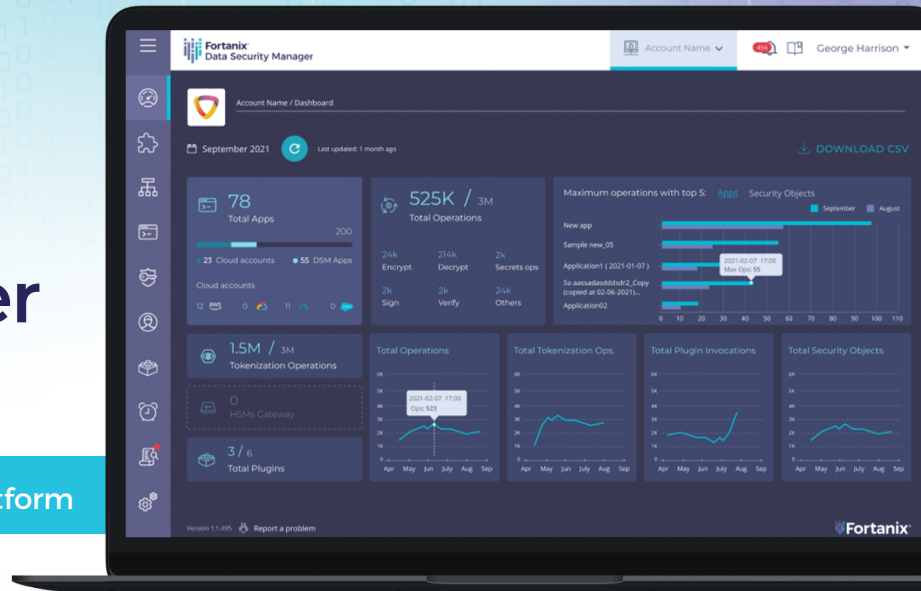




Fortanix Data Security Manager (DSM)

The Industry-Leading Data Security Platform



Unified data security platform, powered by Confidential Computing Technology

As you shift data and applications to new infrastructures, you need a solution that can protect all your data—on-premises as well as in the cloud. Fortanix Data Security Manager (DSM)—a unified data security platform that is DevOps/SecOps friendly, easy to use, and enables customers to centrally implement and manage multiple data security capabilities from a single console. Fortanix Data Security Manager has redefined data security by utilizing the game-changing potential of Confidential Computing.

UNIFIED DATA PROTECTION

Fortanix Data Security Manager delivers HSM, Key Management, Encryption, Tokenization and other security capabilities for your hybrid and cloud-native applications, all from the same integrated solution.

FLEXIBLE DEPLOYMENT

Primarily delivered as a SaaS offering, it also offers other deployment options- on-prem appliance, software, and virtual deployments.

REST API DRIVEN ARCHITECTURE

Powerful RESTful APIs make it easy for developers and DevOps teams to use and integrate data security into their applications.

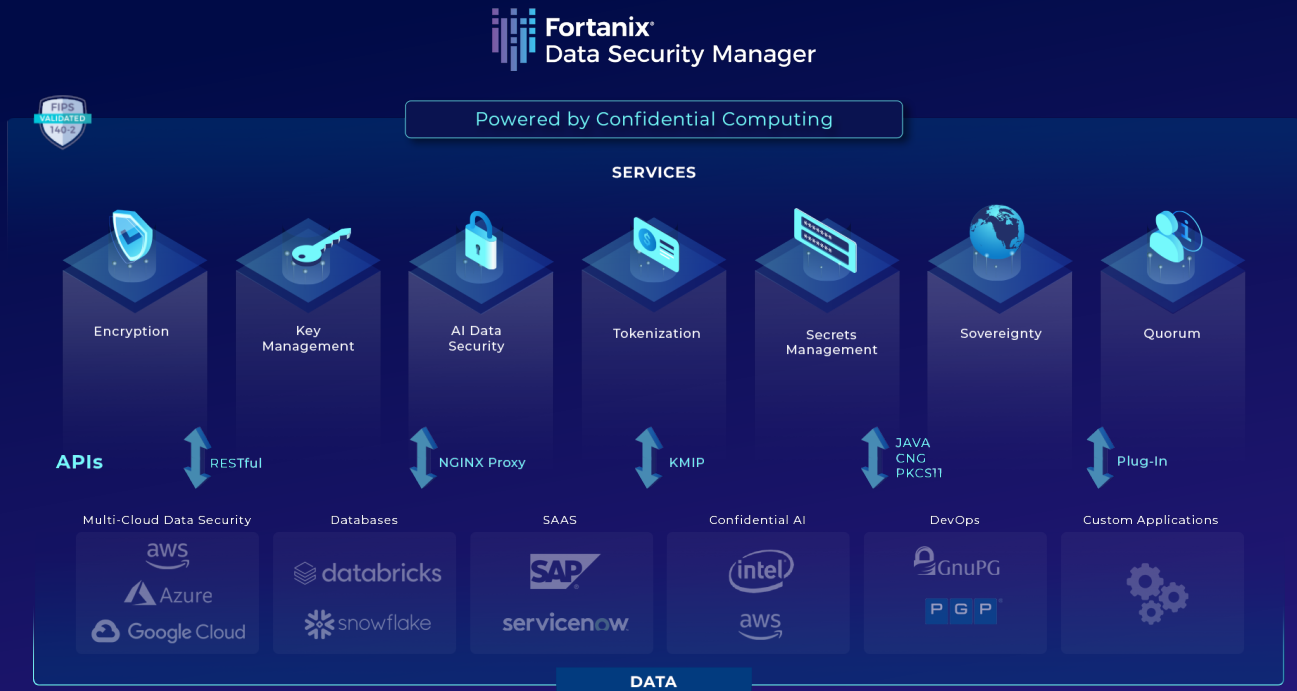


POWERED ON CONFIDENTIAL COMPUTING

With Fortanix Confidential Computing technology powered by Intel® SGX secure enclaves, data always remains secure across its lifecycle- at-rest, in-transit, and in-use.

SUITED FOR ANY IT INFRASTRUCTURE

The platform secures data across your IT infrastructure including all cloud platforms (AWS, Azure, GCP), databases (Oracle, SAP HANA, SQL, Server, and more) and applications like ServiceNow, Snowflake, Salesforce etc.



Flexible Deployment Options - On-Premises Or In The Cloud

Software or Virtual Appliance, Software-as-a-Service (SaaS) and Hardware appliance for on-premises installation

FIPS-validated appliance, software on SGX-enabled servers/laaS, or SaaS provides you with a ubiquitous solution for your hybrid/multi-cloud applications.

CONSUME AS SAAS

- FIPS 140-2 Level 3 backed service
- Built in high-availability
- Capacity on demand in global region of your choice

PURE SOFTWARE/ VIRTUAL APPLIANCE

- Rapid KMS deployment
- Infinite scalability
- Powerful developer APIs
- Fully automate your cryptographic policies



ON-PREM APPLIANCE

- FIPS 140-2 Level 3 appliance
- Native clustering & management
- Powerful developer APIs
- Fully automate your cryptographic policies

Key Benefits

- ✓ **Reduce engagement and deployment friction** with flexible consumption options and centralized management of data.
- ✓ **Meet security and compliance** with a broad set of data security and privacy controls.
- ✓ **Accelerate cloud adoption** by securing greater control of data in the cloud with Bring-Your-Own Key/Key Management Service (BYOK/KMS) capabilities.
- ✓ **Extend security to the larger IT ecosystem, reduce security gaps** with RESTful API driven architecture.

Platform Capabilities

Encryption and Tokenization



HARDWARE SECURITY MODULE

FIPS certified- FIPS 140-2 Level 3 certified HSM delivered as an appliance and service.

Remote management-Geo-graphically scalable service that is 100% remotely managed.

HSM Gateway- Centrally manage your existing HSMS across environments.



KEY MANAGEMENT SERVICE

External key management EKM/Bring-Your-Own-Key BYOK- Externally manage and control keys for GCP (EKM), Azure (BYOK), AWS (BYOK/KMS). **Full key lifecycle management**-Generation, rotation, expiration, and deactivation for secure and consistent key management.

Automate key operations- Automatic key rotation, one-click rotation across regions and clouds, key expiration and key state alerts.



TOKENIZATION

Vaultless Tokenization- No centralized Token database required.

Advanced Data Masking- Dynamically mask an entire field or part of tokenized data.

Tokenize Custom Objects- Tokenize any custom objects to protect any kind of data including credit card or SSN.



POST QUANTUM CRYPTO

Code-based Cryptography (Leda) Supports Leda based on public-key encryption and error-correcting codes.

Lattice-based Cryptography (Round5) Supports Round5 algorithm of NIST Post Quantum Cryptography Standardization project.

Hash-based Cryptography (LMS) Supports Hash function based LMS simple verification and highly secure algorithm.

Cloud Data Security



CLOUD DATA CONTROL

Multi-cloud Key Management

Protect sensitive data across multiple clouds. Supports AWS, Azure and GCP.

Key separation

Extend existing cloud-native key management system (KMS) to separate encryption keys from data.

RBAC

Role-based access control (RBAC) for users, applications, and groups with segregation of duties.



SECRETS MANAGEMENT

Store outside the source code

Sensitive credentials stored outside the source code in FIPS 140-2 level 3 certified HSM.

Supports Kubernetes

The utility can monitor the environment in real-time and inject secrets at runtime.

JSON Web Tokens

Supports JWT authentication to further secure and trust requests.



TRANSPARENT ENCRYPTION PROXY

Dynamically encrypt/decrypt the data

Allows applications to encrypt/decrypt data dynamically by ingesting data in any form.

Application agnostic

Application agnostic, scalable solution that intercepts and encrypts data on the fly.

Implemented as NGINX plugin

Encrypt/decrypt operations via an API call to the TEP which is based on NGINX.

Confidential Computing



CONFIDENTIAL AI

Confidential Compute (CC) based AI

platform- Data teams can work with their sensitive data sets and run AI models in confidential compute.

Easy to deploy/provision infra

Managed CC infrastructure powered on Intel Icelake Xeon processors.

Support for AI/ML models

Supports a range of models such as Yolov5, Decision Trees, SVM, Linear Regression etc.



CONFIDENTIAL COMPUTING MANAGER

Enclave lifecycle management

Turnkey solution to manage the entire confidential computing environment and enclave lifecycle.

Broad application support

Enable existing applications, enclave-native applications, and pre-packaged applications to run in a secure enclave in minutes.

Code Verification

Verifies the identity of code and applications using digital certificates and PKI.

Plugins



SECURE BUSINESS LOGIC

Secure plugins

Plugins allow users to run custom code securely inside enclaves.

Self-service scripting

Plugins can be written in Lua script and easily loaded to the Key Management System (KMS).

Plugin library

Plugin library allows users to view and share frequently used plugins from a common place.

Other platform features

FLEXIBILITY

- SaaS deployment can be accessed publicly via the public cloud and privately through the Equinix Cloud Exchange Fabric™ (ECX Fabric™).
- High availability, intelligent geographic load balancing, resistance to site failure.
- Centralized web-based UI with enterprise-level access controls and single sign-on support.
- Distributed low latency key access.

EXTENSIBILITY

- Support for RESTful APIs, PKCS#11, KMIP, JCE, Microsoft CAPI, and Microsoft CNG.
- Multi-site and hybrid cloud support.
- Leverages open standards including KMIP, SAML/SSO, and PKCS#11.
- Encryption standards include AES, RSA, HMAC, and ECC, Opaque objects to provide the highest levels of security.

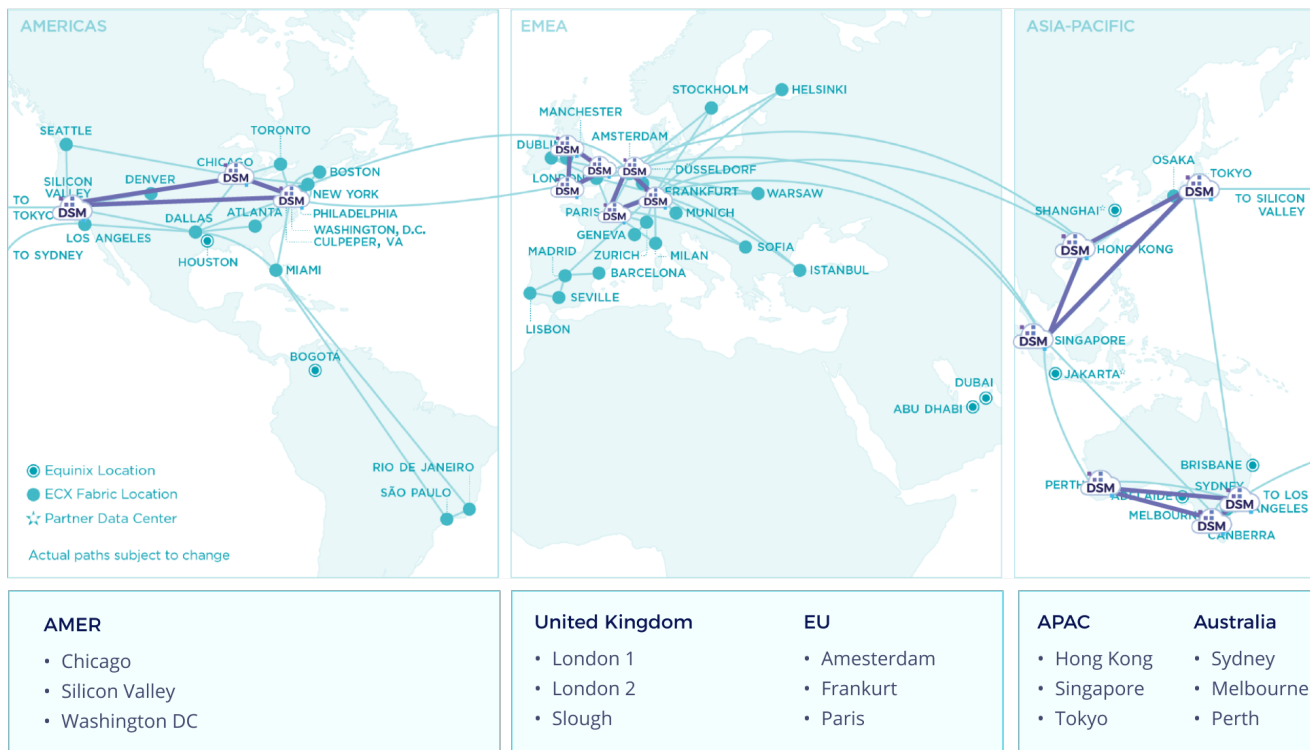
ACCESS CONTROLS & LOGGING

- Quorum approvals to prevent unauthorized access by a single user (or administrator).
- Central-tamper proof logging.
- Integrates with SIEM solutions.
- Enterprise-grade security of Intel® SGX.

Security, wherever your data is

Globally available service across multiple regions, scaling to tens of billions of transactions

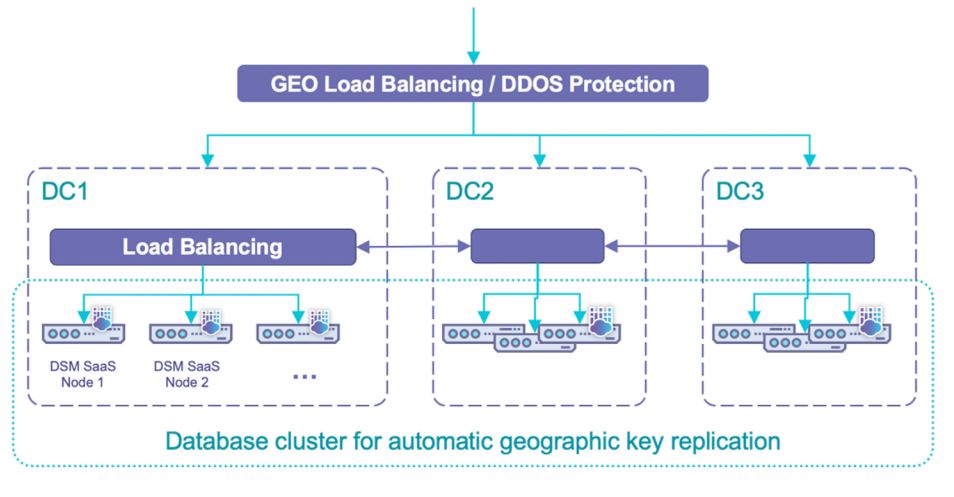
The service currently operates across 15 data centers around the world, giving you the freedom to select the global footprint that best matches your requirements.



Highly resilient, distributed architecture with maximum availability

Multiple clusters with a distributed architecture web-scale architecture

Fortanix DSM is built on a web-scale architecture that's designed to deliver high resiliency and availability for modern cloud environments to select the global footprint that best matches your requirements




Fortanix Runtime Encryption Appliance – FX2200

The only integrated HSM and KMS appliance on the market designed for the cloud.

The FX2200 is designed to deliver secure Key Management, Audit logs, Hardware Secure Module, and Cryptography services.

FX2200 II Node Specification

Cryptography	Full NSA Suite B algorithms
Interfaces supported	REST APIs, PKCS#11, Microsoft CAPI and CNG, JCE, KMIP
Certifications	FIPS 140-2 Level 3*
FIPS key storage	Fortanix proprietary key storage module
Operating environment	Self-Defending Key Management Service™ (running on Ubuntu Linux 16.04)
Management / Monitoring	Centralized Management with Web UI, CLI and APIs Syslog, Splunk integration
High Availability	Scale-out clustered design with built-in HA / DR
Reliability	Non Rotating media- Solid State Devices Dual Redundant Power Supplies, FRU's (Field Replaceable Units) MTBF 250,000 hours (basis of parts count method)
Network Connectivity	Dual Copper 10Gigabit Ethernet, 10GBASE-T, IEEE 802.3an, supporting link aggregation Gigabit Ethernet, 1000Base-T 100 Mb Ethernet : 100BASE-TX 1 x IPMI port Dual SFP28 (Small Form Factor Pluggable) supports: SFI interfaces supports 25GBase-R PCS and 25 Gigabit PMA in order to connect with SFP28 to 25GBase-SR
Processor	Intel® SGX 
Memory	64GB high speed memory



Dimensions	1U Rackmount
Weight	47lbs / 21.319Kg
Power Supply	Dual redundant 300w AC power supplies
Voltage / Frequency	AC input: 100-240v 63-47hz 5-2.5a
Thermal Rating	1,164 BTU/hr (maximum)
Temperature	Operating: -5 to 40 C° / storage -40 to 70 C°
Safety and Environmental	FCC class B, CE, TUV, GS, RoHS, C-Tick, CCC, VCCI



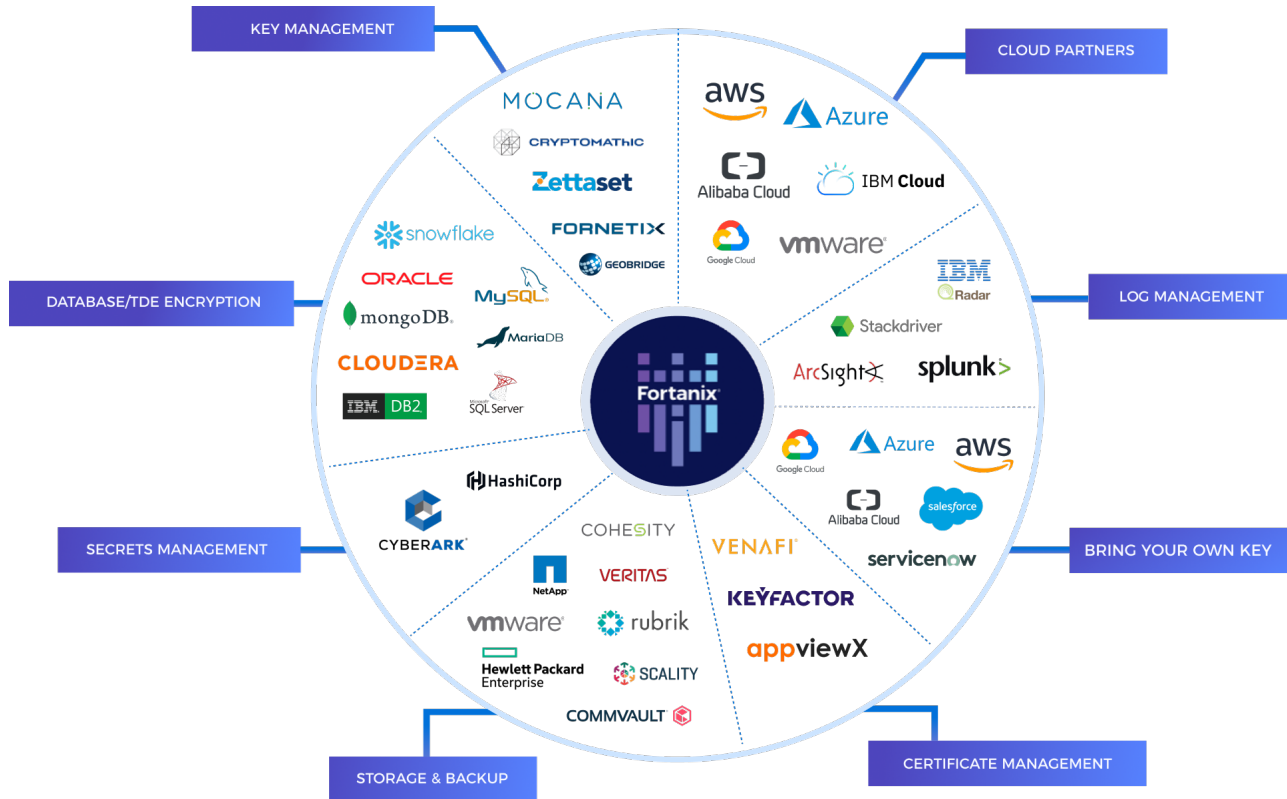
FX2200/2 front view



Tap into an unrivaled partner ecosystem

Seamlessly integrate with 100+ Fortanix partners via RESTful APIs in a developer friendly environment

Unrivaled partner ecosystem of seamless integrations helps expand core functionalities to the larger IT ecosystem and eliminates security gaps.



Certifications

Certified with the highest standards of security and compliance

The platform is certified to the highest standards of security and compliance controls including FIPS 140-2 L3, PCI-DSS, SOC 2 and SOC 3

