securosys

Solution Brief

Enhancing CyberArk Privileged Access Manager With Securosys HSM

Privileged Access Management (PAM) is essential for protecting organizations against cyber threats targeting administrative and high-value accounts. CyberArk Privileged Access Manager (PAM) is widely adopted to secure privileged credentials, enforce access controls, and monitor administrative activity.

Securosys further strengthens this security by integrating on-premises Hardware Security Modules (HSMs) or CloudHSM into the CyberArk architecture. By placing CyberArk's critical server keys inside Securosys' FIPS 140 Level 3 and Common Criteria EAL4+ certified HSMs, organizations achieve the highest level of protection for sensitive credentials.

Challenge

CyberArk's Digital Vault relies on a multilayered encryption hierarchy to safeguard privileged-account credentials, policies, and audit data. However, if the server key used to start the Digital Vault is stored on the application server itself, attackers who compromise that system may gain access to the vault's contents.

Securosys eliminates this risk by securely generating, storing, and managing these critical encryption keys entirely within tamper-resistant hardware.

Solution Benefits

Stronger Security: Securosys ensures that keys never leave the HSM, provides full tamper protection, and uses dual high-entropy hardware with True Random Number Generators (TRNG)

Regulatory Compliance: Securosys meets strict regulatory standards including FIPS 140-2/3 Level 3, Common Criteria EAL4+, and ISO 27001 certification for CloudHSM.

Seamless Integration: Integration is achieved through a native PKCS#11 provider, with easy setup and configuration, and a scalable, partitionable architecture suitable for multiple applications.

Flexible Deployment: Multiple deployment options, including hardware and virtual appliances, with support for on-premises environments or CloudHSM.

High Availability: Automatically synchronized HSM clusters enable continuous operation, with geo-redundant deployments

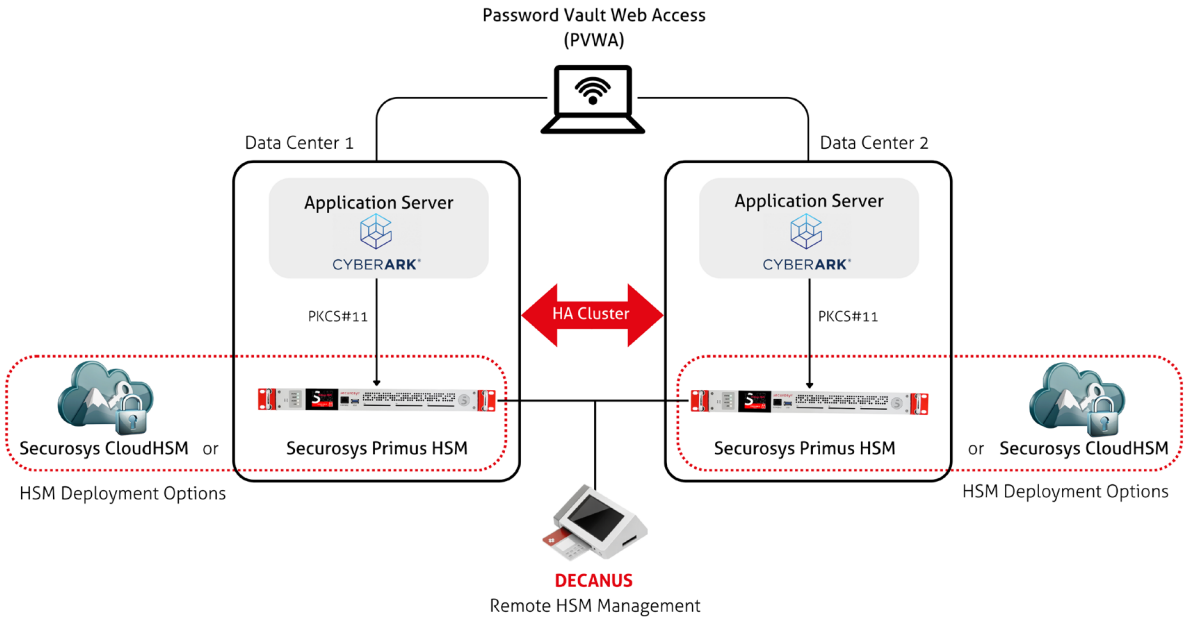
Get started

securosys

Solution Integration

Integrating Securosys Primus HSM or CloudHSM with CyberArk Privileged Access Manager enhances the security of the CyberArk Digital Vault by generating and storing the server key inside a tamper-resistant hardware security module. Instead of residing on the CyberArk server, the key is created within the HSM using high-entropy hardware randomness and accessed exclusively through secure PKCS#11 operations. This ensures that all cryptographic actions remain within the protected hardware boundary and significantly reduces the risk of key compromise.

During both startup and normal operation, CyberArk connects to the Securosys HSM to perform the cryptographic services required to initialize and run the Digital Vault. The HSM provides tightly controlled access to the server key, supporting CyberArk's multi-layer encryption model without ever exposing sensitive key material in software memory. Securosys enables flexible deployment through on-premises Primus HSMs or globally distributed CloudHSM clusters. Once the PKCS#11 provider is configured, CyberArk relies on the HSM for secure vault initialization, strong key protection, and high-availability access across data centers and cloud environments.



Use Cases

Protecting Digital Vault Server Keys Against Insider Threats and Advanced Attacks

By generating the CyberArk server key inside the HSM using high-entropy TRNG and never allowing it to leave the secure boundary, organizations prevent rogue administrators, compromised servers, or malware from extracting the keys that unlock the CyberArk Digital Vault.

Accelerating Cryptographic Operations in Large-Scale PAM Environments

Enterprises with thousands of privileged accounts can leverage Securosys hardware acceleration (up to 4000 RSA-2048 operations per second) to support rapid credential rotations, high-volume vault operations, and strong encryption without performance degradation.

Enforcing Hardware Root of Trust for Privileged Operations

By placing all encryption keys in Securosys HSMs, organizations establish a hardware root of trust for CyberArk functions, securing credential storage, policy enforcement, session isolation, and audit data integrity.

About CyberArk

About Securosys

CYBERARK®