awsmarketplace

Security

Identity as a Service (IDaaS) for Single Sign-on with AWS

Identity and Access Management Challenges

The rapid increase of application use outside datacenter control highlights the limitations of traditional corporate identity and access management solutions. This growing landscape consists of cloud-based applications (Workday, Salesforce, Box, etc.), along with other web and mobile-architected applications. Users must create a separate identity for each application, which are natively accessed outside the corporate directory, introducing vulnerabilities to your security posture.

Identity Simplification

Identities in multiple systems require users to repeatedly sign-on to applications throughout a day. Security threats increase with these identities, since authorization managed outside the corporate directory creates the potential for leaving sensitive data vulnerable to unauthorized access. This loss of identity management and access control over corporate information creates security and compliance risks. Thus, many organizations consider a consolidated identity management scheme to be a best practice in today's corporate application environment.

Identity as a Service for Single Sign-on

In order to achieve consolidated identity management, organizations are turning to Identity as a Service (IDaaS). Single Sign-on (SSO) is commonly defined as the ability for a user to provide credentials a single time in a session to gain access to multiple application services. IDaaS services provide capabilities that span multiple identity and access management functions, for applications behind the customers' firewall and in the cloud. These functions include automating and synchronizing changes to identities held in the IDaaS or obtained from the customers' identity repositories. IDaaS services offer pre-integrated connectors to target applications, which enable SSO to the target applications.

The AWS Solution

Organizations that want to include their Amazon Web Services environment in an SSO scheme can do so with Federated Identity (FID). You can define roles and policies that enable this secure access without having to manually setting up users. These roles and policies dictate what a user can do while they are logged into the AWS account. You can then use your IDaaS provider to allow employees access to the appropriate services in your AWS account through the roles and policies that you have defined.

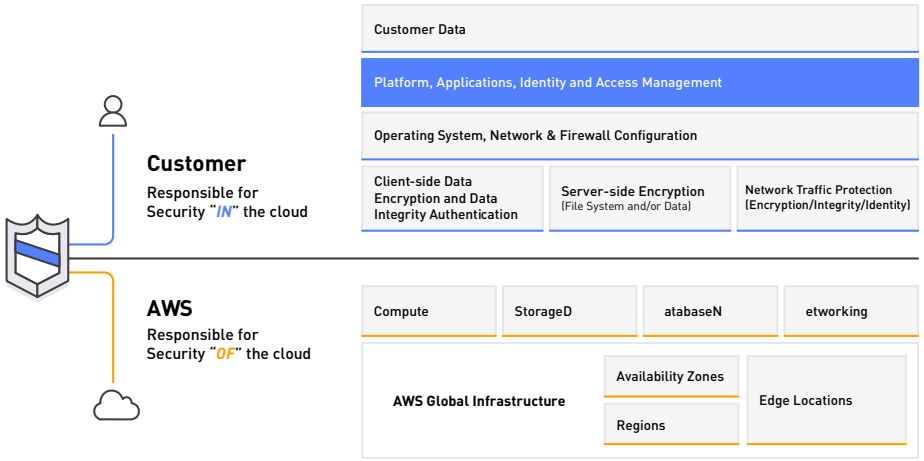

Figure 1: The AWS Shared Responsibility Model

When you choose to deploy on AWS, it's important to understand your role in securing your AWS environment. As the AWS Shared Responsibility Model illustrates (see figure 1), AWS provides a datacenter and network architecture built to meet the requirements of the most security-sensitive organizations, while you are responsible for securing services built on top of this infrastructure. An IDaaS solution can help simplify complexities of identity management, a key component of upholding this responsibility.

IDaaS Deployment Options

IDaaS services available in AWS Marketplace can be purchased and deployed independent of whether an organization uses Amazon Web Services. Doing so allows organizations to enhance their data protection with centralized identity and access control, where the corporate environment includes cloud applications, and web and mobile-architected applications that use identity systems outside the corporate directory.

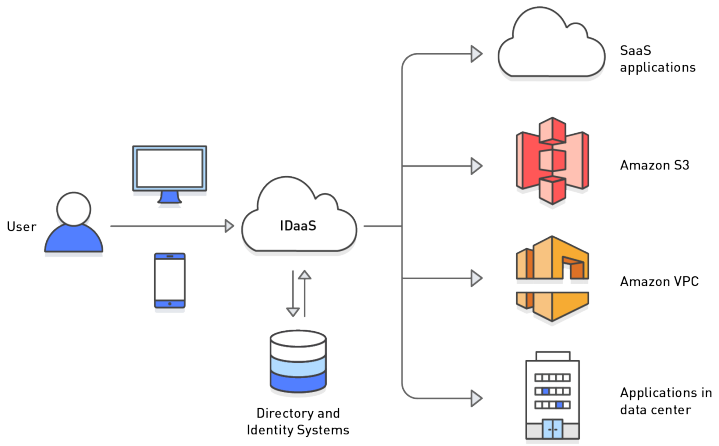

Figure 2: IDaaS for Single SIgn-on with AWS

1 IDaaS with AWS

IDaaS offerings in AWS Marketplace provide capabilities for identity and access management. These vary by ISV offering and can include a range of identity governance and administration, logging, reporting functions, and Single Sign-on implementations. These capabilities can be used with AWS managed services and applications deployed in Amazon EC2 instances. You can connect an IDaaS to your existing directory, whether it resides in your AWS environment or your data center. Using an IDaaS, you can deploy Single Sign-on for secure user access to your AWS environment and other applications available to your organization. See figure 2.

2 IDaaS with cloud-based applications

Organizations can choose to deploy IDaaS offerings from AWS Marketplace to provide identity and access management that must span combinations of on-premises, SaaS, and legacy applications. Often organizations choose an IDaaS to simplify identity and access management, and provide users simple and secure Single Sign-on.

Simplify your identity and access management and provide Single Sign-on with IDaaS offerings in AWS Marketplace.

Get Started with IDaaS at AWS Marketplace

Find and deploy the solution you need in minutes

Save money with pay-as-you-go pricing

Scale globally across all AWS Regions