Microsoft Security

2023 State of Cloud Permissions Risks Report

Executive findings

There's no doubt the world has embraced multicloud. Its elastic nature has opened doors for organizations to access new levels of innovation and automation to evolve their business processes.

But as cloud environments expand, they have inadvertently become more complex to manage. With over 40,000 permissions that can be granted to identities, of which more than 50% are high-risk, it is becoming increasingly difficult for organizations to know who has access to what data, and across which cloud platforms.

Since publishing our inaugural State of Cloud Permission Risks Report in 2021, we have run the data again across over 500 risk assessments. In addition to cloud environments expanding, this year we have observed a significant increase in identity types accessing critical cloud resources.

The rise in workload identities, super admins and inactive identities accessing cloud infrastructure presents new security risks for many organizations.

In fact, this year we have found that workload identities outnumber human identities 10:1, which is double what was recorded in 2021. We also found that over 50% of identities are Super Admins, which are users or workloads that have access to all permissions and resources.

To make matters worse, the dangerous delta between permissions granted and permissions used, what we call the permissions gap, has increased, as identities are now only using 1% of their permissions granted.

Further contributing to the permissions gap, our research shows that over 60% of identities were found to be inactive and haven't used any of their permissions granted in the last 90 days.

Permission
The ability for an identity to perform an action on a resource. High-risk permissions have the ability to cause data leakage, service disruption or service degradation

The permissions gap
The gap between permissions granted and those used.

Inactive identities
Identities that haven't used any of their permissions granted in the last 90 days

Super admins
User/Workload identities that have access to all permissions and all resources.

The permissions gap is a contributing factor to the rise of both accidental and malicious insider threats, which can allow attackers to exploit an identity with misconfigured permissions and access critical cloud infrastructure.

This gap can be reduced through implementing the principle of least privilege and working towards a Zero Trust security model, thus protecting cloud environments. However, this is nearly impossible to do manually and at cloud scale.

Without properly implementing the principle of least privilege across all identities and all clouds, organizations are leaving their critical cloud infrastructure open to permission misuse and potential breaches.

In this report, we share detailed findings about the most common multicloud permission risks and share recommendations for how to ensure least privilege access and achieve Zero Trust security across your entire digital estate.

40,000+

permissions across key cloud infrastructure platforms

>50%

of these permissions are **high-risk**, capable of causing catastrophic damage if used improperly

1%

of permissions granted to identities are actually used

Workload and super admin key vulnerabilities

The number of identities accessing cloud infrastructure is expanding and is greatly driven by the exponential increase in workload identities, which now outnumber human identities 10x. Workload identities include virtual machines, apps, services, containers and scripts. They are often left inactive or over-permissioned, which presents a huge risk for organizations if they are compromised.

1:10 User identities to workload identities

>80% Of workload identities are inactive, double the percentage reported in 2021.

<5% of permissions are actually used

With access to all permissions and all resources across clouds, this year we found a significant presence of Super Admins who are greatly over-permissioned and pose a huge risk to organizations. With an average of <2% of permissions granted actually used, it is imperative that organizations right-size Super Admins to protect against permission misuse.

>50% of identities are super admins

<2% of permissions are actually used

>40% of super admins are workload identities

Key risk findings across cloud infrastructures

The most common risks we found across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) include:

Identities are using only 1% of their granted permissions

Implication:
Over-permissioned active identities are exposed to credential theft risks

Best practice:
Implement the principle of least privilege to all identities based on historical data and grant additional permissions on an on-demand basis

There are an average of 200+ services across cloud providers

Implication:
As new services are released, new permissions are added across clouds that need to be managed

Best practice:
Implement granular visibility to know which services are accessed across multicloud

Workload Identities are using <5% of their granted permissions and >80% are inactive

Implication:
As workload identities accessing cloud infrastructure increase, they become prime targets for permission exploitation

Best practice:
Track workload identities' predictable behavior patterns and right-size their permissions to avoid unauthorized access to cloud resources

Unique key findings: aws

>70% accounts have 1 or more EC2 instances accessing all S3 buckets

Implication:

Attackers can leverage compromised EC2 instances to access sensitive data stores leading to data breaches

Best practice:

Configure S3 bucket policies to restrict broad access

>45% of organizations have Access keys that have not been rotated for at least 6 months

Implication:

Non-rotated access keys increase the risk of compromised credentials and potential data exposure

Best practice:

Ensure access keys are rotated every 90 days to keep resources secure

>40% of identities are inactive

Implication:

Inactive identities leave organizations open to credential misuse or exploitation for malicious activities

Best practice:

Remove inactive users and roles to reduce unauthorized access to resources

Unique key findings: Microsoft Azure

>85% of companies have identities with over-permissive contributor roles

Implication:
If compromised, those identities can move laterally and compromise other systems or modify or delete critical resources

Best practice:
Limit risk by scheduling contributor high-risk permissions and role assignments on a just-in-time basis

>70% of identities have not used any of their permissions granted in the last 90 days

Implication:
Inactive identities are easier targets for compromise or exploitation for malicious activities

Best practice:
When an employee changes roles, revoke all high-risk permissions they have access to

>45% of identities are Super Admins

Implication:
With access to all permissions and resources, Super Admins can cause catastrophic damage if hacked

Best practice:
Closely monitor Super Admin role assignments by setting up alerts

Unique key findings: Google Cloud

>60% of projects have Service accounts with over permissive Owner/Editor roles either directly attached or inherited from folder or organization

Implication:
Owner/Editor roles are high-risk as they give the ability to edit or delete business-critical resources

Best practice:
Right-size identities' permissions based on historical activity

>50% of organizations have user-managed keys for service accounts that are not rotated

Implication:
Not rotating account keys increases your risk of critical cloud data being compromised

Best practice:
Service account keys should be rotated every 90 days to ensure data can't be accessed with old keys that may be compromised

>70% of identities are Super Admins

Implication:
Should an identity be compromised, the hacker will have access to all permissions and all your organization's resources

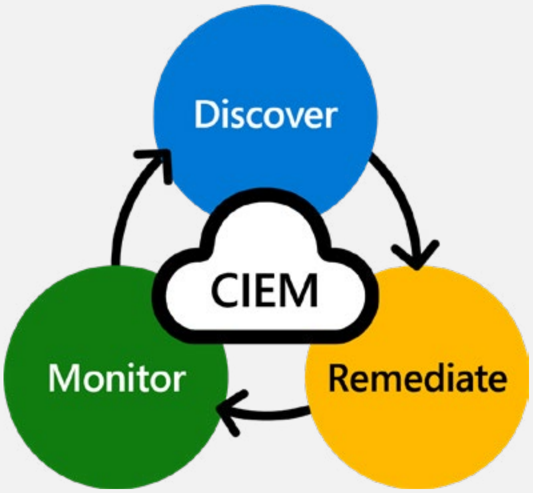
Best practice:
Implement the principle of least privilege for all identities that access your infrastructure

Managing permissions across multicloud with cloud infrastructure entitlement management

To effectively manage permissions across multiclouds, organizations need a Cloud Infrastructure Entitlement Management (CIEM) solution. CIEM fills a crucial gap in the realm of cloud security by addressing the risks posed by human error and unauthorized access in complex cloud environments.

With CIEM, organizations can continuously discover, remediate, and monitor the activity of every unique user and workload identity operating in the cloud. By managing permissions consistently across clouds and enforcing the principle of least privilege for all identities, organizations will reduce their permissions gaps and get one step closer to achieving Zero Trust.

Microsoft Entra Permissions Management, Microsoft's CIEM solution, gives you the granular visibility you need to effectively right-size the permissions of both human and workload identities across AWS, Azure, and GCP.



Recommendations for multicloud permissions management

Right-size permissions based on past activity

- Remove inactive identities and scope permissions automatically for over-permissioned users, workloads, and groups
- Only grant high-risk permissions on-demand with just-in-time access and an integrated approval workflow
- Restrict broad access to critical cloud infrastructure resources

Assess, manage, and monitor identities and access continuously

- Track permission usage for both human and workload identities
- Set alerts to track anomalous identity behavior, privilege escalation scenarios, and inactive identities
- Monitor reports to remediate new cases of inactive, over-permissioned, or even Super Admins

Implement automated continuous identity governance and reporting

- Remove inbound SSH/RDP access in security groups to restrict inbound access to virtual machines
- Enable multifactor authentication (MFA) for all identities with console access
- Rotate keys regularly to reduce risk due to compromised credentials
- Automate custom risk reports across all accounts to track permission creep and other key risks
- Ensure employees who are joining, leaving or switching roles within the company have their permissions right-sized for their new job scope

Permissions management is a team effort

Operationalization of Permissions Management requires a collaborative security approach. Your best bet is to adopt the "Defense in Depth approach", which requires close collaboration between your security operations center (SOC) and identity teams. These recommendations will impact each team in unique ways:

Security team

Permissions Management helps security teams complement existing security solutions by providing an identity perspective of how resources are accessed, This perspective includes automated detection and proactive remediation of potential permission risks. And by tracking their Permission Creep Index (PCI), security teams can also track how their security posture improves over time.

Cloud infrastructure operations team

With Permissions Management, Cloud Infrastructure Operation teams can confidently manage, enforce and report on least privilege access baselines across the organization. This saves operations teams time and effort in detecting, assessing, alerting, and remediating cloud security risks.

Identity and access management team

One of Zero Trust's most important tenants, least privilege, becomes easier to implement with Permissions Management. Identity and Access Management Teams can include Permissions Management into their strategy for identity governance by automating the enforcement of least privilege across both human and workload identities.

Permission creep index (PCI)
A qualitative measure of risk by comparing an identities' permissions granted vs. permissions used and their access to high-risk resources.

Executive conclusion

This report's key findings highlight a critical concern: the growing number of identities across cloud platforms. This rapid increase can leave organizations vulnerable to attacks, resulting in catastrophic losses if not managed effectively.

Recommendations:

- Assess your permissions risks and determine which identity has been doing what, where, and when
- Grant permissions on-demand for a time-limited period or an as-needed basis to ensure least privilege
- Continuously monitor permissions usage across clouds
- Ensure lifecycle monitoring to improve security posture and save security teams time

About Microsoft Entra Permissions Management

Microsoft Entra Permissions Management is a CIEM solution that provides complete visibility into permissions for all identities (user and workload) across all major public cloud platforms (AWS, Azure, GCP) from a unified interface. It helps organizations understand what permissions identities have and what resources they're accessing.

Permissions Management automatically detects which permissions are unused and pose risks so Security and Identity teams can right-size permissions in just a few clicks.

Try Microsoft Entra Permissions Management now

Try Permissions Management and run a comprehensive risk assessment to identify the top permission risk across your multicloud infrastructure. Request a trial at aka.ms/TryPermissionsManagement.

For more information about Permissions Management, visit aka.ms/PermissionsManagement.

Microsoft Security