CYBERARK®

DATA SHEET

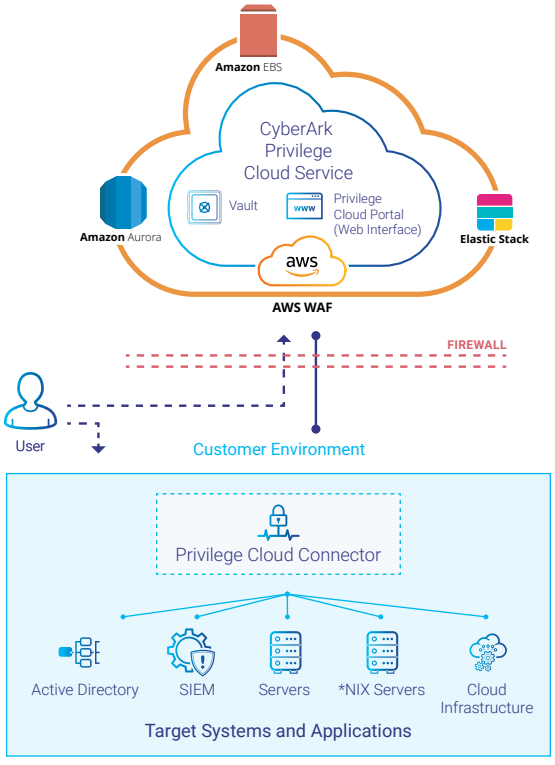
CyberArk Privilege Cloud® Security Overview

Introduction

CyberArk is the leading Identity Security provider, helping organizations secure access to critical business data and infrastructure, protect a distributed workforce and accelerate business the cloud. This includes the SaaS-based CyberArk Privilege Cloud which enables organizations to quickly achieve their privileged access management goals, delivered as a Service. While CyberArk Privilege Cloud is architected to simplify the task of protecting privileged access without having to manage additional on-premises infrastructure, CyberArk is also committed to delivering the most secure SaaS privileged access management offering, so that customers can trust their credentials remain well protected. This paper reviews the stringent security measures CyberArk takes to protect the data and privacy within CyberArk Privilege Cloud.

Built-In Security Measures

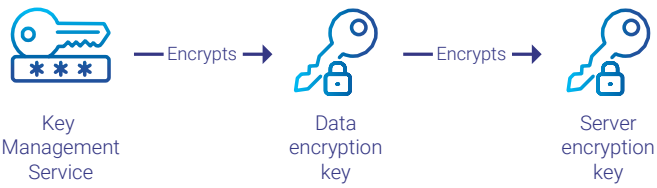
CyberArk Privilege Cloud is engineered for enhanced data durability, integrity and security and is fully SOC 2 Type 2 compliant and **SOC 3 certified**. Furthermore, the service is hosted in premier Tier IV data center facilities that are highly secure, fully redundant and certified for additional SOC 2 and ISO 27001 compliance. The service is built, managed, and secured according to industry standards. CyberArk encrypts data at rest and data in transit designed to avoid leakage and enable privacy, hardens all 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 Privilege Cloud service. The highly secure database maintains customers' 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. Secrets stored in Privilege Cloud are uniquely encrypted using a randomly generated AES-256 key.

This key is then envelope encrypted with a Customer Managed Key (CMK) stored in Amazon Web Services Key Management Service (AWS KMS). Access to data stored in the vault requires decrypt permission to all keys in the encryption hierarchy.



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 TLS websocket 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 Privilege Cloud back end and the 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 secured 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 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 service's security posture.

Stringent Database Access Control Mechanisms

CyberArk Privilege Cloud uses 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. CyberArk employees, as a default, do not have access to safes in which accounts are stored, but where exceptional circumstances require temporary access to assist customers, access is granted for authorized CyberArk employees pursuant to strict access control protocols. This database is encrypted, so even when CyberArk employees are required to do maintenance they do not access any of the data inside, and also are required to get consent from the organization running Privilege Cloud. CyberArk also utilizes the audit, monitoring and session isolation capabilities of Privilege On Premises to track and record the activity of CyberArk employees to assure 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

CyberArk Privilege Cloud supports multi-factor authentication (MFA) for improved security including out of the box capabilities with CyberArk Workforce Identity and Customer Identity. CyberArk strongly recommends customers use MFA for advanced protection. Privilege Cloud supports SAML MFA, LDAP and CyberArk Authentication.

Multi-factor authentication safeguards access to the sensitive information stored within 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 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 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 Web Interface.

Availability and Uptime

The CyberArk Privilege Cloud service provides its customers with 99.95% availability. The CyberArk Privilege Cloud availability is built out from the following pillars:

- **Amazon Relational Database Service (RDS) Aurora:** Every Privilege Cloud customer has their own schema within a shared RDS database. Amazon RDS provides high availability and failover support for DB instances using Multiple Availability Zone (AZ) deployments. Amazon commits to a 99.99% SLA for availability of RDS Aurora
- **Amazon Elastic Block Store (EBS):** All session recordings are stored within Amazon EBS, which offers reliability for mission-critical applications. Each volume is designed to protect against failures by replicating within the AZ. Amazon commits to a 99.999% for EBS

Additionally, the Privilege Cloud portal and vault instances are both fully immutable. They are provisioned automatically, all data is stored and located on the RDS & EBS and in the event of any issues new instances can be immediately and automatically created.

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. Privilege Cloud has 24x7 monitoring tools that constantly monitors the availability and health of all components within the service. Any issues are promptly sent to the operations team and swift resolution actions will be taken when needed. A team of Service Reliability Engineers are tasked with constantly improving Privilege Cloud availability by building additional monitoring tools and enhancing the automated mitigation capabilities of the service.

Privilege Cloud also has committed Service Maintenance, meaning (i) routine weekly maintenance performed by CyberArk during a pre- scheduled window; (ii) other system upgrades, enhancements or routine maintenance which is announced via email at least two days in advance; or (iii) emergency maintenance of the Services outside of the foregoing routine or pre- scheduled maintenance window that is reasonably required to complete the application of patches or fixes, or to undertake other urgent maintenance activities. CyberArk shall strive to limit the Service Maintenance window to the minimum possible to avoid service disruption. Please note that the Maintenance Window for upgrades typically occurs once every 4 months, and requires up to 15 minutes of downtime. Security patches typically occur on a monthly basis which occasionally results in a downtime due to restart that can take up to 4 minutes.

In most cases, the Recovery Time Objective (RTO), is near zero to within 20 minutes. Note that in rare disaster recovery scenarios, where data has to be completely restored from backups, RTO can be between 4-24 hours. For Recovery Point Objective (RPO), for system data, such as privileged accounts stored in the database, the RPO is just seconds from the time of failure, and up to 12 hours for recordings and configuration changes from the last working point.

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 99.95% availability is calculated by excluding scheduled maintenance of the service.

* All uptime and availability commitments will be set forth in the applicable agreement between CyberArk and the customer.

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 our expertise in privileged access management. 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 and has achieved SOC 2 Type 2 compliance. 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®