WHAT IS IDENTITY-AS-A-SERVICE? IDAAS EXPLAINED

Cloud computing brings unprecedented new requirements to manage user identity and access privileges. The average number of cloud-based apps used in enterprises ranges between 900 to 1200 different services. If each service requires its own set of login credentials, users will inherently rely on vulnerable password combinations or avoid using the service entirely. In order to manage authentication across the growing number of online services or internally networked apps, organizations need to manage the authentication credentials for end-users. Capabilities such as Single Sign-On (SSO) may be critical to improve end-user experience and enable transparent authentication procedures for all cloud-based services used within the enterprise network.

Identity as a Service (IDaaS) allows organizations to realize these goals as they work toward improving the security posture of the organization while making it easier for employees to leverage the vast array of cloud services at their disposal.

Identity as a Service is described as the authentication infrastructure managed and hosted by a third-part cloud vendor to provide identity and access management services. IDaaS goes beyond SSO and covers the wider identity governance and administration (IGA), access management and intelligence functions for cloud and networked IT services. In comparison with traditional Identity and Access Management (IAM) systems where the policy framework and technology infrastructure may be devised and managed in-house, IDaaS lets organizations leverage advanced IAM capabilities without having to deal with the complex and rigorous underlying infrastructure, policies and practices necessary to maintain regulatory compliance and high standards of security. In addition to managing employee access and privileges across the growing number of apps,

enterprises also need to understand when, where and how the services are being use. This is a greater challenge in the SaaS-driven enterprise IT segment where the employees resort to Shadow IT practices to access cloud-based services without formal approval of the internal IT departments, opening doors to even greater security issues. In order to address these concerns, organizations can facilitate adoption of the necessary cloud apps without compromising security through effective IAM capabilities available as IDaaS offerings.

Key Components and Functions of Identity as a Service

IDaaS solutions offer a range of features and functionality that vary across vendors and market segments. The most common components that constitute an Identity as a Service offerings include the following:

- **Cloud-Based and Multitenant Architecture:** The IDaaS vendor typically operates a multitenant cloud architecture to deliver the service. With the multitenant service delivery model, the vendor can issue updates, security fixes and performance improvements to every customers immediately as they are available. As a result, customers can enhance their capabilities to manage access provision provisioning and governance effectively. With the cloud-based offering, organizations can scale the usage of IDaaS solutions to meet the evolving IAM needs at the workplace while only paying for the service consumed and saving the initial capital expense.
- **Password Management and Authentication:** As a fundamental requirement of identity and access management, the IDaaS service incorporates all necessary means of authentication and password management. These include features such as multi-factor user authentication via passwords, digital access cards or biometrics that are maintained dynamically across user devices and access points. For the end-users, these mechanisms should be simple and facilitate the security awareness in accessing sensitive business information, resources or premises.
- **Single Sign-On and Federation:** Among the other key IAM features and functionality associated with IDaaS, the service is typically designed to maximize end-user experience while maintaining security and availability of the corporate network to users as intended. With the SSO feature, users can be encouraged to use the safest password combinations without working too hard to remember them to access regular IT services on a daily basis. Similarly, the federation capability of an IDaaS system allows organizations to manage secure authentication for third-party cloud services accessed beyond the control of internal IT departments.
- **Automated Approval Workflows:** Automated approval workflows enable IT departments to enforce and synchronize access privileges across multiple apps fast and effectively. These tools typically offer GUI based configuration capabilities that make it easier for IT admins to manage provisioning and follow a systematic governance framework to reduce risk and costs associated with IAM functions.
- **Analytics and Intelligence:** Advanced IDaaS offerings include the analytics and intelligence capabilities to report the use of access privileges in context of multifaceted relationships between users, their roles and responsibilities, job functions, application and data usage. This information is delivered in a consumable format, allowing organizations to identify anomalies such as active accounts for former employees or usage patterns for a specific type of workforce segment.
- **Configurable IAM Implementation Templates:** Organizations can take advantage of vendors

serving IAM implementations across several customers and devising easy-to-configure templates most suitable for a variety of customers. Flexible provisioning workflows that don't require manual scripting allow IDaaS customers to follow repeatable IAM processes that work effectively and scale across a growing user-base. The best IDaaS solutions allow organizations to perform IAM procedures with minimal customization requirements so that the system remains as simple, extensible and replaceable when needed.

- **Governance, Risk and Compliance:** Organizations can manage governance, risk and compliance by leveraging the automation and intelligence capabilities of an IDaaS system. The technology allows organizations to enforce governance policies and frameworks to mitigate security and compliance risk. For instance, organizations can define and automate application-specific processes to understand the access and usage patterns based on compliance-sensitivity. Similarly, the real-world authentication process and access privileges should align with evolving organizational policies that change based on varying market circumstances, geographic presence and compliance regulations.

Identity theft has emerged as a growing security challenge for enterprises. The Identity Theft Resource Center (ITRC) found that over 91 percent of the identity theft attacks compromised corporate databases in the year 2017. With the introduction of stringent global compliance regulations in the form of GDPR, HIPAA and others, organizations are forced to take extra measures in protecting user accounts of internal workforce, contractors and end-users beyond the organization. As a result, an end-to-end identity and access management functionality is required to ensure strong security posture against the growing risks associated with the adoption of cloud services.