CyberArk Secure Platform

Table of Contents

Overview

CyberArk develops products for managing the enterprise's most sensitive information - the keys of the kingdom. As such, CyberArk is committed to providing "Enterprise-Ready" products with the highest levels of security which are appropriate for the sensitivity of the information that is managed in its products. To achieve this goal CyberArk introduces the "CyberArk Secure Platform".

CyberArk Secure Platform consists of several security layers for securing the machines on which CyberArk products are installed.

The CyberArk Secure Platform

In order to create the appropriate protection in the CyberArk components that manage the sensitive information, and to meet enterprise requirements, CyberArk introduces the CyberArk Secure Platform. The Secure Platform consists of set of security procedures, documentation guidelines, as well as software parts.

CyberArk Secure Platform enables customers to smoothly deploy CyberArk products into the enterprise infrastructure and enable enterprise requirements, such as backup, monitor, remote administration, patch management, and so forth.

Enterprises may apply their own security procedures in addition or instead of CyberArk Secure Platform. This document describes the security and support implications of deviations from the Secure Platform. Once the customer understands the implications of changing the Secure Platform but still wishes to change it, he can refer to CyberArk product documentation as well as to the CyberArk Professional Services team for guidance and support.

CyberArk develops and tests its products on the Secure Platform environment. Therefore, when customers choose to use their own procedures, there is a higher chance that unexpected issues may arise. CyberArk will do its best to assist customers with issues that are raised due to customers' changes in the Secure Platform.

CyberArk Digital Vault Server Secure Platform

The Digital Vault Server component is the core of the CyberArk Secure Platform. It is the secure repository of all sensitive information, and it is responsible for managing all access control to this information, maintaining and providing tamper-proof audit records, and so forth. As such, the security requirements for the server are very strict.

The Digital Vault Server consists of several security layers. It is possible to change the Vault Server security layers, but this should be done with caution and only when you fully understand the security and support implications. Since the Vault Server machine is protected by several security layers, it is almost immune against any known operating system attacks. The high level of security applied in the Secure Platform may change the deployment method for the Vault Server in the enterprise network.

CyberArk delivers tools for backup, monitor and remote control for the Vault Server machine, which provide a full manageability solution. Some enterprises may wish to use their own IT software to manage machines in their enterprise network. In such cases, CyberArk provides special procedures that allow these enterprises to loosen the Vault Server's security layers and enable them to manage the Vault Server using their own IT software.

CyberArk Digital Vault Server Security Layers

Dedicated Machine

CyberArk recommends installing the Vault Server host as a dedicated machine without additional 3rd party software, as it may introduce potential security breaches or require configurations to eliminate interoperability issues. CyberArk Secure Platform requires the Vault Server machine to be installed on a dedicated machine to minimize the risk of vulnerabilities raised by 3rd party software. Installing Vault Servers on a virtualized environment will be reviewed later in this document.

Hardened Operating System

CyberArk installs the Vault Server on a hardened operating system based on Microsoft Specialized Security Limited Functionality (SSLF) server[1] recommendations which define a highly secured Windows server. The hardening process, which is part of the product installation, results in disablement of many operating system services. The hardened Vault Server is designed to serve only CyberArk protocol requests. As such, it may not function as a regular domain member in a Windows network.

Encryption

In order to protect the data files that reside in the Vault, CyberArk employs AES-256 encryption (FIPS 140-2 compliant) with a unique encryption key for each object. The data encryption also protects the information against tampering.

This ensures that, even in case of physical access by an administrator to the Vault server, the critical data files will be protected and inaccessible.

Storing Encryption keys on HSM

The Vault encryption keys are organized in an encryption key hierarchy. The Server Key is a symmetric AES-256 encryption key in the top of this hierarchy.

An additional layer of protection for the Server Key may be required by customers. For this, CyberArk can store the Server Key on an Hardware Security Module (HSM) device, assuring that this critical key will be physically protected and will never leave the HSM.

1 More details can be found on Windows Server 2008 Security Guide - http://www.microsoft.com/downloads/en/details.aspx?FamilyID=fb8b981f-227c-4af6-a44b-b115696a80ac&displaylang=en

Firewall

CyberArk utilizes a hardened firewall on the Vault Server machine that verifies and permits only transmissions that are sent with the Vault protocol, while blocking all other traffic. This restrictive firewall policy dramatically reduces the attack surface that the Vault Server and the underlying operating system are exposed to. CyberArk provides documented methods that allow customers to troubleshoot and customize the firewall rules, for example, to enable access to 3rd party applications hosted on the Vault Server.

The Digital Vault Secure Platform and Enterprise Management Tools

The Digital Vault Server is an enterprise product that is installed on the corporate enterprise network. As such, the product needs to meet enterprise requirements. The Digital Vault Server is an isolated dedicated machine with several security layers, and in some cases, the strict security requirements of the Vault Server machine may make it difficult to use traditional enterprise management methods. In order to preserve the highest level of security that is required from the Vault Server and work seamlessly with the Vault Server security layers, CyberArk provides recommendations and tools to help deploy the Vault Server in the enterprise network.

The following section briefly describes the way CyberArk supports various enterprise requirements and scenarios that may require changes in the Secure Platform's policies:

- Backing up the Vault Server
- Monitoring the Vault Server
- Remote administration of the Vault Server
- High Availability and Disaster Recovery
- Storing Data on External Storage
- Installing the Vault Server on a virtual environment
- Installing Microsoft updates and patches
- Alternate hardening procedures
- Adding the Vault as a member of the domain
- Synchronizing the Vault Server clock
- Storing encryption keys on HSM

More information can be found in CyberArk product documentation.

Backing up the Vault Server

The Digital Vault Server stores sensitive and critical data that requires backup and recovery procedures. CyberArk provides the following methods to backup the Vault Server:

- **CyberArk backup solution:** CyberArk provides a set of backup and restore tools for secure backup of the Vault Server machine, while preserving the Digital Vault Server security layers. CyberArk backup tools are based on a secured replication of the Vault Server data into a backup machine. The machine with the encrypted replicated data can be backed-up using the regular enterprise backup software. CyberArk recommends that customers backup the Vault Server with this method.
- **Installing 3rd party backup software directly on the Vault Server:** For enterprises that wish to install their own backup software on the Vault Server. CyberArk will provide guidance regarding configuration of the Vault Server security layers for integration with common backup software. CyberArk does not recommend installing 3rd party backup tools on the Vault Server and believes that such tools should be used along with the CyberArk backup solution. It is important to be aware that installing 3rd party software on the Vault Server machine requires the Vault Server security layers to be loosened. Furthermore, any third party software installed on the Vault Server machine is a potential source of vulnerabilities.

Monitoring the Vault Server

As a critical component in the enterprise infrastructure, the Digital Vault Server may need to be monitored by the enterprise monitoring system. CyberArk provides the following methods to monitor the Digital Vault Server:

- **CyberArk monitoring solution:** CyberArk provides a comprehensive monitoring solution that is based on SNMP notifications that can be analyzed using the enterprise monitoring system. CyberArk provides notifications about the Vault Server machine status as well as application notifications. In addition to SNMP notifications, CyberArk provides a command line utility that utilizes the CyberArk protocol for remotely polling and querying for monitoring information from the Digital Vault Server. CyberArk recommends that customers monitor the Vault Server in these methods. For security event monitoring, CyberArk seamlessly integrates with leading SIEM vendors via real-time export of the audit records over Syslog protocol.
- **Installing 3rd party monitoring software:** Enterprises may need to install monitoring agents on the Vault Server machine (e.g. HP OpenView). CyberArk will provide guidance regarding configuration of the Vault Server security layers for integration with common monitoring software. It is important to be aware that installing 3rd party software on the Vault Server machine requires the Vault Server security layers to be loosened. Furthermore, any third party software installed on the Vault Server machine is a potential source of vulnerabilities.

Remote Administration of the Vault Server

Remote administration control is a mandatory requirement, as in many enterprises there is limited physical access to the Vault Server machine. CyberArk provides the following methods to remotely administer the Digital Vault Server:

- **CyberArk remote control solution:** CyberArk provides a secured remote control service that enables the enterprise to administrate the Vault Server through the network. All remote control operations are done through the Vault protocol while preserving the Secure Platform security layers. CyberArk recommends that customers administer the Vault Server remotely using this method.
- **Installing hardware-based remote administration:** CyberArk realizes that enterprises may want to install their own remote administration hardware solution (e.g. HP-iLO, KVM). Hardware-based remote administration usually works seamlessly on the CyberArk Secure Platform. In cases that require the Vault Server security layers to be reconfigured, CyberArk will provide guidance as needed. It is important to be aware that physical security is one of the Digital Vault Server Secure Platform pillars. Allowing remote access to the machine through remote-administration tool breaks the physical security protection and weakens the Digital Vault Server security.
- **Installing software-based remote administration:** Enterprises may want to access the Vault Server machine remotely using a software-based remote administration tools (e.g. Microsoft RDP). CyberArk will provide guidance regarding configuration of the Vault Server security layers for integration with common remote administration solutions. It is important to be aware that physical security is one the Digital Vault Server Secure Platform pillars, and that allowing remote access to the machine through remote-administration tool bypasses the physical security protection and may weaken the Digital Vault Server's security.

High Availability and Disaster Recovery

High availability and disaster recovery are required by many enterprises. CyberArk's solutions are mostly deployed as mission-critical systems and, as such, are required to provide high availability and redundancy. CyberArk provides the following solutions for high availability and disaster recovery of the Vault Server:

- **CyberArk HA/DR solutions:** CyberArk provides solutions for full high-availability and disaster recovery of the Vault Server. The high-availability solution is based on Microsoft Server Cluster. CyberArk also provides a disaster recovery solution based on network replication. CyberArk recommends that customers use these methods for achieving high-availability and disaster-recovery for the Vault Server.
- **Installing 3rd party HA/DR solution:** For enterprises that wish to install their own HA/DR solution (e.g. VMotion, Hardware mirroring) for the Vault Server. CyberArk will provide guidance regarding configuration of the Vault Server security layers for integration with common HA/DR solutions. It is important to be aware that installing 3rd party software on the Vault Server machine requires the Vault Server security layers to be loosened. Furthermore, any third party software installed on the Vault Server machine is a potential source of vulnerabilities.

Vault Server Data on External Storage

Enterprises may want to leverage their SAN infrastructure and use it for the Vault Server storage. SAN storage for the Vault Server usually works seamlessly in the CyberArk Secure Platform. Installing the Vault Server storage on SAN compromises the Vault Server physical security which is one of the pillars of the Vault Server Secure Platform, as the Vault Server storage may be accessible to the SAN administrators. CyberArk recommends using dedicated and secured storage for the Vault Server data and allowing access to that storage only through the Vault Server machine.

Vault Server on a Virtualized Environment and Cloud

Customers may want to install the Vault Server on a virtualized environment. While installing the Vault Server on a virtual environment usually works seamlessly in the CyberArk Secure Platform, it also introduces risks that are not present in a standard Secure Platform configuration.

A virtual environment implementation provides a remote attack vector, both from outside of the virtual host environment and from other virtual guest images, bypassing physical datacenter security layers. This may allow an attacker to obtain the whole guest image of the Vault server, introducing risks that are not present in a normal Secure Platform configuration.

Following are the potential security risks associated with a Vault that is hosted on VM/Cloud and CyberArk's recommendations to mitigate these risks:

- An attacker can potentially initiate multiple simultaneous "brute force" password attacks against existing CyberArk users, using multiple copies of the virtual machine. Because an attacker can create unlimited copies of the virtual machine, account lockout mechanisms can be bypassed.
- An attacker's ability to reverse-engineer the encryption of the protected data is increased. To start the Vault application, the attacker must have access to the encryption keys and, because of this, standard implementation practices call for placement of the encryption key on the Digital Vault OS file system. In a secure physical environment, such as an enterprise datacenter, the risk of storing the keys on the file system is mitigated by physical security layers. However, if a an attacker takes possession of a virtual machine, he would have access to the operating system, encryption keys and encrypted data, making reverse-engineering on the encryption possible.

  Note that there are two mitigating controls available for this risk:

  - Utilizing a hardware security module (HSM) to securely store encryption keys off the Digital Vault OS file system.
  - Mounting of encryption keys manually every time they are required. This approach will prevent the DR Digital Vault instance from being available automatically during a disaster.

Running the Vault on AWS

In addition to the above mentioned risks and mitigations associated with a VM Vault, the following conditions are specific to AWS/Cloud environments and require consideration:

- Port 80 needs to be opened to specific AWS addresses.
- By default, the Vault hardening ensures that outbound access from the Vault is limited in time and is used only in cases where the Vault needs to access a 3rd party server for uses such as authentication or provisioning (e.g: LDAP / RADIUS / etc). This is in order to ensure that even if the Vault somehow becomes infiltrated by a malicious party, it would be as difficult as possible to exfiltrate any data from it to the outside world. Hence, while opening ports is required for the health of the AWS image, it introduces a potential security risk.

Vault Server and Anti Virus Software

The Vault Server is a dedicated machine with no 3rd party software installed on it and with connectivity to the network only via CyberArk protocol. In addition, all data files in the Vault are encrypted, so viruses cannot be introduced by uploading an infected file into the Vault. Therefore, CyberArk believes that installing Anti Virus software on the Vault Server machine is not required. Furthermore, Anti Virus software is intrusive and may impact the normal operation of the Vault Server. For customers that still require installation of Anti Virus software, CyberArk will provide guidance regarding configuration of the Vault Server security layers for installing the Anti Virus software. It is important to be aware that installing 3rd party software (including Anti Virus software) on the Vault Server machine requires the Vault Server security layers to be loosened. Furthermore, any third party software installed on the Vault Server machine is a potential source of vulnerabilities.

Note regarding PCI-DSS regulations:

PCI-DSS regulations state that "Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats".

The CyberArk Secure Platform and the Digital Vault Server Security Layers provide compensating controls that place the Digital Vault Server far outside of the "system commonly affected by malware" and, therefore, the Vault meets PCI-DSS requirements without the need to loosen its hardening and install anti-virus agents. These controls include:

- **Hardened Operating System –** During the installation, the underlying operating system is modified, based on Microsoft Bastion Host recommendations (Microsoft SSLF server recommendations).
- **Firewall –** During installation, a Firewall is installed on the Vault server which blocks all access to the Vault aside from the TCP1858 (Vault Protocol, used to communicate with the Vault itself; there is no direct access to the file system), TCP9022 (optional, used for CyberArk Limited Remote Control client with no access to the file system) and ICMP.
- **Data Encryption –** Data that is stored on the Vault server by the Vault application itself is encrypted at all times, so even if an infected file is uploaded to the Vault application by a malicious user or an administrator, it cannot be introduced onto the Vault server itself.

Vault Server and Microsoft Patch Installation

The Vault Server machine is installed on the CyberArk Secure Platform. The Secure Platform is protected by several security layers including hardening the operating system (based on Microsoft SSLF server recommendations, as detailed earlier in this document) and a firewall that accepts only CyberArk protocol transmissions. The main advantage of the Secure Platform is that the attack surface on the Vault Server machine is dramatically narrowed. CyberArk keeps track of security advisories that are related to the Secure Platform, and releases security bulletins to its customers when necessary. Additionally, CyberArk periodically updates the Secure Platform according to the release of Microsoft operating system service packs. Furthermore, CyberArk tests these service packs on the Vault Server prior to updating the Secure Platform.

As an indication that reflects the low chances that the security of the Digital Vault Server will be affected by a Microsoft patch, it should be noted that in the last 7 years CyberArk has released only a single security bulletin that advised customers to install a Microsoft patch. During the same period Microsoft released dozens of security bulletins which were not relevant for the Vault Server based on the hardened CyberArk Secure Platform. This is a good demonstration of the strength of the Secure Platform.

Due to the above, CyberArk believes that, from a security point of view, the monthly Microsoft patches should not be installed automatically as they may introduce operational risks that are inherent during patch deployment.

Enterprises that wish to install the monthly Microsoft patches should first install the patches on a test environment to evaluate their affect. Although this practice is not recommended by CyberArk, if required, CyberArk will provide guidance regarding configuration of the Vault Server security layers that may be required for installing Microsoft patches.

Vault Server and Alternate Operating Hardening Procedure

One of the Vault Server Secure Platform layers is an operating system hardening. CyberArk recommends that customers use the purpose-built Secure Platform hardening developed by CyberArk, which is fully tested and optimized to meet the Vault Server requirements. Enterprises that have analyzed the CyberArk hardening, understand the implications of not using it, and prefer using their own hardening procedure can harden the Vault Server machine with their own standard of hardening procedure. CyberArk cannot estimate or predict the consequences of using different hardening to the Secure Platform hardening but will make its best effort to support and troubleshoot interoperability issues that may arise. In addition, when customers use their own hardening procedures, the security implications of this change are the sole responsibility of the customer.

Adding the Vault Server machine as a member of the domain

In spite of the fact that the Digital Vault Server is a Windows machine, it is designed as an isolated "black-box" machine and does not require any Windows domain services. Furthermore, the Digital Vault security layers only allow communication with the Vault using CyberArk protocol and blocks all other incoming and outgoing transmissions, including Windows protocol transmissions.

Based on this, CyberArk does not recommend adding the Digital Vault Server as a domain member in the enterprise's domain.

In some organizations, procedures may require all Windows systems to be members of the enterprise domain including the Digital Vault Server. CyberArk can provide guidance regarding configuration of the Vault Server security layers to add the Vault as a domain member. It is important to be aware that when the Vault Server is added to the domain, the Vault's security layers are loosened and any domain administrator can potentially access the Vault machine and copy data, run software, or connect remotely to the Vault machine, which negates the Vault machine's isolation and breaches physical security. In addition, the loosened hardening exposes the Vault machine to vulnerabilities that are related to Microsoft protocols to which the Secure Platform is inherently immune.

Synchronizing the Vault Server Clock

Enterprises may require all their systems to be synchronized using an NTP time server. CyberArk will provide guidance regarding configuration of the Vault Server security layers that may be required for utilizing the NTP protocol. Please note that opening the Vault Server to NTP protocol requires the Vault Server security layers to be loosened, and exposes the Vault Server to potential source of vulnerabilities in the NTP protocol.

Modifying the CyberArk Vault Server Secure Platform

CyberArk does not guarantee that any 3rd party software will be able to operate successfully without customizations to the Vault Server's security layers directly, or even by removing them completely.

CyberArk recommends avoiding modifications to the CyberArk Secure Platform since changing the Secure Platform may result in security and support implications. Customers who wish to deviate from the Secure Platform must contact CyberArk Professional Services before changing the Secure Platform.

Security Implications

Modifications in the CyberArk Secure Platform make it impossible for CyberArk to maintain the same security level provided by the Secure Platform. CyberArk does not have the means to analyze and track security vulnerabilities in any potential 3rd party software installed on the Vault Server or any arbitrary customization to the configuration of the Vault Server security layers.

Moreover, installing 3rd party software and directly customizing the security layers affects the security level of the Vault Server (by exposing more vulnerabilities and creating new risks that do not exist in the Secure Platform). CyberArk will still provide the same security information and updates that it provides for customers that use the Secure Platform, but it is the customer's responsibility to analyze the security risks and track vulnerabilities associated with the 3rd party elements introduced to the environment (including the direct customization of Vault Server security layers) which ultimately affect the Vault Server's overall security.

Support Implications

CyberArk develops and tests the Vault Server in the conditions of the CyberArk Secure Platform. CyberArk will provide best-effort support to customers who choose not to run the Vault Server on the Secure Platform. However, it is impossible for CyberArk to predict how any 3rd party software will affect or will be affected by the Vault Server software.

In response to a customer problem, if the problem cannot be reproduced in the lab, it is possible that CyberArk will ask the customer to reproduce the problem in a Secure Platform if CyberArk believes that the deviation from the Secure Platform is the cause of the problem or prevents the isolation of the problem.

In addition, future changes in Vault Server software versions and 3rd party software versions may change the direct customizations required for the 3rd party software to operate successfully on the Vault Server, so another cycle of direct customization may be needed to ensure interoperability.

About CyberArk

CyberArk is the only security company laser-focused on striking down targeted cyber threats; those that make their way inside to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world's leading companies – including 40 of the Fortune 100 – to protect their highest-value information assets, infrastructure, and applications.

For over a decade CyberArk has led the market in securing enterprises against cyber attacks that take cover behind insider privileges and attack critical enterprise assets. Today, only CyberArk is delivering a new category of targeted security solutions that help leaders stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable business harm is done. At a time when auditors and regulators are recognizing that privileged accounts are the fast track for cyber attacks and demanding stronger protection, CyberArk's security solutions master high-stakes compliance and audit requirements while arming businesses to protect what matters most.

With offices and authorized partners worldwide, CyberArk is a vital security partner to more than 1,400 global businesses, including:

- 40 of the Fortune 100
- 17 of the world's top 20 banks
- 8 of the world's top 12 pharmaceutical companies
- 75 of the leading energy companies
- Global brands in retail, manufacturing and telecommunications/cloud

For additional information, visit www.cyberark.com.