MARKET NOTE

Microsoft Azure Active Directory: Enhancing the Power of the Platform with Identity

Jay Bretzmann

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Microsoft Azure Active Directory

As a leader of IT's 2nd Platform (defined by IDC) or client/server LAN era, Microsoft helped many organizations jumpstart their cloud adoption experiences by rolling out Office 365. This was lift and shift done right, and Azure Active Directory (Azure AD) provided the connectivity and continuity bridge back to both the on-premises environment and a simplified, single sign-on path to web-delivered apps. Using Microsoft for Office 365 is a de facto component of a multicloud IT strategy for most. Digital business transformations (DX) can be rough; the odds of succeeding improve as the need for disruptive change declines.

Key Takeaways

- Azure AD currently manages over 250 million daily active users (the majority of whom are Office 365 subscribers) and processes more than 30 billion daily authentication requests.
- Azure AD already has more than 1,000+ single sign-on and 120 SCIM implementations.
- Microsoft’s strategy is to provide a complete identity solution that can support heterogeneous environments that include all SaaS and on-premises applications and all applications and services hosted in any of the public clouds.

Source: IDC, 2020
IN THIS MARKET NOTE

IDC does not separately track Microsoft software revenue as a security-specific offering as it occurs as part of a services bundle rather than associated with a separate SKU. The offering is free with Office 365, and premium services are part of the Enterprise Mobility + Security (EMS) suite. For example, as Microsoft provides MFA for free, MFA now obviously generates no revenue, so revenue cannot be included in market share. But revenue derived from Azure Active Directory (Azure AD) services is large and growing. Some insights are provided.

Azure AD will be presented as a cloud-based identity solution leveraging a platform advantage. Microsoft has many on-premises (1.2 billion) and cloud (250 million) identities it manages and authenticates on a daily basis. The savings offered by Office 365 served to convert a large percentage of Office to a SaaS solution. Self-service password resets and conditional access will help drive premium license sales.

Also, a quick review of Microsoft's passwordless corporate initiative will be provided and it's Zero Trust model critiqued. Tech giants like Microsoft, Google, and Oracle are converting their identity infrastructures over to modern solutions and are sharing their experiences to provide hard- and soft-dollar justifications for others to do the same.

IDC’S POINT OF VIEW

Azure AD is one of many security technologies developed to support Microsoft Azure (the cloud service). Like the others, it immediately inherits an opportunity to extend what Azure customers can accomplish by creating a mass market for a standards-based identity and data access approach. Azure AD closed the open loop for defining SAML, OAuth, OData, and SCIM-compliant commercial implementations available in both free and for-fee – premium – solutions.

Customers buying premium licenses are doing so to benefit from one or more of the following:

- Unlimited single sign-on (SSO)
- Self-service password reset (SSPR)
- Entitlement management (EMS)
- Privileged identity management (just in time [JIT])
- Azure AD conditional access
- Azure AD identity protection

Microsoft is arguably in the pole position for achieving cloud identity dominance and knows it. This is a race it can win and only lose by failing to meet 3rd Platform IT connectivity and communications requirements. There's enough unspecificity in the newly developed web app industry standard specifications that going with a de facto commercial implementation these days is a very good idea. Azure AD already has more than 1,000+ single sign-on and 120 SCIM implementations. It's like choosing DOS in the early days of personal computing. Grab enough of the early market, participate in future standards definitions, and you've likely got a sustainable business.

Azure AD currently manages over 250 million daily active users (the majority of whom are Office 365 subscribers) and processes more than 30 billion daily authentication requests (see Figure 2). It's premium customer base includes 100,000 organizations and is rapidly growing. There's still a lot of upside potential there and passwordless momentum will build rapidly now that MFA is freely available.
to all. IDaaS vendors tend to offer a menu of services based on some dollars per user per month, and depending on the coverage, they can add up quickly. Microsoft list prices are $6 and $9 for premium 1 and premium 2 licenses, respectively, and discounts apply based on total contract value. Other providers can charge more.

FIGURE 2

Azure AD Estimated Usage Supporting Microsoft Azure Cloud Services

![Diagram of Azure AD Estimated Usage]

Passwordless is just one element of Microsoft's Zero Trust security model, but it is a big draw, and a state that can be only be achieved using multiple means of authentication and sufficient risk modelling technologies. Windows Hello, Microsoft Authenticator, and the use of OATH certificates can probably cover >90% of all log-on requirements. Why go passwordless? Microsoft's internal initiative is aimed at improving security while significantly reducing costs including:

- $3 million a year in hard costs
- $6 million a year in lost productivity

Microsoft's definition of Zero Trust is also very pragmatic. Treat everything as if it's coming from an internet source B2E, B2C, and B2B. Restrict corporate (LAN) network access from all but a very few privileged users using least privileged access (LPA) policies and time-limited, just-in-time access. Smart and modern from IDC's perspective.

The company's transition is ongoing and presently moving beyond identity and authentication strengths to device management and support beyond Windows, macOS, and mobile (Android and iOS). It will be years before Zero Trust is fully realized, but the journey will pay increasing dividends along the way.
Azure AD covers all identity management use cases:

- **Azure AD.** IDaaS aimed at B2E users to provide and control access to cloud resources
- **Azure AD B2B.** A feature in Azure AD allowing cross-organization collaboration in applications linking multiple Azure AD tenants
- **Azure AD B2C.** An independent service for building a consumer application identity repository allowing anyone to create an AD identity by leveraging their email or social media provider (Facebook, Google, or LinkedIn)

The future direction is to merge these offerings adding identity protection capabilities to B2C users and broad support for federated endpoints (Google Cloud ID and SAML app) for B2B users. Eventually, the only difference between the offerings will be the pricing model for employees versus external (first 50,000 users are free).

IDC believes this is more evidence toward an eventual merger of the IAM and CIAM markets. The battle will be one of scale as it often is. Any IAM vendors not positioning themselves to support CIAM requirements may end up doing a Yahoo! or an AOL. Providing core identity services at internet scale might be as significant as owning search capabilities from a "let's build an extendable business" standpoint.

There has been and will always be IT buyers that want to pursue a more "open" or specialist route and rightly or wrongly consider Active Directory dependencies to be an element of vendor lock-in. Others simply face needs that a platform solution can't address, and so they seek out point solution products to fill the gaps. In either case, IDC believes there must be sufficient operational efficiency savings to be had by vendors, and recognized by customers, to justify the existence of identity market solution specialists. These early market offerings tended to be built by very smart coders who occasionally created runaway, category-defining products (Salesforce). Some of the identity pioneers included Okta, Ping, SailPoint, and CyberArk. Not surprisingly, all their products work together to deliver cloud directory, authentication, governance, and privilege monitoring.

**LEARN MORE**

**Related Research**

- *Privileged Access: Expanding Beyond the Core and into the Cloud* (IDC #US44775119, September 2019)
Synopsis

This IDC Market Note discusses Microsoft Azure Active Directory services. When measuring identity projects with a fun meter, the needle doesn't rise that high for most organizations. These are big efforts and investments for larger (older) organizations: those running 2nd Platform IT environments where identity "isn't broke yet." But in reality, it really is broke and here's why: environments hanging on to older communications, encryption, and authentication protocols are exposed to security flaws that no vendor is ever going to address with new investments. DX projects built upon a soft foundation are riskier.

Phishing is already the leading cybersecurity attack technique because it's so cheap and effective. It exploits identity weaknesses that exist because aging systems were never designed to defend against sophisticated cybersecurity malware. Companies (e.g., tech examples provided) that have implemented better identity practices have seen phishing and reverse proxy man-in-the-middle attacks almost disappear.

A proliferation of networks, devices, and applications needed to support daily business share one common element – the user. Microsoft has said, "Identity is the control plane. It's critical to establish who the user is as the core of trust for other transactions. If we aren't sure who the user is, no other system access control or security matters." IDC concurs.
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world’s leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2020 IDC. Reproduction is forbidden unless authorized. All rights reserved.