Solution Integration Guide

Privileged Account Security

Fortanix Data Security Manager (DSM) and CyberArk Enterprise Password Vault®

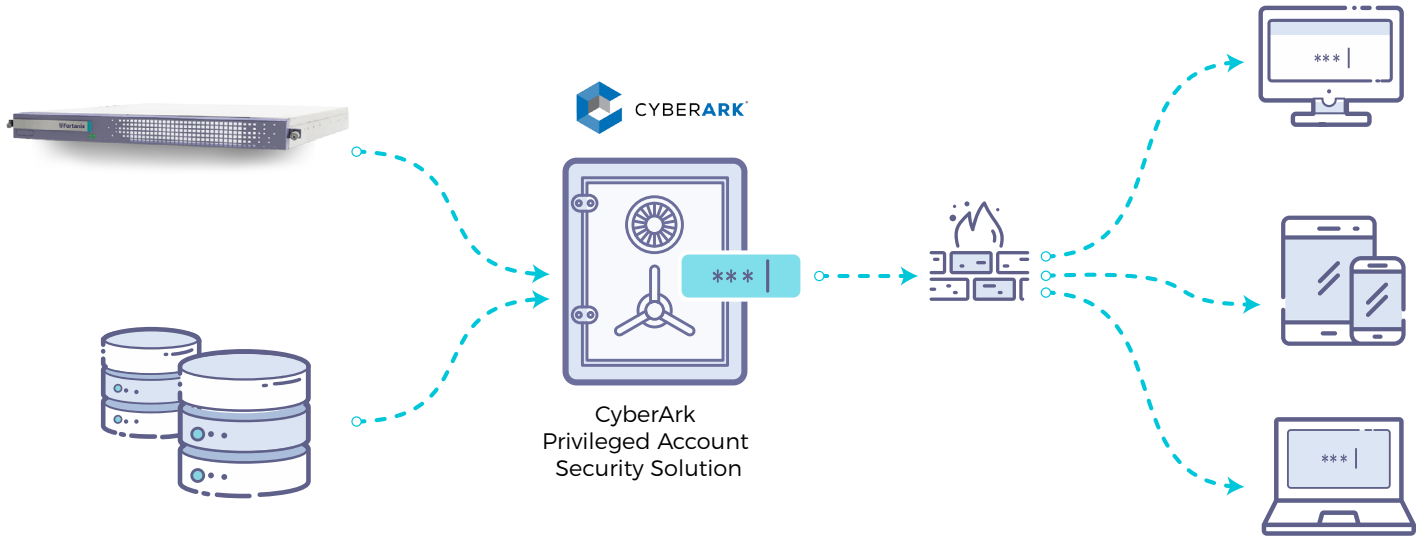
Table of Contents

1. Solution

CyberArk privilege account security solution integrates with Fortanix Data Security Manager to enhance the security and availability of encryption keys. The document contains the necessary information to deploy Fortanix Data Security Manager with the CyberArk Enterprise Password Vault (EPV®) solution.

CyberArk Privileged Account Security Solution is an enterprise class, unified platform that allows organizations to manage and secure all privileged accounts. The solution secures credentials, including passwords and SSH keys, controls access to these accounts, and isolates and records privileged sessions that may assist with auditing and forensics analysis. Fortanix Data Security Manager delivers unified HSM and Key Management capabilities to securely generate, store, and use cryptographic keys and certificates.

The combined solution of Fortanix Data Security Manager and CyberArk Enterprise Password Vault, delivers enhanced security and availability for encryption keys used to access safes or files within the CyberArk solution to ensure confidentiality, integrity, and availability of critical enterprise data. Fortanix Data Security Manager leverages Runtime Encryption™ and Intel® SGX in a FIPS compliant HSM to deliver deterministic security for encryption keys. The joint solution maximizes the security of encryption keys used to protect enterprise credentials and passwords to help guard against threats exploiting insider privileges.



2. Prerequisites

For new deployments, please review the Fortanix Data Security Manager installation guide for pre-requisites and deployment procedures. Once complete you can review the instructions for getting started: https://support.fortanix.com/hc/en-us/articles/360015809372-Getting-Started-with-DSM

3. Fortanix Data Security Manager Configuration for Cyber-

3.1 Sign up for Fortanix Data Security Manager

Your Fortanix Data Security Manager installation should now be accessible from the browser at `https://dsm.<your-domain.com>`.
Sign up as a user on this site.

3.2 Create an account

Use your credentials to login to Fortanix Data Security Manager. Here you can create a new account or accept an invitation to join another account. After entering an account, you can view and manage groups, users, applications, and security objects belonging to the account.

If you have a newly-created account, use the following steps to add your first group and application to Fortanix Data Security Manager .

3.3 Add a group

A group is a collection of security objects created by and accessible by users and applications which belong to the group. The user who creates a group automatically gets assigned the role of the group administrator. You can add more users to the group in the role of administrators or auditors. You can also add applications to the group to enable the applications to create and use security objects in that group.

To add a group, you may specify:
- The title of the group (required).
- A short description for the group (required).
- Users in your account as members.
- Applications in your account to add to the group so that they can use the security objects in the group.

3.4 Add an application corresponding to EPV

An application can use Fortanix Data Security Manager to generate, store, and use security objects, such as cryptographic keys, certificates, or an arbitrary secret. Examples of applications include web servers, PKI servers, key vaults, etc. An application can interact with Fortanix Data Security Manager using the REST APIs or using the PKCS#11, JCE, or CNG providers.

EPV integrates with Fortanix Data Security Manager using the PKCS#11 interface.

To add an application, you may specify:
- Name of the application (required).
- A short description for the application.
- Choose API Key as the form of authentication.
- Select the group created in the previous step for this application.

3.5 Download Fortanix KMS Windows Client and configure it

The Fortanix Data Security Manager client for Windows 64-bit can be downloaded from https://support.fortanix.com/hc/en-us/articles/360018312391-PKCS-11. `FortanixKmsClient.msi` installs the Fortanix Data Security Manager PKCS#11 library.

The Fortanix Data Security Manager URL needs to be configured for the PKCS#11 DLL to communicate with. This is done by running the following command:

```
C:\Program Files\Fortanix\KmsClient\FortanixKmsClientConfig.
exe machine -api-endpoint https://dsm.<your-domain.com>
```

The PKCS#11 DLL gets installed in `C:\Program Files\Fortanix\KmsClient\FortanixKmsPkcs11.dll`. The path to this file needs to be configured in the CyberArk EPV software in the next steps.

4. CyberArk EPV configuration

The following steps describe the configuration that needs to be done at CyberArk EPV to use Fortanix Data Security Manager.

4.1 Network Connectivity

For network access, add the following line to your windows host file on `%SystemRoot%\System32\drivers\etc\hosts:`

```
<IP Address>  dsm.<your-domain>.com
```

Add the following line to the file `C:\Program Files (x86)\PrivateArk\Server\`**`dbparm.ini`**

```
AllowNonStandardFWAddresses=[<IP Address>],Yes,443:inbound/tcp,443:outbound/tcp
```

Restart the Vault using the PrivateArk Server.

*<IP Address> - IP-address of Fortanix Data Security Manager deployment

4.2 Configure path to PKCS#11 DLL

Browse and open the following file `C:\Program Files (x86)\PrivateArk\Server\dbparm.ini`

At the bottom of the file, add the following lines:

```
[HSM]
PKCS11ProviderPath="C:\Program Files\Fortanix\KmsClient\FortanixKmsPkcs11.dll"
```

Save the dbparm.ini file and close it.

4.3 Configure PKCS#11 PIN

Run the following command to configure the PIN for Fortanix Data Security Manager. The program CAVaultManager is located at

```
C:\Program Files (x86)\PrivateArk\Server.
CAVaultManager SecureSecretFiles /SecretType HSM /Secret <hsmpincode>
```

The "hsmpincode" corresponds to the API key for the application generated in Section 4.4. CyberArk restricts the length of the "hsmpincode" to 50 characters, so using the API Key as the parameter for "/Secret" throws an error. The workaround for this is to create a file "C:\tmp\apikey.txt" with the contents:

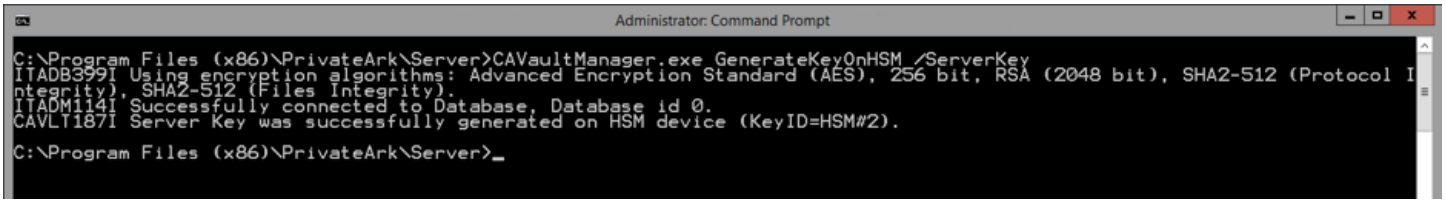
```
api_key = "FEL/ME…j+bt7"
```

Then, use `file://C:\tmp\apikey.txt` as the "hsmpincode". Open dbparm.ini to verify that HSMPinCode parameter was added with the encrypted value of the PIN.

4.4 Generate a new key in Fortanix Data Security Man-

The following instructions assume the CyberArk Vault is already hardened.

1. Stop the vault.
2. Generate a new Operator Key in the Fortanix HSM:
   - `CAVaultManger GenerateKeyOnHSM /ServerKey`



   - Record the HSM slot number returned by the command (**HSM#2** in the example)

3. Verify that the new key has been generated in Fortanix Data Security Manager. To do this, login to the web interface of Fortanix Data Security Manager using your user credentials, and go to the groups tab. Click on the group created in Section 4.3 to see a detailed view of objects in the group. Go to the security objects tab for the group, and find the new security object created by CyberArk EPV. Click on the security object to see the detailed view for the security object. On the bottom right, there should be an audit log stating that the key was created by the CyberArk EPV application at a specified time.

4.5 Re-encrypt Vault

4. Make sure the master key is in the CD, then use the ChangeServerKeys command to re-encrypt the vault with the new key:

```
ChangeServerKeys C:\DemoOperatorKeys\
C:\DemoOperatorKeys\VaultEmergency.pass HSM#2
```

If successfully executed, the vault is now encrypted with the new key that was generated in the HSM. Modify the the ServerKey in the DBPARM.INI:

```
ServerKey=HSM#2
```

5. Start the Vault service using the PrivateArk Server.