



Service Organization Control Report - SOC3 Type 2

Report on CyberArk Software Ltd.'s
description of its Cloud Security system
for the period January 01, 2024 to
December 31, 2024



Table of contents

Section I - Report of Independent Service Auditor	3
Section II - Management of CyberArk Software Ltd.'s Assertion	6
Section III - CyberArk Software Ltd.'s Description of its Cloud Security System	8

Section I

Report of
Independent
Service Auditor



Report of Independent Service Auditors

To the Management of CyberArk Software Ltd.

Scope

We have examined CyberArk Software Ltd.'s (the "Service Organization") accompanying assertion titled "Assertion of CyberArk Software Ltd.'s Service Organization Management" (the "assertion") that the controls within CyberArk Software Ltd. Cloud Security system (the "system") were efficient throughout the period January 01, 2024 to December 31, 2024, to provide reasonable assurance that CyberArk Software Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service organization's responsibilities

CyberArk Software Ltd. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved. In Section II, the Service Organization has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, CyberArk Software Ltd. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service auditors' responsibilities

Our responsibility is to express an opinion on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve CyberArk Software Ltd.'s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve CyberArk Software Ltd.'s service commitments and system requirements based on the applicable trust services criteria



Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within CyberArk Software Ltd.'s Cloud Security system were effective throughout the period January 01, 2024 to December 31, 2024, to provide reasonable assurance that CyberArk Software Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material aspects.

Restricted Use

This report is intended solely for the information and use of CyberArk Software Ltd., user entities of CyberArk Software Ltd.'s system during some or all of the period January 01, 2024 to December 31, 2024, business partners of CyberArk Software Ltd. subject to risks arising from interactions with the system, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the organization's service commitments and system requirements.

A handwritten signature in blue ink, appearing to read 'Kesselman & Kesselman', is written in a cursive style.

Tel-Aviv, Israel
January 23, 2025

Kesselman & Kesselman
Certified Public Accountants (Isr.)
A member firm of PricewaterhouseCoopers International Limited

Section II

Management's Assertion



Management of CyberArk Software Ltd.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within CyberArk Software Ltd. Service Organization's (CyberArk Software Ltd.'s) Cloud Security system (system) throughout the period January 1, 2024, to December 31, 2024, to provide reasonable assurance that CyberArk Software Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in [TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy](#), in *AICPA Trust Services Criteria*. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2024, to December 31, 2024, to provide reasonable assurance that CyberArk Software Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria. CyberArk Software Ltd.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2024, to December 31, 2024, to provide reasonable assurance that CyberArk Software Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by:

B5FBDC05A075481...

Omer Grossman,
Chief Information Officer

Section III

Service
Organization's
Description of its
System

Company Background

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.

Description of Services Provided

Focused on protecting human and non-human identities in the cloud, CyberArk Cloud Security SaaS solutions provide seamless, secure access to their full cloud estate, whilst working to constantly drive the implementation of the principle of least privilege.

CyberArk Cloud Security can help organizations address the connected problems of entitlements sprawl, limited visibility and context around cloud access, and the imperative for velocity in software development. These connected problems require holistic solutions. It is essential for organizations to enhance their cloud identity security hygiene by implementing three practical and progressive steps.

CyberArk Cloud Security

CyberArk Cloud Security solutions covered in this report primarily includes following two services

- Secure Cloud Access (SCA)
- Cloud Entitlement Manager (CEM) / Cloud Visibility

Secure Cloud Access is a CyberArk Identity Security Platform service that provisions access just-in-time with zero-standing privileges to cloud management consoles and services running in AWS, Microsoft Azure (Azure) and Google Cloud Platform (GCP) environments. Secure Cloud Access elevates access just-in-time to roles scoped with just enough permissions to adhere to the principle of least privilege.

By elevating access just-in-time, Secure Cloud Access enables technical teams with permissions to do their job while reducing the risks of credential theft and excessive access. Secure Cloud Access allows users to launch sessions that are protected and monitored natively removing the need to go through a jump server. This enables seamless access while reducing risk and keeping the visibility of end-user behavior to satisfy audit. In the event of a critical situation, Engineers can request unplanned On-Demand elevation of access. Enabling security personnel or application owners the option to control (approve) access, and enabling technical teams, to securely request and rapidly receive the elevated entitlements needed to save the day.

Cloud Entitlement Manager / Cloud Visibility helps organizations identify identity misconfiguration risks and their impact on compliance with regulations; detect dormant identities and excessive permission. Armed with visibility and context of IAM policy across multi-cloud environments, organizations can take highly educated actions to remediate risk without changing how users interact with the cloud.

Principal Service Commitments and System Requirements

CyberArk designs its processes and procedures related to CyberArk Cloud Security SaaS Services System to meet its objectives for its CyberArk Cloud Security SaaS Services System. Those objectives are based on the service commitments that CyberArk makes to user entities, the laws and regulations that govern the provision of CyberArk Cloud Security SaaS Services System, and the financial, operational, and compliance requirements that CyberArk has established for the service. The CyberArk Cloud Security solution of CyberArk is subject to the security and privacy requirements of the relevant privacy and security laws and regulations in the jurisdictions in which CyberArk operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

- Security concepts within the fundamental designs of the CyberArk Cloud Security SaaS solution are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

CyberArk establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in CyberArk's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Cloud Security SaaS solution.

Components of the System

Infrastructure

Primary infrastructure used to provide CyberArk's Cloud Security Services System is in a serverless environment that leverages AWS Lambda functions and includes the following:

Primary Infrastructure	
Production Tool	Business Function
AWS Athena	Serverless interactive query service to analyze customer data
AWS DynamoDB	NoSQL customer database. Persist application data: policies, tenants information, group mappings, checkpoints, audit sessions
AWS Open Search	Index subset of the data to allow free text search
AWS RDS	Relational database to store findings detected on customer cloud environments
AWS Event Bridge	Event bus to route data from event sources to AWS Lambda
AWS Step Functions	Serverless microservice orchestration
AWS Lambda	Serverless compute service
AWS S3	Data store. Data acquired from CSPs, telemetry events persisted in S3, per tenant, per day
AWS Neptune	Graph database
AWS CloudFront	Content Delivery Network
AWS API Gateway	AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs A layer 7 proxy for SCA's backend. It has validation rules and a lambda authorizer which authorizes the backend calls before invoking the lambdas
AWS Cloud Front	Use to host the UI
AWS SSM	Use to persist application configurations and tenant's feature flags
AWS KMS	Keys encryption

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

Primary Infrastructure	
Production Tool	Business Function
AWS Secrets Manager	Manage customer's service account secrets which SCA uses to manage the customer accounts
AWS ElastiCache	Out of process distributed cache that is used to cache tokens, GCP org names and other temporal information for SCA
AWS Backup	Continuously backup SCA's data and before a deployment
AWS SQS	Reliable message queue. Use for communication between micro-services
AWS SNS	Notification service (pub-sub). Use to notify other services that something happens
AWS Athena	Use for telemetry
AWS Kinesis Firehose	Near real-time event router. Currently, it is used for Telemetry. It aggregates telemetry events, enriches them and persists them in S3
AWS Quick Sight	Use for Telemetry visualization
AWS Glue	Help with mapping the data between S3 to Athena
Step Functions	State machine functions that are used for long running waiting process

The in-scope system and supporting infrastructure are hosted by AWS. As per AWS Shared Responsibility Model, AWS provides managed services such as AWS Lambda where the full responsibility of the underlying infrastructure, foundation services, patching and administration is under AWS responsibility.

Software

The primary software used to provide CyberArk's Cloud Security Services System includes the following:

Software	
Production Application	Business Function
AWS CloudWatch	Application and infrastructure monitoring
AWS DynamoDB - Snapshots	Backup/Replication
AWS CloudTrail	Logging
AWS Secrets Manager	Manage production secrets
Microsoft Endpoint Manager	Anti-virus
Snyk	scan, prioritize, and fix security vulnerabilities in your code, open source dependencies, container images, and infrastructure as code
GitHub	VCS
JIRA	Helpdesk/Ticketing system

People

CyberArk staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations.
- Development team - responsible for delivering a responsive system that fully complies with the functional specification.
- Quality assurance team - verifies that the system complies with the functional specification through functional testing procedures.
- System administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by CyberArk in delivering its CyberArk Cloud Security SaaS Solution. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications.
- Alert notifications received from automated backup systems.
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS alerts, or automated patching systems.

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

Processes, Policies and Procedures

Formal Information Technology (IT) policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the CyberArk's policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any CyberArk team member.

Physical Security

Employees are provided with card access and granted access to CyberArk Offices as defined by their roles. The access card/ID system is used to control access in order to enter an office. Certain areas are more sensitive than others and require extra security. Visitors in CyberArk Offices must be escorted and follow the company guidelines beyond the entrance point. Visitors must present a clearly visible visitor badge. Upon an employee's termination of employment, the access is disabled from the facility. The Chief Information Security Officer (CISO) is responsible for assessing and providing physical security solutions to all CyberArk Offices globally.

CyberArk Cloud Security SaaS solution runs on AWS datacenters which are Service Organization Control (SOC) 2 Type II certified, with fully redundant power backup systems, fire suppression systems, and security guards. All data centers are hardened against physical intrusion, and server room access is limited to certified employees.

Logical Access

CyberArk uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. The procedures include the life cycle of user access from the initial registration to the de-registration of users who no longer need access. Resources are protected using native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. Segregation of duty is in place between the group that approves the access and the group that provides the access.

Asset management procedures are in place to define the process of receiving, tagging, documenting and disposing of the equipment. An information security steering committee consisting of the Chief Executive Officer (CEO), General Manager (GM), Chief Information Officer (CIO) and CISO holds periodic meetings to review the information security projects and other necessary management activities.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion. Business-related data is protected by regular backups performed per schedule. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately. The IT department practices procedures to store information to prevent unauthorized use. Periodic restores are performed on certain defined files.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

CyberArk monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements.

CyberArk evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Network bandwidth

CyberArk has implemented a patch management process to ensure contracted customers and infrastructure systems are patched in accordance with vendor-recommended operating system patches. CyberArk's business continuity plan and disaster recovery plans are designed to provide solutions in case of disasters and unexpected interruptions.

Change Control

CyberArk maintains documented change management policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing results are maintained for the changes. Development and testing are performed in an environment that is logically separated from the production environment. Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal Internet Protocol (IP) addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure including firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place. Penetration testing is conducted to measure the security posture of a target system or environment. Vulnerability scanning is performed as a part of the penetration testing. Authorized employees may access the system from the Internet through the use of Virtual Private Network (VPN) technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the CyberArk Cloud Security SaaS solution system performed at CyberArk facilities and/or by its personnel working remotely.

This report does not include the cloud hosting services provided by AWS performed at various facilities.

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of CyberArk's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of CyberArk's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Employees are required to sign a non-disclosure agreement upon hire.
- The hiring process for candidates at CyberArk includes external reference checks. These checks may also include verification of education and previous employment history. Where local labor law or statutory regulations permit, CyberArk may also conduct criminal, credit, immigration and security checks, depending upon the specific jurisdiction and position.

Commitment to Competence

CyberArk's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

CyberArk's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

CyberArk's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

CyberArk's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resources Policies and Practices

CyberArk's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization operates at maximum efficiency. CyberArk's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- According to applicable laws in each jurisdiction, new employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

Risk Assessment Process

CyberArk's risk assessment process identifies and manages risks that could potentially affect CyberArk's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. CyberArk identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of CyberArk's Cloud Security SaaS solution system; as well as the nature of the components of the system result in risks that the criteria will not be met. CyberArk addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, CyberArk's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of CyberArk's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At CyberArk, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly and monthly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate CyberArk personnel via e-mail messages.

Specific information systems used to support CyberArk's Cloud Security SaaS services system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. CyberArk's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Incident Response Controls

CyberArk maintains a formalized incident response plan (IRP) and policy. The incident response policy defines how security incidents are identified, classified, reported, remediated and mitigated throughout incident response stages including post-incident assessments. The CyberArk information security

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

department promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. On an annual basis, CyberArk performs an incident response drill to assess the effectiveness of its incident response plan and activities.

On-Going Monitoring

CyberArk's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in CyberArk's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and maximize the performance of CyberArk's personnel.

Reporting Deficiencies

An internal tracking tool and files are utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common, Availability and Confidentiality criteria were applicable to CyberArk's Cloud Security SaaS solution system.

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at various facilities.

Subservice Description of Services

CyberArk leverages a variety of AWS offerings for hosting CyberArk platform infrastructure. AWS allows for secure, scalable and redundant utilization of cloud computing, storage and network resources. The listing of utilized AWS services is detailed under the “Components of the System: Infrastructure” section of this document.

Complementary Subservice Organization Controls

CyberArk’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the control objectives related to CyberArk’s services to be solely achieved by CyberArk control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of CyberArk.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the control objectives described within this report are met.

Subservice Organization - Amazon Web Services		
Category	Criteria	Control
Security, Availability	CC4.1, CC5.1, CC7.5, A1.3	Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.
		AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.
Security	CC6.1, CC6.8, CC7.1, CC7.2, CC7.5, CC8.1	For AWS Serverless services, AWS manages the underlying infrastructure and foundation services, the operating system, and the application platform.
		AWS applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on Amazon guidelines and tailored to the specifics of each AWS service.
		AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet.
Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

Subservice Organization - Amazon Web Services		
Category	Criteria	Control
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Security, Confidentiality	CC6.5, C1.2	All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
		AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
		AWS retains customer content per customer agreements.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		S3-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		S3-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
		S3-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		RDS-Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

Subservice Organization - Amazon Web Services		
Category	Criteria	Control
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

CyberArk management, along with the subservice organization, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, CyberArk performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and the subservice organization.
- Monitoring external communications relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

CyberArk's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to CyberArk's services to be solely achieved by CyberArk control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of CyberArk.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to CyberArk.
2. User entities are responsible for notifying CyberArk of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of CyberArk services by their personnel.
5. User entities are responsible for providing CyberArk with a list of approvers for security and system configuration changes for data transmission.
6. User entities are responsible for immediately notifying CyberArk of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
7. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize CyberArk services.
8. User entities are responsible for user access administration in the CyberArk SaaS product, including reviewing access for their personnel as needed.

This report is intended solely for the use by the management of CyberArk Software Ltd. And the specified parties, and is not intended and should not be used by anyone other than these parties

9. User entities are responsible for exporting any customer data from the SaaS product to which they desire continued access to within 60 days of termination or expiration of the customer's subscription term.