Microsoft Security

Microsoft Entra Permissions Management Glossary

Introduction

Use this glossary to familiarize yourself with the terms that make up Permissions Management and to understand the essential role Permissions Management plays in the operation and security of your organization.

Term	Definition
Cloud Services	Cloud service describes any service delivered on-demand to users via a third-party provider. The primary service categories include: Infrastructure-as-a-Service (IaaS), Platforms-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Providing appropriate and secure access to these services has become even more complex. Accurately and efficiently managing this volume of cloud services means organizations need a clear purview into their catalog of services and who is accessing them.
Entitlement	Refers to various forms of user permissions in a variety of infrastructure systems and business applications. With the rapid pace of new services being added, cloud infrastructure entitlements are constantly evolving. As a result, cloud infrastructure entitlement analysis requires understanding the underlying services and cloud specific access models. For instance, determining a user's effective access privileges means you need to understand all the different policies attached to the user, such as Cloud Service Provider (CSP)-managed policies and customer-managed policies, as well as policies attached groups, roles, resources, and access control lists.
Least Privilege	When building and supporting a Zero Trust foundation, the principle of least privilege is one of the essential pillars to lay this foundation. Maintaining least privilege means that identities are provisioned with the least privileges they need to complete their day-to-day operations. Considering the explosion of permissions and identities across cloud infrastructures, enforcing the principle of least privilege manually has become almost impossible. Organizations need a solution that helps automate this critical task to help secure their digital estate.

Term	Definition
Permission	Permissions give identities the ability to perform an action on a resource. The rising rate of multicloud infrastructures makes it increasingly challenging to effectively manage permissions. Across major clouds, thousands of permissions can be granted, and over 50 percent are high-risk, meaning they can cause service disruption, service degradation, or data leakage when used improperly. * To help support a viable multicloud strategy and avoid accidental or malicious misuse, streamlined permissions management is essential.
Permissions Creep Index	Permission Creep Index (PCI) is an aggregated metric Permissions Management leverages that analyzes the permissions granted vs. permissions used to determine a level of risk associated with permissions across identities and resources. On a scale of 1-100, 80-100 considered to be "high-risk," the PCI score helps you clearly identify where your most critical risks are in your multicloud infrastructure. Once you have pinpointed your biggest risks, you can begin remediating them by implementing least privilege policies to secure your infrastructure.
Permissions Gap	The permissions gap is the delta between permissions granted verses permissions used. This 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. Organizations need to right-size their identities to eliminate the permissions gap and secure their infrastructure from potential permissions exploitation.
Resources	A resource is an entity that uses compute capabilities, such as virtual machines, serverless functions, network and storage objects, etc. Resources are critical to your infrastructure, so it's important to maintain full visibility over who can perform what actions on the resources.
Roles	A role is a predefined set of permissions that allows a user to perform specific actions. Defining and assigning roles accurately ensures appropriate access which helps support a secure organizational framework.
Super User / Super Identity	A super user or super identity is a powerful identity that can perform any action on all resources across the cloud infrastructure. They are particularly important to manage and right-size considering that these identities are powerful and over-permissioned by nature. Any malicious or accidental permission misuse is a great risk to the organization's security.

Term	Definition
Workflows	Workflows involve coordinating tasks to support essential functions such as access approvals, notifications, escalations, manual fulfillment requests, and integration with other business processes. For example, a successful workflow can help managers or resource owners approve or deny requests. Workflows need to be set up thoughtfully and managed regularly to ensure they make processes easier. Automating workflows helps ensure nothing slips through the cracks and helps free up managers and resource owners.
Workload Identities	A workload identity (often referred to as a non-human identity) is the identity assumed by software workloads, such as containers, VMs, applications, and services, so that they can authenticate and access other services and resources. Like human identities, workload identities are exponentially increasing in multicloud environments and are expected to outnumber the growth of human identities by a huge margin. As workload identities continue to increase and are often automated, they have become increasingly critical and difficult for organizations to manage.
Zero Trust	A proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to remediate threats.

*Statistics taken from 2021 State of Cloud Permissions Report

About Microsoft Entra Permissions Management

Microsoft Entra Permissions Management provides a single, unified platform to manage permissions for all identities – users and workloads – across all major cloud infrastructures. It allows organizations to discover, monitor, and remediate permissions risks and achieve Zero Trust security by implementing least privilege policies across their entire digital estate.

To try Permissions Management, log into Azure AD and click on our tile: http://aka.ms/TryPermissionsManagement.