International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 3 (May-June, 2016), PP. 322-325

PRIVILEGE IDENTITY MANAGEMENT-CYBERARK

Priyanka Sarode, Prof. Sujata Pathak
Information Technology(Info. Security),
K J Somaiya College of Engineering,Vidyavihar East,
Mumbai, India
Priyanka.dpsarode@gmail.com

Abstract— **CyberArk's Privileged Identity Management Security solution, a full life-cycle solution for managing the most privileged accounts in the enterprise, enables organizations to secure, provision, manage, control and monitor all activities associated with all types of Privileged Identities such as administrator on a Windows server, Root on a UNIX server, Cisco Enable on a Cisco device, as well as embedded passwords found in applications and scripts. Privileged passwords, as well as the audit information associated with using them, must be protected according to the highest security standards. The CyberArk Privileged Account Security solution utilizes the Patented Digital Vault, certified as highly secure by independent security evaluators (such as ICSA Labs). CyberArk's Digital Vault is the heart of the Privileged Account Security solution and was designed to meet the highest security requirements for the "keys to the kingdom". The Digital Vault provides numerous underlying security capabilities for authentication, encryption, tamper-proof audit and data protection.[7][8].**

I. INTRODUCTION

As per TechTarget "**Recent research showed 72% of temporary workers and contractors are given administrative privileges on their employers' systems. After the Snowden incident many organizations obviously cautious about too many users with admin privileges.**"[5]

Snowden is an American computer professional, former Central Intelligence Agency (CIA) employee, and former contractor for the US Government who copied classified information from the United States National Security Agency (NSA) in 2013 without prior authorization

So Privilege identity management is solution to minimize exposure of sensitive activities and Information. Privileged Identity Manager protects, automates and audits the use of privileged identities to help thwart insider threats and improve security across the extended enterprise

Organizations considering Privileged Identity Management solutions must prioritize security as a requirement because privileged accounts are frequently targeted by external attackers and malicious insiders to access sensitive data and gain control of the IT infrastructure.[1][6][5]

- **Privileged Identity Manager:**

- Provides centralized privileged identity management: to address insider threats, improve control and reduce risk.
- Addresses compliance, regulatory and privacy requirements.
- Provides automated password management.

According to kuppingercole report CyberArk has been one of the pioneers of PIM; its password vault solution has been one of the first in the market. The vendor provides hypervisor support,

outstanding application-to application, and database connection pool password management. CyberArk also uses its SIM integration for privileged threat detection and mitigation[11].

II. WHAT IS CYBERARK

CyberArk: Primary purpose of their product suites are for identifying each privileged user. CyberArk's focus on identity management tends to be a burden on IT in the long run, due to the over-complexity of their check-in/check- out password rotation requirements Privileged accounts represent the largest security vulnerability an organization faces today.

In the hands of an external attacker or malicious insider, privileged accounts allow attackers to take full control of an organization's IT infrastructure, disable security controls, steal confidential information, commit financial fraud and disrupt operations. Stolen, abused or misused privileged credentials are used in nearly all breaches. With this growing threat, organizations need controls put in place to proactively protect against, detect and respond to in- progress cyber attacks before they strike vital systems and compromise sensitive data.[3][6]

CyberArk is the trusted expert in privileged account security. Designed from the ground up with a focus on security, CyberArk has developed a powerful, modular technology platform that provides the industry's most comprehensive Privileged Account Security Solution. Each product can be managed independently or combined for a cohesive and complete solution for operating systems, databases, applications, hypervisors, network devices, security appliances and more. The solution is designed for on-premise, hybrid cloud and OT/SCADA environments.

The CyberArk Privileged Account Security Solution is based on CyberArk Shared Technology Platform, which combines an isolated vault server, a unified policy engine, and a discovery engine to provide scalability, reliability and unmatched security for privileged accounts.[8][9]

A. With CyberArk's Privileged Account Security solution, enterprises can easily:

a)

1) Set the main policy rules that define how you manage accounts in your organization using the Master Policy

The Master Policy offers a centralized overview of the security and compliance policy of privileged accounts in your organization while allowing you to configure compliance driven rules that you define as the baseline for your enterprise.

2) Manage and Protect all Privileged Accounts

Utilize a secure Digital Vault in order to store, protect, manage and control access to Privileged Accounts at a centralized point using a robust policy management engine. CyberArk's patented Vaulting Technology software utilizes a fully integrated model of critical security layers, interwoven to meet the highest security needs.

3) Control Access to Privileged Accounts-

The Privileged Account Security solution offers a simple access control interface that easily pinpoints who is entitled to use privileged accounts and initiate a privileged session, when and why.

4) Initiate and Monitor Privileged Sessions-

As a central control point, the Privileged Account Security solution also provides privileged single sign-on for initiating privileged sessions, as well as recording any activities that occurred during these sessions. PIM utilizes the Digital Vault as a tamper-proof secure storage for these session recordings.

5) Manage application and service credentials

PIM provides sophisticated and transparent solutions for securing and managing critical applications as well as Application Server accounts, and eliminating the use of hard-coded and embedded passwords, making them invisible to developers and support staff.

6) Comply with audit and regulatory requirements

The Privileged Account Security solution provides an easy way to create audit reports required by Sarbanes-Oxley, PCI and more. It allows enterprises to enforce corporate security policies to ensure compliance with regulatory needs and security best practices related to access and usage of privileged accounts for both human and application (unattended) access.

7) Streamline management of Privileged Accounts

PIM eliminates manual administration and overhead by providing instant and automatic changing of passwords for thousands of network devices and applications, including scripts and parameter files. Its high level of automation ensures highly reliable and uninterrupted service with minimal administrator overhead and increased productivity.

8) Seamlessly integrate with enterprise systems

With an industry leading performance, scalability and robustness, PIM can protect and manage up to hundreds of thousands of passwords across a highly heterogeneous IT environment, with complex and distributed network architectures. PIM can leverage existing enterprise infrastructure and integrate with corporate core systems.

9) Easily set up and deploy

PIM ensures quick deployment and implementation proven in over 400 enterprise customers, providing immediate ROI by improving IT productivity[2][1].

III. MAIN COMPONENTS OF CYBERARK

A. Enterprise Password Vault

CyberArk's Password Vault (EPV) enables organizations to secure, manage, automatically change and log all activities associated with all types of Privileged Passwords

The Vault is the most secure place in the network where sensitive data can be stored. The Vault is designed to be installed on a dedicated computer, for complete data isolation.

Constant access to your passwords is extremely important. However, when a Server fails to process requests, access to your passwords is prevented. The Vault can be installed as a high-availability cluster of servers which provide constant access to the passwords in the Vault. In this implementation, there is always at least one Server connected to the cluster that is on standby for when any other Server in the cluster fails to process requests.

The Vault is a full LDAP (Lightweight Directory Access Protocol) client, and can communicate transparently with LDAP-compliant directory servers to obtain User identification and security information. This enables automatic provisioning and creation of unique and individual users based upon the external group membership and attributes. The Privileged Account Security Disaster Recovery Site ensures that your Vault is replicated to a Disaster Recovery Vault regularly, and can take over immediately when the Production Vault stops processes requests suddenly.

The Vault is installed with an interface that enables the Administrator to start and stop the Vault, and to monitor its operation.[3][4]

B. PrivateArk Client

The PrivateArk Client is a regular Windows application that is used as the administrative client for the Privileged Account Security solution. It can be installed on any number of remote computers, and can access the Vault by any combination of LAN, WAN or the Internet. In addition, the User must be authenticated by the Vault before being allowed access. The Privileged Account Security solution ensures a highly secured system of User authentication using a customizable combination of passwords, physical keys, and certificates.

After authentication, a User can work with the PrivateArk Client to set up a Vault hierarchy and create Safes and Users. Safe properties determine how each Safe will be accessed, and specific User properties determine the passwords that each Use can access and the level of control that they have over these passwords. Users are also able to monitor and track their password activities, including who has accessed their information, when and from where.

Each command, request, file transfer and User configuration is encrypted before being transmitted between the Vault and the PrivateArk Client to ensure maximum protection for data at all times.

C. The Central Policy Manager

The Privileged Account Security solution provides a revolutionary breakthrough in password management with the CyberArk Central Policy Manager (CPM), which automatically enforces enterprise policy. This password management component can change passwords automatically on remote machines and store the new passwords in the EPV (Enterprise password vault), with no human intervention, according to the organizational policy. It also enables organizations to verify passwords on remote machines, and reconcile them when necessary.

D. The Password Vault Web Access Interface

The Password Vault Web Access (PVWA) is a fully featured web interface that provides a single console for requesting, accessing and managing privileged passwords throughout the enterprise by both end users and administrators.

Automatically produced lists of frequently used passwords and recently used passwords for each user facilitate speedy access and usage. In addition, the Mobile.

PVWA enables users to access privileged accounts from mobile devices, enabling seamless connectivity and optimum workflows.

The PVWA's simple, intuitive wizard enables users to define new privileged passwords, while a powerful search mechanism enables you to find privileged passwords and sensitive files with minimum effort.

CyberArk‘s PVWA dashboard enables you to see an overview of activity in your Privileged Account Security solution, as well as statistics about all the activities that have taken place. The dashboard shows you a graphic representation of the passwords that have been managed, and links to specific information about users and passwords that require special attention

E. Privileged Session Manager –

The Privileged Session Manager (PSM) enables organizations to secure, control and monitor privileged access to network devices. Using the Vault technology, it manages access to privileged accounts at a centralized point and facilitates a control point to initiate privileged sessions. The PSM interface pinpoints users who are entitled to use privileged accounts and initiate a privileged session, when, and for what purpose. The PSM can record all activities that occur in the privileged session in a compact format and provide detailed session audits and DVR-like playback. Recordings are stored and protected in the Vault server and are accessible to authorized auditors.

PSM can be leveraged by enterprises to provide secure remote access to their sensitive network resources by third party vendors, without disclosing sensitive passwords, and while recording the entire session.

PSM separates end users from target machines, and initiates privileged sessions without divulging passwords.

In addition, PSM can display a broad overview of all activity performed on every privileged account, without exception. All activities are fully monitored and meet strict auditing standards.

PSM is integrated transparently and seamlessly into existing enterprise infrastructures and does not require changes in user’s workflow or password access procedures [3][4].

IV. CHALLENGE

Cyber-Ark PIM is defined as a suite by the vendor. However, it is more sort of an integrated product with several common elements and different feature sets, going beyond the typical suite approach. But there is one big challenge which effects usability of this product. Many organizations are using Virtual Machine for cost saving and If CyberArk is implemented on Virtual Machine only 60-70 end user concurrent connections on Privilege Session manager server and observed high CPU utilization so need to improve performance of Privilege Session manager so that it will consume less number of CPU utilization and 100-110 concurrent connections are possible.

V. CONCLUSION

It is mandatory to quickly address the PIM challenges which exist in any IT environment. This requires solutions which cover all (or at least most) of the different aspects of PIM in an integrated solution, for a heterogeneous environment.

Cyber-Ark itself names the common elements as “Privileged Identity Management Infrastructure”. Defining the product as a suite however fits to the licensing approach which allows for selecting the required elements – even while, when looking at the PIM challenge, implementing the entire suite with all features typically is the best approach.

Cyber-Ark PIM suite is amongst the leading-edge products in the emerging PIM market, provide one of the most comprehensive feature sets in the entire markets. The well-thought architecture allows for scalability as well as ease- of-use. A particular strength of the product is the platform support which covers virtually all core systems in today’s IT environments.

Thus it is strongly recommended to include the Cyber-Ark Privileged Identity Management Suite in evaluations for PIM tools – even more in complex, heterogeneous enterprise environments.

VI. ACKNOWLEDGEMENT

I am pleased to acknowledge my indebtedness to Prof. Sujata Pathak, for her invaluable guidance and perspective suggestions at every stage. She has been a perennial source of inspiration throughout paper work.

I offered my profound gratitude towards Dr. Shubha Pandit, principal, KJ Somaiya College of Engineering,Vidyavihar, Mumbai for providing me all excellent academic facilities

require to complete the work. I would like to express my sincere thanks to all staff members of Information Security department for extending valuable source of information during the course.

I am also thankful to staff members of Information Security laboratory, KJ Somaiya College of Engineering, Vidyavihar, Mumbai, and to all my friends who have extended me corporation during completion of this work. I am thankful to my parents and family for the support needed to complete this worK.

REFERENCES

[1] How can organizations get control over privileged identity management? By Randall Gamby

[2] Privileged Account Security Installation Guide Version 9.0.1 by CyberArk-

[3] Privileged Account Security Implemetation Guide Version 9.0.1 by CyberArk

[4] Privileged Account Security End User Guide Version 9.0.1 by CyberArK

[5] http://www.cyberark.com/privileged-identity-management/

[6] Privileged Identity Management: Take Control of Your Administrative Credentials Philip Lieberman

[7] Market Guide for Privileged Access Management by Felix Gaehtgens | Anmol Singh dated 27 May 2015

[8]https://en.wikipedia.org/wiki/Privileged_Identity_Management

[9] ObserveIT vs. CyberArk (EPV and PSM), Key feature differentiators, COMPETITIVE COMPARISON

[10]https://www.kuppingercole.com/report/mkpr_cyber_ark_pim22122010

[11]https://www.kuppingercole.com/report/leadershipcompass_pxm71100101215

[12]https://cyberark.my.salesforce.com/sserv/login.jsp?orgId=00D300000000HNg