THALES

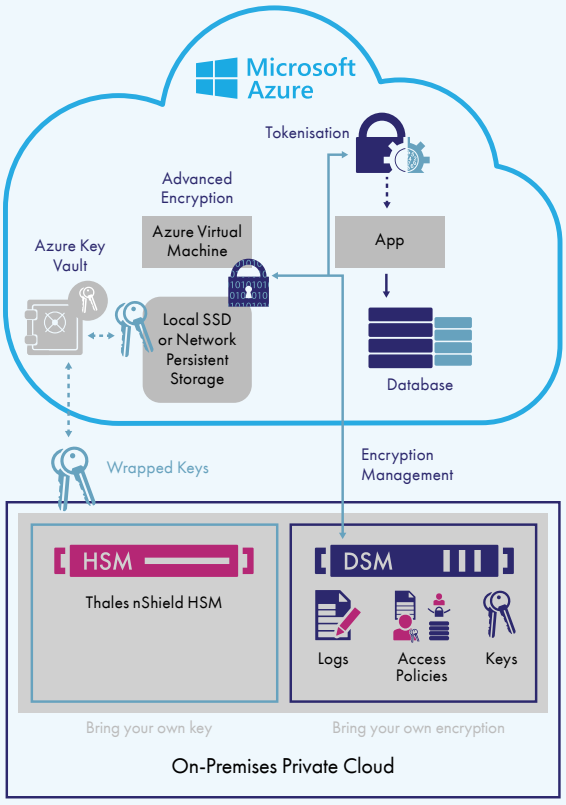
www.thalesesecurity.co.uk

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 Microsoft Azure, with centralised, independent encryption management
- Take secure advantage of the Microsoft Azure Key Vault Service with FIPS 140-2 Level 3 certified Hardware Security Modules (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
- Architect applications for the cloud with built-in security using vaultless tokenisation with dynamic data masking

‹Thales e-Security›

THALES SOLUTIONS FOR MICROSOFT AZURE



SECURE WORKLOADS ACROSS HYBRID CLOUDS INCLUDING MICROSOFT AZURE

Information technology workloads in Microsoft Azure can offer convenience and cost savings. However, you still need to follow security, privacy and compliance rules, as well as best practices, for protecting 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 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, Microsoft Azure, and other cloud providers.

Customers using Azure Storage Encryption can manage Azure Key Vault encryption keys with Thales nShield hardware security modules.

Microsoft Azure

THALES SOLUTIONS FOR MICROSOFT AZURE

ADVANCED ENCRYPTION FOR MICROSOFT AZURE WORKLOADS AND BEYOND

If you're 100% Microsoft Azure-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 Microsoft Azure, you need an advanced encryption solution. Vormetric Transparent Encryption from Thales e-Security protects your files and databases stored anywhere, including Microsoft Azure, without any changes to applications, databases, infrastructure or business practices. Vormetric Transparent Encryption for Microsoft Azure enables you to:

- Strengthen data security with controls against unauthorized 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 (SIEM) solution of your choice
- Attain a faster return on investment with a non-intrusive, flexible implementation. Encryption agents operate on Azure Virtual Machine compute instances or any other server accessing storage, and are available for many Windows versions and Linux distributions

CENTRALISED, SECURE KEY MANAGEMENT

Available on the Microsoft Azure Marketplace, the Vormetric Data Security Manager (DSM) provides centralised key, policy and log management for Vormetric Transparent Encryption for Microsoft Azure. The DSM is available as a FIPS 140-2 Level 2 or 3 physical appliance appropriate for on-premises deployment, or a FIPS 140-2 Level 1 virtual appliance such as on the Azure Marketplace.

ACCELERATED PCI-DSS COMPLIANCE

Vormetric Tokenisation with Dynamic Data Masking reduces the cost and effort required to comply with security policies and regulatory mandates like the Payment Card Industry Data Security Standard (PCI DSS). Tokenisation secures and anonymize sensitive assets in the data center, big data environments or the cloud. Format-preserving tokenisation 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.

The Vormetric Tokenisation Server is available as a virtual appliance on the Microsoft Azure Marketplace.

BRING YOUR OWN KEYS TO MICROSOFT AZURE KEY VAULT SERVICES

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 Microsoft Azure Key Vault, giving you control over the encryption keys that protect your sensitive cloud data. With nShield BYOK for Microsoft Azure, your on-premises nShield HSM generates, stores, wraps, and exports keys to the Microsoft Azure Key Vault 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 Microsoft Azure Key Vault gives you the following advantages:

- Safer key management practices combined with cloud benefits of scale, cost and convenience
- Greater control over keys—you drive key generation, storage, and export of keys used in the Microsoft Azure Key Vault
- 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 Google Cloud Platform

FULFILL YOUR DATA PROTECTION REQUIREMENTS

Thales e-Security simplifies securing your Microsoft Azure workloads to help you achieve compliance with internal, government, and industry data security regulations. Vormetric data security products available on the Azure marketplace -- Transparent Encryption and Tokenization -- operate seamlessly on workloads in Microsoft Azure, managed service providers and on your premises delivering centralized policy and key management. And nShield BYOK for Microsoft Azure Key Vault gives you control over encryption to achieve compliance and safeguard your data.

LEARN MORE

Visit us at **www.thalesesecurity.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