised? Further, how do security teams employ safeguards in these cloud storage environments while contending with the explosive growth in the volume of data that needs to be secured, including inside and outside the enterprise?

VORMETRIC CLOUD ENCRYPTION GATEWAY

FAST, EFFICIENT CLOUD STORAGE SECURITY

Thales eSecurity offers robust solutions that enable organizations to contend with both proliferating data and security threats. The Vormetric Data Security Platform from Thales eSecurity delivers capabilities for transparent file-level encryption, tokenization, application-layer encryption, integrated key management, and security intelligence. All these capabilities are delivered through a centralized, uniformly managed platform that enables customers to protect data across their physical, cloud, and big data servers—and do so with unparalleled administrative efficiency and cost effectiveness.

The Vormetric Data Security Platform features the Vormetric Cloud Encryption Gateway which enables customers to safeguard sensitive data in cloud storage environments, such as Amazon S3 or Google Cloud Storage. With the Vormetric Cloud Encryption Gateway, organizations can encrypt files in cloud storage, without having to add another point tool that compounds the complexity IT teams have to contend with.

ESTABLISH STRONG CONTROLS WHILE MAXIMIZING EFFICIENCY

The Vormetric Cloud Encryption Gateway encrypts sensitive data before it leaves your premises and is saved in the cloud storage environment, enabling security teams to establish the visibility and control they need around sensitive assets. With the Vormetric Cloud Encryption Gateway, organizations can leverage a strong set of capabilities:

> **Robust, persistent controls.** When the solution is implemented, sensitive data may be copied, shared, and distributed in an array of environments, but security teams can manage keys and policies on their premises, so they retain localized visibility and control.

> **Detailed visibility and auditability.** The Vormetric Cloud Encryption Gateway gives administrators detailed visibility into data access.

> **Agile performance.** Through its virtualized appliance architecture, the gateway offers elastic scaling that enables IT teams to efficiently accommodate changing performance and scalability demands.

> **Intelligent risk detection.** The Vormetric Cloud Encryption Gateway can automatically scan cloud environments discover unencrypted files that violate security policies, and encrypt them. As a result, security teams can effectively mitigate the exposure associated with having users circumvent policies.

> **Transparent, efficient implementation.** IT teams don't need to modify applications or workflows when deploying the solution.

> **Flexible service extensibility.** The solution is built on an extensible architecture that enables rapid addition of new protected cloud storage environments.

ABOUT THALES eSECURITY

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on: