THALES

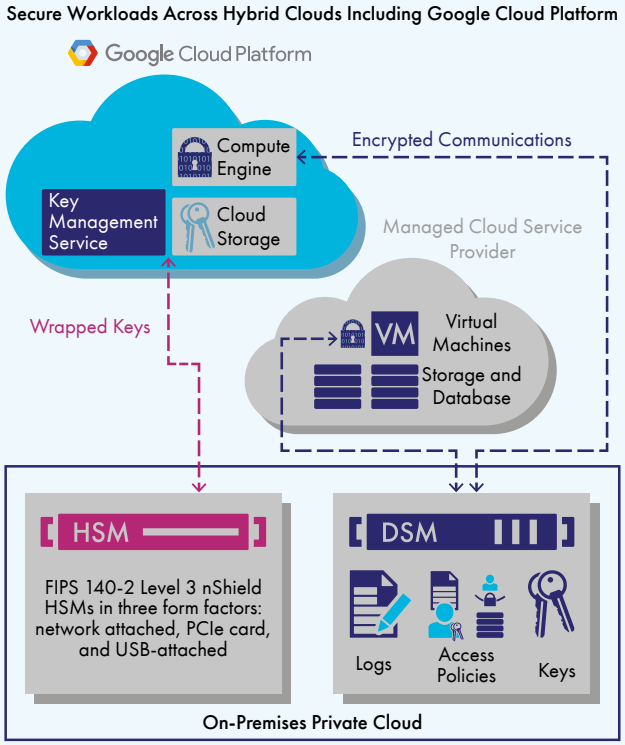
www.thalesesecurity.co.uk

ADVANCED ENCRYPTION WITH COMPREHENSIVE KEY MANAGEMENT

- Reduce or eliminate risks arising from compromised credentials with advanced encryption including privileged user access controls
- Take Secure advantage of Google Cloud Platform Cloud Key Management Services with FIPS 140-2 Level 3 certified HSMs
- Efficiently and securely spread workloads and data across multiple cloud vendors including Google Cloud Platform with centralised, independent encryption management
- Identify attacks faster with data access logging to industry-leading SIEM applications

‹Thales e-Security›

THALES E-SECURITY SOLUTIONS FOR GOOGLE CLOUD PLATFORM



Thales nShield HSMs generate, wrap and export customer-supplied encryption keys (CSEK). Keys are protected and stored on the HSM.

You can deploy the Vormetric Data Security Manager virtual appliance on your premises, in Google Cloud Platform, or in any other Cloud.

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. Thales e-Security solutions help you meet these needs with advanced encryption and centralised 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 can manage customer-supplied encryption keys (CSEK) with Thales nShield hardware security modules.

THALES E-SECURITY SOLUTIONS FOR GOOGLE CLOUD PLATFORM

DATA ENCRYPTION FOR GOOGLE CLOUD PLATFORM WORKLOADS AND BEYOND

If you're 100% Google Cloud Platform-based with stringent internal or industry 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. Vormetric Transparent Encryption from Thales e-Security protects your files and databases stored anywhere, including Google Cloud Platform, without any changes to applications, databases, infrastructure or business practices. Vormetric Transparent Encryption for Google Cloud Platform enables you to:

- Strengthen data security with controls against unauthorised access based on granular, least-privileged user access policies, including user identity (including for administrators with root privileges), process, file type and time of day, among many others
- Accelerate breach detection and satisfy compliance mandates with detailed file access logs. You can direct the logs to the security information and event management solution of your choice
- Attain a faster return on investment with a non-intrusive, flexible implementation. Encryption agents operate on a Google Compute Engine 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 centralised key, policy and log management for Vormetric Transparent Encryption for Google Cloud Platform. 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.

BRING YOUR OWN KEYS TO GCP

Thales nShield hardware security modules (HSMs) combine field-proven, FIPS-140-2 Level 3 tamper-resistant hardware with a unique software architecture enabling industry-leading scalability and key management convenience. nShield HSMs let you bring your own keys to the Google Cloud Platform Cloud Key Management system, giving you control over the encryption keys that protect your sensitive cloud data. With nShield BYOK for Google Cloud Platform, your on-premises nShield HSM generates, stores, wraps, and exports keys to GCP on your behalf. nShield HSMs are available in three form factors— network attached, PCIe card, and USB-attached—to suit your application requirements and performance needs. nShield BYOK for Google Cloud Platform gives you the following advantages:

- Safer key management practices combined with cloud benefits of scale, cost, convenience
- Greater control over keys—you drive key generation, storage, and export of keys used in GCP KMS
- Stronger key generation using nShield entropy and FIPS-certified hardware
- Consistent on-premises key management for the leading public cloud providers including Amazon Web Services and Microsoft Azure

SECURITY FOR YOUR DATA PROTECTION REQUIREMENTS

Thales e-Security 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 centralised policy and key management. And nShield BYOK for Google Cloud Platform Key Management Services gives you control over encryption to achieve compliance and safeguard your data.

TEST DRIVE

Create your own Vormetric Transparent Encryption for Google Cloud platform laboratory at **gcp-testdrive.orbitera.com**

LEARN MORE

Visit us at **www.thales-esecurity.co.uk** to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

Follow us on:

Americas – Thales e-Security 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@thalesesecurity.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@thalesesecurity.com