HELPNETSECURITY

www.helpnetsecurity.com | June 16, 2021

How to secure data one firewall at a time

The need for secure data access management is top-of-mind in the C-suite and boardroom. The question I keep hearing from IT departments is how to do it right, that is, how to ensure security and governance without frustrating users or slowing innovation.

Canming Jiang

CEO, Datawiza

By taking advantage of the as-a-service strategy, which has revolutionized IT and transformed business models, a new data access management approach, Access Management as a Service (AMaaS) may provide an answer.

With the COVID-19 pandemic, companies have accelerated their cloud journeys, migrating more data and applications to multiple cloud providers and adopting more cloud services to provide new capabilities faster to a greater number of people. This includes at-home employees and contractors, many of whom will continue to work remotely for the long term.

Less and less data lives where IT can easily secure it, residing instead everywhere, including across hybrid multi-cloud environments and on user devices outside the firewall. Think about a "work from home" customer support technician using a personal computer who requires access to half a dozen corporate databases located on multiple public and private clouds around the world, as well as on on-premises infrastructure.

This distribution of data has broken down the distinction between the assumed safety inside the corporate firewall and the assumed risk outside it. The new model is zero trust, where access by every device and user, whether inside or outside the firewall, requires verification.

In addition, it is no longer sufficient to achieve trust simply through authentication – ensuring people are who they say they are. We must also reduce risk through authorization – ensuring only the right people have access to sensitive information, something that can change quickly and must be acted on immediately. This is the only way to comply with evolving data privacy regulations such as GDPR and CCPA.

According to Gartner, "As remote work increases access management tool adoption, and security controls shift to identity, the ability to secure access with AM strategies aligned with continuous adaptive risk and trust assessment is paramount."

In this environment, you must create a comprehensive, manageable way to authenticate and authorize every attempt to access data – based on a fine-grained access principle – while still providing users with the secure self-service access they need.

"By taking advantage of the as-a-service strategy, which has revolutionized IT and transformed business models, a new data access management approach, Access Management as a Service (AMaaS) may provide an answer.

The limits of today's strategies

Identity access management (IAM) includes two major competencies that have remained distinct: identity management (IM) and access management (AM).

Over the last few years, we have seen significant innovation in the IM space, with the rise of several popular modern IM solutions such as Azure AD, Okta and Auth0, which are now referred to as Identity as a Service (IDaaS).

However, we have seen little innovation in the AM space, and the IDaaS solutions alone cannot create a complete enterprise solution for authentication and authorization. Tools like Symantec SiteMinder, which was introduced more than 15 years ago, were powerful in their day, but they were never designed for modern hybrid multi-cloud environments and do not integrate well with IDaaS. Trying to use them to solve the modern authentication and authorization challenge has several critical disadvantages, including:

- Expensive and costly to implement
- Long time to value
- High total cost of ownership
- Difficult to install and manage
- Don't work well in hybrid multi-cloud environments

Companies have told me that moving their applications from a legacy authentication system to a modern one required significant and painful application rewriting, and multiple time-consuming manual configuration steps that led to frequent errors. Even integrating new applications with solutions like Azure AD or Auth0 required heavy integration work, for example, learning the modern authentication/authorization protocols (e.g., OIDC/OAUTH), learning different platforms' SDKs/APIs, writing integration code for each app, and so on.

This has been especially hard on enterprises that had to migrate hundreds or thousands of applications, causing IT bottlenecks that frustrated employees and even increased the very security vulnerabilities they were trying to reduce. Companies have also found that rewriting a custom authentication system based on new protocols is a lengthy and expensive proposition and requires security expertise, delaying the move to zero trust.

Similarly, companies that have written custom authentication solutions based on outdated protocols, such as basic auth, cannot implement the latest security best practices or take advantage of IDaaS without significant rewriting.

So how can you migrate your legacy applications to IDaaS without rewriting them? How can you integrate your new applications to IDaaS in a no-code/low-code fashion? And once you have your apps migrated/integrated with IDaaS, how do you enable a unified, policy-based authorization across your hybrid environment (which may include multiple IDaaS providers and multiple private and public clouds) without creating an administrative bottleneck that hinders user productivity or requires constant attention from security professionals? Finally, how can you accomplish all this cost-effectively and with a quick time-to-value and low total cost of ownership?

A framework for AMaaS

Access Management as a Service, like most "as a service" offerings, provides an easy-to-deploy solution that simplifies, centralizes, and automates key business processes. This frees IT (system admins, DevOps and developers) from complex and costly activities that distract from more strategic tasks, while also allowing businesses to consume the service on a subscription basis and reduce Capex costs.

An AMaaS solution should satisfy these goals while also meeting the access management challenges with the following capabilities:

• **Security and trust** – The secure access management environment must authenticate and authorize every employee, customer, contractor or partner each time they access data – based on modern security protocols, zero trust, and MFA (multi-factor authentication) – with fine-grained access controls.

• **Support for hybrid multi-cloud environments** – The AMaaS must

> “
>
> **You must create a comprehensive, manageable way to authenticate and authorize every attempt to access data – based on a fine-grained access principle – while still providing users with the secure self-service access they need.**

work with every environment (on-premises, multi-cloud, hybrid-cloud), no matter where the applications and data reside.

- **User productivity** – The solution must support SSO (single sign-on) across siloed environments, such as multiple clouds, so each user needs to have only a single login ID and password to verify who they are and their access rights across every application and data source.

- **Ease of maintenance** – Administrators should not need to keep policies, roles and permissions updated across dozens or hundreds of applications. The AMaaS should promulgate a single update across hybrid multi-cloud environments.

- **Ease of deployment/faster time to value** – It should be possible to create a secure AM environment without deploying hardware or installing and maintaining a suite of complex enterprise software. AMaaS should also eliminate or minimize the need for rewriting applications or writing new integration code.

- **Centralized management** – The entire AM environment should be visible from a single pane of glass with access to analytics regarding data access and usage.

- **Future proof** – The AMaaS should rely on published APIs so it maintains the relationships between the AMaaS and IM systems and between the AMaaS and corporate applications as the IM systems and the applications are updated.

With data security, regulatory fines, user productivity and brand reputation at stake, you can no longer rely on legacy access management solutions or complex and disconnected custom strategies that frustrate IT administrators and users alike. AMaaS, in conjunction with modern IM solutions (IDaaS), must form the foundation for enabling a zero-trust model with SSO and MFA. This will enable organizations of all sizes to provide users with the secure access they need – with simple, streamlined, and centralized management.

> **Access Management as a Service, like most "as a service" offerings, provides an easy-to-deploy solution that simplifies, centralizes, and automates key business processes.**