THALES

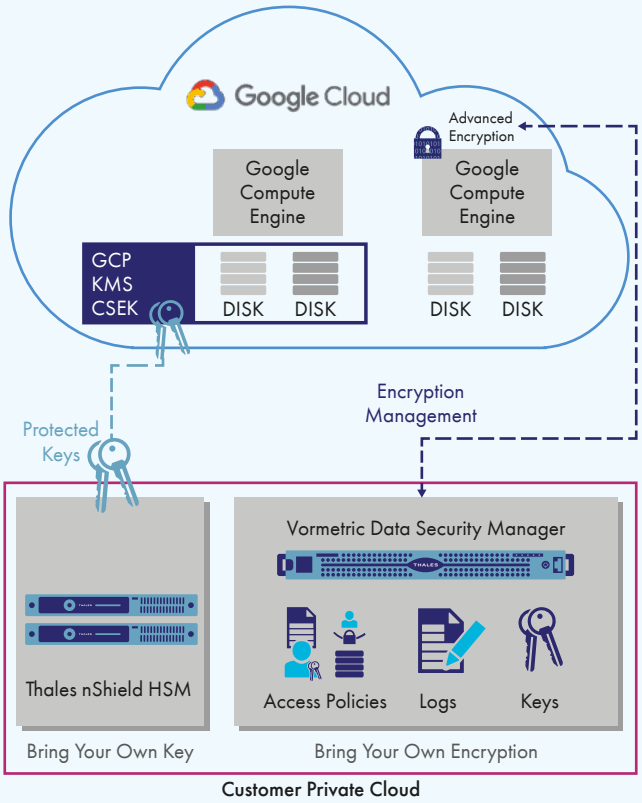
www.thalesesecurity.com

ADVANCED ENCRYPTION WITH COMPREHENSIVE KEY MANAGEMENT

- Avoid 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
- Take Secure advantage of Google Cloud Platform Cloud Key Management Services with FIPS 140-2 Level 3 certified HSMs
- 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

‹Thales eSecurity›

THALES eSECURITY 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. Thales eSecurity solutions help you meet these needs. You can bring your own encryption (BYOE) with advanced capabilities and centralized key management giving you protection and control of data stored on your premises, Google Cloud Platform, and other cloud providers.

Customers who prefer Google Cloud Platform Key Management Services (KMS) can manage customer-supplied encryption keys (CSEK) with Thales nShield hardware security modules.

THALES eSECURITY SOLUTIONS FOR GOOGLE CLOUD PLATFORM

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 eSecurity 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.

CENTRALIZED, SECURE KEY MANAGEMENT

The Vormetric Data Security Manager provides centralized key, policy and log management for Vormetric Transparent Encryption. 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 worldwide across any cloud provider. The virtual appliance is available in many virtualization formats including VMware and KVM as well as for Amazon Web Services and Microsoft Azure.

BRING YOUR OWN KEYS TO GCP

Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using Thales nShield Bring Your Own Key (BYOK).

Thales nShield hardware security modules (HSMs) let you bring your own keys to GCP and are available in three form factors: network attached, PCIe card, and USB-attached, to suit your application requirements and performance needs.

nShield BYOK offers the following advantages:

- Safer key management practices combined with cloud benefits of scale, cost and convenience
- Greater control over keys—you can control key generation and storage of keys used in GCP, Amazon Web Services Key Management Services (AWS KMS), and Microsoft Azure Key Vault.
- Consistent on-premises key management for the leading public cloud providers.

SECURITY FOR YOUR DATA PROTECTION REQUIREMENTS

Thales eSecurity simplifies securing your Google Cloud Platform workloads to help you achieve compliance with internal, government, and industry data security regulations. Vormetric data security products operate seamlessly on workloads in GCP, managed service providers and on your premises delivering centralized policy and key management. And nShield BYOK for Google Cloud Platform gives you control over encryption keys to achieve compliance and safeguard your data.

LEARN MORE

Visit us at **www.thalesesecurity.com** to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

Follow us on:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • 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 – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com