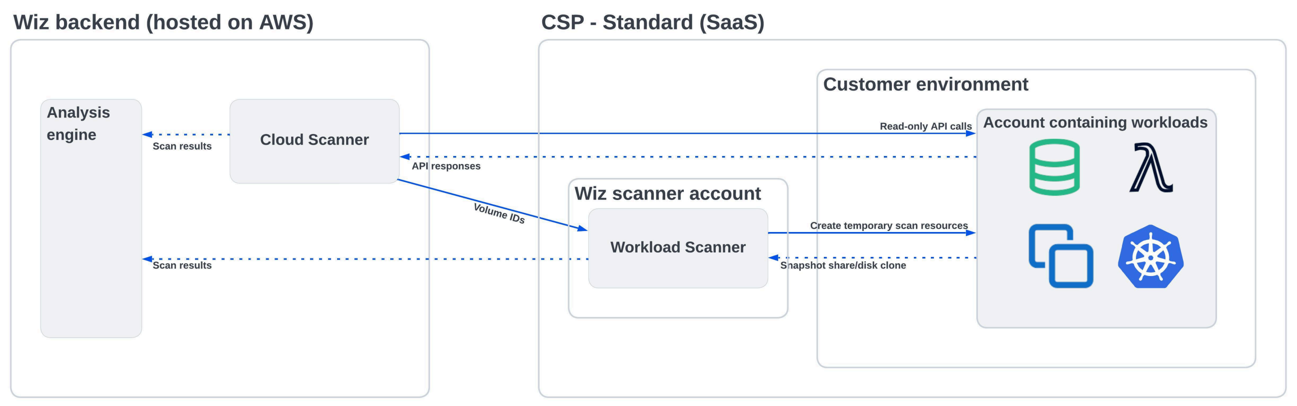
Agentless Scanning

Wiz uses several techniques to scan your entire cloud environment without a single agent or sidecar deployed on your workloads. This assures that you can get Wiz up and running across your environment in minutes without suffering from the coverage gaps that the limited deployment of agents typically causes.

How it works



* The Wiz backend resides only in AWS, while the Workload Scanner clusters can be found in each Wiz account in the CSPs. Therefore, this schema slightly varies in an AWS scenario, since there the Workload Scanner and the Wiz backend are hosted on the same CSP (but in different accounts).

Wiz's Connectors are agentless cloud-native scanners that leverage your CSP's platform APIs to perform a full-stack analysis of your environment across networks, identities, vulnerabilities, secrets, application endpoints, and more. The Workload Scanner scans workloads and data and resides in the same CSP region as your workloads and data stores. It leverages both dynamically allocated public IPs and service/VPC endpoints.

The analysis is performed in two phases:

Phase 1: Cloud API interrogation

The Cloud Scanner connects using read-only permissions to your cloud APIs (AWS, Azure, GCP, OCI, Kubernetes, etc.) in order to list your cloud resources and interrogate the control plane for their configuration.

Phase 2: Workload scanning

Agentless scanning is the new way to perform workload scanning. Instead of using an intrusive agent, Wiz leverages cloud-native tools to perform scans without interrupting or impacting production workloads. Just like an MRI performs a 3D scan of the body without affecting the body itself, agentless scanning achieves deep analysis of the workload without any impact or interruption to the live workload.

At its core, agentless scanning is a very simple process. In order to scan the workload, a snapshot or a disk is created from the running workload and is then scanned by Wiz to extract vulnerabilities, secrets, malware, and misconfigurations. This is a non-intrusive process that happens at the cloud platform level without impacting the workload's performance or operation in any way.

The results of the scan are then sent back to the Wiz backend. For a detailed list of the results sent, see below.

> ✓ The read-only CSP APIs do not incur any additional costs to your CSP account billing. The Workload Scanner incurs a minor cost due to the snapshot storage in your environment.

Depending on the CSP, the workload scanning process leverages either disk cloning or snapshots to scan the disks; disk cloning is the preferred method since it is more efficient and is used whenever possible.

Workload scanning using disk cloning (GCP, OCI, and Azure non-ADE encrypted disks)

1. Scan configuration—A list of OS and non-OS (if enabled) disks for scanning is composed by the Cloud Scanner, leveraging the CSP's platform APIs. It is then sent to the Wiz Workload Scanner.
2. Disk creation—The Workload Scanner[1] creates disks directly in the Wiz/Outpost scanning account, leveraging cloud-native APIs. No temporary resources are created during this process in the scanned account.
3. Disk scan—The disks are mapped as read-only volumes and scanned. The scan results are sent to the Wiz backend and include metadata on vulnerabilities, secrets, malware, and misconfigurations.
4. Removal of scan resources–Once the analysis of the disk is completed, the disks are deleted from the scanning environment.

> [1] The Workload Scanner runs in a dedicated account or it can be deployed via Outpost (learn about Wiz Outpost).

Workload scanning using snapshots (AWS and Azure ADE encrypted disks)

English ▲

1. Scan configuration—A list of OS disks for scanning is composed by the Cloud Scanner, leveraging the CSP's platform APIs. It is then sent to the Wiz Workload Scanner.
2. Snapshot creation—The Workload Scanner[1] creates snapshots and shares them with the scanner cluster. These snapshots are created with both the original tags of the scanned volume (to accommodate for customer-defined policies) and a `wiz:auto-gen-snapshot` tag, to help identify them. They are the same size as their corresponding VM system volumes. By default, they are stored in the same region as the VM[2].
3. Snapshot scan—The snapshots are mapped as read-only volumes and scanned. The scan results are sent to the Wiz backend and include metadata on vulnerabilities, secrets, malware, and misconfigurations.
4. Removal of scan resources–Once the analysis of the disk is completed, the disks are deleted from the scanning environment.
5. Cleanup—When a scan is completed, the snapshots are immediately deleted from the scanned account.
6. Garbage collection—A "garbage collection" process runs on a daily basis and deletes all scans created by Wiz to ensure no stale snapshots remain in your environment.

> [1] The Workload Scanner runs in a dedicated account or it can be deployed via Outpost (learn about Wiz Outpost).
>
> [2] In Azure, it is possible to specify a Resource Group in which all snapshots are created.

Scan frequency

Wiz automatically scans your entire environment every ~24 hours. Scan duration varies depending on the number of resources and disks contents. By default, Wiz can scan up to 20 disk snapshots concurrently.

You can initiate manual scans on an individual resource from its details drawer, on a Subscription, or on a Connector. You cannot, however, schedule scans of your entire environment for a specific time of the day, since Wiz's scans are staggered and optimized to avoid overloading the Wiz backend. This means there is some inherent variability around when exactly each Subscription, VM, etc. was last scanned and will be scanned again.

> Non-OS disk scanning is disabled by default. You can enable it to improve risk detection. Enabling non-OS disk scanning generates additional billable workloads.

English ▲

Inactive VMs

Wiz also scans inactive VMs, which are no less risky than active VMs for several reasons:

- A VM can be turned on very easily. It's better to know about its risks before it is turned on.
- VMs can be turned off for good security reasons, but you still want to know about their potential risks.
- A VM that was safe when it was turned off can become unsafe due to newly disclosed vulnerabilities, other infrastructure changes, etc.
- With sufficient permissions, malicious actors can identify vulnerable inactive VMs in much the same way Wiz does, turn them on, and then move laterally through your environment, escalate privileges, or gain access to sensitive data.

Ephemeral resources

Because there is no single attribute across all cloud providers that identifies a resource as ephemeral, Wiz uses an in-house dictionary that captures different types of short-lived resources. These various definitions are normalized on the Security Graph as the ephemeral property.

All ephemeral resources that exist when the snapshot is created are represented on the Security Graph. Moreover, Wiz groups all ephemeral resources instantiated from the same parent into a single Compute Instance Group, which is a persistent object on the Security Graph. All Issues associated with ephemeral resources are attached to their parent Compute Instance Groups in order to prevent duplication. Findings and vulnerabilities are still associated with the ephemeral VMs within the Compute Instance Group.

> ⚠ Wiz does not retroactively track the number of ephemeral resources, so the number of ephemeral resources in a Compute Instance Group does not reflect its "history". For instance, if a particular Compute Instance Group included 1,000 VMs at 10:00 am but 990 of them were taken down at 12:00 pm, then Wiz would show only the 10 VMs that still existed when the scan occurred the following night.

Compute instance groups

Wiz groups together VMs and presents them as compute instance groups in three cases:

1. Native groups in the CSPs (which are normalized in Wiz)
2. Synthetic groups created by tags you define in Wiz

English ▲

3. Synthetic groups identified by Wiz based on a closed list of common tags from the CSPs:
    i. `spotinst:aws:ec2:group:id`
    ii. `aws:ec2:fleet-id`
    iii. `gitlab_autoscaler_token`
    iv. `goog-dataproc-cluster-uuid`
    v. `DatabricksInstancePoolCreatorId`
    vi. `aws:autoscaling:groupName`
    vii. `aws:ec2spot:fleet-request-id`

Encrypted volumes

Wiz supports encrypted volumes for all cloud-native encryption types in AWS, Azure, GCP, and OCI.

- In AWS, this is achieved without Wiz having access to the original encryption key thanks to the permission `kms:ReEncryptTo`.
- In Azure and GCP, this is supported with the standard snapshot and volumes permissions required by the Azure Connector and GCP Connector. No additional permissions are required, as creating a volume from a snapshot of an encrypted volume does not require additional permissions or encryption methods.

API throttling

Wiz throttles its API calls in a few ways:

- API calls rate has a default value of 20 calls per second per service per Subscription.
- Daily Connector scan—Each Connector is scanned every ~24 hours, but not all at the same time
- Time between subsequent manual rescans—Default value is 5 minutes
- If a service returns a throttle error, we start exponential backoffs
- For workload scanning, Wiz implements a rate limiting process to prevent exceeding the allowed quota for creating and copying snapshots. In case of throttling, there is a built-in retry process.

In most cases, this logic prevents Wiz from hitting CSP limits. However, if you encounter problems with a particular service, which can happen because of company-specific automation, all of these parameters can be customized per tenant as required.

> ℹ Decreasing the number of API calls per second per service, increasing scan intervals (both automatic and manual), and lengthening backoff periods all slow down the data fetching cycle.

English ▲

Workload scanning results

The following cloud resource metadata (i.e. attributes and parameters) are transferred for each resource:

- List of installed packages + versions
- List of programming languages libraries + versions
- Local users
- Authentication configuration
- Operating system info
- Hashes of all files
- CIS benchmarks output
- Secret metadata (without the sensitive info)
- Data classifier metadata (without the sensitive info)
- Deployed Git repositories
- Deployed containers
- For Windows machines: installed programs, services, and installed KBs
- Specific logs and artifacts from the VM disks (see the full list)[1]

> [1] Only collected if you enable the Forensics package collection feature

Supported operating systems, file systems, container runtimes, virtual appliances, and Docker images

Wiz scans disks with:

- Operating systems—See below the fully supported and partially supported
- File systems—NTFS, ext2, ext3, ext4, XFS, OSTree, ZFS, UFS
- Encrypted file systems—Crypto_LUKS (Azure integration) and BitLocker (Azure integration)
- Container runtimes—Docker, containerd, CRI-O
- Virtual appliances—F5 BIG-IP Advanced Firewall Manager, FortiOS, IBM Security Access Manager (ISAM), IBM Security Verify Access (formerly ISAM), PAN-OS
- Docker image types, such as AMD64 and ARM64.

> ℹ
>
> - VMs running containers with a supported OS image on a non-supported host OS are still scanned by Wiz.
> - Partial support means that Wiz does not detect all vulnerabilities and technologies.

English ▴

- The table below applies to the operating system itself. If the running file system or encryption method is not supported, the entire set of capabilities is not supported as well, even if the OS itself is.

Fully supported

OS	Detection	Technologies	Vulnerabilities	Malware
Alibaba Cloud Linux 2	▯	▯	▯	▯
Alibaba Cloud Linux 3	▯	▯	▯	▯
AlmaLinux	▯	▯	▯	▯
Amazon Linux	▯	▯	▯	▯
Amazon Linux 2	▯	▯	▯	▯
Amazon Linux 2023	▯	▯	▯	▯
Amazon Linux AMI	▯	▯	▯	▯
AWS BottleRocket	▯	▯	▯	▯
CBL-Mariner	▯	▯	▯	▯
Container-Optimized OS	▯	▯	▯	▯
Flatcar Linux	▯	▯	▯	▯
Linux Alpine	▯	▯	▯	▯
Linux CentOS	▯	▯	▯	▯
Linux Debian	▯	▯	▯	▯
Linux Gentoo	▯	▯	▯	▯
Linux openSUSE	▯	▯	▯	▯
Linux Oracle	▯	▯	▯	▯
Linux Photon	▯	▯	▯	▯
Linux Red Hat	▯	▯	▯	▯
Linux Ubuntu	▯	▯	▯	

English

OS	Detection	Technologies	Vulnerabilities	Malware
macOS	□	□	□	□
NixOS	□	□	□	□
Rocky Linux	□	□	□	□
SUSE Linux Enterprise Server	□	□	□	□
Windows 7	□	□	□	□
Windows 8.1	□	□	□	□
Windows 10	□	□	□	□
Windows 11	□	□	□	□
Windows Server	□	□	□	□
Windows Server 2003	□	□	□	□
Windows Server 2003 R2	□	□	□	□
Windows Server 2008	□	□	□	□
Windows Server 2008 R2	□	□	□	□
Windows Server 2012	□	□	□	□
Windows Server 2012 R2	□	□	□	□
Windows Server 2016	□	□	□	□
Windows Server 2019	□	□	□	□
Windows Server 2022	□	□	□	□
Wolfi/Chainguard	□	□	□	□

Partially supported

English ▴

OS	Detection	Technologies	Vulnerabilities	Malware	Se
Appgate SDP		Partial	Partial		
Arch Linux		Partial	Partial		
Aruba ClearPass Platform		Partial	Partial		
Barracuda CloudGen Firewall		Partial	Partial		
Buildroot		Partial	Partial		
Clear Linux OS		Partial	Partial		
Common Base Linux Delridge		Partial	Partial		
Darktrace OS		Partial	Partial		
F5 TMOS Linux		Partial	Partial		
FreeBSD		Partial	Partial		
Imperva SecureSphere		Partial	Partial		
Linux Fedora		Partial	Partial		
McAfee Linux OS		Partial	Partial		
MgmtOS		Partial	Partial		
N-centralOS Linux		Partial	Partial		
Oracle Linux Server		Partial	Partial		
PAN-OS		Partial	Partial		
PexOS		Partial	Partial		
Sangoma Linux		Partial	Partial		

English ▴

OS	Detection	Technologies	Vulnerabilities	Malware	Se
Silver Peak VXOA	▯	Partial	Partial	▯	
TanOS	▯	Partial	Partial	▯	
Trend Micro Smart Protection Server	▯	Partial	Partial	▯	
Wind River Linux	▯	Partial	Partial	▯	

Scan status

The Security Tool Scan object on the Security Graph contains information about the status of every attempted scan, details about why the scan failed or was skipped (if relevant), and when a scan last succeeded.

You can query for only failed or skipped scans.

Status	Status Details	Description
Failed	ADE-encrypted disks with restricted network access	In order to scan ADE-encrypted disks, Wiz must have network access to the disk. To allow Wiz to scan it, configure the disk to have public access.
Failed	crypto_LUKS/Encrypted file system: BitLocker	Wiz cannot scan disks that leverage BitLocker or Crypto_LUKS when used outside of the cloud provider implementation (Azure Disk Encryption), as the keys for these disks aren't available through the cloud provider APIs.
Failed	EBS snapshot copy requests exceed the number of concurrent copy operations limit	AWS limits the number of concurrent copy requests of EBS snapshots. In environments with many large encrypted EBS volumes, some scan processes may time out because no additional copy operations are possible. By default, each re

Status	Status Details	Description
		limited to 20 concurrent snapshot copy operations, Wiz will utilize up to 10 slots. You can contact Wiz support to request Wiz to increase the utilization or query the Security Graph to identify customer-managed keys that you then share with Wiz to grant access to the original snapshot; this eliminates the need to copy encrypted snapshots and re-encrypt them with a Wiz key. Learn about CMK sharing.
Failed	Internal error	The Wiz backend failed to complete the scan.
Failed	Missing Key Vault permissions to read the ADE encrypted disk secret	Follow the guide to grant permissions to the specified Key Vault.
Failed	Missing permissions: *	Either the Wiz Connector is missing the required permission or there exists a policy that blocks Wiz from accessing a required resource.
Failed	NoValidPartitionWasFound: No valid partition was found. Either an unsupported, corrupt, or encrypted filesystem/OS	Wiz could not identify a valid partition on the disk to mount and scan. This could be a result of appliance vendors using custom operating systems, multiple partitions sharing a logging location, LVM configuration spanning a volume group on more than one volume, unsupported filesystem, or file-level encryption that does not have access to the keys.
Failed	Too many tags on original resource and/or custom scanner tags	Cloud providers restrict the maximum number of tags that can be assigned to a resource (AWS/Azure - 50, GCP - 64, OCI - 10 free form tags). When Wiz creates temporary resources, it appl original resource's tags as well as

Status	Status Details	Description
		any defined custom scanner and `wiz:auto-gen` tags. If the total number of tags exceeds the number of allowed tags, the creation of the resource will fail. You can disable tag inheritance, exclude specific tags from inheritance, or reduce the number of custom scanner tags. In OCI free form tags are inherited to the cloned disk with no ability to exclude them.
Failed	Unexpected error	The Wiz backend failed to complete the scan.
Failed	VolumeIsFull: Unable to attach full volume	To ensure the attached disk has the correct volume to scan, Wiz writes to that volume scan-related identifiers. Therefore, Wiz cannot scan volumes that are completely full.
Failed	VolumeIsReadOnly: Unable to operate on read-only volume	Wiz is unable to scan read-only volumes as it requires writing scan-related metadata to the copied disk (the original disk in your environment is never changed).
Skipped	Automatic backup snapshots are required to scan this database and could not find one less than 3 days old	Creating a manual snapshot in single AZ RDS instances can cause performance issues, so Wiz will skip scanning the instance if a recent snapshot isn't found. Create a manual snapshot or enable automatic snapshot to fix this.
Skipped	Azure App Service or Function App is inactive	Disabled app services cannot be scanned by Wiz. Enable the application to allow Wiz to scan it.
Skipped	Azure system database	Scanning of the Azure system databases is skipped (master, tempdb, etc.) as these are c used, and managed by the S

English ▲

Status	Status Details	Description
		Server instance itself to support its core functionalities.
Skipped	Databricks	Wiz does not fetch/scan the disks of Databricks instances.
Skipped	Databricks managed storage account	Storage accounts created by Databricks are managed by the service and have a deny assignment applied preventing read access.
Skipped	Data scanning disabled	Unsupported data stores are not scanned. Data scanning of container images is being developed; until it is complete, container images may report that they were skipped. This is expected behavior.
Skipped	Driver not supported	Containers created with an unsupported storage driver (Wiz supports scanning of Overlay2, Overlay, and Windows Filter).
Skipped	Instance group sampling	Instead of scanning all disk volumes in an instance group, Wiz samples only one.
Skipped	Locked by: *	The specified resource group is locked and therefore Wiz cannot delete snapshots. To fix this, either remove the lock from the specified resource group or use the Dedicated Resource Group option in the Connector settings to set a dedicated resource group in which snapshots will be created, scanned and then deleted by Wiz.
Skipped	PremiumV2_LRS disks not supported / UltraSSD_LRS disks not supported	Azure Premium SSD v2 and Ultra disks only support incremental snapshots. Wiz performs full snapshots as they can be shared across Subscriptions (required for the agent-less scanning process).

English ▲

Status	Status Details	Description
Skipped	Region not supported	The region where the disk is hosted is missing in the Wiz scanning account: 1. SaaS deployments—This can happen if you are using an opt-in region; contact Wiz support to request enabling this region. 2. Outpost deployments—Ensure the region is enabled.
Skipped	Resource inaccessible	Network inaccessible app services residing in private VNETs and/or behind a strict firewall. This disallows both Wiz scanner traffic and Microsoft internal app service proxy traffic ,and does not support backups (i.e. App Service Environment hosted functions, or dynamic SKU functions)
Skipped	Resource not found	Ephemeral resources seen by the Wiz fetcher but, by the time the Workload scanner attempts to scan them, they no longer exist
Skipped	Resource unsupported	Azure serverless functions which are currently unsupported.
Skipped	Scanning of multi-attached disks is not supported	Multi-attached non-OS disks are not supported for workload and data scanning.
Skipped	Secret External ID: *	Access to the specified secret is blocked from Wiz, which is required to perform the scan on encrypted disks.
Skipped	Serverless scan skipped due to excessive size	Serverless function exceeds the allowed limit.
Skipped	Unmanaged disk	Azure unmanaged VM disks do not support snapshot tagging, which is fundamental for Wiz to track, maintain, and act on resources that were created by Wiz and avoid unnecessary costs.

English ▲

Status	Status Details	Description
Skipped	Volume contains tag "wiz"	Temporary volumes that Wiz creates for scanning encrypted disks. Because the original volume is scanned by Wiz, there is no need to scan this temporary volume again.
Skipped	Volume not found	VMs or ephemeral resources that existed when Wiz initiated the scan, but were destroyed later when Wiz tried to create a snapshot.
Skipped	Policy violations: (unavailable)	Azure policy prohibits the creation of Wiz temporary scan resources (volume, snapshot)

System Health Issues

Wiz generates System Health Issues when required or recommended permissions are missing, when CSP restrictions or limitations prevent scanning, and when disk scans fail, according to a calculated percentage of failed scans per Connector, Subscription, and region.

You can view all existing System Health Issues on the Settings > System Health page. After a successful scan, the System Health Issue is removed from Wiz (similar to other Issues).

> If the VM on which the scan failed was deleted from your environment before the next scan, the stale System Health Issue remains in Wiz for a period of 3 days.

Skipped cloud services & limits

Due to cloud provider limitations, Wiz cannot scan the OS disks of the underlying workloads used by the following services: Amazon SageMaker Notebook (SageMaker Domain is supported), Amazon WorkSpaces, and Azure Synapse Analytics.

This means that vulnerability, secret, and malware detection, along with any other analysis or threat detection that depends on access to workload disks, do not work for these services. They are, however, still subject to cloud scanning for misconfigurations.

Moreover, some cloud services are subject to numerical limits in order to ensure the stability and responsiveness of the Wiz backend. Learn more.

English ▲

The services listed below are cloud provider native types, which may be normalized to other terms in Wiz.

CSP	Service	Limit(s)
AWS	Accounts	AWS Account tags and creation times are fetched only for Organization connectors due to permission limitations. Wiz attempts to set the value of `providerID` using DescribeAccount: • For accounts scanned via an organizational Connector, the call succeeds • For accounts scanned via an account-level Connector, the call fails, so `providerID` it is set to empty
AWS	Athena Workgroups	• 10 data usage alerts per workgroup • Only Workgroups on regions with recent queries are scanned
AWS	Bedrock Agent	Only the latest agent version is fetched
AWS	Certificate Manager	10,000 per account
AWS	CloudWatch Log Group	10,000 per account
AWS	DynamoDB Table	1,000 per region per account
AWS	Elastic Block Store (EBS)	100 public snapshots per account 100,000 total snapshots per account
AWS	Elastic Container Registry (ECR)	1,000 container images per ECR repository
AWS	EMR Serverless Applications	200 per account and region
AWS	IAM Policies	IAM Policies are not fetched with tags
AWS	Identity Center (SSO)	20,000 users per SSO instance
AWS	Identity Center (SSO)	10,000 group members per SSO group
AWS	Lambda Layer	• Only versions with attached resource policy • 1,000 maximum versions per layer

English ▲

CSP	Service	Limit(s)
AWS	Launch Template	Only the default version and versions used by autoscaling groups are fetched
AWS	RDS	100 cluster or database instances public snapshots per account
AWS	SageMaker	Disks are not scanned
AWS	Simple Email Service (SES)	1000 verified identities per region per account
AWS	Simple Notification Service (SNS)	• 10,000 SNS topics per Account • SNS Topic subscriptions are not fetched
AWS	Simple Queue Service (SQS)	10,000 SQS queues per Account
AWS	Simple Storage Service (S3)	10,000 S3 buckets per Account
AWS	Workspaces	Disks are not scanned
Azure	Microsoft Entra ID (AAD)	10,000 group members per Microsoft Entra ID (AAD) group
Azure	Blob Storage	10,000 Blob containers per Storage Account
Azure	Service Bus Queues	10,000 queues per Account
Azure	Container Registry (ACR)	1,000 container images per ACR repository
Azure	Key Vault	1,000 secrets, keys, and/or certificates per Key Vault
Azure	OpenAI	Training datasets are scanned in the [same region as your Wiz data center]
Azure	Synapse Analytics	Disks are not scanned
GCP	Cloud Storage Buckets	10,000 storage buckets per GCP Project
GCP	Compute Snapshot	Only snapshots encrypted with Google keys are scanned
GCP	Container Registry	1,000 container images per Container Registry
GCP	DNS Records	100,000 DNS records per DNS zone
GCP	DNS Zone	1,000 DNS Zones per GCP Proj

English ▲

CSP	Service	Limit(s)
GCP	Google Workspace	2,000 group members per Google Workspace group
GCP	Organization policies	Organization connector is needed to view all of the inherited policies
OCI	ManagedCompartmentForPaaS	Not scanned due to an OCI limitation

FAQ

Questions? Take a look at the FAQ.

Updated about 3 hours ago

← API Calls Used by Wiz

Cloud Inventory →

Did this page help you? Yes No

English ▴