|  |
| --- |
|  |
| APP CLOUD SECURITY |
| QUESTION 5 |

|  |
| --- |
| Kiran Katticaran  4-20-2021 |

It's entirely up to you to enforce cloud application protection. If something goes wrong, you won't be able to blame a committee of system administrators and enterprise developers like you might when you designed conventional enterprise apps, where all you had to think about was a user ID and a password. Usually, businesses fail to consider their requirements and problems before developing a strategy, designing a solution, and choosing an IAM technology. Each IAM product takes a unique approach. While some products are geared toward cloud computing, others are designed for more conventional business models.

IAM must be seen as a market engine as well as a security technology, similar to encryption. IAM software developers must concentrate on both the core business processes and the details of the security mechanism when deploying it. That's a significant change from when most people thought of protection as a nerdy term with no regard for business drivers. You, the app developer, are in charge of putting the security plan into action.

The good news is that you can simultaneously reduce identity management costs by implementing mature IAM capabilities while still being more flexible in supporting new business initiatives. I believe that IAM functions will be needed in more than half of all existing applications that are migrated to the public cloud, as well as in nearly 90% of new cloud-based applications.

Furthermore, as companies modernize security techniques and technologies to comply with the usage of the public cloud, the use of IAM within cloud application deployments can back-fill into the enterprise. IAM would be sold as a service back into the business in some instances. As a result, the transition to IAM-enabled cloud applications would improve the quality of current enterprise security systems. Resulting in this, cloud applications will be more stable than traditional on-premises enterprise apps. Developers who learn to incorporate IAM capabilities into cloud apps will likely layer those apps back into conventional on-premises systems. If consistent level of protection across the enterprise needs to be maintained, both in the cloud and on-premises settings, this is a must.

Developers must first understand their core specifications before choosing and implementing IAM for cloud-based platforms. Every problem domain is unique, and each security solution is as well. However, you'll need resources in these four areas in any case:

* Identity management services
* Access management services
* Authentication services

***Identity management***services Identity lifecycle management, access provisioning, centralized function management, and process design and implementation are all terms used to describe identity lifecycle management. The concept is to provide core identity management services that allow you to identify core identities for all resources and actors, grant access to those resources, store and read those identities in a centralized, enterprise-wide mechanism, and manage how you can operationally utilize each.

***Access management services***refer to services such as single sign-on, federation, role-based access, and platform access. This in sync with identity management services, helps in granting access based on authorization using identity information.

***Authentication services***Multifactor authentication, out-of-band authentication, and managed authentication services are all examples of managed authentication services. The critical point here is that you, as the developer, must be familiar with the core components of the IAM framework you choose based on your requirements. To find the best solution, make a list of your most important IAM specifications and compare the solution components offered by each IAM technology provider.

From the beginning, integrate cloud-based identity management tools with enterprise protection. Protection should be holistic, and those in charge of developing security applications should use precise application security approaches to do so. It makes no difference whether you're in the cloud or not.

Prioritize the design and architecture of your security solution before deciding on technology. Although the design of your solution would be more complex, it should be able to withstand many technological changes.

Integrate security testing into the DevOps pipeline. This entails ensuring that the applications are adequately protected and conform to the requirements you've scripted. Any kind of automation of these tests and checks are essential for deploying stable, cloud-based applications consistently.

When creating your concept, keep success in mind. While most IAM systems do not slow things down, they do in certain circumstances; encryption, for example, can cause significant latency. These kinds of problems are more difficult to resolve after deployment. Furthermore, they appear to cause problems with your security systems because users, frustrated by the slowness, easily find out how to get around your carefully designed security mechanisms.

Understand the security legislation and enforcement standards in your business. If you have them, you can control them via IAM's identity governance scheme, and you can use them to decide the type of encryption you need. It's difficult to make changes to your enforcement policies after being implemented, so make sure you know what you're getting into upfront.

https://techbeacon.com/app-dev-testing/cloud-app-security-how-not-fail