Executive Summary

Since most of the businesses are now digital, corporations need systems to run and support the business processes. Without these systems, the business processes would not be able to function or thrive. Our cloud journey started way back at the time when Yahoo and Hotmail came into effect. Since then, the journey has come a long way and core business applications are being newly designed and deployed and lifted or shifted over the landscape. This, however, has both positive and negative outcomes.

To secure cloud-native applications, we need to analyze what are the security requirements for each new layer of the application stack. We must also recognize that we need a modern security toolset across the CI/CD development pipeline.

This whitepaper elaborates our point of view of how important it is to protect our applications in the times of Cloud and what are the primary ways to protect our cloud-native applications from identity and access risks.
Understanding Identity and Access Management Risks

In a typical environment, the cloud-native applications would secure all their endpoints, giving access only to authenticated users or services. Every request for an application’s resources includes information about who is making the request and what access role and privileges they have, whether one is an application administrator or a business user.

As sensitive containers and micro services and resources are accessed from anywhere on the Internet, we must establish the identity of a user with certainty, especially if users include other micro services, employees, contractors, administrators, developers, partners, and customers. In case of a micro services-based cloud-native application, we want to ensure that identity management toolset and access control enforces business rules.

Need for Identity and Access Management

Identity and access authentication enables applications deployed to the cloud to authenticate users at an application level, based on a range of identity providers. A solution is needed that should have the capability to store user data, such as application preferences or information from the user's public social profiles, that can be leveraged in the application to support engagement.

What is needed is a trusted platform that would act as an identity foundation enabling us to provide secure, scalable, and smart experiences. The platform should be seamlessly managing an enterprise client’s digital identities for its workforce and customers.

Modern cloud-native identity solutions use open standards to achieve secure application access from clients. These clients range from human users on PCs or phones, to other apps hosted anywhere online, to set-top boxes and IOT devices running any software platform anywhere in the world.
Coforge Domain Capability in Identity and Access Management

Coforge has a dedicated offering for Identity and Access Management called ACE (Access Control & Entity Management) that helps our customers understand the exact problems and ways to deal with them.

The scenarios below help us further understand the benefits of ACE.

Scenario 1: Identification and mitigation of risks driven by access granted to users

Organizations today face several challenges in identifying and mitigating risks arising due to users having access to systems:

- Difficulty in identifying suspicious users due to lack of visibility across security solutions
- Exponential influx of identities makes governance of identity and access beyond human capacity
- Due a lack of insights on the required action, rubber stamping has become a norm

Coforge has a full-blown solution that helps in mitigating identity-related risks through Identity Analytics. Some of the features of our solution are:

- Highlight anomalies in peer groups
- Configure policies aligned to business needs
- Risk scores for users, entitlements, and applications
- Help in deciding the course of action
- Act on any identified risk
- Build customized remediation workflow’s

Benefits

The solution leads to a host of benefits:

- **Better Security Insights**
  - Highlight anomalies in peer groups
  - Configure policies aligned to business needs

- **Increased Operational Efficiency**
  - Risk scores for users, entitlements, applications
  - “Help me decide”

- **Quicker Response Time**
  - Act on identified risks
  - Build customized remediation workflows

Scenario 2: Gaining synergistic value when multiple siloed security products are deployed

Due to the deployment of multiple siloed security products, organizations are unable to achieve synergistic value and face the following challenges:

- Determine who should have access to encrypted data
- Need to attest access for privileged users in a systemic manner
- Already have a corporate portal for self-service access request and don’t want another interface for users

Coforge provides a solution that is extensible and provides an ecosystem of integrations.

Benefits

With reference to the given scenario, the solution provides the following benefits:

- **Integration with Data Governance**
  - Strengthens data access governances

- **Integration with PAM**
  - Centrally manages all IDs
  - Recertifies “privileged users”

- **Integration with ServiceNow**
  - Adds identity capabilities to existing access portal
  - Simplifies user experience
Coforge is a global digital services and solutions provider, that leverages emerging technologies and deep domain expertise to deliver real-world business impact for its clients. A focus on very select industries, a detailed understanding of the underlying processes of those industries and partnerships with leading platforms provides us a distinct perspective. Coforge leads with its product engineering approach and leverages Cloud, Data, Integration and Automation technologies to transform client businesses into intelligent, high growth enterprises. Coforge’s proprietary platforms power critical business processes across its core verticals. The firm has a presence in 21 countries with 25 delivery centers across nine countries.
Learn more about Coforge at: www.coforge.com

Stay connected:  

For more information, contact information@coforge.com
© 2022 Coforge. All rights reserved.