Microsoft Entra Simplifies Identity Management While Improving Security

Thousands of organizations already depend on Azure Active Directory (Azure AD) for identity and access management. But they may not be aware of all that Azure AD provides or of additional identity management services now available. The Microsoft Entra product family, including Azure AD, provides a streamlined identity platform while strengthening security.

Cloud migration and remote work have changed the face of cyber security forever. Even a small to medium business must manage access for thousands of identities, from employees to contractors, devices, and services. However, traditional methods for verifying identity and managing permissions are labor-intensive and leave too many security gaps.

Microsoft Entra aims to close security gaps by supporting the zero trust security model. At the same time, Entra components provide simplified, centralized identity management across hybrid cloud and multi-cloud environments.

Improved Security and Privacy with Support for Zero Trust

Cyber security has grown much more complex in the past decade. Securing a perimeter, like building a moat around a castle, no longer suffices. With numerous workloads in the cloud, various IoT devices, and employees and third parties using multiple devices to access critical systems, hackers have thousands of possible access points.

Consequently, security experts recommend a zero-trust approach. With zero trust, the system must verify every user, device and workload attempting to access the network. This involves several key principles:

1. Users, devices, and workloads need trustworthy, verifiable identities.
2. Organizations need to enforce a principle of least privilege, granting users the minimum amount of privilege necessary to accomplish their work.
3. Security teams must monitor systems to evaluate permissions anomalies and identify unused privileges.

Microsoft Entra aims to strike a balance by enabling strict authentication protocols while making it easier for trustworthy users and devices to quickly access the services and files they need. For instance, Microsoft Entra Verified ID provides the capability for decentralized identity (DID).

With DID technology, users have verifiable credentials that work across multiple applications and services. Users gain control over their digital identity with a level of security that proves nearly impossible to hack. At the same time, organizations and services can quickly verify identity and block fraudulent access.

Additionally, Microsoft Entra Permissions Management provides a Cloud Infrastructure Entitlement Management (CIEM) solution. Designed specifically for the multi-cloud environment, the service delivers visibility into everything identities access across all platforms. It also enables the automation of least privilege.

Streamlined Identity Management for All Identities

In addition to supporting verifiable credentials and providing a CIEM solution, Microsoft Entra simplifies governance for identities of all types. This includes users and devices, of course. But now this also extends to workloads.

Thus, at the recent Ignite conference, Microsoft announced that the new Microsoft Entra Workload Identities product will come available in November 2022. In the cloud environment, workloads include any service, application or feature that uses cloud-based resources. Examples include databases and virtual machines. Like users, workloads need identities and permissions.

To simplify identity governance, improve productivity and help organizations achieve compliance, Microsoft Entra automates many aspects of identity lifecycle maintenance. This ensures that the right users (or devices or workloads) have the right access to the resources they need when they need them.

Improved Visibility and Control with Centralized Management

Microsoft Entra unifies identity management with a centralized Admin Center. The Admin Center delivers visibility into all identities, all applications, all access requests, and all platforms, whether on-premises or in the cloud. This provides one-stop shopping for viewing access anywhere in the system.

Microsoft Entra Permissions Management also includes the analytics necessary to identify and remediate permissions gap, ensuring that users do not have excessive or unused permissions. And it allows organizations to deliver consistent security policies across platforms.

What is Microsoft Entra?

The Microsoft Entra product family builds on abilities organizations already have in Azure AD, adding additional solutions for streamlined identity management. Products include the following:

- Microsoft Azure AD – The cloud identity product organizations have been using, but with an ever-expanding list of capabilities.
- Microsoft Entra Permissions Management – Microsoft's cloud infrastructure entitlement management product.
- Microsoft Entra Verified ID – Delivering decentralized identity capabilities.
- Microsoft Entra Workload Identities (Available in November 2022) – Solution for governing and securing non-human identities.
- Microsoft Entra Identity Governance (Preview) – Building on capabilities available in Azure AD, provides more advanced tools for identity governance. This includes lifecycle workflows and the ability to provision on-premises applications as well as those in the cloud.

Microsoft Entra Experts

As an award-winning Microsoft Partner, Messaging Architects, an eMazzanti Technologies company, helps organizations choose and configure the right identity governance capabilities in Microsoft Entra to maximize productivity and security.