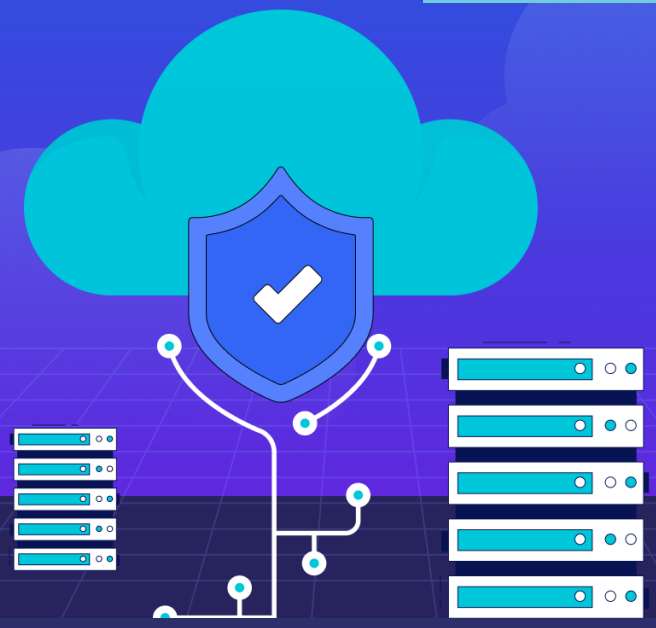
Fortanix®

Solution Brief

Fortanix for Imperva



Bolster up your Imperva Cloud Web Application Firewall (WAF) with FIPS 140-2 L3 grade HSM capabilities powered by Fortanix Data Security Manager.

Business Case

From email hacking and mobile malwares to more prominent data breaches—insecure websites and vulnerable web applications have become a de facto standard to commence all types of attacks. As businesses continue to lean on mobile applications and IoT devices to facilitate business interactions, many online transactions occur at the application layer. Attackers often target these applications to reach the sensitive data stored in the backend database—that can be accessed through web applications.

A web application firewall (WAF) protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others.

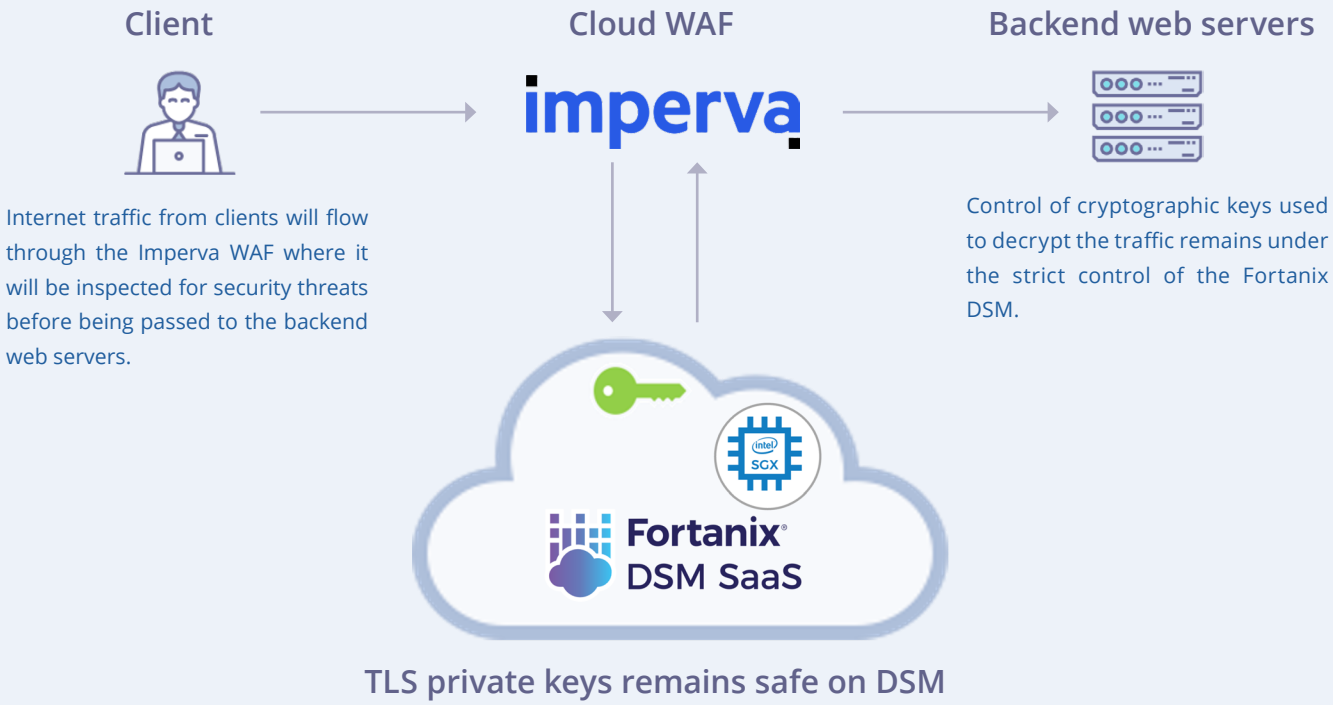
WAFs are important for a growing number of organizations that offer products or services online—this includes mobile app developers, social media providers, and digital bankers. WAFs can help businesses protect sensitive data, such as customer records and payment card data, and prevent leakage.

While it's important to have a WAF to protect critical information in-transit between the users and the applications, it's equally important to combine it with other security measures. Such as, securing the encryption key used by WAF when decrypting the TLS HTTPS encryption.

alliances@fortanix.com | +1 (650) 943-2484 | 3910 Freedom Circle, Suite 104, Santa Clara CA 95054

Extending Fortanix FIPS 140-2 Level 3 Security to Imperva Cloud WAF

Imperva Cloud WAF is delivered by multiple cloud-based points of presence globally. Fortanix works with Imperva WAF to ensure that the cryptographic keys used to secure the TLS connections are protected and controlled in a manner commensurate with requirements of standards and rulings such as PCI-DSS, Schrems II and HIPAA.



Using Fortanix DSM in conjunction with Imperva WAF means the encryption keys are stored and secured safely within Fortanix Data Security Manager, separate from Imperva's servers ensuring separation of key material from the data and a tamper proof audit trail of cryptographic key usage with the ability to immediately disable a key rendering it unusable if required.

The protection of encryption keys in Fortanix DSM gives customers assurance that traffic between clients and the protected web servers cannot be decrypted by any unauthorized party.

alliances@fortanix.com | +1 (650) 943-2484 | 3910 Freedom Circle, Suite 104, Santa Clara CA 95054

Key Capabilities

- FIPS 140-2 level 3 certified HSM.
- Separation of key material from data.
- Tamper proof audit log of key usage with SIEM integration available.
- Single pane of glass key and cryptographic policy management.
- DSM SaaS architecture allows for easy scaling of transactional throughput capability to support any level of load.
- Highly available with intelligent load balancing built in.

Solution Highlights

- **Certified solution supported by Fortanix and Imperva.**
- **DSM SaaS is a cloud native subscription-based solution.**
- **Cloud powered with the robust protection of an on-prem solution**
- **Hold Your Own Key solution (HYOK) where there is a regulatory need to ensure keys are separated from your data.**
- **Enterprise level access control and audit logging.**

alliances@fortanix.com | +1 (650) 943-2484 | 3910 Freedom Circle, Suite 104, Santa Clara CA 95054

Multiple Key Storage and Security Options

Flexible deployment options with on-prem HSM appliances, SaaS, or software only in the cloud. Store and protect encryption keys with FIPS 140-2 Level 3 HSMs to maintain the highest possible compliance and entropy.

Centralized Policy Management and Controls

Policy management and quorum approvals that can integrate seamlessly with existing authentication identity providers. RBAC provides added security and controls.

Full Key Lifecycle Management

Fortanix delivers full key lifecycle management such as generation, rotation, expiration, deactivation to ensure secure and consistent key management across on-premises and multicloud environments, including bring your own key (BYOK) and bring your own key management service (BYOKMS).

Complete Data Security Management

Add Tokenization, automated cloud key management, management of legacy HSMs, and other capabilities to create a single comprehensive solution.

Automate Key Operations

KMS offers state of art automation features like automatic key rotation, one click rotation across regions and clouds, automatic key expiration based key rotations, automatic alerting based on key state changes.

alliances@fortanix.com | +1 (650) 943-2484 | 3910 Freedom Circle, Suite 104, Santa Clara CA 95054

Top Benefits

Single Platform

Fortanix manages data security for multiple public clouds and hybrid environments through a single platform that can scale and cluster between global sites. Allows businesses to seamlessly move data between on-premises and public cloud infrastructures with a single consistent set of cryptographic services and keys.

Unified Management

Fortanix provides a “single pane of glass” modern, multi-tenant, and intuitive user interface for simplified administration and increased control, including extensive logging and auditing across your entire infrastructure.

DevOps and Cloud Friendly APIs

KMS supports extensive RESTful APIs, PKCS#11, KMIP, JCE, Microsoft CAPI, and Microsoft CNG. Easily support all existing and new applications, whether operating in public, private, or hybrid cloud.

Scalable platform with automated load-balancing, DR/HA

DSM is built to scale horizontally and vertically as your demand for managing your keys and secrets increases. This is ensured while providing automated load-balancing, fault-tolerance, disaster recovery, and high availability. Fortanix KMS can be deployed globally and for hybrid or multicloud environments.

Fortanix®

Security, *wherever* your data is

alliances@fortanix.com | +1 (650) 943-2484 | 3910 Freedom Circle, Suite 104, Santa Clara CA 95054