CYBERARK PRIVILEGED ACCESS SECURITY AND VORMETRIC TRANSPARENT ENCRYPTION FROM THALES

Highlights

- Harden all CyberArk components and ensure that data security considerations are being robustly managed

- Limit access to binaries, files and users

- Protect Operator Keys, component and vault configuration files

Storing, managing and securing operator keys, data encryption keys, data access policies, administrative domains and administrator profiles can help to ensure continuous protection for the most critical digital assets in an organization's infrastructure. By integrating Vormetric Transparent Encryption (VTE) from Thales with the CyberArk Core Privileged Access Security Solution, customers obtain an additional level of security, hardening all CyberArk components. The combined solution also addresses the frequently arduous task of convincing auditors that data security considerations are being satisfactorily managed.

The Solution and its Benefits

VTE consists of a Data Security Manager (DSM) hardware appliance as the central management component, and at least one VTE agent residing on the protected vault host. The joint solution is based on the Vormetric Data Security Platform with the DSM serving as a fireproof vaulting location for both the Master Key files and Native Vault Administrator password. Using the Vormetric DSM function of vaulting unmatched keys without validation, it provides secure Data-at-Rest protection and access controls. Organizations are able to provide a highly secured, enterprise level Master key files and Master user password management mechanism and processes with the same amount of simplicity as defining a basic set of firewall policies. Additional applications of the VTE hardening CyberArk's Core Privileged Access Security Solution include:

- Enterprises can opt to protect Operator Keys on the vault hard drive instead of a dedicated HSM. This prevents any tampering, deleting, copying, etc., and extends the Thales Vormetric DSM protection to the Operator keys on-premises of the Vault OS.

  - Dbparm.exe is the only entity that can access the Operator keys in typical business operations, and if a re-key is required, a pre-determined process of adjusting the policy to support the rekey tools can be temporarily introduced and synched to the VTE agent by temporarily opening the required VTE ports.

  - Should the DSM go down, and/or the VTE agent is removed for any reason, the encryption and protection policies stay in place, under client choice of encryption algorithm.

- Protect component and vault configuration files from unauthorized changes. As the VTE protects at the Folder level, binaries and executables can be protected with thorough testing.

- Master Key Management processes provide full separation of duties and allow distributed and global support teams a way to implement a Disaster Recovery process in the event of an outage in a simple, easy-to-follow, highly-secured way.

- The DSM CLI (VMSSC) wrapper script files open a remote DSM TCP port automatically only when it runs ("add or extract key") and at the end of every run, it deletes the temporary remote port.

Partner Products

- Thales Vormetric Transparent Encryption (VTE)

CyberArk Products:

- The CyberArk Privileged Access Security Solution
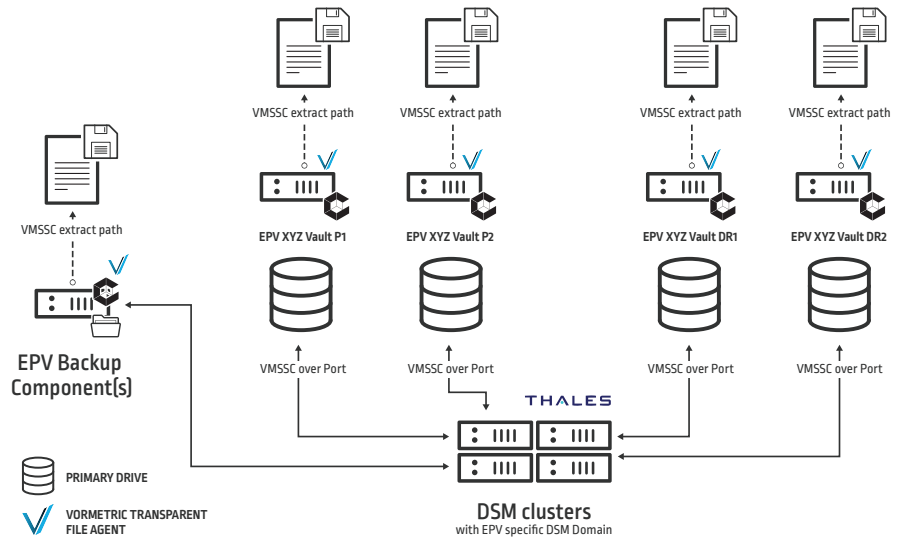
Architecture Diagram for Master Data Management Solution

Customer Example and Overview

This solution has been designed, developed, and deployed, by SEGMENTECH in collaboration with CyberArk and Thales, across 8 production environments at a major financial CyberArk customer. The DSM CLI (VMSSC) wrapper batch files open a remote DSM TCP port automatically only when it runs (add key or extract key) at the end of every run, it deletes the temporary remote port. At any given time, the vault OS firewall is operating under the hardened firewall setting with no custom ports open.

About CyberArk

CyberArk is the global leader in privileged access management, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan. For more information, visit www.cyberark.com.

About Thales

Thales is a leader in advanced data security solutions and services delivering trust wherever information is created, shared, or stored. Thales protects critical data on-premises, in the cloud, and in virtual environments, to support digital transformation strategies without sacrificing business agility. Security professionals rely on Thales to confidently accelerate their organization's digital transformation.

About SEGMENTECH

SEGMENTECH is an IT Security Services consultancy focusing on the design, implementation and operations automation of secure IT solutions and systems. SEGMENTECH operates as a strategic professional services partner of CyberArk. SEGMENTECH specializes in identifying and leveraging upstream/downstream/custom solutions around the CyberArk Privileged Access Security components to improve CyberArk clients' stance with audit and control challenges. For more information, visit www.segmentech.com