COMPLETELY CONTROL DATA ENCRYPTION KEY GENERATION AND USAGE WITH BRING YOUR OWN KEY (BYOK) CAPABILITIES

- Strangely segment cloud and other multi-tenant environments by enabling tenants to bring their own data encryption keys.
- Use encryption keys generated by Thales nShield Hardware Security Managers (HSMs), third party HSMs or other key sources with Vormetric Data Security Platform products.
- Choose high-assurance key sources to meet optimum key strength and compliance requirements.

BRING YOUR OWN KEYS
For Data Encryption with Vormetric Platform Products

A basic IT security maxim is that whoever controls the keys, controls the data. Never has this been truer – As organizations increasingly place business-critical data not only within the traditional four walls of a data center but also within multiple cloud environments. Enterprises with financial data, PII, intellectual property and other secrets to protect, or compliance requirements to meet are front and center for this problem, as attacks increase in sophistication and data breach rates continue to rise. In these circumstances, cloud and other service providers that offer Bring Your Own Key (BYOK) services to their customers enable the higher level of encryption key control needed by enterprises to expand adoption of their solutions and drive new business. While enterprises that want more control of encryption within their data centers can control the complexity, randomization and overall levels of assurance of the keys that directly protect their data.

To make this possible, the Vormetric Data Security Platform includes the capability for these data encryption keys to be sourced from trusted hardware device (such as a Thales or third party HSM), or other applications of their choosing. This capability puts control of data encryption keys used to protect information fully in the hands of the organizations that own it, enabling digital transformation with greater use of sensitive data within cloud environments, while also making possible the level of assurance and key control that most fits their needs.
BYOK FOR THE VORMETRIC DATA SECURITY PLATFORM

HOW IT WORKS
RESTful APIs or a Web GUI can be used to bring data encryption keys used with Vormetric data security platform products into the platform’s management environment, the Vormetric Data Security Manager (DSM), and then used for data encryption with platform products:

- **Vormetric Transparent Encryption**: Data encryption keys used with policy-based encryption and access controls for files and volumes within systems (local or in the cloud), big data environments and containers.
- **Vormetric Application Encryption**: Programmatic or RESTful encryption commands can now use data encryption keys generated and managed by the enterprise.
- **Vormetric Key Management**: Provide the master encryption key used with Oracle and SQL Transparent data encryption.

USES FOR CLOUD AND MULTITENANT ENVIRONMENTS
Internal private clouds offered by IT services or public cloud providers can now offer business units or organizations that they serve the capability to use Vormetric platform products from Thales with encryption performed utilizing keys entirely under their control.

To do this, each tenant is given the capability for import and control of the data encryption keys used to access their data. Typically, a cloud or service provider will create their own application for customers to enable this, and integrate it with their Vormetric infrastructure via RESTful APIs.

ORGANIZATIONS THAT NEED THE HIGHEST LEVEL OF CONTROL OVER THEIR ENCRYPTION KEYS
For organizations with high IT security standards, it is often not enough to know that their data is protected from threats with encryption and access controls. They also prefer to completely control those keys, knowing that they are generated and managed directly by representatives from their organization or applications that they directly control. And, that the keys are of an assurance level that meets their stringent requirements.

These organizations needs are directly met by the platform’s BYOK capability. Keys can be generated by the application or hardware environment of their choice according to internal standards and requirements. The platform allows them the control and ownership desired of keys used for their data, regardless of whether that data is stored locally or within cloud environments.

**MAINTAIN COMPLETE CONTROL OF ENCRYPTION KEYS, EVEN WITHIN MULTI-TENANT CLOUD ENVIRONMENTS**

![Diagram showing data encryption key management process](chart.png)

Customers generate their own keys from in-house resources.

- **Customer 1** uses nShield Connect HSM.
- **Customer 2** utilizes a 3rd Party HSM.
- **Customer 3** imports keys from other sources.

Customers export wrapped data encryption keys to the Virtual DSM via REST API or GUI.

Wrapped keys can be imported by Vormetric applications and used for encryption.

- **Vormetric Transparent Encryption**
- **Vormetric Application Encryption**
- **Transparent Database Encryption**

Follow us on: [Thales eSecurity](https://www.thalesesecurity.com)