OPTIMAL IdM
Identity & Access Management

Info Sheet

API Enablement

How to gain the benefits of APIs while controlling risk.

APIs expose businesses' data and digital services to a complex interconnected ecosystem of partners, vendors, customers, IoT devices, and other apps. That exposure brings benefits, but it also carries risks. APIs need to be treated with the same cautions that are applied to human users. Each must have an identity, and that identity must be protected against attacks that exploit vulnerabilities in authentication, authorization, and session management. Optimal IdM helps customers navigate API enablement to eliminate risk and ensure proper security protocols are followed.

The Role of Business Owners

API authentication and authorization rules need to be handled by someone with the security experitse to harden the code and the business knowledge to tie the roles and privileges to the business model. Business owners should take a leading role in the API development process to ensure the API includes the appropriate user authorizations.

Managing Roles and Privileges

When dev teams set up an API, often times the business owner is prevented from making changes that become necessary as the business model evolves. Changes have to be fed into the software development framework, where they then wait to be prioritized and executed. The result is hindered agility. In addition, hard-coded authentication and authorization rules make compliance difficult. An auditor would have to understand each API in order to determine its compliance. For the same reasons, governance also becomes unmanageable when rules are hard-coded. A global approach to API enablement is the gold standard.

Risks of APIs

An APIs interface may be exposed or misconfigured on an application which contains sensitive information about a business's infrastructure. Malicious actors can leverage this information to plan an attack tailored to exploit the organization's vulnerabilities. In addition to APIs being susceptible to an attack, unprotected APIs can be used to launch attacks, like Distributed Denial-of-Service (DDOS), that can cause service outages across the entire API ecosystem. This type of attack is on the rise because it is less costly to execute than a DDOS attack against other network layers and is difficult to detect in real-time.

Highlights

Best Practices for Secure API Enablement

Developers have traditionally been expected to focus on functionality and agility. Today, they need to focus on security as well. To ensure that APIs are enabled securely, Optimal IdM provides developers with the resources, training, and guidelines necessary to ease development and strengthen the organization's defensive posture.

Here are a few Optimal IdM best practices for secure API enablement:

- Recognize inherent risk
- Use existing libraries rather than writing new code
- Use automated tools to test APIs for pre- and post-login capabilities
- Place authentication and authorization decisions with the business owner
- Do not embed system traces in error messages
- Do not register internal API names in public DNS databases
- Enable deep reporting and use auditing and logging
- Formalize "continuous security" practices

Optimal IdM has cataloged 7,000+ claims-aware, federated applications that are pre-integrated into the The OptimalCloud™. These include legacy on-premises and well-known SaaS services and applications. The OptimalCloud is a scalable and customizable Identity and Access Management (IAM) solution that combines directory services, advanced identity governance, application access management and a rich open standards-based platform for developers. That means Optimal IdM manages the service, configurations, customizations and can provide concierge support for application onboarding assistance.

For customers, this means that federation and development skills are not needed and depending on the application, neither is application retooling and synchronization. Software agents on servers and cleanup of existing directory services are not needed. More applications are added every day.

For more information on API enablement, e-mail us at info@optimalidm.com and visit www.optimalidm.com/application-integration.

OPTIMAL IdM