

Thales solutions for Microsoft Azure



Secure workloads across hybrid clouds including Microsoft Azure

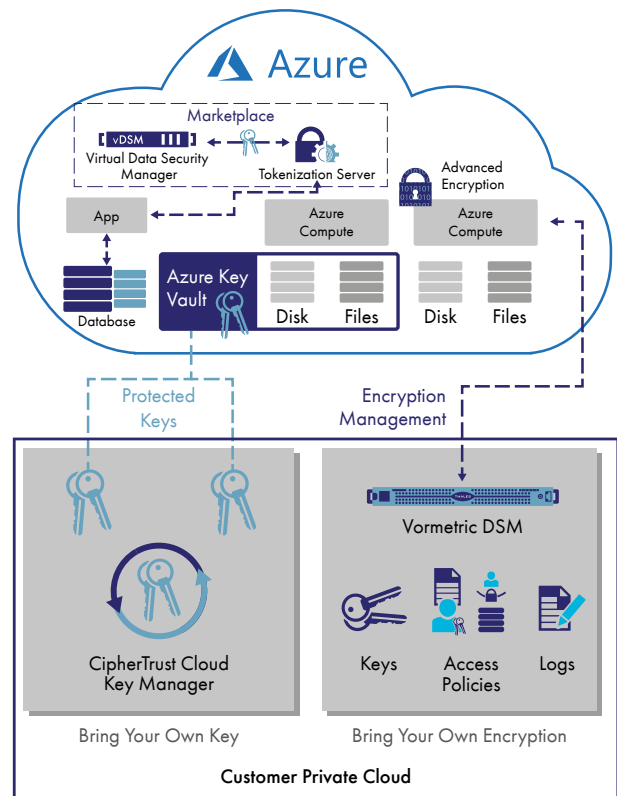
Information technology workloads in Microsoft Azure can offer convenience and cost savings. However, you still need to follow security, privacy and compliance rules, as well as best practices, for protecting data. Further, you need rapid data mobility across all clouds you use and those in your future,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

Advanced encryption with comprehensive key management

Effective, secure use of cloud services 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, Microsoft Azure, 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 Microsoft Azure, with centralized, independent encryption management
- Take secure advantage of Azure Key Vault with centralized key management that spans multiple clouds
- 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 tokenization with dynamic data masking



Advanced encryption for Microsoft Azure and beyond

If you're 100% Microsoft Azure-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 Microsoft Azure, you need an advanced data encryption solution. Vormetric Transparent Encryption protects your files and databases stored anywhere, including Microsoft Azure, without any changes to applications, databases, infrastructure or business practices. Bring your own encryption to Microsoft Azure and other infrastructure as a service providers!

[Vormetric Transparent Encryption:](#)

- Strengthens data security with 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 satisfy 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 Azure compute instances or any other server accessing storage, protect Azure Disk and Azure Files, and are available for many Windows versions and Linux distributions

Centralized, secure key management

The [Vormetric Data Security Manager](#) centralizes key, policy and log management for Vormetric Transparent Encryption, available as a FIPS 140-2 Level 2 or 3 appliance for on-premises deployment, or a FIPS 140-2 Level 1 instance on the Azure Marketplace.

Accelerated PCI-DSS compliance

[Vormetric Tokenization with Dynamic Data Masking](#) secures and anonymize 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.

The Vormetric Tokenization Server is available on the Microsoft Azure Marketplace.

Multicloud encryption key management

Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using [CipherTrust Cloud Key Manager](#).

The CipherTrust Cloud Key Manager leverages cloud provider Bring Your Own Key (BYOK) API's to reduce key management complexity and operational costs by giving customers lifecycle control of encryption keys with centralized management and visibility. The solution is available on the Microsoft Azure Marketplace, or can be deployed on premises or in any private cloud deployment to meet more stringent compliance requirements.

CipherTrust Cloud Key Manager 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 Microsoft Azure, Microsoft Azure Stack, Azure Government, Azure Germany and China National Clouds, AWS KMS, and more!
- Enhanced IT efficiency with multi-cloud key management from a single console that offers automated key rotation and comprehensive key life cycle management

Fulfill your data protection requirements

Thales simplifies securing your Microsoft Azure workloads and helps achieve compliance with data security regulations. Vormetric Transparent Encryption and Tokenization operate seamlessly on workloads in Microsoft Azure and on your premises delivering centralized policy and key management. And CipherTrust Cloud Key Manager brings you into compliance with best practices and data protection mandates pertaining to cloud 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.