CYBERARK®

DATA SHEET

CyberArk Identity Technical Overview

November 2022*

CyberArk, a leading Identity Security provider, empowers organizations to secure access to critical business data and infrastructure, protect a distributed workforce, and accelerate business in the cloud. With CyberArk Identity, CyberArk's Identity and Access Management solution, organizations can quickly achieve their workforce identity security goals while enhancing operational efficiency. CyberArk Identity is a SaaS-delivered solution designed for easy consumption and scalability. This technical overview deep dives into the stringent security measures CyberArk has taken to protect the data and privacy within CyberArk Identity.

Built-in Security Measures

CyberArk Identity is engineered for enhanced data durability, integrity, and security and is SOC 2 Type 2 compliant. 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 and is designed to avoid leakage and enable privacy. It hardens all components to reduce attack surfaces and implements multi-factor authentication and policy-based access controls to protect against unauthorized access and data disclosure.

Data Center Locations

CyberArk currently runs SOC 2 Type 2 certified Identity-as-a-Service (IDaaS) on AWS datacenters in the USA, UK, Germany, Canada, Australia, India, Japan, Singapore, and other possible future locations. The Identity services can be accessed globally. For information on AWS security and compliance reports, please see **here**.

AWS data centers are housed in nondescript facilities where physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means. Authorized staff uses multi-factor authentication mechanisms to access data centers, and all physical access by employees is logged and audited routinely.

Data center access and information are only provided to employees and contractors who have a legitimate business need for such privileges, and when an employee no longer requires these privileges, their access is immediately revoked—even if they continue to be an Amazon employee. All visitors and contractors are required to present identification before being signed in and continuously escorted by staff.

For more information, please refer to **AWS Data Center Controls**.

* The information in this document is subject to change without notice.

CyberArk Identity Certifications & Compliance

- GDPR
- ISO 27001:2013
- ISO 9001:2015
- SOC 2 Type II
- CSA STAR Level 1
- FedRAMP High: In Process

For more, please refer to the CyberArk Trust Center.

Hierarchical Encryption for Data at Rest

Tenant data is stored in Amazon Aurora and encrypted (AES 256) using unique Tenant Keys. Tenant Keys are stored in a POD Global database, encrypted using a Pod Master Key. The Pod Master Key is encrypted using Amazon Web Services Key Management Service (AWS KMS) and stored in a Vault with very limited DevOps access upon well-defined SOC 2 complaint processes. CyberArk leverages multi-layered hierarchical encryption algorithms to protect the database and its data. An AES-256 key is used for symmetric encryption, and an RSA-2048 key pair is used for asymmetric encryption.

Encryption in Transit

All communications with the CyberArk Identity tenant use TLS 1.2 with strong encryption algorithms and keys (2048-bit RSA). Traffic between services inside AWS are encrypted using TLS 1.3 and each micro-service uses mutual TLS authentication.

Encryption when Integrated with Self-hosted CyberArk Password Vault

When the CyberArk Cloud is integrated with a self-hosted CyberArk Password Vault, the encryption is at rest on self-hosted CorePAS vaults (AES-256 encryption).

When the CyberArk Cloud is integrated with a self-hosted CyberArk Password Vault, end-to-end encryption is implemented between an end user's browser and the CyberArk self-hosted PAM Vault. This ensures that the business user's credentials which are stored and fetched from the Vault, cannot be decrypted by CyberArk Identity during transit. With this additional security measure, only the end-user can view and manage their business credentials in the CyberArk self-hosted PAM Vault.

- SHA-256 hashing is used when users update a stored password
- All connections are over TLS 1.2
- Asymmetric RSA 2048 is used for the encryption of passwords between the Identity Connector and the Browser or Browser Extension
- Connector calls are all outbound via port 443. No inbound ports are required.

* The information in this document is subject to change without notice.

CyberArk Connector Security

The CyberArk Identity Connector is required for integrating CyberArk Identity with on-premise directories, facilitating RADIUS authentication, or enabling access to internal web applications without the need for a VPN. The CyberArk Identity Connector is a lightweight Windows application that runs behind a customer's firewall to provide real-time authentication, policy, and access to user profiles without synchronizing directory passwords to the cloud. The CyberArk Identity Connector seamlessly integrates with Active Directory without opening extra ports in an organization's firewall or adding devices in their DMZ.

The CyberArk Identity Connector delivers the following security capabilities:

- For each tenant, a unique PKI Certificate is issued from the CyberArk Identity tenant to the CyberArk Identity Connector during registration
- All communications between the CyberArk Cloud and the CyberArk Identity Connector are encrypted and mutually authenticated for each tenant using these unique certificates
- All the traffic between the CyberArk Cloud and the CyberArk Identity Connector cannot be read by the AWS infrastructure
- All the traffic between the CyberArk Cloud and CyberArk Identity Connector is sent over TLS 1.2

User and Admin Portal Security

CyberArk Identity authenticates users from either the built-in CyberArk Identity tenant Directory, an external directory service such as Active Directory, or an external Identity Provider.

Password compliance can be enforced through CyberArk's built-in password policies for CyberArk Cloud Directory users, password policies from external directory services, or SAML integration with an external Identity Provider.

CyberArk Identity additionally provides multiple built-in security layers for accessing the Admin Portal, including CAPTCHA, security image, adaptive multi-factor authentication (MFA), and various other login attack mitigations for improved security. CyberArk can also integrate with third-party MFA solutions.

Administrative rights can be limited through delegated administration roles, application-level permissions, or delegated administrators for Organizations.

CyberArk Cloud Agent Security

CyberArk Cloud Agents connect to the Internet using corporate settings and communicate with the CyberArk Identity tenant over an SSL/TLS-encrypted tunnel for all types of communication (data sending and "keep alive" checks). The HTTPS connection to the service supports TLS 1.2 and above Cipher Suites. All data transferred between the agent and the CyberArk cloud over HTTPS is encrypted in transit.

Stringent Access Control Mechanisms

CyberArk employs strict policy-based access controls to protect the CyberArk Identity cloud infrastructure. CyberArk employees, by default, do not have administrative access to customer tenants, but temporary read-only access can be granted by customers in support situations. Tenant databases are encrypted, so even when CyberArk employees are required to do maintenance, they are not able to access any of the data inside. CyberArk uses a privileged Identity management system to manage and audit CyberArk personnel's access to the Identity cloud environment. The 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 logs on a target system.

CyberArk performs background checks on all CyberArk employees who have access to operate and support the service, and they are required to attend security awareness training. Access to Identity Services networks and systems is managed in accordance with our access policy and is granted only to individuals who are responsible for operating and supporting the Identity Services, based on least privilege principles. CyberArk service administrators perform all functions through a VPN connection. Segregation of duty isolates personnel who approve access from personnel who provide access. Access to the Identity cloud is periodically reviewed. Access rights of individuals who leave CyberArk are promptly revoked. Security logs of access by CyberArk personnel are collected and stored for six months.

Additionally, audit reports that include logins and actions performed by CyberArk personnel in the console are generated where required.

Third-party contractors are not allowed to connect to Identity SaaS production servers and systems.

Vulnerability Management

All Identity SaaS instances are scanned by an enterprise vulnerability management solution and handled according to **CyberArk's security vulnerability policy**. In addition, all security updates for the Operating System and critical applications are applied.

For more information, please refer to **CyberArk's security vulnerability policy**.

Penetration testing

CyberArk uses an internal penetration testing team and an external vendor to run automatic and manual penetration testing on CyberArk Identity, including network and web app vulnerability, at least annually.

Distributed Denial-of-Service (DDoS) Defense

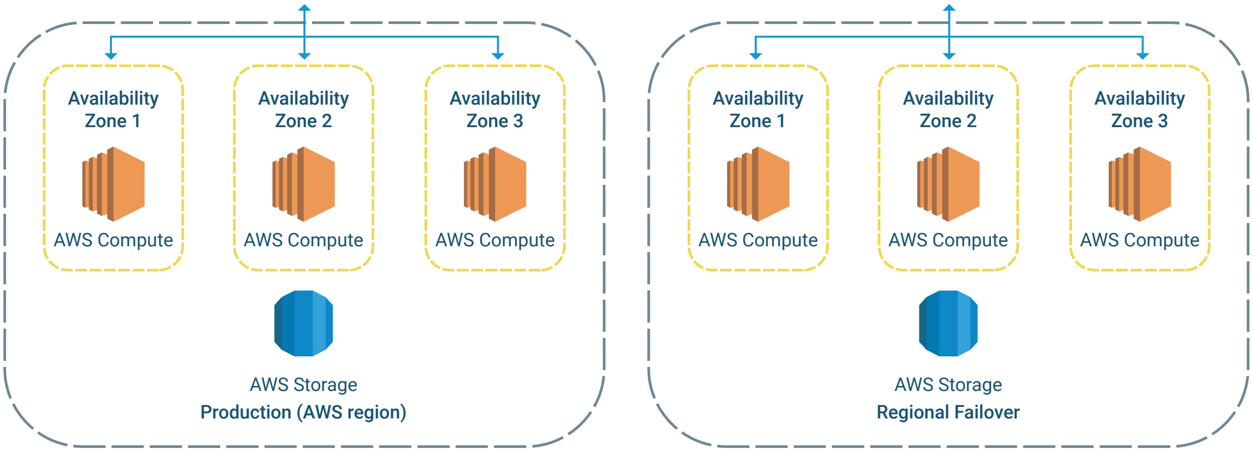
CyberArk utilizes technologies and platforms to detect, mitigate, and prevent DDoS attacks, such as Web Application Firewall (WAF).

Service Availability

The Identity Services SLA is detailed in the Identity SaaS Service Level Agreement (Service Availability) document. The uptime service commitment for CyberArk Identity is 99.99%. This availability level is achieved by orchestrating multiple services and solutions to make sure that we have near-constant uptime for the Identity service. Identity has 24x7 monitoring tools that constantly monitor 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 Identity availability by building additional monitoring tools and enhancing the automated mitigation capabilities of the service.

CyberArk 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 four months and requires up to 15 minutes of downtime. Security patches usually occur on a monthly basis which occasionally results in a downtime due to restart that can take up to 4 minutes.

CyberArk Identity is deployed on an AWS platform and replicated on three different Availability Zones (AZ), in case of outages in one of the AZ datacenters. Each Availability Zone includes the application and all the supported entities required for the solution's proper functionality, monitoring, and automatically triggered mitigations.



*Each AZ is at least 100 miles from the other AZs in the same region.

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

A watchdog service triggers automatic procedures based on alerts the monitoring system generates. 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 99.99% availability is calculated by excluding scheduled maintenance of the service.

* All uptime and availability commitments are subject to the terms and conditions set forth in CyberArk's Identity Service Level Agreement (Service Availability).

Disaster recovery and business continuity

CyberArk maintains disaster recovery and business continuity policies for the Identity Services, in which backup files are stored in S3 on a per Region basis and then programmatically updated on a daily basis to a DR Region.

To view the list of tenant and DR locations, please refer to CyberArk Identity component locations.

Recovery Point Objective (RPO)

The RPO for CyberArk Identity, is up to 24 hours from the last working point in time.

Recovery Time Objective (RTO)

The RTO for Identity SaaS is 24 hours, but recovery may occur between a few seconds and 24 hours, depending on the type of failure, although in most cases, it is much lower than 24 hours.

For more information, please refer to the Identity cloud status page.

* The information in this document is subject to change without notice.

Software Development Security

CyberArk Identity follows CyberArk's Secure Software Development Life Cycle, integrating security-related activities into the development cycle; this includes following industry security requirements, secure design practices, secure coding, security tests, code, and design reviews, etc. All security reviews are conducted against industry security standards (such as NIST and OWASP Top 10) and threat modeling (based on STRIDE methodology).

CyberArk Corporate Security Standards and Practices

In compliance with ISO 27001 and SOC 2, CyberArk applies strict security controls and practices to the CyberArk cloud infrastructure and CyberArk's corporate environment, including:

- Personnel security
- Network, application and infrastructure security
- Physical security
- Risk management
- Business continuity plan and disaster recovery plan

For more information, please refer to the CyberArk Corporate Security White Paper: Standards and Practices.

About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®

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.

* The information in this document is subject to change without notice.