Security Considerations for the Vault Installation on a VM Platform

Best Practices

Documentation Information

Document No.	CAUSPS0009
Document Type	Best Practices
Classification	CyberArk Restricted
Intended Audience	CyberArk Employees and PIM Customers
Author	Dmitriy Sokolovskiy, Director of Implementation Services
Date Authored	February 5, 2014
Abstract	This document describes security considerations for implementations where the Vault server is being installed on the VM

Revision History

Revision Number	Author	Revision Summary
201402-01	D. Sokolovskiy	First Draft
201402-02	D. Sokolovskiy	Second Draft
201402-03	G. Lansing	Third Draft

Definitions

This document describes the various security considerations that the customer should be aware of when making a decision to install the Vault on a virtual platform.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

CyberArk recognizes the global trend of increasing investment in virtual infrastructure and fully supports installing the Digital Vault software on a virtual server. However, installing the Digital Vault in a virtual environment introduces security risks not present when it is installed on dedicated hardware. These risks should be reviewed by the customer prior to making a decision to utilize a virtual server for the Digital Vault software.

Encryption Keys and Data

The Server Key is a symmetric key (AES-256) used by the Vault for business-as-usual encryption and decryption operations; it must be available to the Vault when it starts. It must never be stored on the same medium as the Digital Vault’s data. Storing the Server Key in this manner in a virtual environment increases the risk that an attacker may be able to obtain they key and the data remotely. It is highly recommended that the Server Key be stored (or generated) on a hardware security module (HSM). The HSM ensures that the key cannot be extracted, and performs the encryption and decryption tasks on behalf of the application. In the absence of an HSM, the Server Key may be stored on a separate physical disk from the Vault Data. Limit access to the key to the Digital Vault.

Remote Attack Vectors

A virtual environment implementation provides a remote attack vector, bypassing physical security layers normally present when physical hardware is utilized in a secure data center environment. This may allow an attacker to obtain the whole guest image of the Digital Vault server, enabling following attacks:

- Simultaneous brute force password attacks, using multiple copies of the virtual machine, against existing Vault users. Because an attacker can create unlimited copies of the virtual machine, account lockout mechanisms can be bypassed
- Replacement of the image with a modified or corrupt image compromising the integrity and/or availability of the data
- Deletion of the image causing an outage and potential loss of data

Internal Attack Vectors

In addition to remote attack vectors, installation on a virtual server presents risks associated with the virtual host environment itself:

- Escape-to-Host and Guest-to-Guest attacks, due to vulnerabilities of virtual host operating system and software
- Virtual infrastructure and SAN administrators, intentionally or unintentionally compromising both data integrity and availability through the virtual host management console

Recommendations

Many of these attack vectors can be mitigated through the implementation of additional controls and an effective virtualization security program. Consult with the vendor of your virtual infrastructure for guidance on how to protect the sensitive Digital Vault server.