

Primus HSM & CloudHSM solution brief

Securing CyberArk Privileged Access Manager using Securosys CloudHSM or Primus HSM

Introduction

Privileged Access Management (PAM) solutions protect organizations from cyber threats by monitoring, detecting and preventing unauthorized access to critical resources by users with elevated capabilities, such as admins or root.

Integrating CyberArk Privileged Access Manager with Securosys Primus HSM or CloudHSM enhances security by securing user passwords with FIPS 140 Level 3 and Common Criteria EAL4+ certified hardware-protected encryption keys.

Storing secrets

To accomplish the tasks of a privileged account security solution, any PAM system stores the passwords or keys that unlock access to sensitive data, mission-critical applications, and operational systems. As such, it is crucial that privileged account management software is purposefully designed and the infrastructure upon which the software runs is hardened. And still, by storing the privileged-access manager server key on the application server, attackers may be able to gain access to the solution and all the sensitive privileged-account information stored inside. To avoid this risk, the keys that provide access to the account information must be protected by hardware.

PAM hardening with hardware-protected encryption keys

At the core of the CyberArk Privileged Access Manager Solution is the CyberArk Digital Vault, which contains a highly secure database that stores privileged-account credentials, access-control policies, credential management policies, and audit information. To protect both the Digital Vault database itself and the data stored within the database, CyberArk uses a multi-layered encryption hierarchy.

Each individual file and safe within the Digital Vault database is uniquely encrypted using a randomly generated encryption key. At the top of the key hierarchy, CyberArk utilizes a unique server key and a unique recovery key. The server key is required to start the Digital Vault, and in accordance with the CyberArk Digital Vault Security Standard, this encryption key should be stored within a hardware security module (HSM).

By integrating Securosys Primus HSM or CloudHSM into the CyberArk PAM architecture, the server key can be generated with true randomness (TRNG) inside the HSM, and it can be assured that this key will never leave the secure boundaries of the HSM. Additionally, Primus HSM can be set up in an automatic synchronizing high-availability (HA) cluster to meet any availability level, including geo-redundancy.

Regulatory requirements of various industries, including finance, healthcare, and government, are met by the FIPS 140 Level-3 and Common Criteria EAL4+ certified, high-performance, and tamper resistant Securosys HSM solutions.

Benefits

Increased Security

- Keys are never exposed outside the HSM
- Tamper protection during transport, storage and operation
- Two high entropy hardware true random number generators
- Highest availability
- Designed, developed and manufactured in Switzerland

Compliance

- FIPS 140 Level 3
- Common Criteria EAL4+
- ISO 27001 (CloudHSM)

Simple Integration

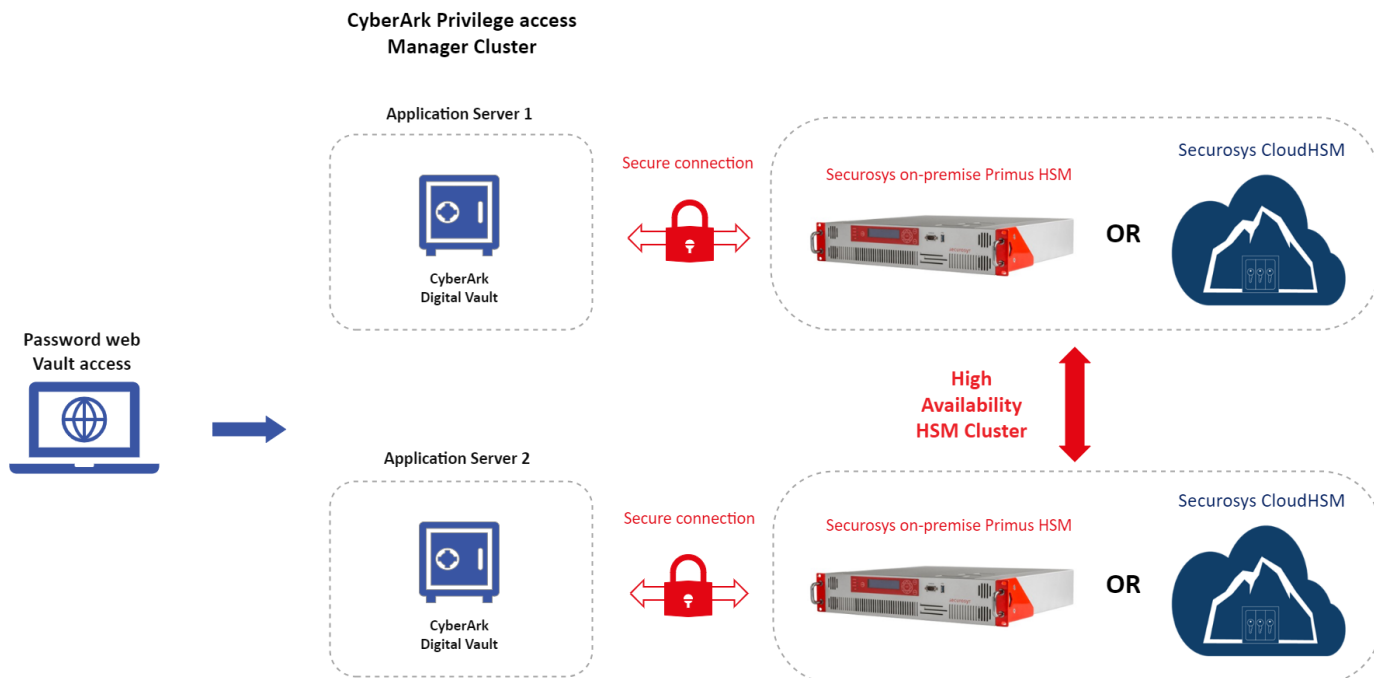
- Via PKCS#11 Provider
- Simple setup, configuration and maintenance
- Scalable and flexibly partitionable to support additional use cases

Application Performance

- Hardware accelerated digital signing, up to 4000 RSA 2048-bit signings per second
- Manage larger key sizes without severe performance penalty

Integration Overview

CyberArk Privileged Access Manager connects to the Securosys HSMs via PKCS#11 API. The solution is quick and easy to integrate. Securosys PKCS#11 provider needs to be installed and configured on the application server communicating with the Securosys HSMs. The CyberArk server key can be either generated directly on the HSM or imported from a different source to the HSM.



The Securosys Hardware Security Module is available as on-premise solution (Primus HSM) or as cloud service (CloudHSM). CloudHSM minimizes customer's time for evaluation, setup, operation, redundancy, and maintenance of the HSM infrastructure. Moreover, it is scalable according to customer needs. By combining different regions into a single world-wide cluster, the redundant cluster architecture fits perfectly into CyberArk's Vaulting Technology®.

About CyberArk Solution

CyberArk Privileged Access Manager Self-Hosted is a full lifecycle solution for managing the most privileged accounts and SSH keys in the enterprise. It enables organizations to secure, provision, manage as well as control and monitor all activities associated with different types of privileged identities, such as:

- Administrator on a Windows server,
- Root on a UNIX server,
- Embedded passwords found in applications and scripts.

About Securosys HSM Solutions

- Scalable and flexible solution
 - X-Series (high performance)
 - E-Series (price-performance)
 - CloudHSM (HSM as a service)
- Secure Remote Control with Decanus
- Multi-tenancy, up to 120 partitions, each 240MB
- Strict authentication, 4-eyes principle, 2-factor authentication
- Clustering, secure "real-time" synchronization across data centers
- Constant tamper protection
- Designed, developed, and manufactured in Switzerland