Vormetric transparent encryption
Deployment Guide for CyberArk Vault

This guide describes the deployment of Vormetric Transparent Encryption with CyberArk Vault. As a partner in the Alliance for Solutions and Applications Provider (ASAP) program, CyberArk proactively stops advanced cyber threats that exploit insider privileges. To protect the heart of the enterprise, CyberArk targeted security solutions protects against cyber threats before attacks can escalate and do irreparable business damage. The deployment of Vormetric Transparent Encryption with CyberArk Vault ensures confidentiality, integrity, and availability of critical enterprise data.

Deployment overview
The components necessary for protecting the CyberArk Vault are a Data Security Manager (DSM) cluster with a minimal node configuration of two nodes, and a Vormetric Transparent Encryption agent deployed at the Windows Server running the CyberArk Vault.

At a high-level, the deployment and configuration of the CyberArk-Thales solution involves the following steps:

- Install and configure DSM cluster.
- Install and configure the Vormetric Transparent Encryption agent on the Windows Server intended to run CyberArk Vault.
- Install, configure, and harden the CyberArk Vault.
- Make a single, post-installation change to the CyberArk Vault DBPARM.INI file to allow specific and secure communication to the DSM.
Deployment steps

Following the deployment and installation steps described below will ensure a working CyberArk-Thales high security solution.

Install and configure the dsm cluster

To install and configure a DSM Cluster, follow the instructions provided in the Thales support site from the following guides:

- DSM Installation and Configuration Guide
- DSM Administrators Guide

Make sure you select the guides that match your version of the DSM. The CyberArk-Thales solution should work with any version of DSM v5.3 or above.

Install and configure Vormetric transparent encryption agent

To install and configure the Vormetric Transparent Encryption agent, follow the instructions provided in the Thales support site from the following guides:

- VTE Agent Install and Configuration Guide

Make sure you select the guide that matches your version of the Vormetric Transparent Encryption agent. The CyberArk-Thales solution should work with any version of Vormetric Transparent Encryption agent v5.3 or above.

Installation of the Vormetric Transparent Encryption agent will require a reboot of the Windows Server. Once the server is rebooted, the server will be in a ready state for the CyberArk Vault installation. No other changes are necessary.

Install, configure, and harden Cyberark vault

To install, configure and harden CyberArk Vault, follow the installation instructions provided by CyberArk. No other considerations are required to install and configure CyberArk Vault. The Vormetric Transparent Encryption agent on the Windows Server is passive and does not interfere with normal CyberArk Vault installation.

Post-installation steps

After both the Thales solution and the CyberArk Vault are installed, a post-installation step is required to allow specific and secure network access to the DSM.

- Stop the CyberArk Vault. See CyberArk documentation for stopping and starting the CyberArk Vault.
- Edit the DBPARM.INI file at this location with a standard text editor such as Notepad or TextPad:
  C:\Program Files (x86)\PrivateArk\Server\DBPARM.INI

- Under the [MAIN] section of the INI file, add the following lines exactly as follows for each DSM in the Thales DSM cluster:
  AllowNonStandardFWAddresses=[<DSM IP Address>],Yes,8443-8447:outbound/tcp,7024/inbound/tcp
  AllowNonStandardFWAddresses=[<DSM IP Address>],Yes,8080:outbound/tcp

  Where <DSM IP Address> is the numeric IP address of each DSM cluster member. If the DSM IP addresses are for example 10.0.0.2 and 10.0.0.3, then add the following four lines:
  AllowNonStandardFWAddresses=[10.0.0.2],Yes,8443-8447:outbound/tcp,7024/inbound/tcp
  AllowNonStandardFWAddresses=[10.0.0.2],Yes,8080:outbound/tcp
  AllowNonStandardFWAddresses=[10.0.0.3],Yes,8443-8447:outbound/tcp,7024/inbound/tcp
  AllowNonStandardFWAddresses=[10.0.0.3],Yes,8080:outbound/tcp

- Start the CyberArk Vault. See CyberArk documentation for stopping and starting the CyberArk Vault.
- Deployment is complete.

> thalesgroup.com <