Solution Brief

Automating Certificate Management and Secure Key Orchestration with Fortanix and AppViewX

Business Case

Public Key Infrastructure (PKI) has become standard for enterprises trying to secure data and authenticate machines on the move. X.509 certificates, often leveraged in the form of SSL/TLS certificates, are one of the many PKI systems widely adopted by enterprises. The complexity of deploying and managing public key infrastructure (PKI) setups has multiplied manifold over the last decade.

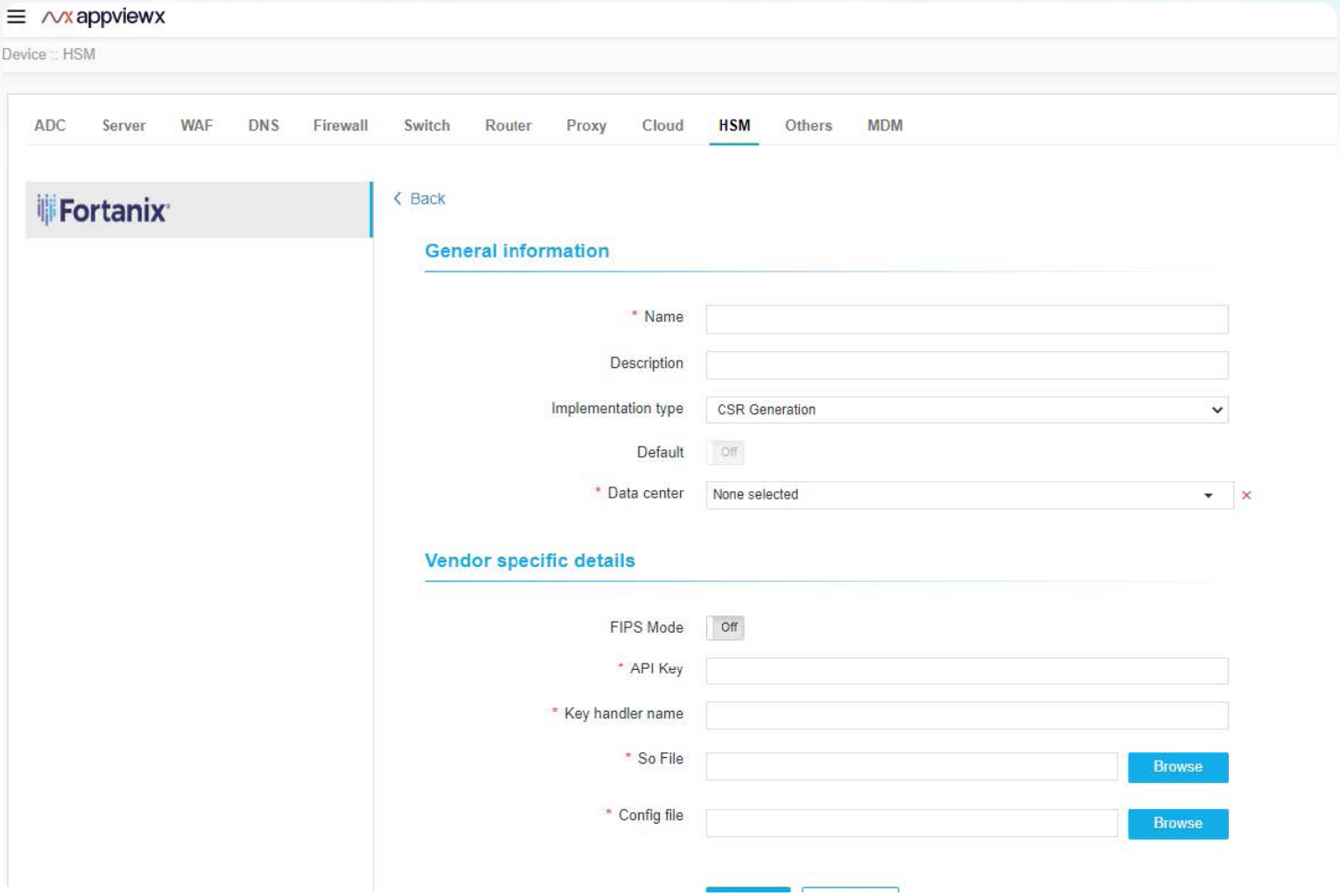
Even the best-designed PKIs require supporting systems for managing them by streamlining certificate tasks, key rotations, and other PKI operations. An efficient certificate lifecycle management (CLM) will enable administrators to renew, revoke, or install certificates from a single interface and weave together multiple vendors (certificate authorities or CA's, hardware security modules or HSM's, identity and access management or IAM tools, et al.) and allow them to work in synergy with PKI.

All these systems operate on the principle of private and public encryption keys, which are used to encrypt and decrypt information, respectively. This makes a private key the single most important asset of any security infrastructure. When a private key is uncovered by malicious actors, valuable data is compromised through the impersonation of an enterprise's servers. And unfortunately, many enterprises are still using faulty, and often non-compliant key management processes that leave their most valuable data susceptible to theft and misappropriation.

There is a need for certificate management systems that integrate with key security structures such as HSMs, to ensure that key circulation remains a closed-loop process.

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040

Fortanix - AppviewX Joint Solution



The partnership between AppViewX and Fortanix helps enterprises overcome the challenges brought by managing private keys in a complex infrastructure. For enhanced security and compliance, private keys must be encrypted before they are stored in an enterprise's infrastructure. Our combined solution gives the enterprise multiple options that cater to the specific needs of that infrastructure. AppViewX acts as the lifecycle management and orchestration platform of X.509 certificates, and Fortanix Data Security Manager ensures the security of the private keys associated with those certificates in the cloud, on-premises or as a hybrid solution.

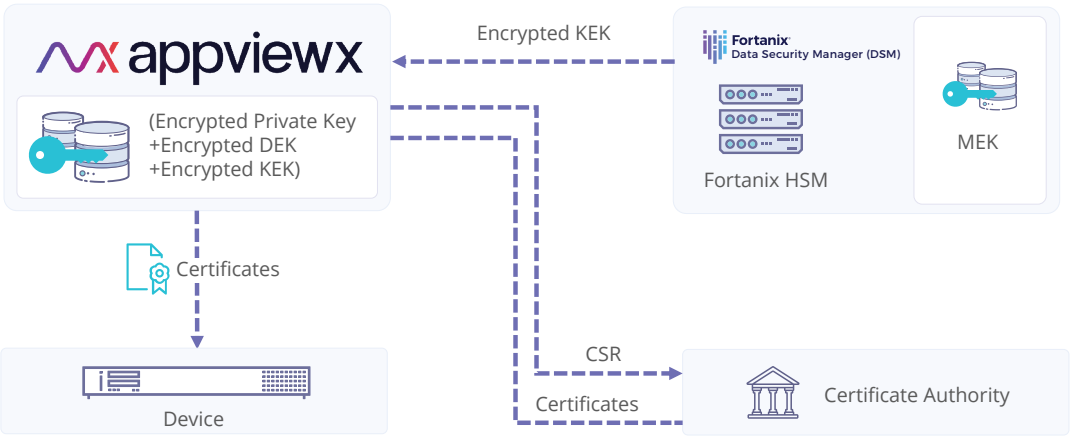
info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040

Benefits of the solution

- Encrypt and protect private keys using industry-standard, FIPS 140-2 Level 3 certified Fortanix HSM with the flexibility of either on-premises, cloud-based or hybrid services.
- Manage and automate multi-vendor X.509 certificates across multiple devices
- Ability to generate, store and manage hundreds of millions of keys with automation across key lifecycle.
- Gain visibility and control across all certificates and its keys
- Enforce policies and ensure compliance across the network

Solution Highlights

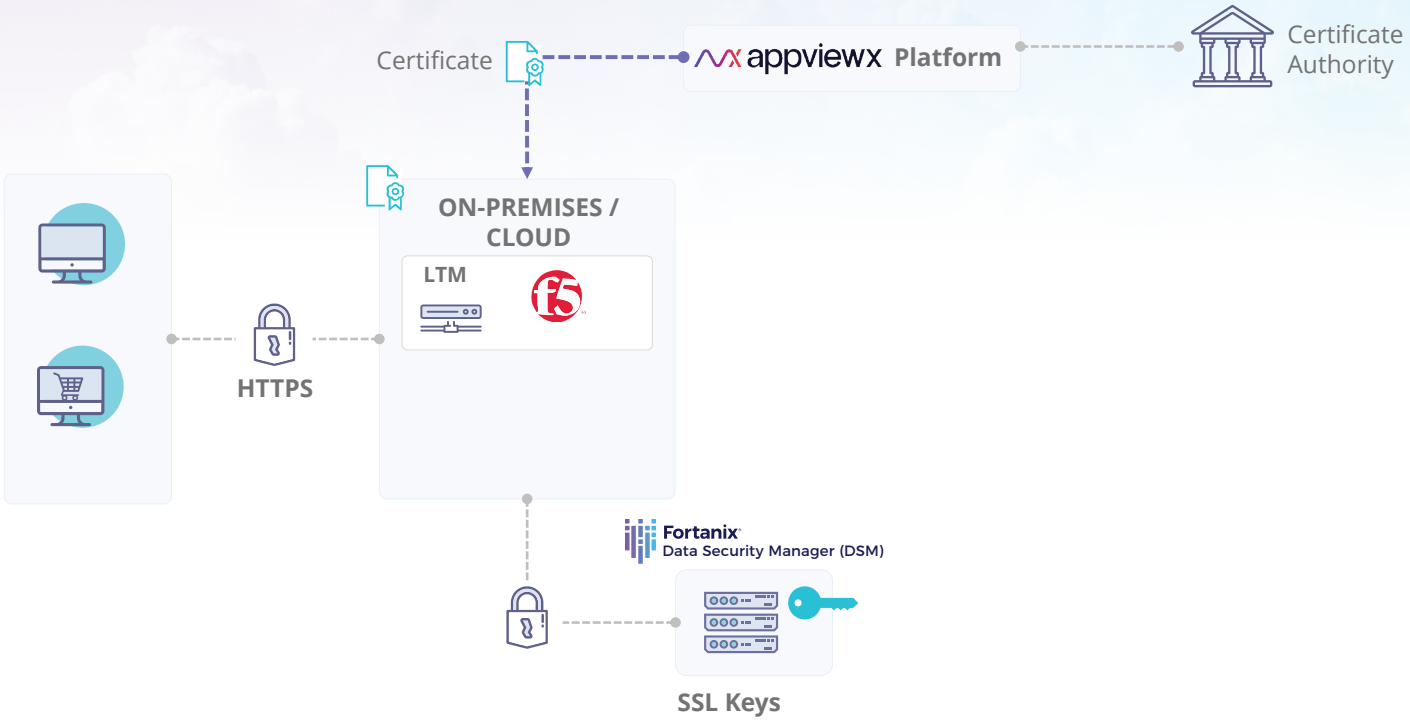
Certificate Management with Encrypted Private Key Storage in AppViewX



This solution is useful for enterprises seeking to generate and store private keys within AppViewX and limit their encryption to the Fortanix DSM for optimum resource utilization — this is accomplished via Transparent Data Encryption (TDE). The private key, before it is stored in an AES-256 encrypted database, undergoes multiple layers of encryption by Data Encryption Key (DEK), Key Encryption Key (KEK) and Master Encryption Key (MEK). While the encrypted private key, encrypted DEK, and encrypted KEK reside inside AppViewX, the MEK is stored inside the FIPS 140-2 Level 3 certified Fortanix HSM and cannot be retrieved. For any crypto-operation MEK never leaves the Fortanix HSM. This solution is suitable for all ADC and server devices.

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040

Featured Use case: Certificate management and SSL Keys protection for F5



Fortanix Data Security Manager and AppViewX platform are fully integrated with F5 BIG-IP® platform and are compatible with all the latest versions of the platform. The solution allows users to centrally manage, automate, and orchestrate TLS certificates and keys of F5 BIG-IP devices across data centers. AppViewX enables discovery and management of certificates on F5 devices as well as those on application servers, web servers, and proxy servers. The Fortanix Data Security Manager provides both a key management and a FIPS 140-2 Level 3 HSM solution that integrates with BIG-IP deployments. The Fortanix appliance stores and manages all the SSL keys and performs crypto operations when called by the F5 platforms.

Summary

Digital certificates are the face of your enterprise online. Given the high level of security associated with PKI technology, the need for digital certificates is only going to increase. This will inevitably leave enterprises with an abundance of private keys to safeguard and without an efficient mechanism to safeguard them with. Using the AppViewX and Fortanix joint solution, enterprises can apply the visibility and security that their private keys and certificates demand, all while maintaining the agility and compliance needed to adapt to rapidly changing business needs. By leveraging the full-cycle certificate management suite of AppViewX and the key security capabilities of Fortanix Data Security Manager, enterprises can maximize the efficiency of their certificate and key management while protecting keys from theft or misuse.

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040

About Fortanix Data Security Manager

Secured with Intel® SGX, Fortanix Data Security Manager is a unified HSM, Key Management and Tokenization solution. DSM provides flexible consumption options — a hardened appliance, HSM as a service, or software running on cloud. DSM offers central management, tamper-proof logging, rich access control, REST APIs and massive scalability. Organizations use DSM to secure their sensitive cloud and traditional applications, including digital payments, PKI systems, IOT applications, silicon manufacturing, and remote TLS terminations — all while drastically reducing integration complexities and expenses.

About AppviewX CERT+

AppViewX CERT+ is a next-gen machine identity and PKI management platform available as a SaaS and on-prem solution to simplify and enhance enterprise security with a unified approach for certificate lifecycle management. It allows for end-to-end automation of certificate and key lifecycles across environments and vendors. It makes certificate management streamlined and efficient, allowing for endless upward scalability and cryptographic agility.

NEXT STEPS

To learn more about this joint solution, visit www.appviewx.com/partners/technology-partners/ or www.fortanix.com/partners/

Get more information about individual product lines here:
AppViewX CERT+ | Fortanix Data Security Manager (DSM)

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040