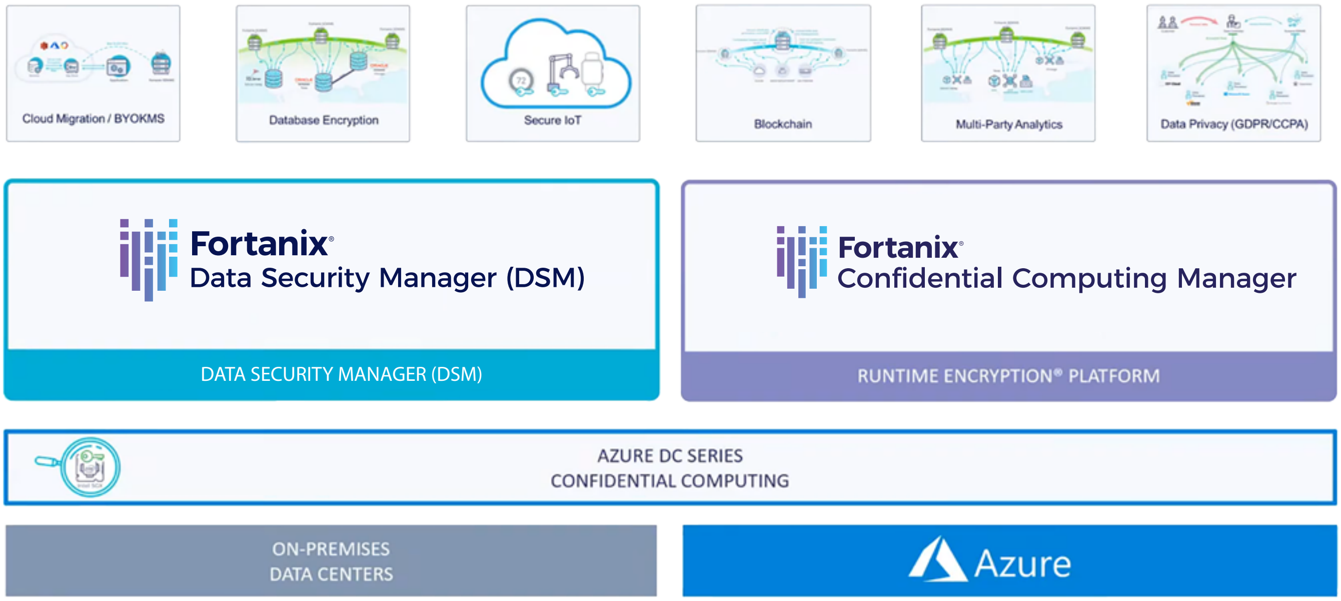
Fortanix®

Solution Brief

Fortanix Solutions for **Microsoft Azure**

Overview

Microsoft Azure is one of the most widely adopted cloud infrastructure platform. It is critical that organizations get the highest levels of data security to confidently migrate to cloud and meet compliance regulations. Fortanix offers security offerings for the Azure cloud platform that allows Azure customers to protect their most sensitive data and securely migrate data to cloud. Fortanix gives Azure customers an additional layer of comprehensive protection for their data and applications throughout its lifecycle – at rest, in-transit and in use.



Fortanix® Data Security Manager (DSM)

DATA SECURITY MANAGER (DSM)

Fortanix® Confidential Computing Manager

RUNTIME ENCRYPTION® PLATFORM

AZURE DC SERIES
CONFIDENTIAL COMPUTING

ON-PREMISES
DATA CENTERS

Azure

"Microsoft Preferred solution" and customers' purchase through Azure Marketplace and will contribute towards customers' Azure consumption commitments.

Fortanix Solutions for Azure

Fortanix Data Security Manager

Fortanix Data Security Manager, a unified platform for protecting enterprise data across cloud and on-premises environments, is now available in the Azure Marketplace.

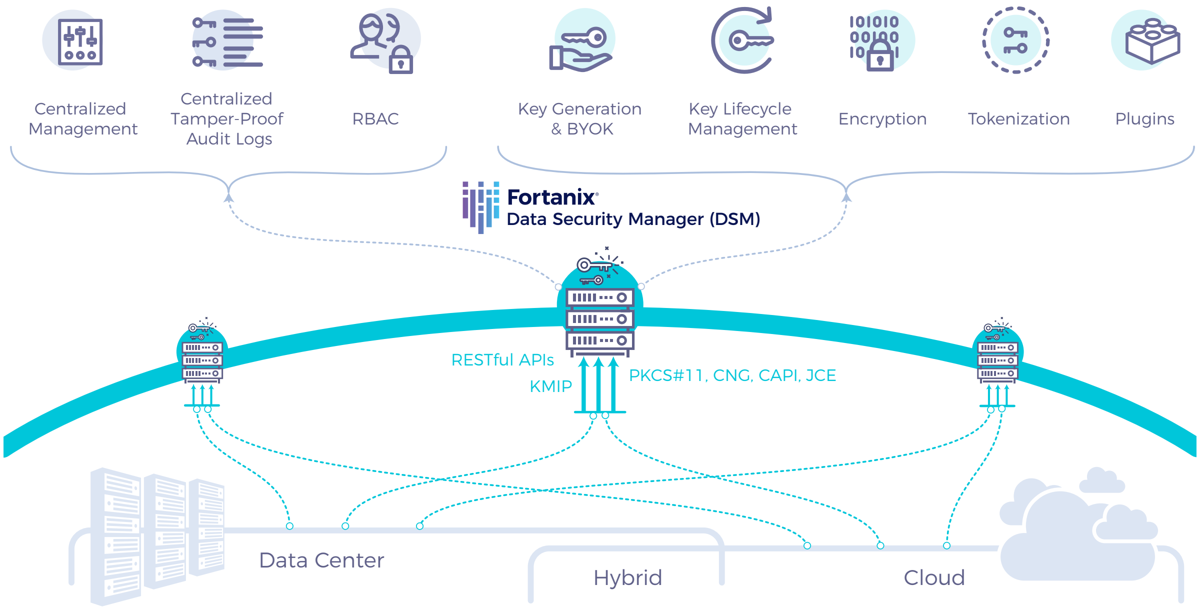
Fortanix Confidential Computing for Azure

Fortanix Confidential Computing Manager, the first solution for end-to-end management of secure enclaves, is now available as an Azure Managed Application.

Fortanix Data Security Manager and Fortanix Confidential Computing Manager are both available today in the Azure Marketplace. Fortanix products can be deployed to any Azure region that offers DC series VMs.

01 Fortanix Data Security Manager

Fortanix Data Security Manager (DSM) is a unified platform for data security that combines encryption, key management, tokenization, and secret management in a single solution. A "run anywhere, protect everywhere" deployment architecture means that customers can now use Fortanix DSM from the Azure marketplace to protect their data across public cloud, on-premises, and hybrid infrastructures. Fortanix DSM in Azure can also connect seamlessly to Fortanix DSM running on-premises, to legacy HSMs running on-premises, or to Azure managed HSMs all of which can provide FIPS 140-2 Level 3 certified security.

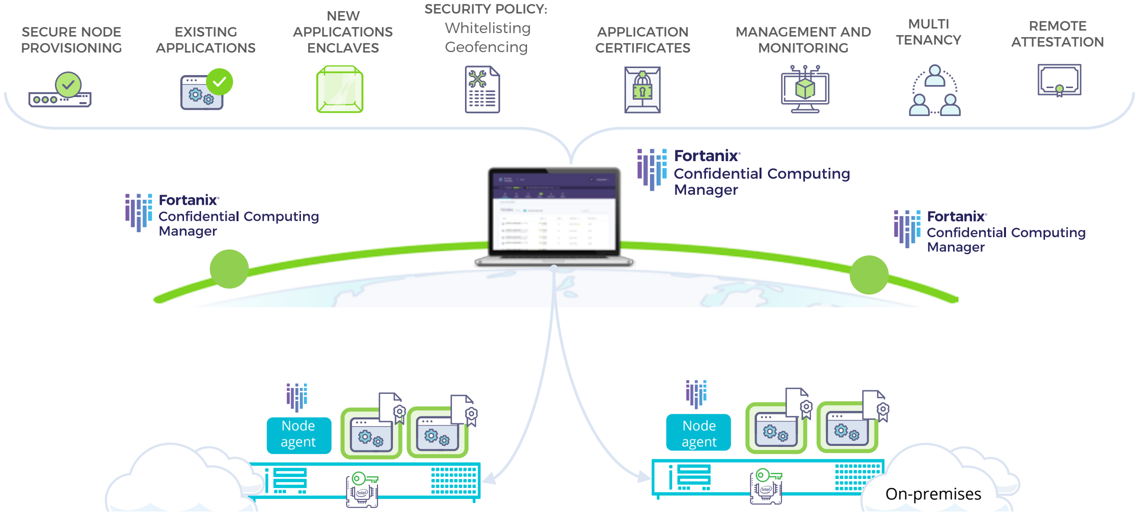


Key Features

- **Unified data protection platform**: Fortanix Data Security Manager is a unified Key Management, HSM, Tokenization and Secrets Management solution secured with Intel® SGX.
- **'Run anywhere, protect anywhere' deployment architecture**: With DSM customers can protect data across public, on-prem and hybrid infrastructures from a single platform.
- **FIPS 140-2 level 3 certified HSM**: Fortanix provides an integrated secure, scalable, and high performance FIPS 140-2 Level 3 HSM that protects keys, secrets, and tokens across multiple public, private, and hybrid clouds.

02 Fortanix Confidential Computing Manager for Azure

Fortanix Confidential Computing Manager (CCM) enables "lift-and-shift" for applications to run inside secure enclaves without requiring any modification and provides complete enclave lifecycle management from creation to migration to termination. While previously available in the Azure Marketplace, Fortanix CCM is now also available as an Azure Managed Application. Integration allows Fortanix users to authenticate accounts using Azure Active Directory.



Key Features

- **Enclave Lifecycle Management**: Fortanix is the only turnkey solution that manages the entire confidential computing environment and enclave lifecycle.
- **Cryptographically enforced policy and auditing**: Fortanix manages and enforces security policies including identity verification, data access control, and attestation to ensure the integrity and confidentiality of data, code, and applications.
- **Available as an Azure Managed Application**: Fortanix Confidential Computing Manager Managed Service is available as an embedded service in Azure portal and as a SaaS service.

Why Fortanix Solutions for Azure?

Unified security across cloud and hybrid environments:

Fortanix capabilities support cloud migration by giving organizations unmatched flexibility by efficiently managing keys, secrets, and tokens across public cloud and hybrid environments from a single, unified platform.

Ensure compliance

Many regulated industries including financial services, healthcare, and retail require that encryption keys be stored in FIPS 140-2 Level 3 validated HSMs. Unlike cloud-native key management services, Fortanix provides FIPS 140-2 Level 3 protection for all encryptions keys, secrets, and tokens, enabling regulated industries to move sensitive data to the public cloud without risking compliance.

Get greater control over cloud keys with Azure BYOK:

Fortanix offers a Key Management System that allows organizations to Bring Your Own Key (BYOK) for Azure cloud. With this approach customers bring or import their own master key (CMK), which Azure can store in their key management system (KMS). and encrypt all Data Encryption Keys (DEKs) under that key. This provides customers with greater control over data and keys.

Unlock the power of confidential computing with Intel SGX on Azure:

Fortanix DSM and Fortanix CCM run on Azure Confidential Computing DC series Intel SGX VMs/DCsV2-series of VMs. Fortanix products and Azure Confidential Computing are built on the security capabilities of Intel® Software Guard Extension (Intel® SGX), including the recently announced Ice Lake 3rd Gen Intel® Xeon® Scalable processors. Intel® SGX enables hardware-secured trusted execution environments that can be used to protect data in use, at rest, and in motion while preventing unauthorized access by a cloud provider, administrator, or user.

Consume easily from the Azure Marketplace:

Fortanix Data Security Manager and Fortanix Confidential Computing Manager are both available in the Azure Marketplace and can be easily consumed. “Microsoft Preferred solution” and customers’ purchase through Azure Marketplace and can contribute towards customers’ Azure consumption commitments.