Case Study

O.C.Tanner Protects Customer Data Across Hybrid, MultiCloud, and Multi-Site Environments

Unified Key Management and Shared Secrets Service Protects Client Data

O.C.TANNER Fortanix® aws

O.C.Tanner develops strategic employee recognition and reward solutions that help people accomplish and appreciate great work. For 2002 Winter Olympics, O.C.Tanner manufactured medals provided to the athletes. To this day, they still provide the Olympic Rings to all athletes that qualify for the Olympics.

13.5
MILLION USERS

150+
COUNTRIES

5.3
MILLION AWARDS DELIVERED ANNUALLY

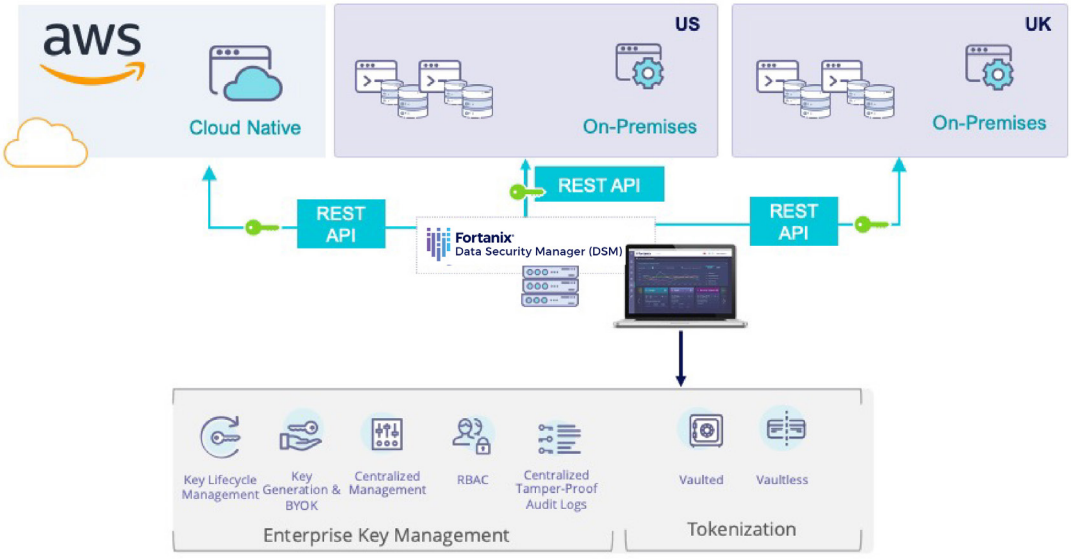
O.C.Tanner's Data Protection Challenge

To provide employee recognition and reward solutions, O.C. Tanner developed an innovative hybrid cloud strategy for their core applications that leveraged a combination of on-premises infrastructure and Amazon Web Services (AWS). O.C. Tanner needed to protect their own and their client's' sensitive data. What mattered is who has access to this sensitive data, how access is managed and how this data is secured. Therefore, it was critical for O.C. Tanner and their clients that the organization protects data by maintaining control of all encryption keys, tokens, and shared secrets for all client data. Adding to the challenge, O.C. Tanner operated multiple sites and wanted the option to operate in multiple clouds.

As O.C.Tanner considered their options, the AWS native key management services didn't meet their own and their client's security requirements, while traditional Hardware Security Modules (HSMs) didn't have the application interfaces to support a public cloud deployment, easily manage multiple sites or provide tokenization.

> One of the nice things about Fortanix is the ability to leverage the solution on premises and with public cloud.

Niel Nickolaisen
Chief Technology Officer
O.C.Tanner



Fortanix Data Security Manager(DSM) was previously known as Fortanix Self-Defending Key Management Service (SDKMS).

Fortanix DSM Solution

We chose Fortanix to manage our most sensitive data and protect it well. What matters is who has access to this data, how access is managed and how this data is secured. We are working with Fortanix DSM in terms of privileged access management, how to tokenize the data, restrict who sees what.

Niel Nickolaisen
Chief Technology Officer
O.C.Tanner

O.C.Tanner turned to Fortanix DSM to provide a unified key management, tokenization and shared secret solution that could be delivered as a service across their on-premises infrastructure, multiple clouds, and multiple sites in the U.S. and United Kingdom. With the Fortanix RESTful APIs, O.C.Tanner was able to provide their developers with a single data protection interface to integrate into all their applications for client and server-side encryption.

Through DSM, O.C.Tanner also seeks to bring their own key to DSM. They searched around for a solution to help in all these areas and found Fortanix. They are a global company and have clients all over the world. Their clients have required that they be the only ones controlling the encryption keys for the data.

Bring Your Own Key (BYOK) with Fortanix DSM

BYOK is a solution in which the customer, rather than the cloud service provider (CSP), controls the encryption keys and therefore the data. To support BYOK, CSPs provide a method to transfer customer's keys to their domain in order to support data encryption within their services, thus eliminating the need for the application to perform any cryptographic operations.

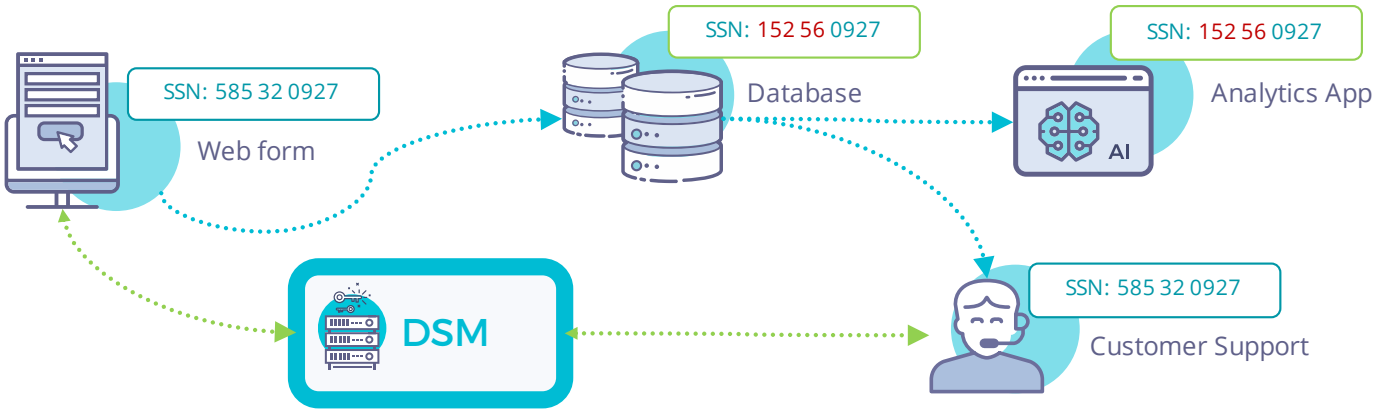
AWS has had support for BYOK for some time now; however, this requires the use of its Key Management Service (KMS). To get started with KMS, you generate a Customer Master Key (CMK), which gets used to derive other keys. You can import your own 256-bit AES key as the CMK, thus enabling BYOK. AWS provides a wrapping key and a token to securely import customer keys. We can also set expiration date and user access policies for the keys in KMS. Once imported, you can use any of the KMS integrated services (S3, EBS, RDS, Redshift, etc) for server-side encryption.

BYOK with DSM

Fortanix DSM is purpose-built to effectively address these scenarios across multicloud deployments. DSM provides an extensive suite of client libraries, including PKCS11, Microsoft CNG, JCE, and Java and Python SDKs, that can be readily used with modern applications.

Fortanix DSM Tokenization

- Unified Key Management, HSM, and Tokenization capabilities lowering the TCO.
- Vault-less tokenization approach with a cloud-scale architecture for better and faster performance.
- Data protection that adapts to evolving infrastructure (private, hybrid, public, multi-cloud).
- Granular group access controls to ensure only authorized users or applications can perform tokenization and de-tokenization.
- Support variety of data types (PAN, PII, SSN, email, etc.) with a variety of App integration interfaces (REST) APIs, libraries and more.
- Supports custom tokenization fields with variable token and masked data lengths.
- Reduce compliance scope/costs (PCI-DSS, PHI, GDPR).
- Protection with minimal application changes.
- Reduce sensitive data exposure (PII and PAN).
- Intuitive and easy to use UI.
- Masked access allows administrators to set different masking rules for different identities. Masking rules allow specific users to see only portions of the data.



Why did O.C.Tanner choose Fortanix DSM:

O.C.Tanner conducted a thorough pilot and security audit to Fortanix DSM. Specifically:

- Overall security of DSM.
- Ease of use BYOK to leading providers such as AWS, Google Cloud Platform and Microsoft Azure.
- Ease of set-up, integration with O.C.Tanner's IT environment and directory services.
- Ability to leverage the solution on-premises and in public clouds.
- Broad supported use-cases, primarily tokenization as a service and enterprise key management.
- Ability to serve any environment with scalable distributed key management, automated load balancing, high availability and replication.
- Ease of use, flexibility and extensibility.
- Easily secure sensitive data during migration to public cloud, while assuring data sovereignty and meeting customers' requirements regarding the security and control of the encryption keys.