



Cloud Security Standard

DOC-IT-IS-15-2
Revision 2.0
NOVEMBER 1, 2025

REVISION HISTORY

This revision history lists all changes to this document, the date of each revision, and the reason for each revision.

<u>Rev.</u>	<u>Rev. Date</u>	<u>Revision Description</u>
1.0	11/01/2022	Initial Version
2.0	11/01/2025	RXO, Inc. Revisions, annual review

Table of Contents

1 Executive Summary4

2 Purpose.....4

3 Scope.....4

4 Cloud Security Standard5

 General Requirements.....5

 Security Stack Requirements6

 Definitions.....10

1 Executive Summary

This document provides a framework for cloud security requirements for the four major CSP's (Cloud Service Providers), AWS, Azure, GCP, and OCI. As RXO, Inc. including its subsidiaries, divisions and any other entities (collectively, "RXO") continues to move more services to the cloud, the security requirements traditionally covering on-premise devices must be adjusted to fit the unique risks created by moving to IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) cloud deployment models.

Each hosting provider has different tools to accomplish security requirements. In some cases, the preference will be for the current RXO solution. In other cases, the value-add for the additional tools is more advantageous. For some solutions, there are no comparable controls that can be put in place for specific requirements. The matrices covering each section break down the approved tools matching the requirements identified by the GSO.

This standard should be used in conjunction with the Cloud Security Requirements developed by the CCOE, as well as the RXO Project Security Assessment.

2 Purpose

The purpose of the RXO Cloud Security Standard is to provide information security requirements for the provisioning and management of cloud-based services.

3 Scope

This standard applies to RXO, Inc., including all subsidiaries, divisions, and operating entities. All directors, officers, employees, contractors, and third parties acting on behalf of RXO must comply with this policy.

Cloud based application, services, and systems hosted on Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP) and OCI. Services included in scope would include hosted virtual machines (VMs), bare metal devices hosted offsite, hosted services (including but not limited to web, mail, FTP, database, etc.), and enclave networks.

Systems or processes that cannot comply with these standards require an exception from the GSO.

4 Cloud Security Standard

General Requirements

DATA PROTECTION REQUIREMENTS

- RXO Information stored on cloud services must be protected according to the RXO Information Classification Standard and any requirements set forth in customer contracts

NETWORK REQUIREMENTS

- All hosts and services should be behind a firewall with only ports required for operation and management open.
- All traffic ingressed from the internet must be protected with a WAF.
- Traffic that contains confidential or sensitive data must be encrypted in transit using approved encryption protocols.
- All enclave networks must be protected by an IPS, whether a virtual appliance or by routing traffic through the RXO managed datacenters.
- Management access should be restricted to trusted RXO sites or trusted devices.
- Remote User Access - Only authorized users are permitted to access the network remotely.
- Third Party Access – A risk assessment must be completed by the BU BISO prior to providing access to a third party.
- Site to site connections must be reviewed and approved by the networking and security teams prior to implementation.

OPERATING SYSTEM REQUIREMENTS

- New deployments should be released at the most current stable OS version.
- The RXO Server Security Standard must be followed when configuring a server operating system.
- All cloud hosted virtual machines must have the security stack, as defined in this document, installed, and configured prior to hand-off to the business owner.
- Server operating systems must be at the current patch revision and go through the vulnerability scanning process prior to hand-off to the business.
- A standard patching lifecycle must be defined and followed.
- Management access should be restricted to trusted RXO sites or trusted devices.

APPLICATION REQUIREMENTS

- The application owner must define the ports used by the application to be documented in the CMDB.
- In-house development of applications must go through code review processes before deployment.
- Outsourced applications must be properly vetted by the BISO prior to deployment. These applications must also be updated as per vendor recommendations and timelines.
- Any dependencies for applications must be tracked and updated
- Architectural diagrams, application information, and application ownership should be cataloged in the CMDB for troubleshooting purposes.
- All applications should undergo the SAST and DAST testing as approved by the GSO and be in compliance and meet the release requirement.

ACCESS CONTROL REQUIREMENTS

- Passwords to cloud environments must follow the requirements in the RXO Password Management Standard.
- Role Based Access Controls should be put in place for group management and usage, including but not limited to the platform, VMs, and applications.
- Unique service accounts should be used for each task requirement. Where possible, managed service accounts should be used. Service accounts must adhere to the service account policy for interactive logon as described in the RXO Access Control Policy. Users should be provisioned and managed according to the RXO Identity team. This includes a best effort to use a preexisting identity provider for external services to centrally manage roles and accounts.

CLOUD PLATFORM HARDENING REQUIREMENTS

- Where applicable CIS Benchmarks must be used as a guide for securing the cloud platform.
- When CIS Benchmarks conflict with RXO policies, RXO policies should be followed.
- Cloud platforms without a CIS Benchmark should be referred to the appropriate BISO for additional hardening requirements.

Security Stack Requirements

All RXO cloud instances must be enrolled in the relevant cloud posture management tool. Currently this is ORCA for GCP and Azure, and Prisma for OCI.

VIRTUAL MACHINES (VMS)

All CSP's provide the ability to host Windows or Linux virtual machines (VM) in a cloud environment. In this Platform as a Service scenario, RXO is responsible for maintaining the OS as well as the installed applications without the need to manage the underlying hypervisor and hardware.

The current security stack used by the GSO is available for use if the underlying OS chosen is compatible with the individual applications.

The expectation for virtual machines is that, prior to going into production, the tools listed in the VM Security Stack Reference Chart must be installed and configured.

VM SECURITY STACK REFERENCE CHART

Requirement	Azure	AWS	Google	Oracle
Endpoint Protection	Crowdstrike	Crowdstrike	Crowdstrike	Crowdstrike
Integrity Monitoring	Crowdstrike	Crowdstrike	Crowdstrike	Crowdstrike
Malware Monitoring	Crowdstrike	Crowdstrike	Crowdstrike	Crowdstrike
Anti-Exploit Protection	Crowdstrike	Crowdstrike	Crowdstrike	Crowdstrike
Script Control	Crowdstrike	Crowdstrike	Crowdstrike	Crowdstrike
Endpoint Management	Tanium	Tanium	Tanium	Tanium
Deployment Capabilities	Tanium	Tanium	Tanium	Tanium

Behavioral Analysis	Tanium	Tanium	Tanium	Tanium
Network Protection				
Cloud Proxy	Zscaler	Zscaler	Zscaler	Zscaler
Firewall	Azure Firewall	Palo Alto	Google Firewall	Oracle Firewall
Log Aggregator				
Host-Based Logging	Chronicle	Chronicle	Chronicle	Chronicle
Service-Based Logging	Chronicle	Chronicle	Chronicle	Chronicle
Forensics				
Image Capture	EnCase	EnCase	EnCase	EnCase
Evidence Gathering	EnCase	EnCase	EnCase	EnCase
Remote Vulnerability Management				
Vulnerability Scanning	Insight VM	Insight VM	Insight VM	Insight VM
Patch Management				
Access Logging	Chronicle	Chronicle	Chronicle	Chronicle
Deployment Capabilities				
Authentication	On-Prem, AAD or Local	On-Prem, AAD or Local	On-Prem, AAD or Local	On-Prem, AAD or Local
Health Monitoring				
	Solarwinds	Solarwinds	Solarwinds	Solarwinds

DATABASES

Database services is an IaaS offering from the CSP's without the overhead of managing a virtual machine or the underlying infrastructure. These databases will most likely be used in support of apps also hosted at the CSP's environment, giving a need for proactive monitoring and protection. These databases should not be directly accessible from the internet and should be managed in accordance with the standards laid out in this document.

All logging for these services should be shipped to the SIEM standard currently in use by RXO. As of the current draft, Chronicle should be used with logs sent to an internal Chronicle UF through ExpressRoute for Azure and AWS and through Google Cloud Interconnect for Google.

The expectation for databases is that, prior to going into production, the tools listed in the Database Security Stack Reference Chart must be installed and configured.

DATABASE SECURITY STACK REFERENCE CHART

Requirement	Azure	AWS	Google	Oracle
Network Protection				
Firewall	Azure Firewall	AWS Firewall	GCP Firewall	Oracle Firewall
IPS	Palo Alto	Palo Alto	Palo Alto	Palo Alto
Log Aggregator				
Host-Based Logging	Chronicle	Chronicle	Chronicle	Chronicle
Service-Based Logging	Chronicle	Chronicle	Chronicle	Chronicle
Remote Vulnerability Management				
Vulnerability Scanning	Insight VM	Insight VM	Insight VM	Insight VM
Patch Management				
Access Logging	Chronicle	Chronicle	Chronicle	Chronicle
Authentication				
	AAD	AAD	Federated AAD	AAD
Health Monitoring				
	Solarwinds / Azure	Solarwinds / Azure	Solarwinds / GCP	Solarwinds/Oracle

CLOUD SERVICES

Cloud Services can be used to create applications and APIs by developers. OS and available applications are updated and patched automatically, with health checks and monitoring built in.

OS access is not available and infrastructure access is not available. You will be limited as to what you can add from our security stack. **This makes it imperative to ensure the CSP's are meeting our expectations outlined in all SLA/PLA, Contracts and SOC reports.**

Relative to Azure, Cloud services should utilize Microsoft Antimalware for Azure Cloud Services and VMs for protection. Using the same platform as Windows Defender, Microsoft Antimalware for Azure is a single-agent solution for apps and tenant environments, scaling with the environment. Realtime protection and scheduled scans are baked in, with remediation for malware removal. Exclusions can be managed by designated administrators to ensure compatibility with hosted applications.

The expectation for services is that, prior to going into production, the tools listed in the Cloud Services Security Stack Reference Chart must be installed and configured.

CLOUD SERVICES SECURITY STACK REFERENCE CHART

Requirement	Azure	AWS	GCP	Oracle
Endpoint Protection				
Integrity Monitoring	Azure antimalware	AWS Managed	GCP Cloud Security Scanner	Oracle Managed
Malware Monitoring	Azure antimalware	AWS Managed	GCP Cloud Security Scanner	Oracle Managed
Network Protection				
Firewall	Azure Firewall	AWS Firewall	GCP Firewall	Oracle Firewall
IPS	Palo Alto	Palo Alto	Palo Alto	Palo Alto
Log Aggregator	Chronicle	Chronicle	Yes	Chronicle
Host-Based Logging	Chronicle	Chronicle	Chronicle	Chronicle
Service-Based Logging	Chronicle	Chronicle	Chronicle	Chronicle
Remote Vulnerability Management	Insight VM	Insight VM	Insight VM	Insight VM
Vulnerability Scanning	Insight VM	Insight VM	Insight VM	Insight VM
Patch Management	Azure	AWS	GCP	Oracle

Access Logging	Chronicle	Chronicle	Chronicle	Chronicle
Authentication	AAD	AAD	AAD	AAD
Health Monitoring	Solarwinds	Solarwinds	Solarwinds	Solarwinds

Definitions

CSP – Cloud Service provider; Azure, AWS, Google or Oracle.

Customer Data – Any information shared between RXO and the customer, or private to the customer.

Enclave Networks – Also referred to as virtual networks. Private network used to facilitate communication between backend services.

Hosted Services – Network based service where the underlying OS is managed by the hosting provider rather than RXO, but the service itself is.

Logging:

Service Monitoring – Mandatory auditing and alerting on service and application health. Chronicle Audit Logging – Access and authentication logging.

Application Logging – Diagnostic and transactions.

Alerting – Stability alerts should be sent to infrastructure and application teams. Security alerting should be designed and sent to the SOC.

Point to Point Network – A connection between a cloud provider and an RXO managed datacenter that provides communication between on-prem and cloud resources.

Proprietary Data – Any information that is RXO or partner owned that is not for public dissemination.

Public Data – Any information that is freely obtainable and has no negative impact to the company.

Virtual cloud hosted machine – Any virtual machine operated and hosted from a remote cloud server where the operating system is managed by RXO.

Certificate of Review

Cloud Security Standard

December 18th 2025 10:27:54 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 3:01 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:59 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:27 AM EST