KuppingerCole Report

EXECUTIVE VIEW

By Paul Fisher

July 19, 2022

Microsoft Entra Permissions Management

As organizations adopt multi cloud infrastructures to support business workflows involving user and workload identities it's increasingly difficult to know who has access to what data across which platforms. It increases the risk of unauthorized identities having access to critical resources. This lack of visibility often leads to excessive permissions and unused standing privileges which can be exploited by attackers. This report covers a feature overview, as well as strengths and challenges of Microsoft Entra Permissions Management, a Cloud Infrastructure Entitlement Management solution that helps organizations manage identities, permissions, and resources in expanding multi-cloud environments.

By **Paul Fisher**
pf@kuppingercole.com

Content

1 Introduction

A dynamic multi-cloud, multi-hybrid IT architecture is coming to dominate enterprise networks, as business leaders and IT vendors understand that a paradigm shift is necessary for organizations to become fully digital and deliver improved business value.

The speed and dynamic nature of this architecture is essential for organizations create the applications and tools needed for fast changing markets and operating conditions. Developers and other agile teams within organizations have come to rely on dynamic clouds to complete workloads on a Just-In-Time (JIT) basis, in response to demands from internal customers. All the while, networks are much more open to employees, third party users, suppliers, and customers; what was once considered "privileged" is becoming the norm as collaboration and data sharing become ubiquitous.

A greater number of workload identities such as applications, containers and scripts are gaining access to cloud-based resources and becoming increasingly important components of the new environment as process automation takes hold. The downside of this is keeping track of permissions in expanding cloud architectures with industry figures suggesting that 90% of identities use less than 5% of permissions granted - with too many undocumented permissions and activity sitting outside traditional IAM tools.

The speed at which these environments operate has put severe pressure on the capabilities of traditional access management platforms such as role-based IGA, IAM and PAM. While workloads have long been present in servers and private clouds these tended to be static and not time critical. What has changed is the breadth of access, but primarily the dynamic/agile/volatile nature of what needs to be managed. It is not about setting up a server on a physical machine that runs for years anymore, but about constantly changing workloads.

KuppingerCole has responded to this paradigm with our Dynamic Resource Entitlement & Access Management (DREAM) classification for access management and entitlement platforms that can manage the challenges in the computing environments mentioned above. Fundamentally, DREAM platforms must operate at the speed of the cloud with permissions based on tasks, toolchains and workloads rather than roles - and to ensure the right identities receive the right access permissions.

DREAM also encompasses CIEM (Cloud Infrastructure Entitlement Management) platforms that offer rapid access to cloud infrastructure itself and in some more advanced examples, offer granular control of cloud-based resources. Also included within DREAM are the newer PAM for DevOps tools that extend the traditional functionality of PAM for toolchain focused access for DevOps teams.

All included platforms must address the protection of the clouds themselves, the assets held in the cloud, and include those assets which remain on-premises but are needed to connect to the cloud. We are addressing such common components as VMware, Linux/Windows Servers, Web Servers, SaaS, IaaS, databases, containers, code, confidential data, secrets, credentials and privileged accounts.

The IT environment has inevitably become complex just as the business environment has made it harder to be competitive and profitable with the shifts in consumer behaviour and new delivery models of goods and services. None of this will stop; more likely the speed of change will accelerate as new technology, such as the metaverse and Web 3.0, opens new markets and opportunities. New technology, business practices and cultures are arising that will further put a strain on traditional Identity and Access Management solutions for multi-hybrid environments.

Organizations understand the business and operational imperatives for these environments but how to make them successful and to be secure is less well understood. And the tools for enhanced access and identity requirements are only just emerging. It is within this new environment that Microsoft Entra Permissions Management must compete as part of the software giant's wide-ranging effort to manage access and permissions in multi-cloud operating environments.

2 Product Description

Microsoft Entra Permissions Management is a CIEM platform intended to make permissions management more dynamic and compatible with the DREAM specification in multi-cloud environments. Fundamental to this is a shift away from managing permissions based on roles and towards analysis of historical usage and activity.

The platform has been created to engender Just-In-Time temporary access to high risk permissions and to provide always on monitoring to right size identity access and prevent excess standing privileges. The platform offers visibility and control over permissions for any identity and any resource within Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP). The number of IaaS platforms supported is highly likely to be expanded as Microsoft develops the platform. Microsoft Entra Permissions Management provides visibility and control of major identity providers, including Azure Active Directory and Google Workspace.

The platform uses a modern dashboard interface to provide admins or IT managers with an easy-to-understand window into activity across cloud infrastructures, including the multi-cloud installations. It is now more common for different cloud providers to be deployed within a single organization as individual LOBs or departments choose their own provider based on cost or usability for specific tasks.

A primary capability of an effective CIEM platform is full discovery and onboarding of identities and attached permissions in the cloud. Microsoft Entra Permissions Management uses bots that crawl networks and scan existing permissions and highlight which identities have used these permissions, how they have been used and those permissions granted but remain unused.

This informs a key part of the platform; the Permissions Creep Index which assesses the risk level associated with unused or excess permissions and the gap between permissions granted and actively used.

Customers that already use Microsoft Defender for Cloud will benefit from automatic access to Microsoft Entra Permissions Management from that platform's dashboard - we expect many more integrations with Microsoft applications over time. Microsoft has already made rapid advances to fashion the original CloudKnox CIEM platform it acquired in 2021 into an improved and recognizably Microsoft product.

To deploy Microsoft Entra Permissions Management customers are required to have an Azure Active Directory (Azure AD) account to sign in - but not Azure itself. Once established, customers with a Global Admin role can Permissions Management on their Azure AD tenant, and then onboard their AWS, GCP or Azure cloud accounts as needed. Only authorized business cloud accounts can be found so rogue cloud instances set up by individuals or teams will be missed by the platform.

Once discovery has been completed the platform has useful permissions management capabilities: it can automatically delete permissions that have been unused for more than 90 days, new permissions can be

granted on-demand and automated just-in-time access for cloud resources. All such actions can be triggered by a request for access from an identity, and all activities are recorded for analytics purposes. The user experience is the same for any identity type, identity source (local, enterprise directory, or federated) and cloud. A human identity can also request access on behalf of a workload identity which is a neat and forward-thinking capability.

For one-off scenarios where an identity needs to perform a specific set of actions on a set of specific resources, the identity can request those permissions on-demand for a limited period with a self-service workflow. Just-In-Time (JIT) and temporary access is possible for identities that need elevation to access certain resources or for a one-off project for a limited time. Flexibility is built into the platform and brings elements of traditional PAM elevation but at a more dynamic rate.

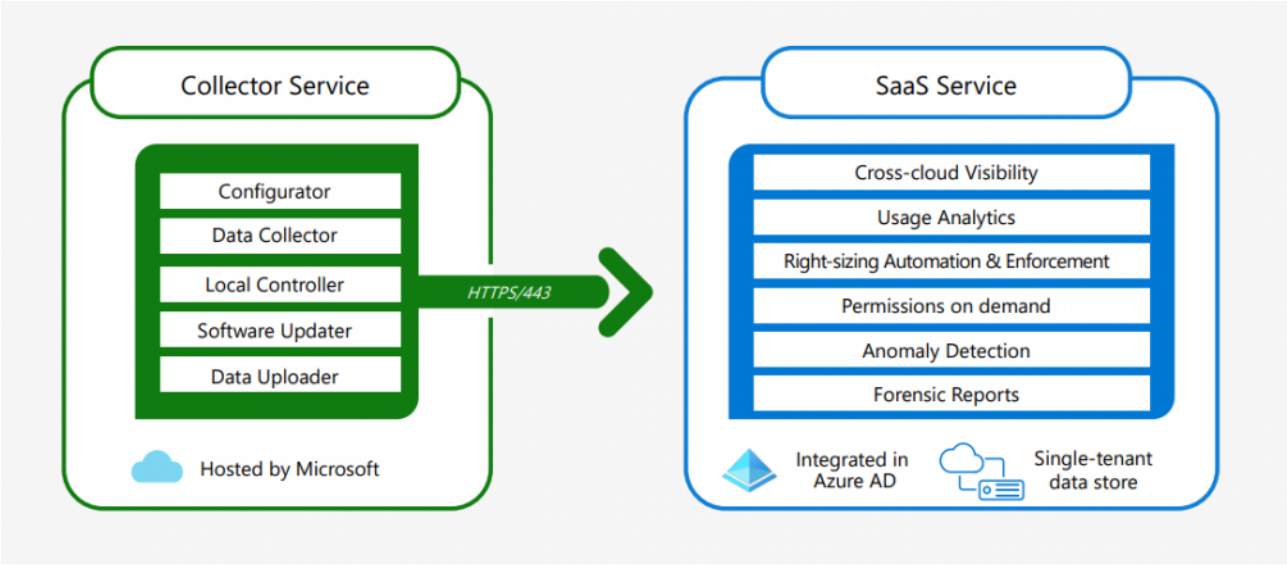

Figure 1: The deployment architecture for Microsoft Entra Permissions Management (Source: Microsoft)

Microsoft Entra Permissions Management offers out-of-the-box forensic reports which are also fully customisable to meet the needs of the reporting channels. Reports can be scheduled or produced on-demand in response to an incident or investigation and distributed by mail.

Future development will include refinement of the UX and dashboard to mirror that of other Microsoft platforms. More importantly, Microsoft says it will support more IaaS services across the board as well as VMware.

Permissions Management is available as a standalone solution, priced at $125 per resource, per year. Microsoft is offering a free 90-day trial to Permissions Management so customers can run a comprehensive risk assessment scan across multi-cloud infrastructures.

3 Strengths and Challenges

Microsoft has made a fine start to integrating the CloudKnox platform it acquired and fashion it into a simple to deploy CIEM - if you have Azure AD to begin with, which will not be an issue for many customers. It currently supports only the three main IaaS providers (AWS, GCP, Azure) but we believe Microsoft will make good on its promise to fully widen the choice of cloud services supported. It cannot yet trace activity on non-business subscribed cloud accounts but that is a greater technical challenge and for many customers, getting grip on what is happening in their business supported clouds will of great value ion itself.

The platform is also easy to use, benefits form a clear UX (which will only get getter) and has a relatively rapid onboard period. One fully installed the analytics engine refreshes the Permissions Creep Index every hour, making the platform a reliable barometer of what is happening across multi-cloud entitlement usage and permissions. There is also a useful level of options available to admins wishing to add or change permissions or grant access for JIT or limited time basis, which provides some level of PAM capability.

Thera are some omissions, we would like wider cloud support, there is not yet support for hybrid cloud (public and private) environments or Sovereign clouds and more ITSM support would be invaluable to many potential customers. Finally, the ability to run Microsoft Entra Permissions Management without Azure AD would be attractive. Overall, however, this product will undoubtedly have an impact on the burgeoning CIEM market given its rapid deployment, logical UX, strong analytics capabilities and cloud native support out of the box.

Strengths

- Simple architecture allows rapid and easy deployment and fast scanning or identities and permissions
- Supports the big three IaaS providers with native scanning capability
- Strong capability to manage identities and permissions as well as rapid access request process for end users
- Supports workload and human identities and developer environments such as containers
- Complements Azure AD PIM for just-in-time access for admin roles in Azure
- The original platform was good, Microsoft has already made it better
- Free 90-day trial available

Challenges

- The platform currently doesn't support hybrid cloud environments or Sovereign clouds as yet
- We look forward to integrations to the ITSM solutions in the pipeline.
- Pricing model based on resources may not be attractive to all customers, or easy to map accurately

4 Related Research

Blog: PAM Can Reduce Risk of Compliance Failure but is Part of a Bigger Picture
Blog: Privileged Access Management Can Take on AI-Powered Malware to Protect
Blog: Taking One Step Back: The Road to Real IDaaS and What IAM is Really About
Market Compass: Data Governance Platforms -71137
Leadership Brief: Privileged Account Management Considerations - 72016
Leadership Compass: Identity Provisioning - 70949
Leadership Compass: Identity Governance & Administration - 71135
Leadership Compass: Privileged Access Management - 80636

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.