CYBERARK®

CYBERARK UNIVERSITY

Core PAM Review and Security

CyberArk Training

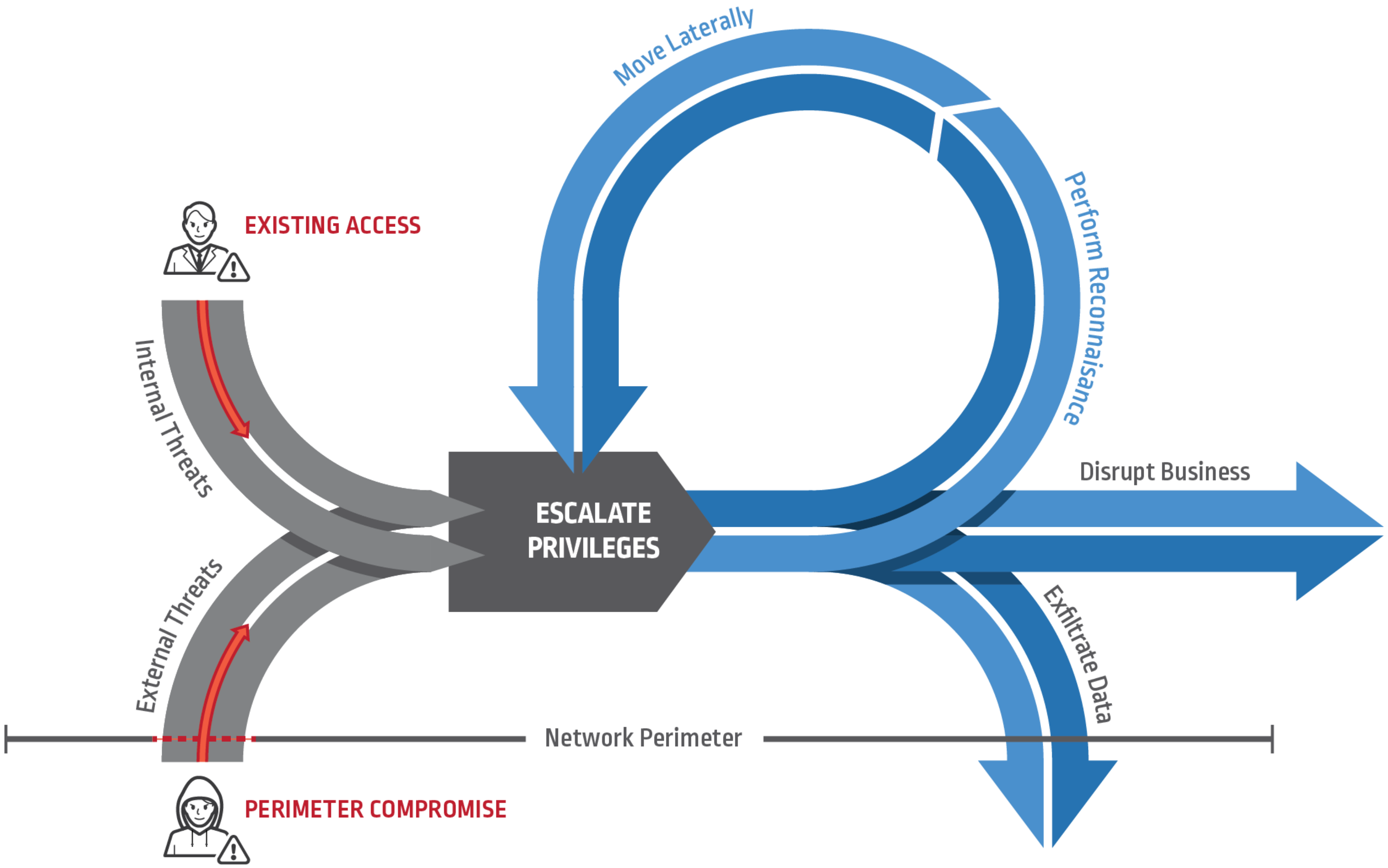
OBJECTIVES

By the end of this lesson, you will be able to:

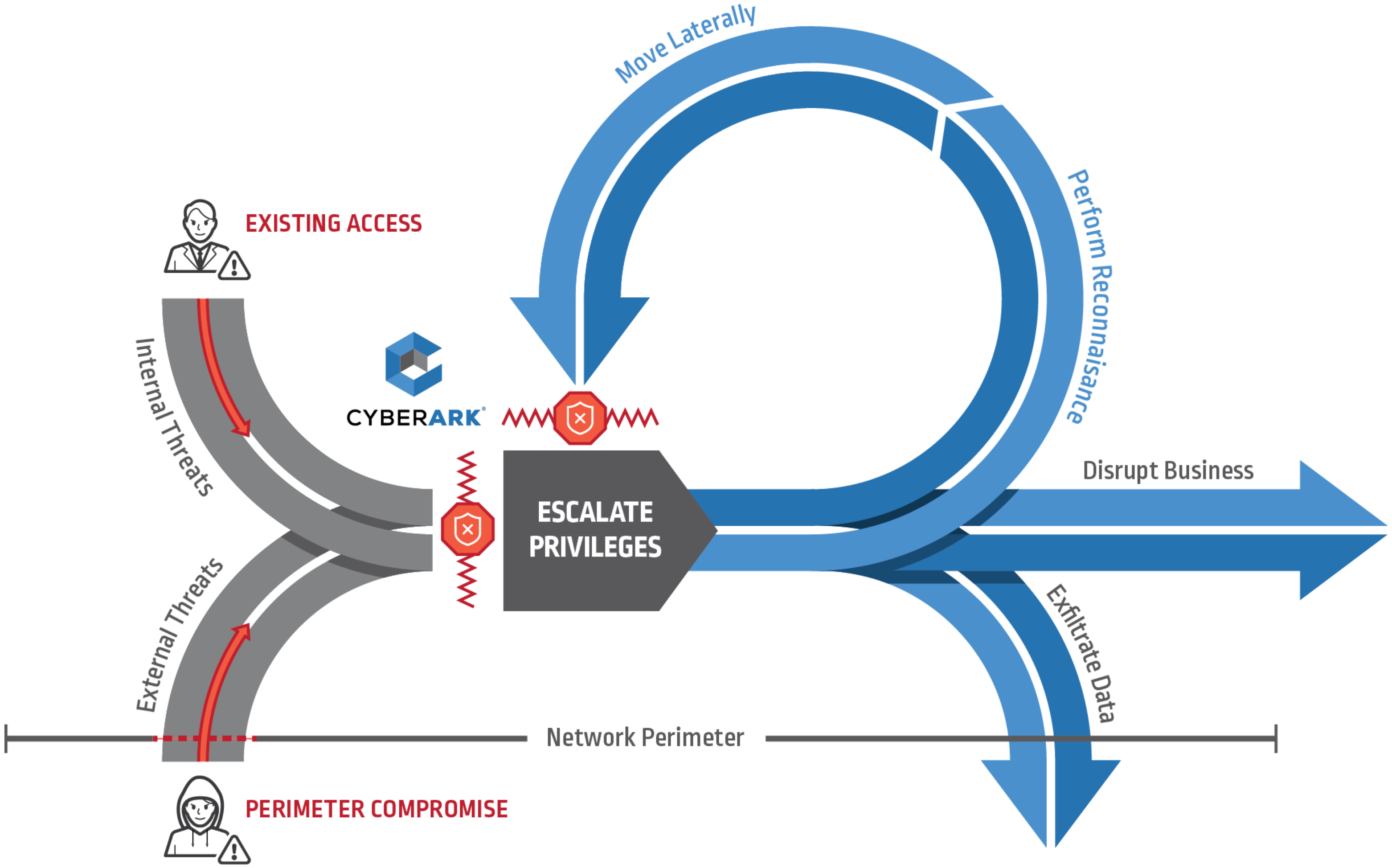
- Describe the Architecture of the Privileged Access Manager solution
- Describe the CyberArk Components that comprise the Privileged Access Security solution
- Describe the key recommendations for protecting the CyberArk PAM environment

REVIEW

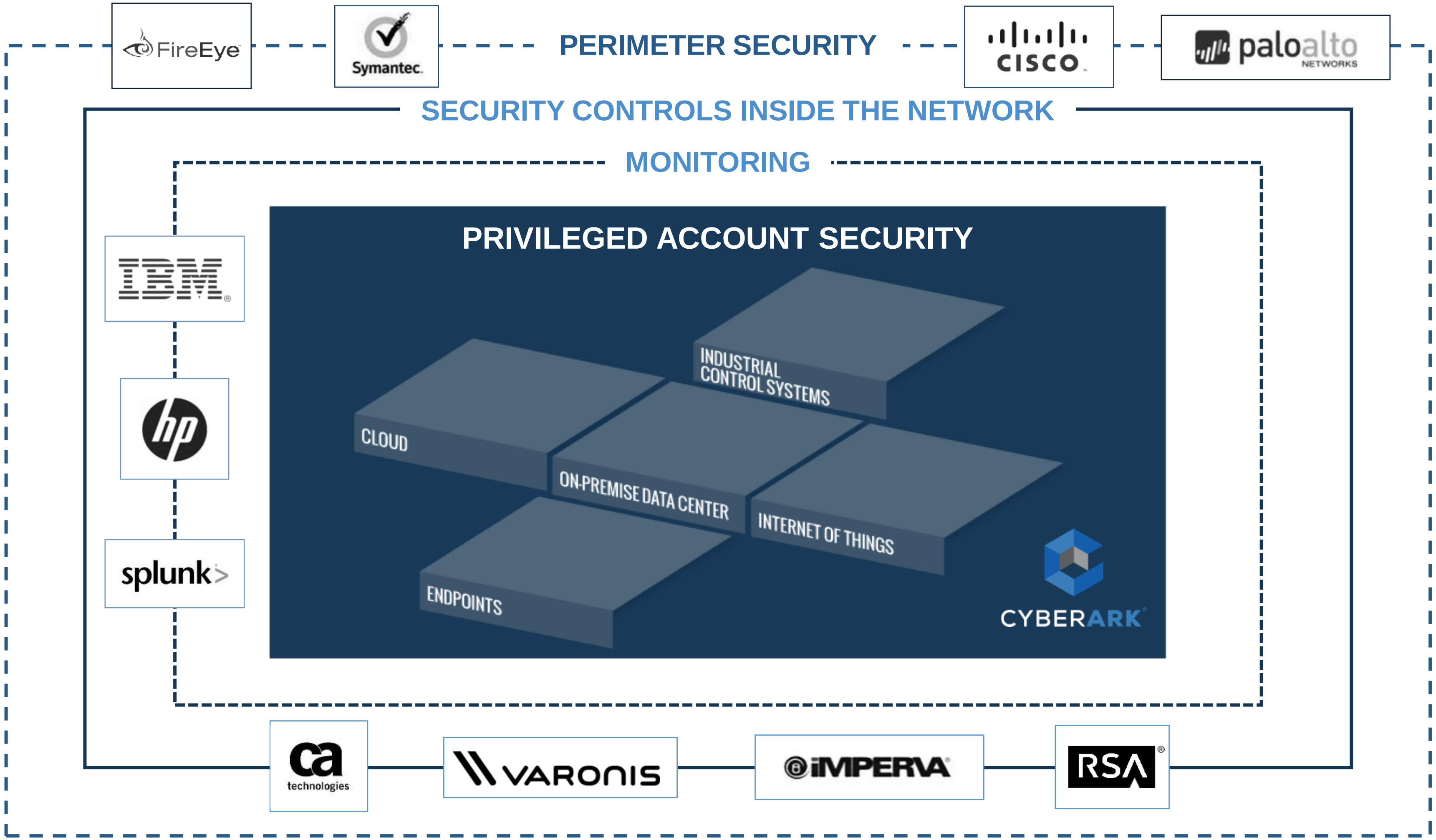
PRIVILEGE IS AT THE CENTER OF THE ATTACK LIFECYCLE



CYBERARK PAM BREAKS THE ATTACK CHAIN



CYBERARK PAM DELIVERS A NEW CRITICAL SECURITY LAYER



COMPREHENSIVE CONTROLS ON PRIVILEGED ACTIVITY

Lock Down Credentials

Protect privileged passwords and SSH keys

Isolate & Control Sessions

Prevent malware attacks and control privileged access

Continuously Monitor

Implement continuous monitoring across all privileged accounts

PRIVILEGE ON-PREMISES COMPONENTS

Digital Vault

- A hardened and secured server used to store privileged account information
- Based on a hardened Windows server platform

Password Vault Web Access (**PVWA**)

- The web interface for users to gain access to privileged account information
- Used by Vault administrators to configure policies

Central Policy Manager (**CPM**)

- Performs the password changes on devices
- Scans the network for privileged accounts

Privileged Session Manager (**PSM**)

- Isolates and monitors privileged account activity.
- Records privileged account sessions

Privilege Threat Analytics (**PTA**)

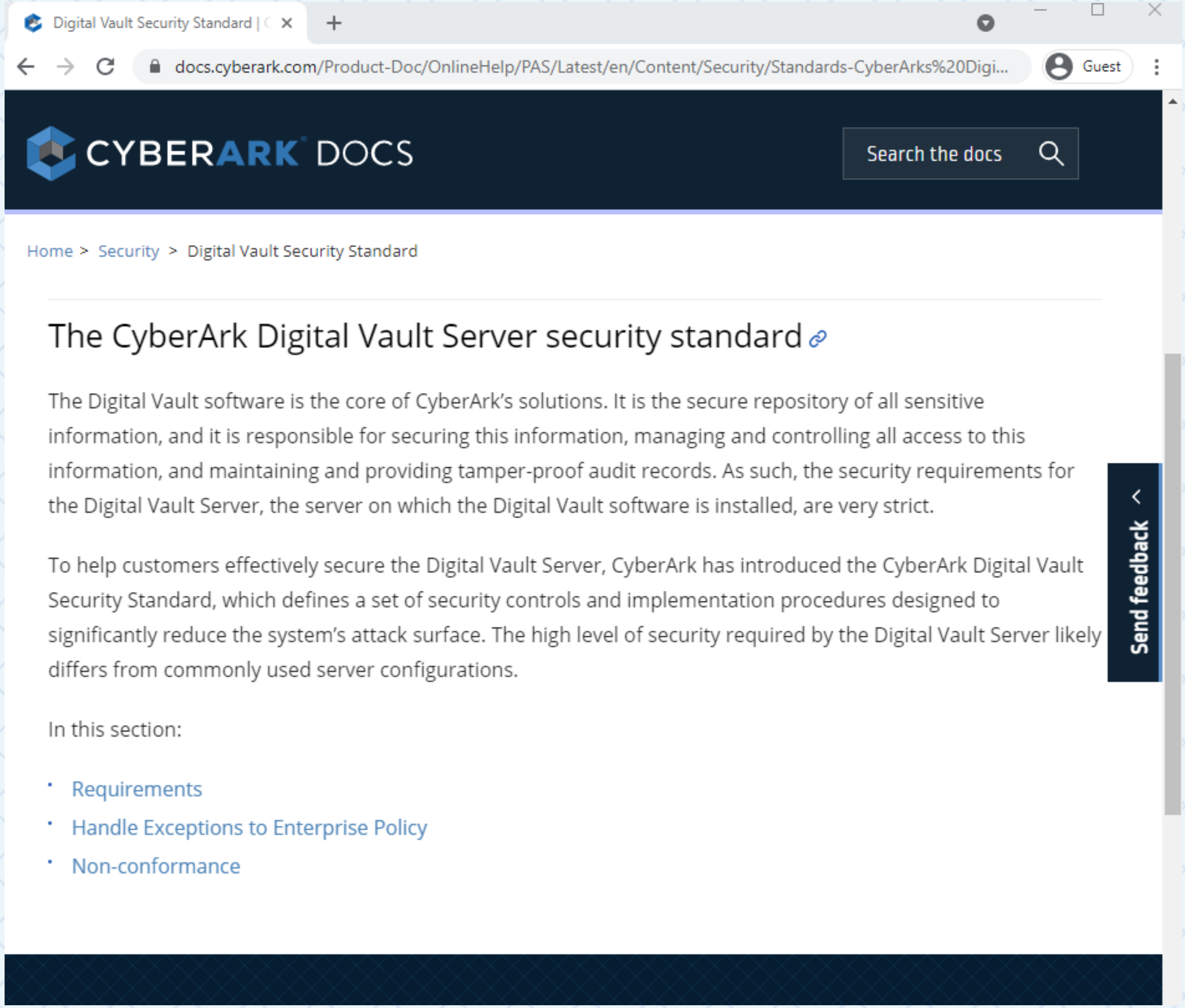
- Monitors and detects malicious privileged account behavior.

ENTERPRISE PASSWORD VAULT

(EPV)

DIGITAL VAULT

- A hardened and secured digital vault used to store privileged account information
- Implemented in compliance with the CyberArk Digital Vault Server security standard results in a highly secure repository for privileged account passwords



Digital Vault Security Standard | C
docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/Security/Standards-CyberArks%20Digi...
Guest
CYBERARK DOCS
Search the docs
Send feedback

Home > Security > Digital Vault Security Standard

The CyberArk Digital Vault Server security standard

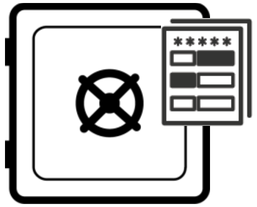
The Digital Vault software is the core of CyberArk's solutions. It is the secure repository of all sensitive information, and it is responsible for securing this information, managing and controlling all access to this information, and maintaining and providing tamper-proof audit records. As such, the security requirements for the Digital Vault Server, the server on which the Digital Vault software is installed, are very strict.

To help customers effectively secure the Digital Vault Server, CyberArk has introduced the CyberArk Digital Vault Security Standard, which defines a set of security controls and implementation procedures designed to significantly reduce the system's attack surface. The high level of security required by the Digital Vault Server likely differs from commonly used server configurations.

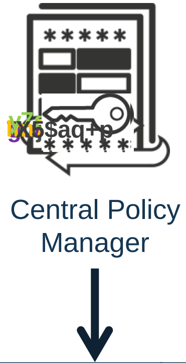
In this section:

- Requirements
- Handle Exceptions to Enterprise Policy
- Non-conformance

CPM – CENTRAL POLICY MANAGER

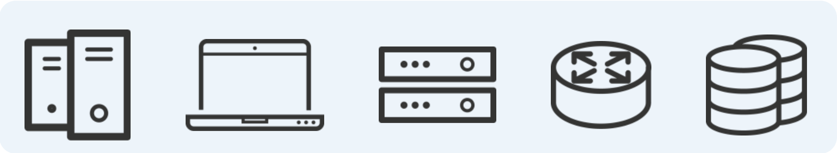


- The CPM performs password changes and SSH key rotations on devices based on the policies set by Vault Administrators
- The CPM is also responsible for Accounts Feed operations
  - Discover – Automates privileged account discovery
  - Analyze - Provide an easy view of all discovered accounts
  - Provision - The scope of the accounts to manage can be provisioned in the Vault in a simple and intuitive way



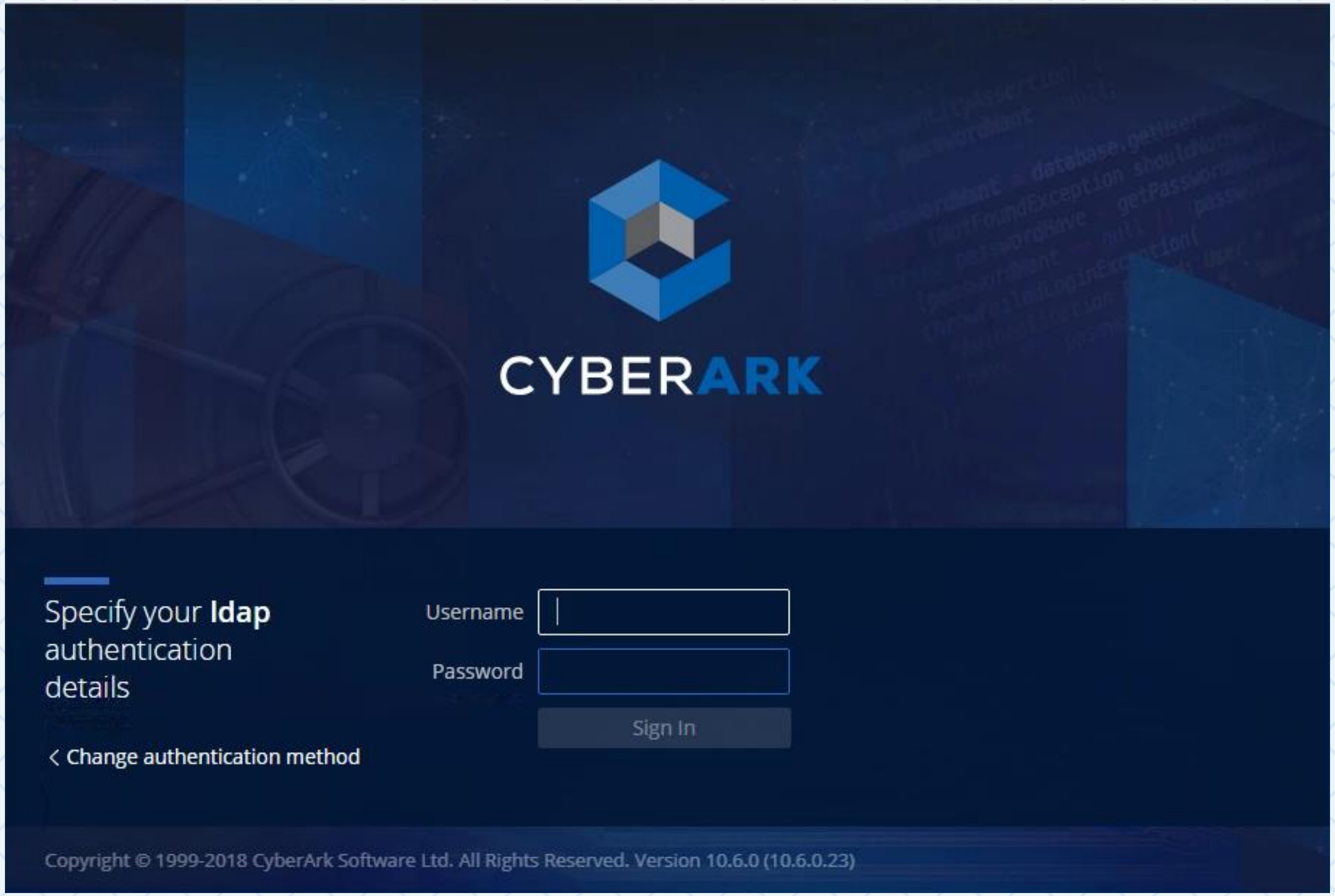
Central Policy Manager

System	User	Pass
Unix	root	**tops3cr3t**
Oracle	SYS	**tops3cr3t**
Windows	Administrator	**tops3cr3t**
z/OS	DB2ADMIN	**tops3cr3t**
Cisco	enable	**tops3cr3t**



PVWA - PASSWORD VAULT WEB ACCESS

The web interface used by Administrators to perform administrative tasks and by end users to gain access to privileged account information.



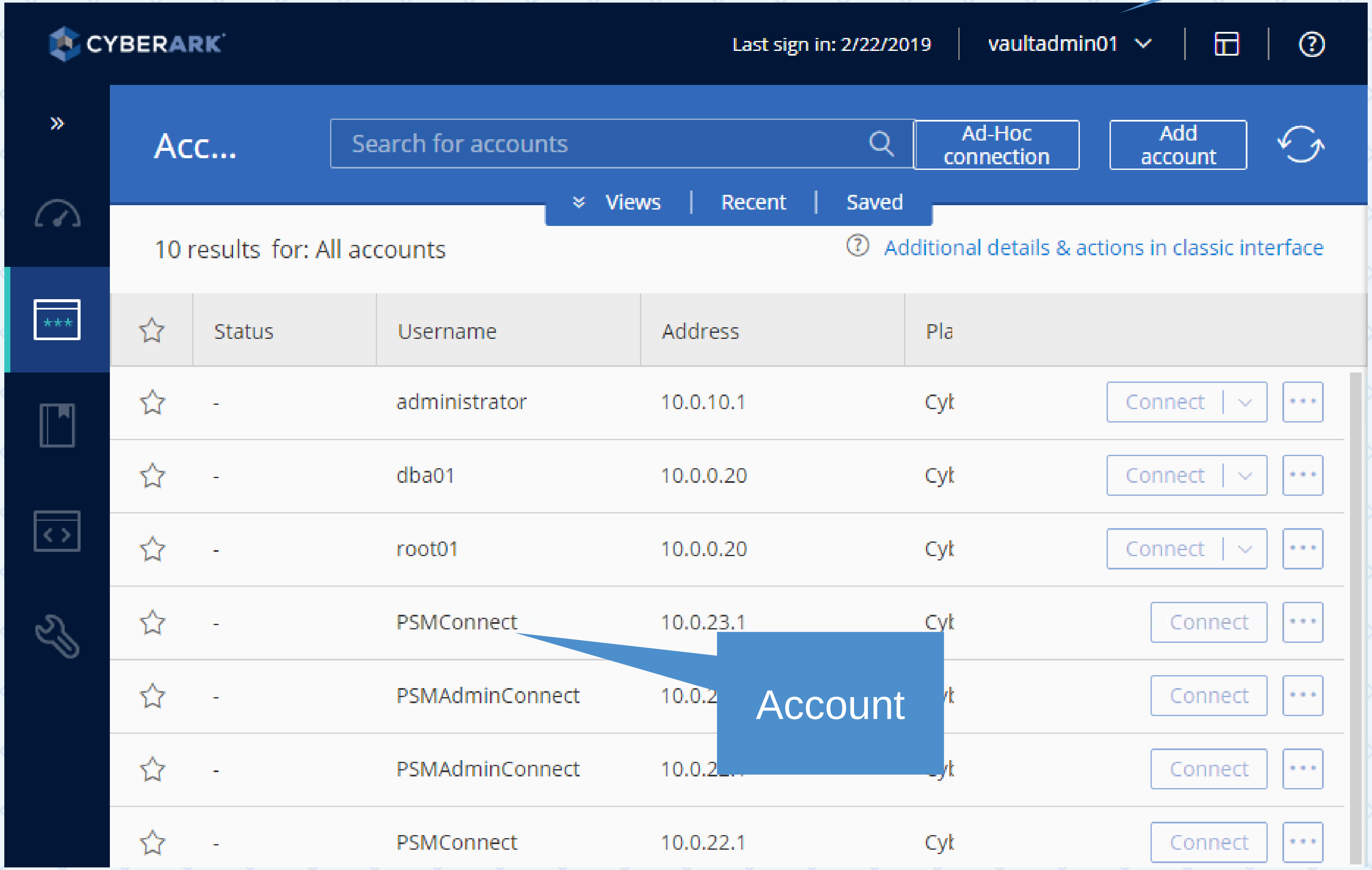
Specify your **ldap** authentication details

Username

Password

Copyright © 1999-2018 CyberArk Software Ltd. All Rights Reserved. Version 10.6.0 (10.6.0.23)

PVWA - PASSWORD VAULT WEB ACCESS



10 results for: All accounts

Additional details & actions in classic interface

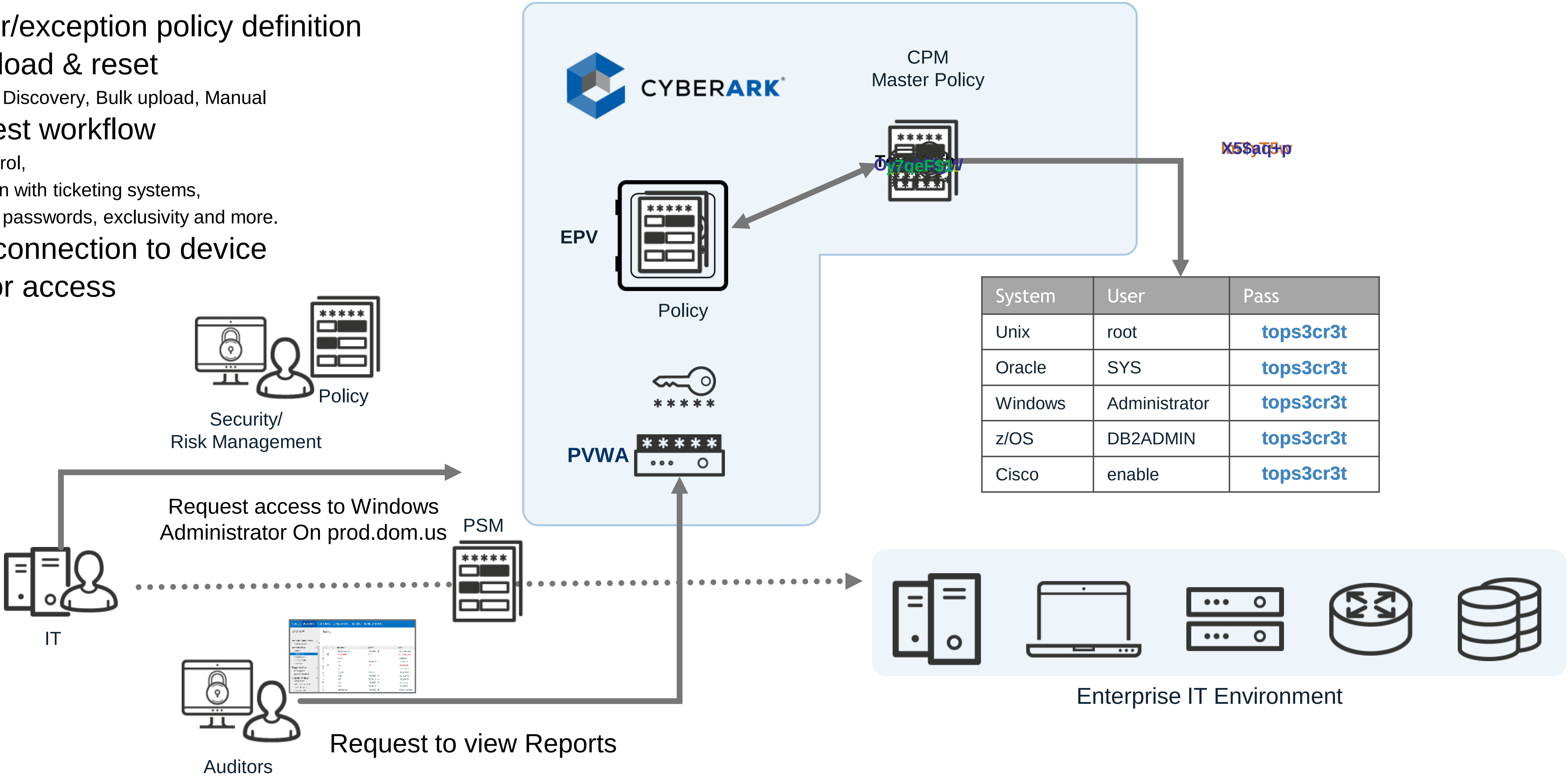
☆	Status	Username	Address	Pla	
☆	-	administrator	10.0.10.1	Cyb	Connect ⌄ ···
☆	-	dba01	10.0.0.20	Cyb	Connect ⌄ ···
☆	-	root01	10.0.0.20	Cyb	Connect ⌄ ···
☆	-	PSMConnect	10.0.23.1	Cyb	Connect ···
☆	-	PSMAdminConnect	10.0.2		Connect ···
☆	-	PSMAdminConnect	10.0.2		Connect ···
☆	-	PSMConnect	10.0.22.1	Cyb	Connect ···

User

Account

ENTERPRISE PASSWORD VAULT SOLUTION OVERVIEW

1. Master/exception policy definition
2. Initial load & reset
   Accounts Discovery, Bulk upload, Manual
3. Request workflow
   Dual control,
   Integration with ticketing systems,
   One-time passwords, exclusivity and more.
4. PSM connection to device
5. Auditor access



System	User	Pass
Unix	root	tops3cr3t
Oracle	SYS	tops3cr3t
Windows	Administrator	tops3cr3t
z/OS	DB2ADMIN	tops3cr3t
Cisco	enable	tops3cr3t

PRIVILEGED SESSION MANAGEMENT

(PSM)

VALUE OF PRIVILEGED SESSION MANAGEMENT

ISOLATE

Prevent cyber attacks by isolating desktops from sensitive target machines

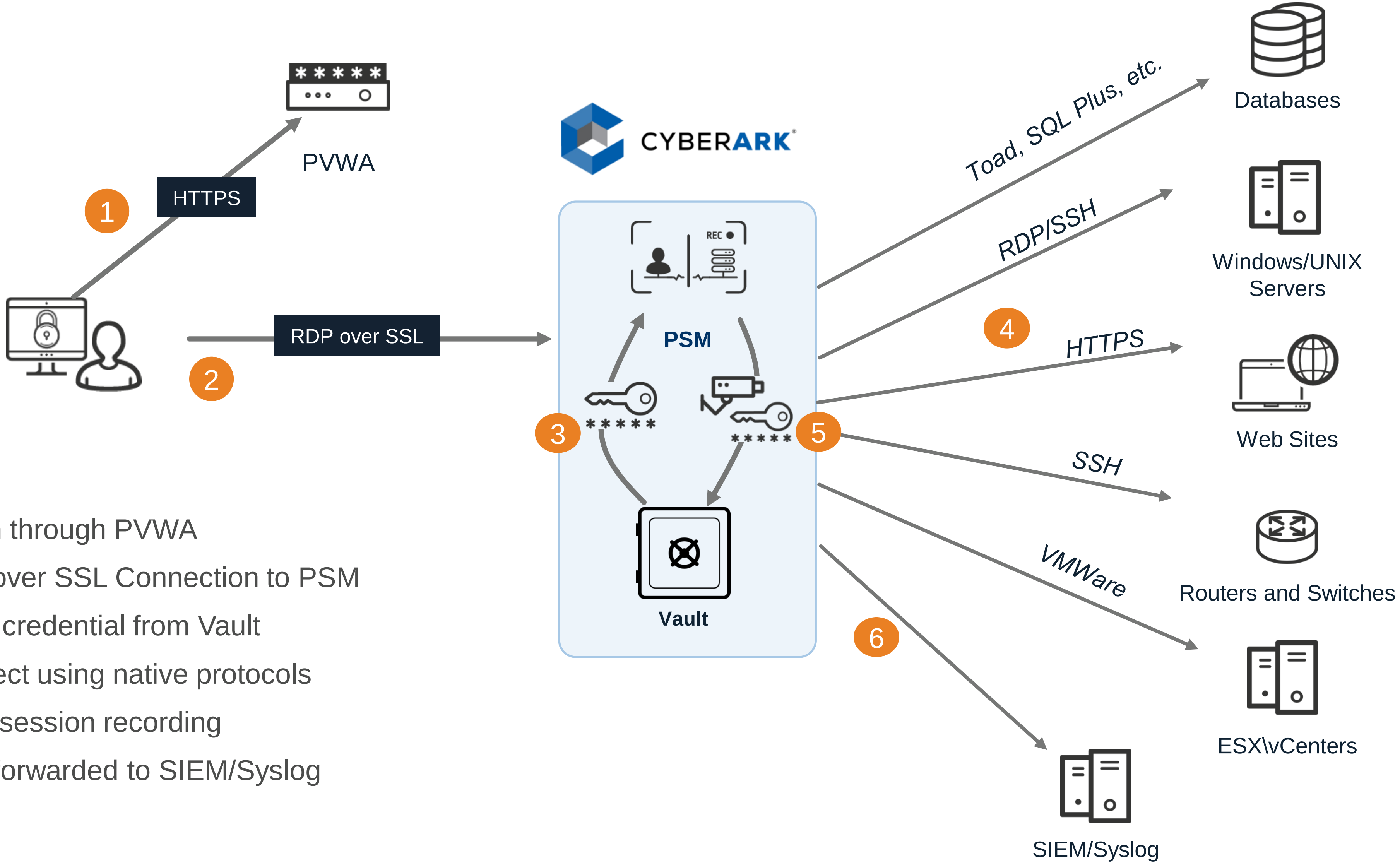
CONTROL

Create accountability and control over privileged session access with policies, workflows and privileged single sign on

MONITOR

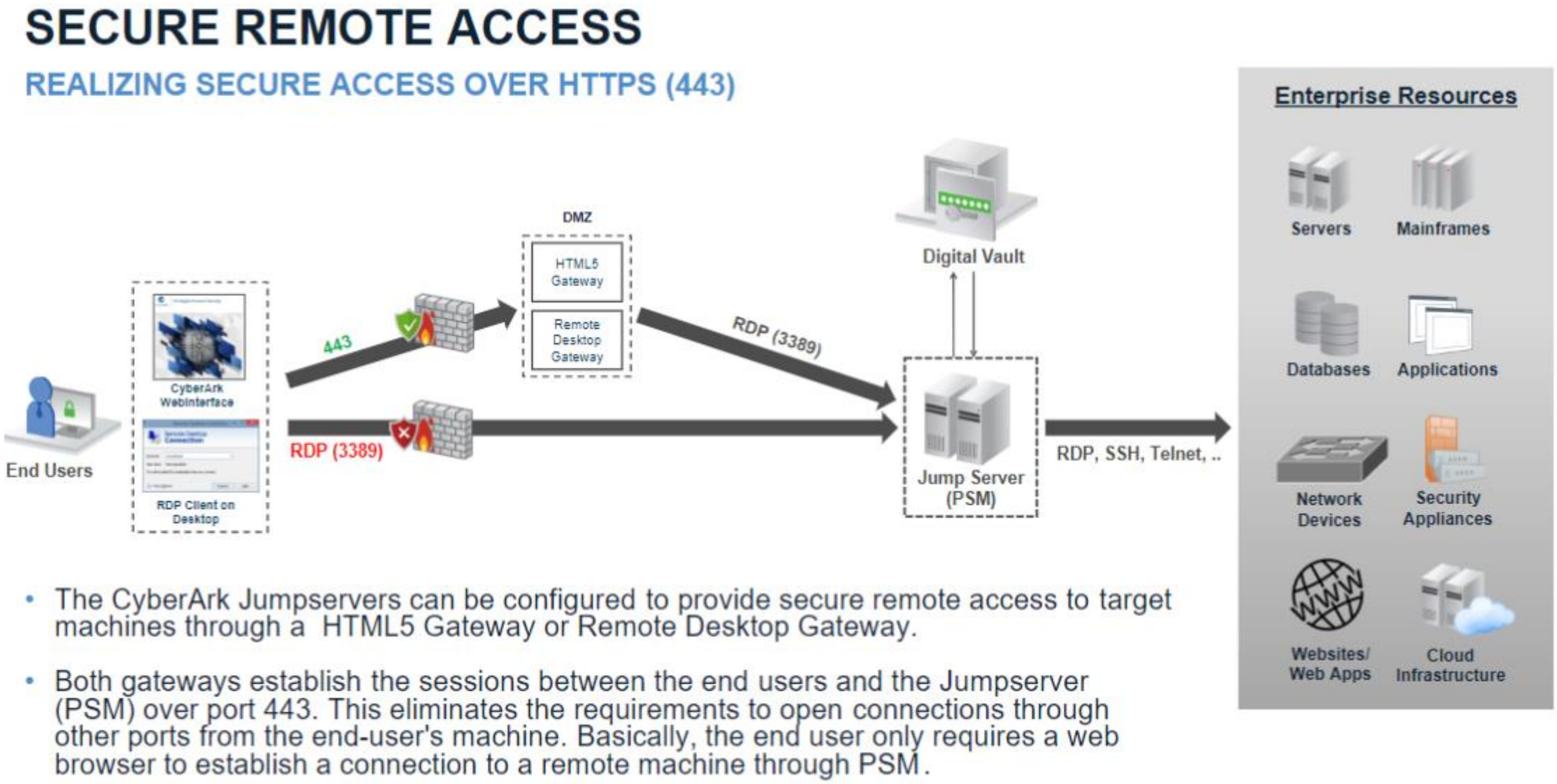
Deliver continuous monitoring and compliance with session recording with zero footprint on target machines

CYBERARK PRIVILEGED SESSION MANAGER



1. Logon through PVWA
2. RDP over SSL Connection to PSM
3. Fetch credential from Vault
4. Connect using native protocols
5. Store session recording
6. Logs forwarded to SIEM/Syslog

CYBERARK PRIVILEGED SESSION MANAGER HTML5 GATEWAY



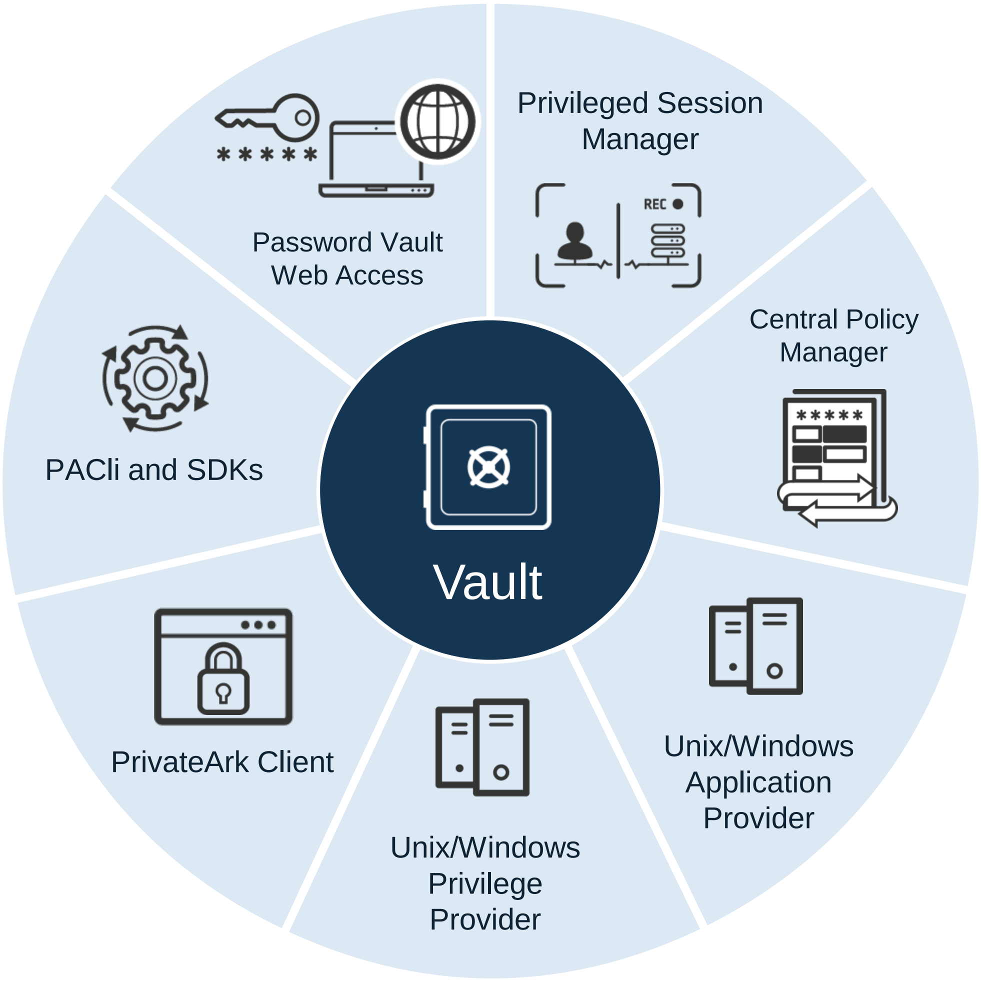
SECURE REMOTE ACCESS

REALIZING SECURE ACCESS OVER HTTPS (443)

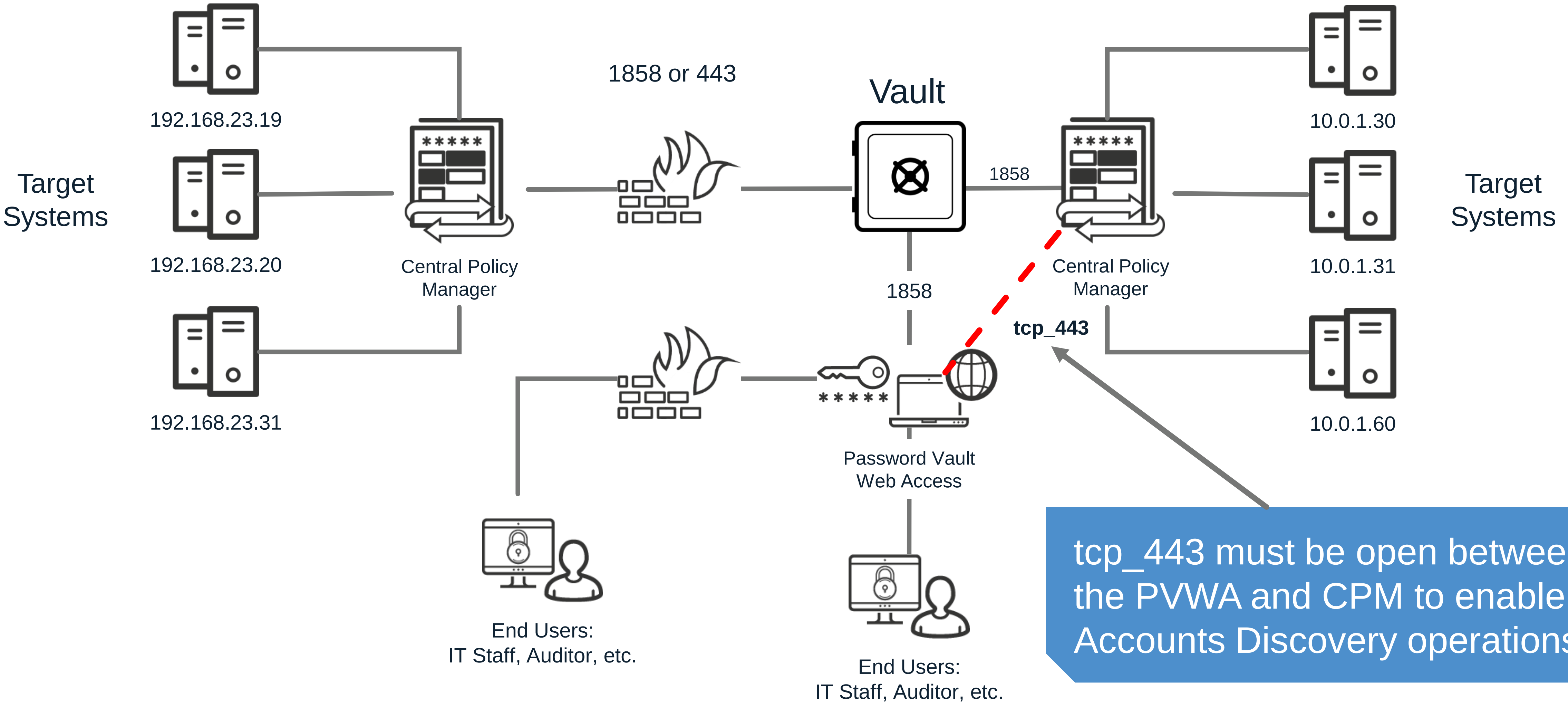
- The CyberArk Jumpservers can be configured to provide secure remote access to target machines through a HTML5 Gateway or Remote Desktop Gateway.
- Both gateways establish the sessions between the end users and the Jumpserver (PSM) over port 443. This eliminates the requirements to open connections through other ports from the end-user's machine. Basically, the end user only requires a web browser to establish a connection to a remote machine through PSM.

HIGH LEVEL SYSTEMS DESIGN

VAULT AND COMPONENTS


Vault
Password Vault Web Access
Privileged Session Manager
REC
Central Policy Manager
Unix/Windows Application Provider
Unix/Windows Privilege Provider
PrivateArk Client
PACli and SDKs

BASIC DEPLOYMENT, MULTIPLE SITES



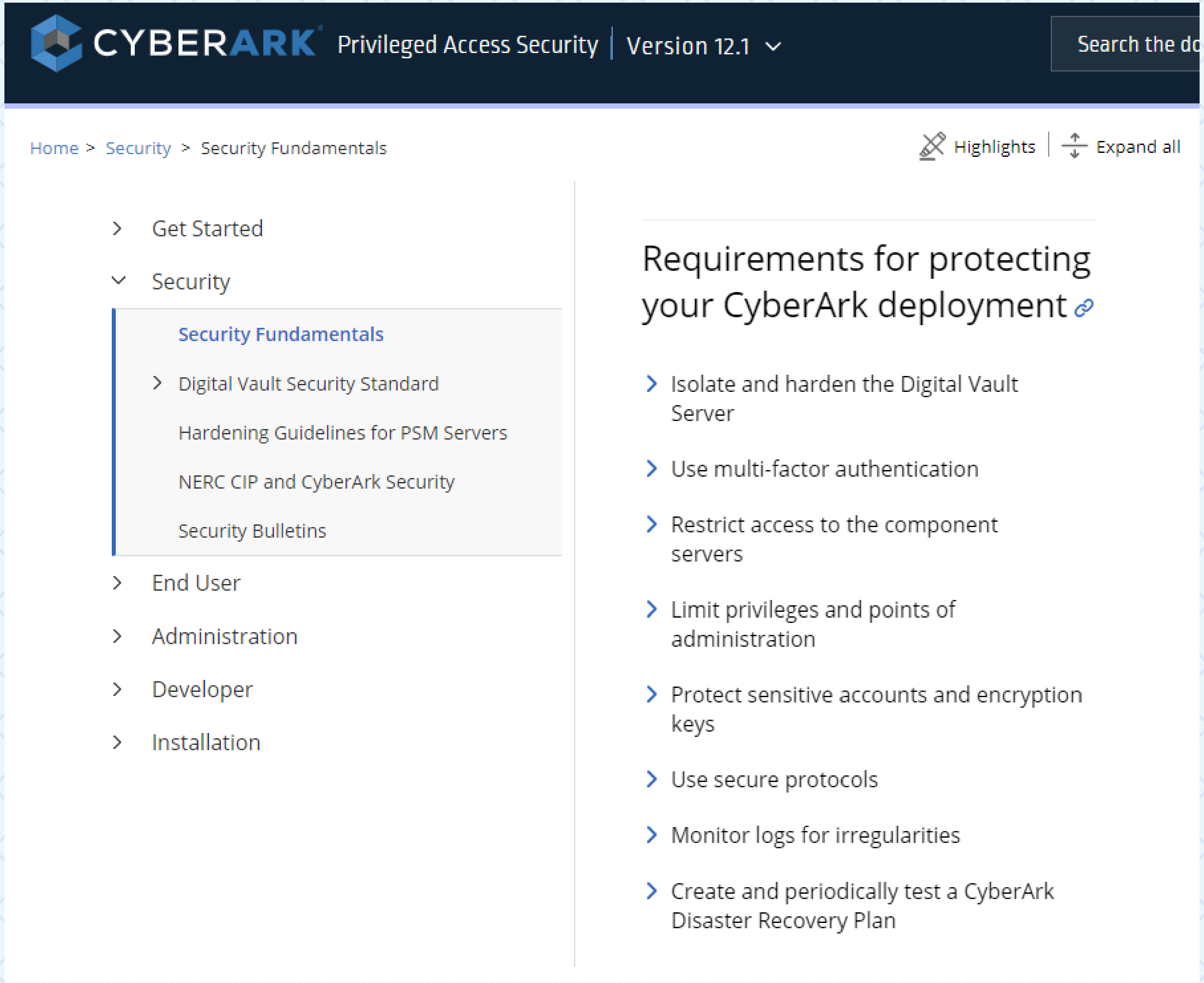
tcp_443 must be open between the PVWA and CPM to enable Accounts Discovery operations

CYBERARK

CYBERARK PRIVILEGED ACCESS SECURITY FUNDAMENTALS

CYBERARK SECURITY FUNDAMENTALS

- It is essential to deploy CyberArk in a secure manner and ensure the security controls you have implemented are not circumvented by an attacker.
- For more information please refer to the ***Security Fundamentals*** documentation at https://docs.cyberark.com.



CYBERARK
Privileged Access Security | Version 12.1
Search the do
Home > Security > Security Fundamentals
Highlights | Expand all
Get Started
Security
Security Fundamentals
Digital Vault Security Standard
Hardening Guidelines for PSM Servers
NERC CIP and CyberArk Security
Security Bulletins
End User
Administration
Developer
Installation

Requirements for protecting your CyberArk deployment

- Isolate and harden the Digital Vault Server
- Use multi-factor authentication
- Restrict access to the component servers
- Limit privileges and points of administration
- Protect sensitive accounts and encryption keys
- Use secure protocols
- Monitor logs for irregularities
- Create and periodically test a CyberArk Disaster Recovery Plan

1

ISOLATE AND HARDEN THE DIGITAL VAULT SERVER

Recent attacks have shown that it is common for threat actors to leverage vulnerabilities in Kerberos protocol to move throughout the environment undetected. It is therefore required that the Digital Vault server run on an isolated and trusted platform.

Critical principles of this control are:

- Not be and never have been a member of a Windows Domain
- No Third-party software
- Network traffic is restricted to CyberArk protocols
- Physical servers (recommended)

2

USE TWO-FACTOR AUTHENTICATION

- **Multi-factor Authentication (MFA)** is an authentication method that uses two or more distinct mechanisms to validate a user’s identity, rather than relying on just a simple username and password combination.
- Using two-factor authentication enables you to mitigate common credential theft techniques such as basic key loggers or tools that are capable of harvesting plaintext passwords.
- CyberArk recommends that customers deploy multi-factor authentication to the CyberArk Digital Vault.

3

RESTRICT ACCESS TO COMPONENT SERVERS

CyberArk components (PVWA, CPM and PSM) are sensitive assets. The core principle of this control is to treat CyberArk infrastructure with the highest level of sensitivity.

Critical principles of this control are:

- Consider installing each component on a dedicated server
- Consider installing on workgroup rather than domain joined servers
- Do not install non-CyberArk applications on the component servers
- Limit the accounts that can access component servers and ensure that any domain accounts used to access CyberArk servers are unable to access domain controllers
- Use network-based firewalls and IPsec to restrict, encrypt and authenticate inbound administrative traffic
- Use the PSM and the local administrator account to access component servers
- Deploy application whitelisting and limit execution to authorized applications
- Additional recommendations can be found at https://docs.cyberark.com.

4

LIMIT PRIVILEGES AND POINTS OF ADMINISTRATION

Reducing the number of privileged accounts and/or the extent of their privileges reduces the overall privileged account attack surface.

The core principle of this control is that there should only be a few CyberArk administrators, and they should only possess limited privileges, unless elevated through a strong approval process.

Critical principles of this control are:

- Reduce privileges of CyberArk administrative accounts
- Eliminate unnecessary CyberArk administrative accounts
- CyberArk administrators should not have access to all credentials
- Require privilege elevation (with Dual Control or Ticketing Integration)
- Use the PSM to isolate and monitor CyberArk administration
- Require two-factor authentication for all avenues of administrative access

5

PROTECT SENSITIVE ACCOUNTS AND ENCRYPTION KEYS

- CyberArk Internal Administrative Accounts:
  - ***Administrator account***
  - ***Master user account***
- The Vault utilizes two encryption keys to secure data:
  - ***Operator Key*** used for runtime encryption tasks.
  - ***Master Key*** used for recovery operations.

Critical principles of this control are:

- Store the Master Password separately from the Master Key. Assign each to different entities within an organization
- Store the Master Key and Password in a physical safe
- Do not store the Operator Key on the same media as the data. If possible, use a Hardware Security Module (HSM) to secure the Operator Key

6

USE SECURE PROTOCOLS

The use of insecure protocols can easily render other controls void. To reduce the risk of eavesdropping and other network-based attacks, use encrypted and authenticated protocols for all communications.

Critical principles of this control are:

- HTTPs for the PVWA
- LDAPs for Vault-LDAP integration and CPM Windows scans
- RDP/TLS for connections to the PSM and from PSM to target machines
- SSH (instead of telnet) for password management

7

MONITOR LOGS FOR IRREGULARITIES

- In order to detect problems early, it is essential to monitor the logs generated by both the CyberArk and the infrastructure on which it runs.
- Early detection is one of the key elements in reducing the impact of any issue, whether security or operational.

Critical principles of this control are:

- Aggregate CyberArk logs within your SIEM
- Monitor and alert upon excessive authentication failures, logins to the Vault server OS, and logins as Administrator or Master
- Consider implementing CyberArk Privileged Threat Analytics (PTA) for continuous monitoring of the use of privileged accounts that are managed or not yet managed in PAM

CYBERARK

8

CREATE AND PERIODICALLY TEST A DR PLAN

- Having a documented disaster recovery plan, and **periodically validating** it, will ensure that you can quickly recover your data and restore operations
- A good disaster recovery plan begins with an assessment of the various risks, the likelihood of occurrence and impact
- The disaster recovery plan should provide information about the physical infrastructure, key contacts, processes to access out-of-band credentials and procedures to recover from likely and/or high-impact problems

SUMMARY

In this session we covered:

- The CyberArk Components that comprise the Core Privileged Access Security solution.
- The Architecture of the EPV and PSM solutions.
- The key recommendations for protecting the CyberArk environment.

THANK YOU