CYBERARK®
The Identity Security Company™

PAM Administration

Vault Security

Agenda

In this session, we will look at:

1. Vault security controls
2. Vault Encryption and Key Management

Vault Security Controls

The Vault: An Island of Security

Isolating the Server

- No domain membership or trusts
- No DNS or WINS
  - Uses a manually configured Host file

Hardening the Server

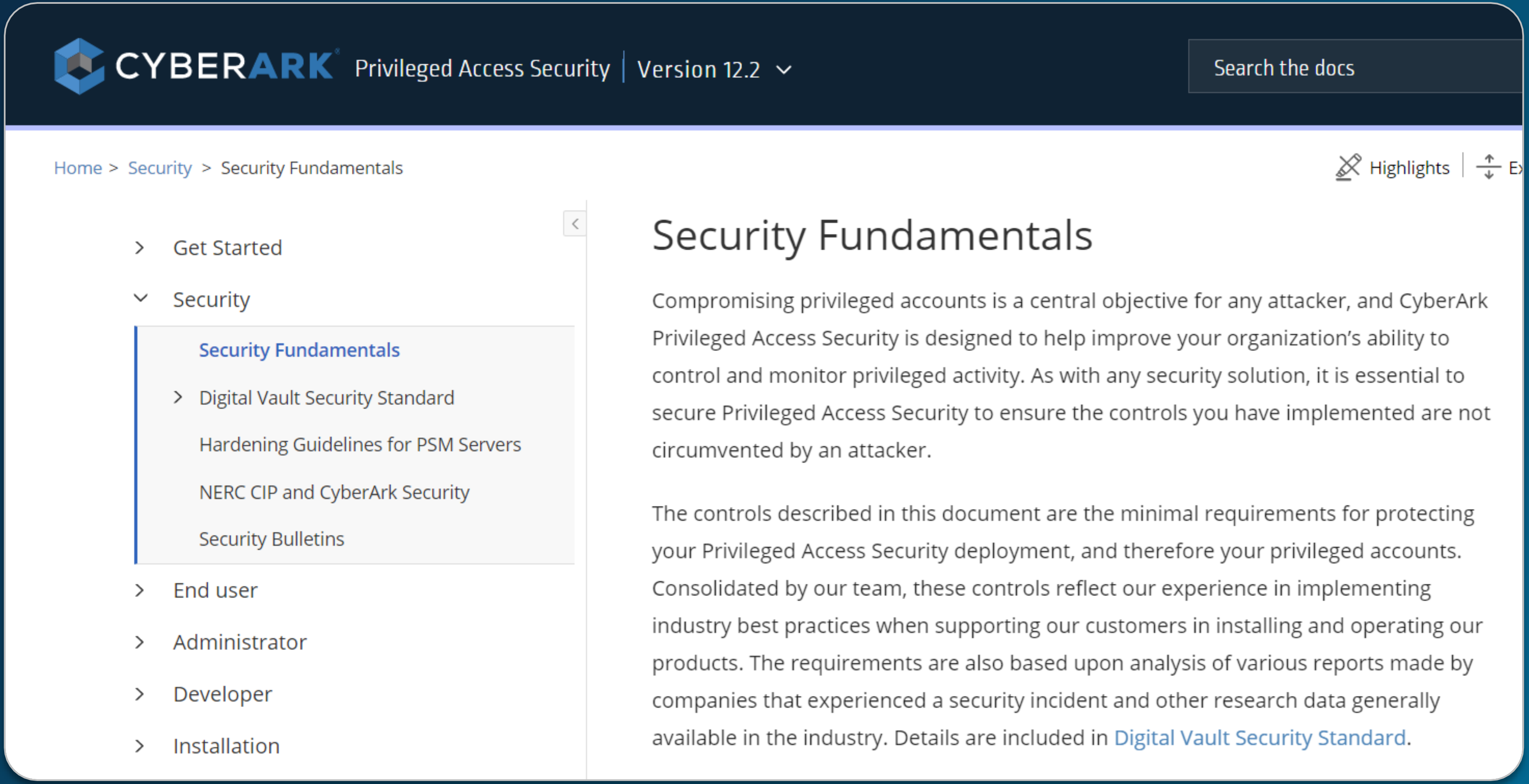
- Remove unnecessary services
- Secure configuration for remaining services
- Only Vault Server and PrivateArk Client are installed
- No additional applications

Documentation Resources

There are several documents that are key to successfully protecting your implementation

They include:

- Security Fundamentals
- Digital Vault Security Standard


CYBERARK
Privileged Access Security
Version 12.2
Search the docs
Home > Security > Security Fundamentals
Highlights
Ex
Get Started
Security
Security Fundamentals
Digital Vault Security Standard
Hardening Guidelines for PSM Servers
NERC CIP and CyberArk Security
Security Bulletins
End user
Administrator
Developer
Installation

Security Fundamentals

Compromising privileged accounts is a central objective for any attacker, and CyberArk Privileged Access Security is designed to help improve your organization's ability to control and monitor privileged activity. As with any security solution, it is essential to secure Privileged Access Security to ensure the controls you have implemented are not circumvented by an attacker.

The controls described in this document are the minimal requirements for protecting your Privileged Access Security deployment, and therefore your privileged accounts. Consolidated by our team, these controls reflect our experience in implementing industry best practices when supporting our customers in installing and operating our products. The requirements are also based upon analysis of various reports made by companies that experienced a security incident and other research data generally available in the industry. Details are included in Digital Vault Security Standard.

Security Fundamentals

Details eight controls to protect your CyberArk deployment and, therefore, your privileged accounts

1. Isolate and Harden the Digital Vault Server
2. Use Two-Factor Authentication
3. Restrict Access to Component Servers
4. Limit Privileges and Points of Administration
5. Protect Sensitive Accounts and Encryption Keys
6. Use Secure Protocols
7. Monitor Logs for Irregularities
8. Create and Periodically Test a CyberArk Disaster Recovery Plan

CyberArk Digital Vault Security Standards

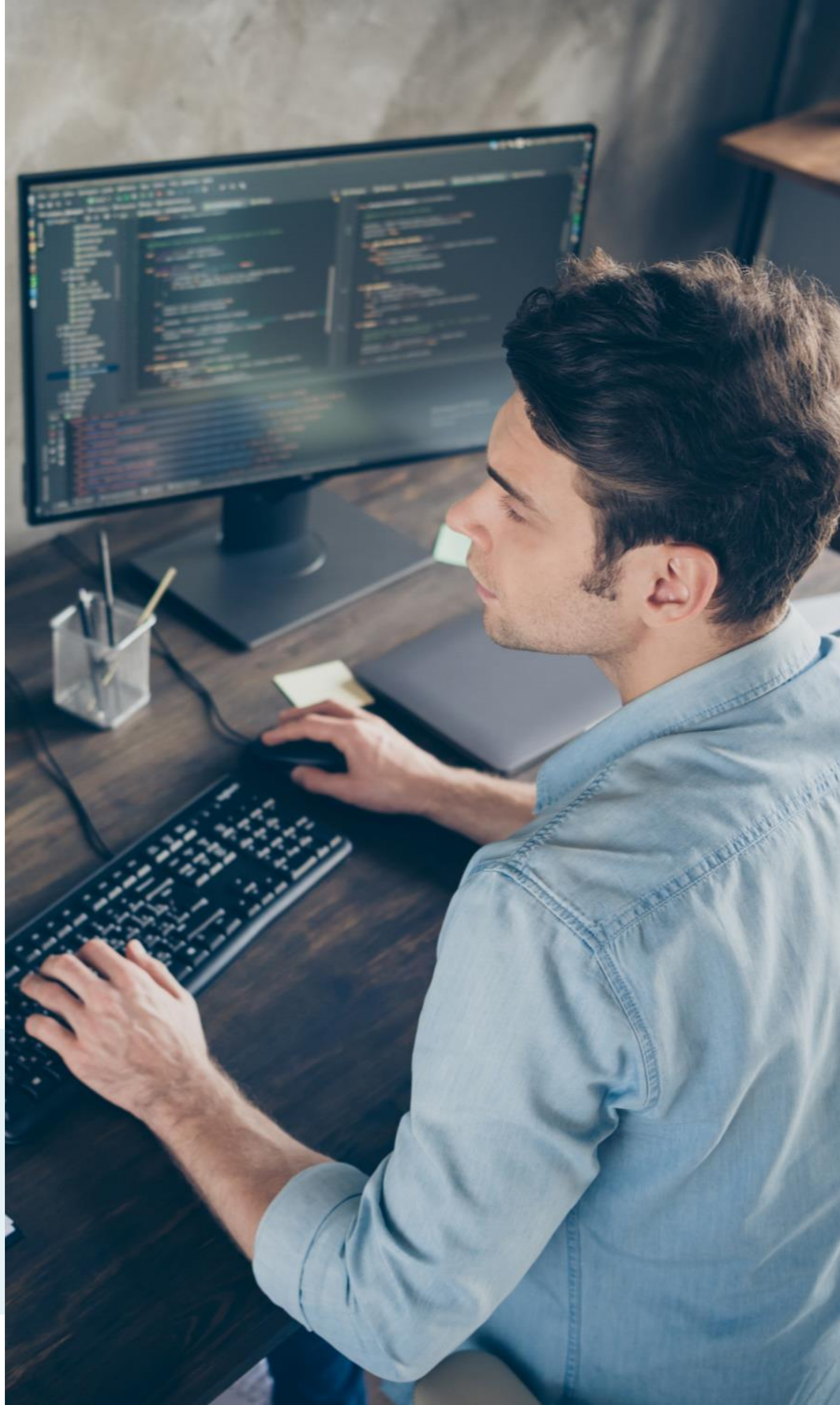
Securing your CyberArk implementation is CRITICAL!

The ***CyberArk Digital Vault Security Standard*** describes how to securely configure and maintain the digital vault. It details:

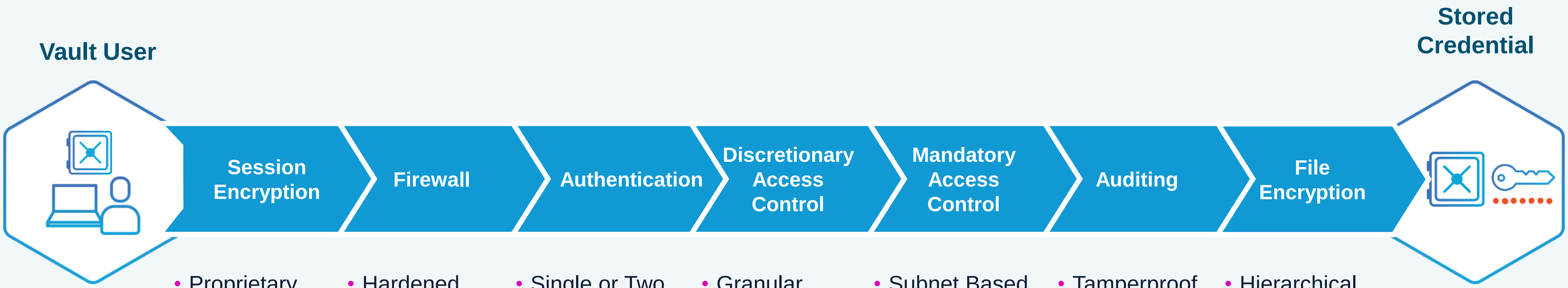
1. The Vault Security Layers
2. The Digital Vault Secure Platform and Enterprise Management Tools, including:
   - Backup/HA/DR
   - Monitoring the Vault
   - Remote Administration
   - External Storage
   - Virtualization of the Vault
   - Vault domain membership
   - Anti-virus

In almost all cases, installing third-party applications, virtualization, and external storage result in a relaxation of security.

All customers and partners should carefully read the Secure Platform document.



The Vault: End-to-End Security



Vault User

Session Encryption

Firewall

Authentication

Discretionary Access Control

Mandatory Access Control

Auditing

File Encryption

Stored Credential

Session Encryption

- Proprietary Protocol
- OpenSSL Encryption

Firewall

- Hardened built-in Windows Firewall

Authentication

- Single or Two Factor Authentication (recommended)

Discretionary Access Control

- Granular Permissions
- Role Based Access Control

Mandatory Access Control

- Subnet Based Access Control
- Time Limits and Delays

Auditing

- Tamperproof Audit Trail
- Event-based Alerts

File Encryption

- Hierarchical Encryption Model
- Every object has unique key

Vault Encryption and Key Management

Encryption Keys

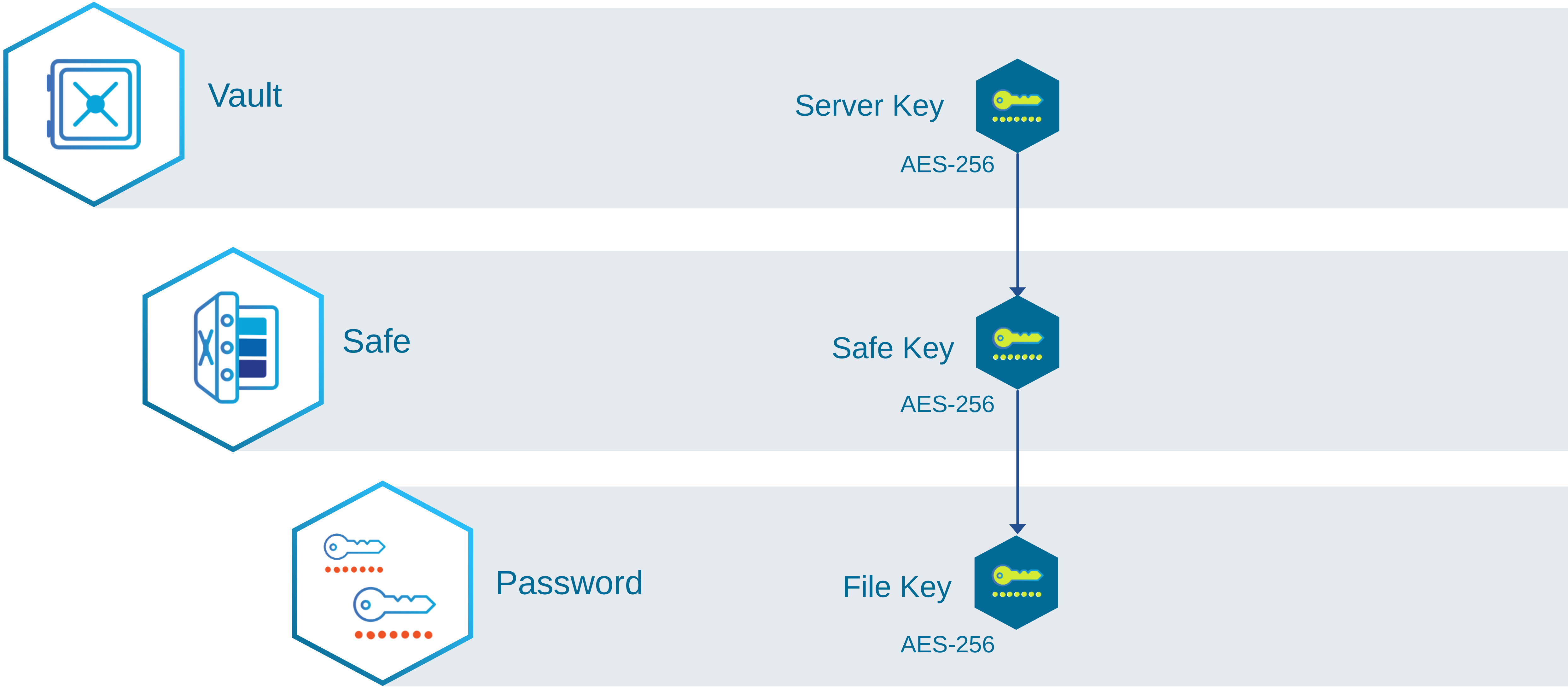
There are three files that form the cornerstone of the CyberArk PAM solution encryption methodology. These encryption key files are required to install and operate CyberArk PAM.

They are:

- **Server Key**
- **Recovery Public Key**
- **Recovery Private Key**

Let’s have a look at how these keys are used to protect the keys to your kingdom.

Vault Object Encryption – Day-to-Day Operations



Vault

Server Key

AES-256

Safe

Safe Key

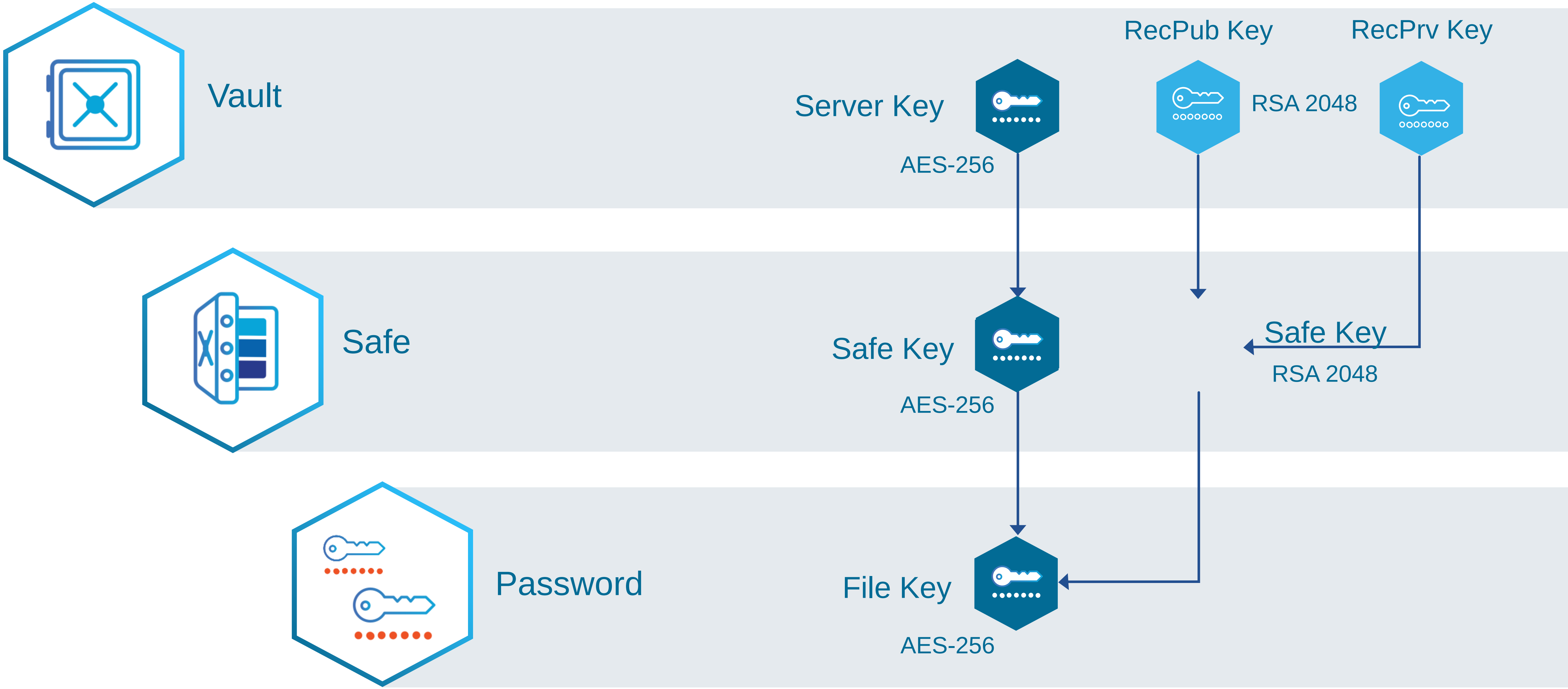
AES-256

Password

File Key

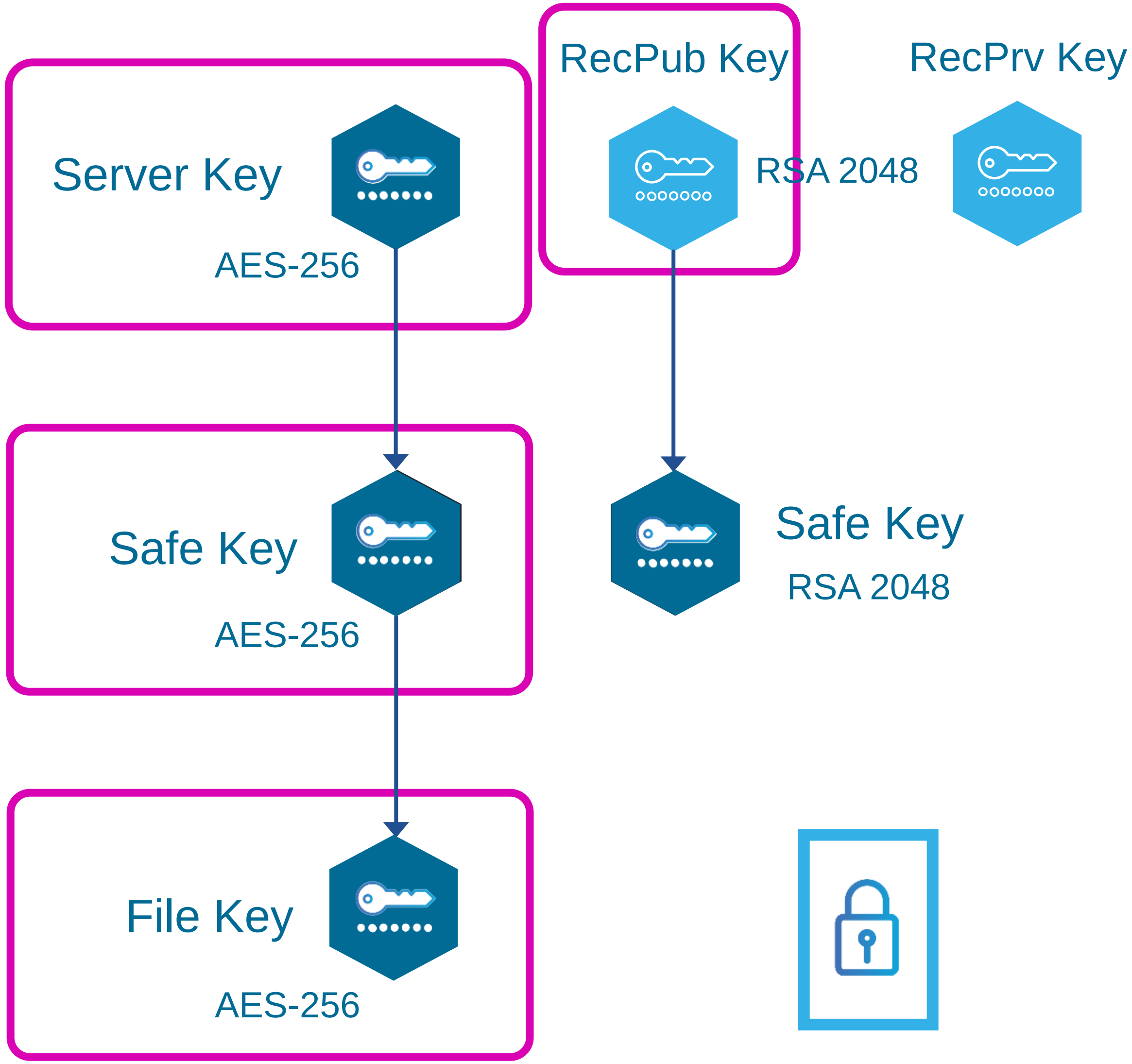
AES-256

Vault Object Encryption – Emergency Measures



File Encryption Process

- Each Credential is stored as an encrypted file on the Vault
  - The **File key** is a unique symmetric key generated for each file
  - The File Key is then encrypted with the **Safe key**, which is a symmetric key unique to the Safe
  - The Safe key is then encrypted with the symmetric **Server key**, which is unique to the Vault
- **Server Key**
  - The Server Key is loaded into memory when the Vault starts
- **RecPub Key**
  - A copy of the relevant Safe Key is encrypted with the RecPub Key and stored with the Safe



How Encryption Keys are Distributed

- Previously, the encryption keys required to install and operate the CyberArk PAM solution were physically delivered in the form of CDs containing the files.
- As of March 2022, CyberArk now delivers these encryption key files via a secure email service.
- You can go to the link below for more information on key delivery.

https://cyberark-customers.force.com/s/article/Digitized-Encryption-Keys-Delivery-End-User-Guide

Recovery Private Key Storage Strategies

The **Recovery Private Key*** must be copied to physical media and stored in at least two separate and secure locations:

One on the **Primary** site
and one on the **Disaster Recovery** site.

***** AKA the “Master Key”***

Server Key Storage Strategies

Strong

- Copy the key to external medium (USB drive, CD-ROM) and store it in a physical safe.
- Insert the medium whenever starting/restarting the Vault.
- Key in RAM

Convenient

- Copy the key to direct attached storage of the Vault server(s) and secure with NTFS permissions or by encrypting the key with a 3rd-party tool.
- Always available.
- Key in RAM

Strong & Convenient

- Store the Server key in a Hardware Security Module (HSM).
- Always available.
- Key NOT in RAM

Summary

Summary

In this session we discussed:

- The security controls protecting the Vault and encryption keys
- The encryption mechanisms protecting Vault data

CYBERARK®