thalesgroup.com

THALES

Thales Solutions for Google Cloud Platform

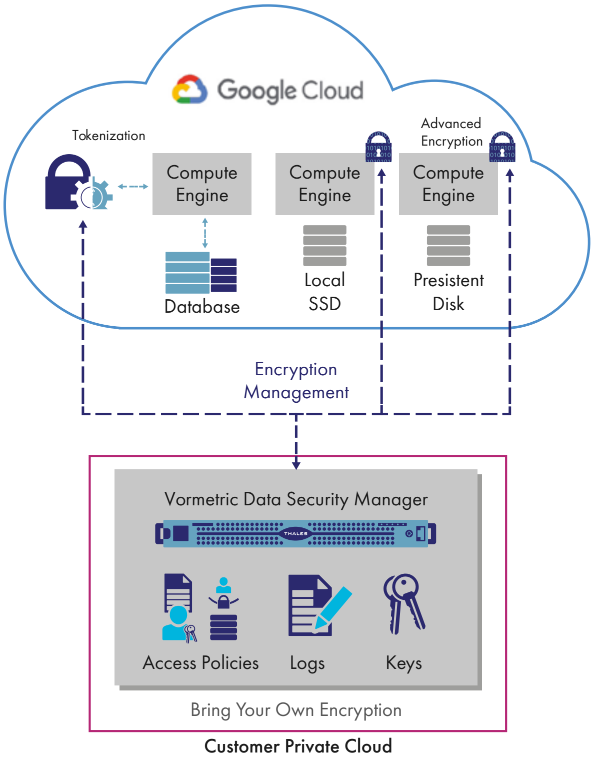
Secure workloads across hybrid clouds Including Google Cloud Platform

Information technology workloads in Google Cloud Platform (GCP) can offer convenience and cost savings. However, you still need to follow security, privacy and compliance rules, as well as best practices for your data. Further, you need rapid data mobility across all clouds you use and those in your future, a need which can be compromised with cloud-vendor-specific encryption solutions.

Advanced encryption solutions with comprehensive key management

Effective, secure cloud use involves an increasing number of decisive moments, such as when you consider using sensitive data in any cloud. You can rely on Thales to secure your digital transformation. Thales advanced encryption and centralized key management solutions give you protection and control of data stored on your premises, Google Cloud Platform, and other cloud providers. Thales technology enables you to:

- Avoid cloud vendor encryption lock-in and ensure the data mobility you need while you efficiently and securely spread workloads and data across multiple cloud vendors, including Google Cloud Platform, with centralized, independent encryption management
- Identify attacks faster with data access logging to industry-leading SIEM applications
- Reduce or eliminate risks arising from compromised credentials with advanced encryption including privileged user access controls
- Architect applications for both the cloud and PCI-DSS scope reduction using vaultless tokenization with dynamic data masking



Data encryption for Google Cloud Platform workloads and beyond

If you're 100% Google Cloud Platform-based with stringent data security controls, or if you're running hybrid clouds with data distributed across your on-premises private cloud, multiple cloud providers, and on Google Cloud Platform, you need an advanced encryption solution. While Google Cloud Platform encrypts data at rest by default, it serves unencrypted data to operating systems, exposing data to OS-level risks. Vormetric Transparent Encryption from Thales protects your files and databases stored anywhere, including Google Cloud Platform, without any changes to applications, databases, infrastructure or business practices.

Vormetric Transparent Encryption:

- Strengthens data security with operating system-level controls against unauthorized access based on granular access policies, including user identity (including for administrators with root privileges), and process, among many others
- Accelerates breach detection and satisfies compliance mandates with detailed file access logs, directed to your security information and event management (SIEM) system
- Delivers a fast return on investment with a non-intrusive, flexible implementation. Encryption agents operate on Google Compute Engines or any other server accessing storage and are available for many Windows versions and Linux distributions

Accelerated PCI-DSS compliance

Vormetric Tokenization with Dynamic Data Masking for Google Cloud Platform secures and anonymizes sensitive assets in the data center, big data environments or the cloud for simplified PCI-DSS compliance. Format-preserving or random tokenization protects sensitive fields while maintaining database structure, for a non-disruptive implementation. Then, it's easy to add policy-based dynamic data masking to applications.

Centralized, secure key management

The Vormetric Data Security Manager provides centralized key, policy and log management for Vormetric Transparent Encryption and the Vormetric Tokenization Server. The Vormetric Data Security Manager is available as a FIPS-140-2 Level 2 or 3 physical appliance or a FIPS-140-2 Level 1 virtual appliance. The physical appliance is appropriate for your on-premises locations to manage encryption agents installed on Google Compute instance virtual machines or elsewhere. The virtual appliance is available in many virtualization formats including VMware and KVM as well as for Amazon Web Services and Microsoft Azure.

Security for your data protection requirements

Thales simplifies securing your Google Cloud Platform workloads to help you achieve compliance with internal, government, and industry data security regulations. Vormetric Transparent Encryption Agents and the Vormetric Tokenization Server operate seamlessly on workloads in GCP, managed service providers and on your premises delivering centralized policy and key management.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com