Microsoft Security

2021 State of Cloud Permissions Risks Report

Executive Introduction

As organizations modernize IT and adopt multi-cloud infrastructures to support evolving business processes involving user and workload identities (e.g., virtual machines, web apps, containers, scripts, etc.), it's increasingly difficult to know who has access to what data across which platforms. This lack of visibility leads to excessive permissions and higher security risks exposing identities and resources.

Regardless of where an organization is in their cloud migration process, it's important to implement robust cloud infrastructure security. Without it, their cloud environment is left vulnerable to attacks and accidents.

Microsoft collected data from risk assessments performed with over 150 organizations worldwide and discovered that more than 90% of identities are using less than 5% of permissions granted. This gap between permissions granted and those used is what we call the permissions gap.

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 least privilege access policies and working towards a Zero Trust security model, thus protecting cloud environments. However, this is nearly impossible to do manually and at cloud scale.

Today, over 40,000 permissions can be granted to identities across the key cloud infrastructure platforms and nearly 50% of these permissions can be classified as high-risk, meaning they can cause catastrophic security and business damage - service disruption, service degradation or data exfiltration - if used improperly.

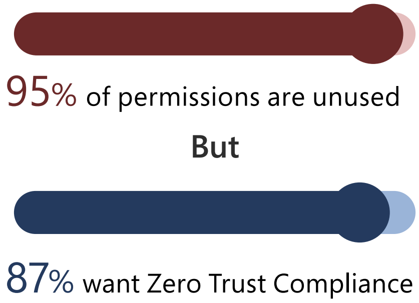
In this report, we share detailed findings about the most common cloud permissions risks we observed and share recommendations to ensure least privilege access and achieve Zero Trust security across your entire digital estate.

Cloud Infrastructure Security Trends

7x Growth of identities accessing cloud services

+

20K+ High-risk permissions



95% of permissions are unused

But

87% want Zero Trust Compliance

However, organizations need to first fix the permissions gap to achieve Zero Trust Compliance

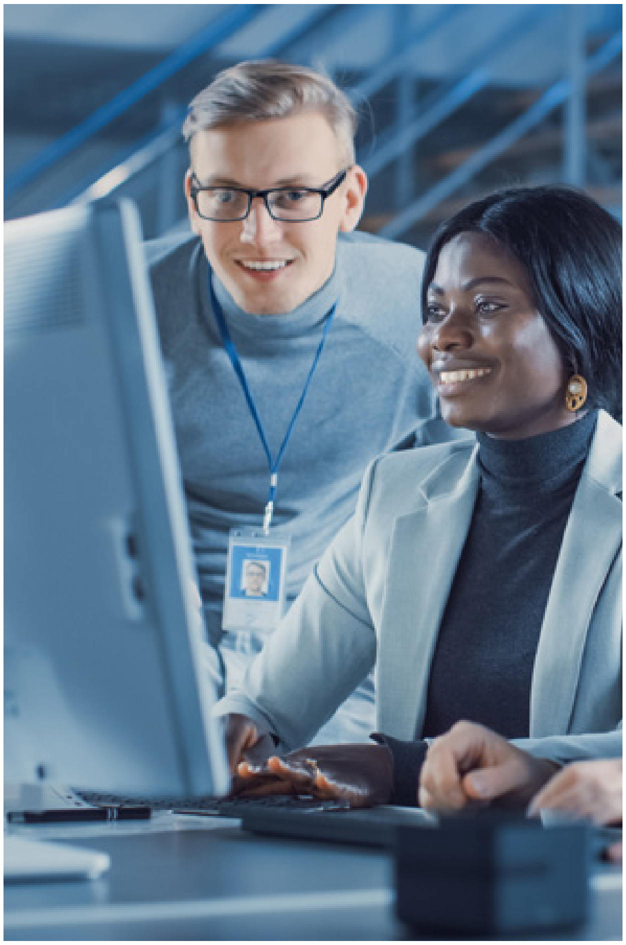
Closing the Permissions Gap with Cloud Infrastructure Entitlements Management

The principle of least privilege access is nothing new – it's one of the foundational concepts of Zero Trust:

- **Never trust, always verify**
- **Assume breach**
- **Enforce least privilege access**

However, with the rising complexity of multi-cloud environments, it has become increasingly difficult to implement least privilege access consistently across clouds. Without it, organizations are left susceptible to severe consequences.

In the past, organizations had fewer identities to manage, typically only including employees, partners, or customers. As the world has become increasingly more digital, these identities have expanded to include developers, third-party contractors, a host of workload identities like web apps, virtual machines, containers, or scripts, and a variety of compute types like EC2 instances and serverless functions. These workload identities can have the same high-risk permissions and access to sensitive resources that users do.



In order to lay out a framework for organizations to approach identity, access and permissions management in their multi-cloud environments, Gartner recently created the category Cloud Infrastructure Entitlement Management (CIEM). CIEM is a next-generation solution for managing permissions consistently across all cloud infrastructures and ensuring least privilege access for all identities and resources, helping to reduce the permissions gap and getting one step closer to a Zero Trust security framework.

Key Risk Findings Across Cloud Infrastructures

Some of the risks contributing to the permissions gap span across the three main cloud providers— Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP)—while others are unique to each provider.

The most common risks we found in all three main cloud providers include:

High-risk permissions are continuing to rise, with more than 90% of identities using less than 5% of permissions granted	**Implication:** Excessively permissioned active identities are exposed to credential theft risks	**Best practice:** Right-size permissions based on the past activities of these identities and grant additional permissions on an on-demand basis
Cross-account access is frequently granted to external identities	**Implication:** Cross-account access enables identities to access all resources in target accounts, leading to data leakage or malicious service disruption	**Best practice:** Right-size scope of roles/policies to access limited resources and limit access to specific identities in other accounts
Lack of separation of duties: Users with excessive roles/policies in both development and production subscriptions/accounts	**Implication:** Leveraging the same roles/policies and permissions in development and production environments exposes your infrastructure to insider threats and malicious external threats	**Best practice:** Right-size permissions in development environments and clone permissions into production only as a starting point, then right-size permissions to tighten controls
Workload identities are over-permissioned and greater than 40% of them are inactive	**Implication:** Inactive identities leave organizations open to credential misuse or exploitation for malicious activities	**Best practice:** Remove inactive roles/policies and identities to avoid unauthorized access to resources

Unique Key Findings: aws

Two thirds of all organizations have EC2 instances with access to all S3 buckets

Implication:

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

Best practice:

Restrict broad access to all resources for applications on EC2 instances

More than 50% of enterprises have identities with privilege escalation ability to elevate to super admin role

Implication:

Identities with hidden privilege escalation ability can self-elevate to admin privileges and gain unauthorized access

Best practice:

Regularly review all identity policies for any privilege escalation possibilities

Misconfigured security groups with inbound Secure Shell (SSH) port open and attached to EC2 instances

Implication:

Open security groups allow network-based attacks to gain access to EC2 instances

Best practice:

No security groups should allow unrestricted ingress access to any ports

Admins typically don’t have Multi-factor Authentication (MFA) enabled and access keys not rotated for at least 6 months

Implication:

Admins without MFA enabled login or non-rotated access keys increase the risk of compromised credentials

Best practice:

Enable MFA for all users with console access and rotate access keys every 90 days

Unique Key Findings: Microsoft Azure

65% of enterprises have anonymous public read access enabled for blob containers in production environments

Implication:

Confidential data in public storage accounts is exposed to anonymous unauthorized identities

Best practice:

Provide controlled just-in-time access to blob containers to prevent anonymous/ unauthorized access

Users assign permissions and access outside of security and audit processes

Implication:

Unknown permissions assignments create a significant blind spot and unwanted risks for the organization

Best practice:

Allow access through approval-based permissions on-demand to track for identity governance and compliance

Remote Desktop Protocol (RDP), SSH access from the internet is enabled for network security groups in production environments

Implication:

Attackers can use various brute force techniques to gain access to Azure virtual machines

Best practice:

Disable RDP/SSH access on network security groups from the internet

More than 70% of subscriptions have identities (users and workloads) with over-permissive contributor roles

Implication:

Identities with contributor roles significantly increase risks due to their ability to delete business-critical resources

Best practice:

Replace high-risk contributor roles with lower-risk right-sized roles based on past activities

More than 85% of organizations have over-permissive users and service principals left orphaned after project completion

Implication:

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

Best practice:

Remove all inactive users and service principals automatically to avoid unauthorized access to resources

Unique Key Findings: Google Cloud

More than 80% of projects have Service accounts with over-permissive Owner/Editor roles either directly attached or inherited from folder or organization

Implication:

Service accounts with Owner/Editor permissions significantly increase security risk due to their ability to delete business-critical resources

Best practice:

Replace high-risk owner/editor roles with lower risk roles based on past activities and right-size all service accounts

More than 85% of organizations have user-managed keys for service accounts that are not rotated

Implication:

Rotating service account keys reduces malicious usage risks of access keys associated with a compromised or terminated account

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

More than 50% of organizations have project wide SSH Keys enabled for virtual machine instances

Implication:

Project-wide SSH keys can be used to login into all the instances within a project. When compromised, they pose significant security risks that can impact all the instances

Best practice:

Use instance specific SSH keys that limit the attack surface in the case the SSH keys are compromised

More than 75% of organizations have identity permissions creep ranging from Viewer to Owner

Implication:

Identities with high-risk permissions expand the attack surface due to their ability to delete business-critical resources

Best practice:

Persistently monitor the Permissions Creep Index, a metric that is the function of the number of unused high-risk permissions and the total number of resources that an identity can access, for all identities and right-size permissions to maintain security posture

Recommendations for Multi-Cloud Permissions Management

Right-size permissions based on past activity

- Remove or scope down permissions automatically for over-permissioned users, workloads, and groups verify
- Grant high-risk permissions only on-demand with just-in-time access using an integrated approval workflow
- Restrict broad access to critical cloud infrastructure resources
- Remove inactive identities to avoid unauthorized access to resources

Assess, manage, and monitor identities and access continuously

- Migrate from static, assumption-based permission grant process to continuous, activity-based permission management
- Monitor, receive alerts, and remediate anomalous identity behavior, unauthorized identities, and roles/policies
- Monitor, receive alerts, and remediate permissions for privilege escalation scenarios and inactive identitiesRemove inactive identities to avoid unauthorized access to resources

Implement automated continuous identity governance and reporting

- NIST 800-53, CIS Benchmarks, and AWS Well-Architected reporting and built-in remediation to drive toward better compliance
- Restrict inbound access to virtual machines by removing inbound SSH/RDP access in security groups
- Enable Multi-Factor Authentication for all identities with console access
- Rotate keys regularly to reduce risk due to compromised credentials
- Automate and schedule custom risk reports across all accounts

Executive Conclusion

These key findings highlight areas where organizations should increase their cloud infrastructure security through implementing least privilege access policies. Left unmanaged, the permissions gap can leave organizations vulnerable to attacks that can lead to catastrophic losses.

Key recommendations:

- Assess your permissions risks and identify 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 access
- Continuously monitor permissions usage across clouds

About CloudKnox Permissions Management

CloudKnox Permissions Management is a cloud infrastructure entitlement management (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. CloudKnox Permissions Management automatically detects which permissions are unused and pose risks and allows Security and Identity teams to right-size permissions in just a few clicks. Thanks to high-precision ML-based anomaly detection capabilities, CloudKnox Permissions Management streamlines threat detection and response and allows organizations to maintain a strong security posture.

Try CloudKnox Permissions Management now

CloudKnox Permissions Management is now available for Public Preview! If you have any questions or are interested in joining Public Preview, please fill out the form at aka.ms/CloudKnoxPublicPreview.

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

Microsoft Security

©2021 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.