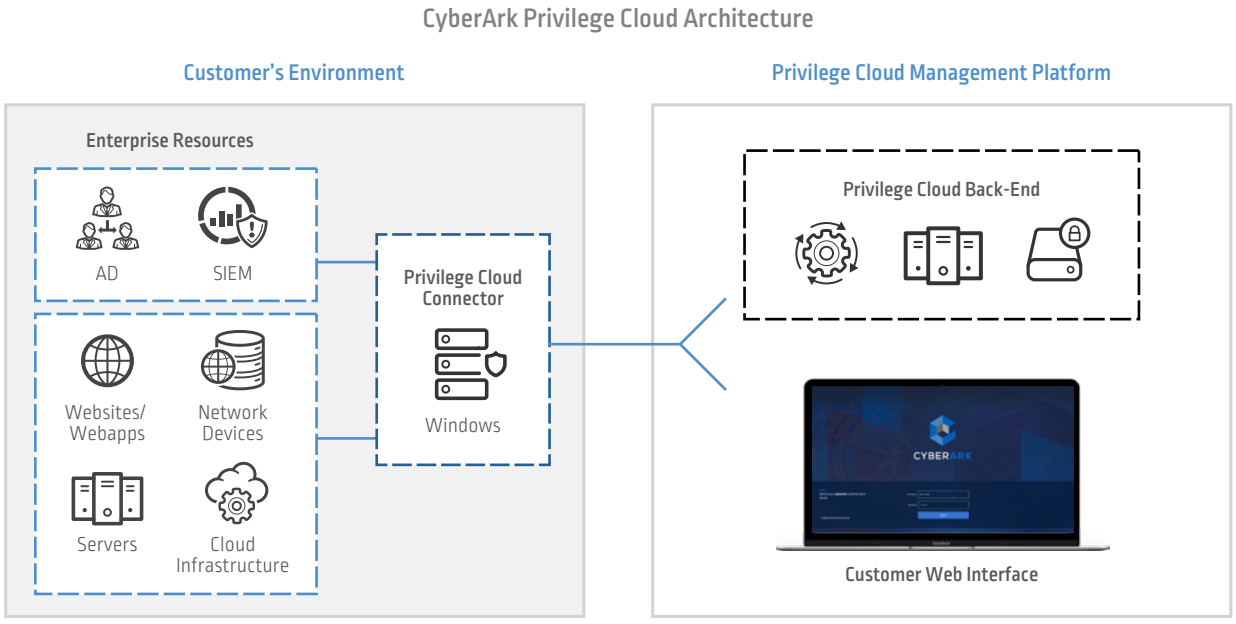
DATA SHEET

CYBERARK® PRIVILEGE CLOUD™ SECURITY OVERVIEW

JULY 2019

INTRODUCTION

CyberArk is the leader in privileged access security solutions, including the SaaS CyberArk Privilege Cloud which enables organizations to quickly achieve their privileged access security goals. CyberArk is an award-winning creator and vendor of privileged access security solutions often recognized for its leadership and vision. While the CyberArk Privilege Cloud is architected to simplify the task of protecting privileged access, CyberArk is also fully committed to delivering the most secure SaaS privileged access security solution, so that customers can trust their credentials remain well protected. This paper reviews the stringent security measures CyberArk takes to protect the integrity of the CyberArk Privilege Cloud.



BUILT-IN SECURITY MEASURES

CyberArk Privilege Cloud is engineered for extreme data durability, integrity and security. The service is hosted in premier Tier IV data center facilities that are highly secure, fully redundant and certified for SOC-2 and ISO 27001 compliance. The solution is built, managed, and secured according to industry standards. CyberArk encrypts data at rest and data in transit to avoid leakage and enable privacy, hardens all solution components to reduce attack surfaces and supports multi-factor authentication and policy-based access controls to protect against unauthorized access and data disclosure.

Hierarchical Encryption for Data at Rest

The CyberArk Digital Vault is the cornerstone of the CyberArk Privilege Cloud solution. The highly secure database maintains privileged account credentials, access control policies, credential management policies and audit information. CyberArk leverages FIPS 140-2-compliant multi-layered hierarchical encryption algorithms to protect the Digital Vault and its data. An AES-256 key is used for symmetric encryption and an RSA-2048 key pair is used for asymmetric encryption.

Each individual file and safe within the CyberArk Privilege Cloud is uniquely encrypted using a randomly generated encryption key. At the top of the key hierarchy, the CyberArk Privilege Cloud utilizes two unique keys per customer: a server key and a recovery key. The server key is encrypted using Amazon Web Services Key Management Service (AWS KMS). The server key, hosted in the AWS KMS, is required to start the Digital Vault. The recovery key is a unique private key that is required only in the event of a system restoration.

SESSION ENCRYPTION FOR DATA IN TRANSIT

CyberArk also uses advanced encryption algorithms designed to secure all data in transit. Communications with customer-operated systems (Active Directory servers, Security Information and Event Management servers.) are encrypted via a SSH tunnel between the CyberArk Privilege Cloud Connector (deployed in the customer environment) and the Privilege Cloud back end (deployed in the CyberArk Cloud).

The CyberArk Digital Vault employs a proprietary protocol designed to secure sensitive privileged account information transmitted between the CyberArk Privilege Cloud back end and the CyberArk Privilege Cloud Connector installed on the customer's network. The proprietary session encryption mechanism uses a unique AES-256 session key and is FIPS 140-2 compliant. With this level of encryption, network traffic is undecipherable to help prevent information from being exfiltrated for illicit purposes.

Digital Vault Server Hardening at the Heart of Privilege Cloud

The CyberArk Digital Vault server operating environment is hardened according to industry standards for strong security. In addition, based on extensive security research and testing, CyberArk has defined a series of additional configuration changes to further harden the Digital Vault server and reduce attack surfaces without compromising functionality.

The Digital Vault software installation package includes operating system hardening processes based on the Microsoft Security Compliance Manager recommendations. To further reduce attack surfaces and minimize risks, CyberArk makes additional system configuration changes, such as disabling all unnecessary services, restricting access to the server, and restricting access to the Digital Vault file system.

CyberArk has also automated the hardening of the CyberArk Privilege Cloud Connector and the underlying OS, which remain on-premises, in the customer's infrastructure. This will save customers' time and help increase confidence in the solution's security posture.

Stringent Database Access Control Mechanisms

CyberArk Privilege Cloud is using a multi-tenant scheme mechanism to store customer information using an elastic SaaS-ready system provided by Amazon Web Services. The Digital Vault manages the movement of data entering and leaving the system.

CyberArk employs strict policy-based access controls to protect the CyberArk Privilege Cloud database where privileged account audit trails and session logs are maintained. Information stored in the CyberArk Privilege Cloud database can only be viewed by authorized CyberArk employees. CyberArk also utilizes the audit, monitoring and session isolation capabilities of the CyberArk Core Privileged Access Security Solution to track and record the activity of CyberArk employees to certify to customers that their environments remain secure. The audit trails and session logs maintain a complete and accurate record of any action that has occurred in the system, such as a nefarious administration insider deleting or tampering with an audit trail on a target system.

Support for Authentication Technologies

The CyberArk Privilege Cloud solution supports multi-factor authentication (MFA) for improved security. CyberArk strongly recommends customers use MFA for maximum protection. The CyberArk Privilege Cloud supports SAML MFA, LDAP and CyberArk Authentication.

Multi-factor authentication safeguards access to the sensitive information stored within the CyberArk Privilege Cloud. In addition, customers can centrally extend multi-factor authentication to all other privileged accounts (on- premises, in the cloud or in DevOps environments) by storing and managing their credentials in the CyberArk Privilege Cloud.

CyberArk Privilege Cloud Monitoring

CyberArk proactively monitors the security and integrity of the CyberArk Privilege Cloud service, including the underlying infrastructure and all CyberArk software components. CyberArk leverages field-proven security monitoring tools, methods and procedures based on extensive customer experience.

Shared Responsibility Model

CyberArk Privilege Cloud security and operations are a shared responsibility between CyberArk and the customer. The customer is responsible for onboarding users and managing their credentials and privileges. CyberArk is responsible for managing encryption keys and all the hardware and software components of the Privilege Cloud service, including the data repositories. The operator of the data center hosting the CyberArk Privilege Cloud shares the responsibility for the physical security of the solution in the hosting facility.

Responsibility	Customer	CyberArk	Data Center Provider
Backup and Restore		x	
Authentication and Authorization	x		
Encryption key management		x	
Physical Security		x	x

* Customers should follow the provided CyberArk best practice recommendations to maintain the highest levels of security. An example of this would be to utilize multi-factor authentication when connecting to the CyberArk Password Vault Web Access (PVWA).

AVAILABILITY

The CyberArk Privilege Cloud service provides its customers with 99% availability.

This availability level is achieved by orchestrating multiple services and solutions, to make sure that we have near constant uptime for the Privilege Cloud service.

How is it done?

CyberArk Privilege Cloud is deployed on an AWS platform and resides on three different Availability Zones (AZ), in a case of outages in one of the AZ data-centers. Each AZ includes the application and all the supported entities that are required for the proper functionality of the solution, monitoring and automatic triggered mitigations.

The monitoring systems collect all the service elements (OS metrics, system and applications log, network data, audit and components heartbeat), analyzes them and alerts in case of availability issues or other suspicious indications.

A watchdog service is responsible for triggering automatic procedures based on alerts generated by the monitoring system. The watchdog eliminates the need for human intervention in mitigating issues with the service (e.g. spin up a new application server in one or more AZs and terminate the old one without any manual steps.)

Note: Achieving 99% availability is calculated by excluding scheduled maintenance of the service.

CONCLUSION

CyberArk is first and foremost a security company. As such, all CyberArk products and services—including CyberArk Privilege Cloud—are designed with a "security-first" mindset based on 20+ years real-world privileged access security experience. CyberArk uses advanced encryption algorithms to protect data at rest and data in transit, hardens all CyberArk Privilege Cloud components to reduce attacks surfaces and supports multi-factor authentication and policy-based access controls to help avoid unauthorized access and data disclosure.

In addition, CyberArk Privilege Cloud core technology is submitted to external organizations for independent testing and security validation. Through this process, the CyberArk Privileged Account Security Solution has achieved ISO 9001, Common Criteria and United States Department of Defense UC APL certifications.

To learn more about these certifications or CyberArk Privilege Cloud, please contact your CyberArk sales representative or contact us at sales@cyberark.com.

©CyberArk Software Ltd. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 07.19. Doc. 367087481

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.