AppOmni

TECHNICAL WHITEPAPER

USING ROLES FOR CONTINUOUS SAAS SECURITY MONITORING

TABLE OF CONTENTS

ROLE-BASED MONITORING

Understanding the ins and outs of effective access, permissions, and sharing in Software-as-a-Service (SaaS) applications can be challenging for even the most mature security and IT organizations. When you scale this problem across thousands or tens of thousands of supported employees in multiple SaaS clouds the complexity of the problem scales exponentially. AppOmni solves this problem by allowing you to explore, monitor, and alert on representative Roles within your SaaS clouds and see which of your users are represented by that Role - and which aren't.

ACCESS CONTROL IS HARD

Role Based Access Control (RBAC) continues to be an industry-standard strategy in controlling and granting access to SaaS users for good reason - it makes sense to provision access based on job function and business need. But when it comes to implementing an RBAC strategy in practice it can be incredibly complex.

Large enterprises must support thousands or tens of thousands of internal users. This number grows in magnitude when external cloud users for service, support, and relationship management systems are considered. Multiply that by accounts in many different clouds and an effective security team must now find a way to understand hundreds of thousands of accounts in their cloud environments.

ACCESS CONTROL DRIFT ACCELERATES A LOSS OF CONTROL

As SaaS applications add new features and businesses acquire new technologies or platforms, the access granted to users in the enterprise naturally grows as well. When new features or clouds are deployed IT teams find themselves under pressure to grant access as soon as possible and Security teams may be left trying to catch up. Under business pressure and facing increasingly complex permission schemas it is easy to see how individual users or groups may be inadvertently over permissioned in cloud applications.

A single over-permissioning issue rarely remains that way. New users' permissions and access are frequently provisioned by cloning existing users. Mistakes in access controls and permissions are then propagated, growing the number and complexity of over-permissioned users. Incomplete or misunderstood attempts at fixing individual issues compound this problem. After a few release cycles of this, the entire enterprise consists of snowflake permission and access configurations. IT and Security teams are not given the tools to easily find or fix these issues, especially when there is

a potential business impact to incorrectly removing permissions. The end result is an access control model optimized for least friction instead of least privilege.

THE SOLUTION: STANDARD PERMISSIONS AND ACCESS

The solution to this problem points back to the original intention behind RBAC frameworks: there should be a very limited number of differing permission and access sets across an organization. The Effective Access of a given employee or external users should, in most cases, be identical to that of another employee or user with the same job function.

The key, then, is to give Security and IT teams the ability to quickly visualize the Effective Access of a given Role across a cloud application as well as to report on what users share the same permission bundle - and which users do not. Users identified as having abnormal permissions bundles or incorrect effective access can then be brought into compliance with tooling that shows administrators exactly which permissions bits or permission sets are granting the erroneous effective access

Solving the problem of understanding and standardizing access requires giving Security and IT powerful, easy-to-use tools to quickly and accurately visualize the actual, effective access of a given SaaS user or cohort of users. This is critical to addressing the gap between intention and implementation when it comes to the complex control planes that govern access to data in SaaS applications. Security teams often have policies and guidelines for how data access should work. What they lack is the ability to quickly and easily evaluate effective access relative to intended access. In addition, these teams need tooling that helps them catch outliers - users who have, either through mistakes or permission drift - been granted abnormal access.

With this tooling, Security and IT teams can work together to bring order to chaotic cloud environments. 10,000 employee users with 10,000 different permissions bundles can be quickly organized into 15-25 clearly defined Roles each with uniform Effective Access.

CONTINUOUS ROLE MONITORING

Giving Security and IT teams the tools they need to clean up permissions drift and implement a solid RBAC strategy is only half the battle, though. Once SaaS applications are in a known-good access control state it requires constant effort and attention to keep them that way. Without that continuous monitoring it is almost certain that permissions drift will creep back into the applications' configuration and require repetitive assessment and clean-up efforts.

Instead of requiring fire drills around per-release, per-quarter, or per-audit assessment and remediation tasks, automated monitoring and alerting is necessary to maintaining an effective RBAC strategy in real-time. Smart automation can assess SaaS applications' configuration and effective access by interrogating real-time permissions models. Any deviations from an approved security policy can be immediately alerted on and remediated. If integrated with sandbox or pre-release environments, these policy deviations can be prevented from ever affecting live data.

YOUR INTENDED ACCESS CAN BE EFFECTIVE ACCESS

Automation that accomplishes the goals of an effective, consistent, and continuously monitored RBAC policy is not theoretical - it is available today. AppOmni's patented SaaS permissions modeling technology allows you to gain immediate, actionable insight into the effective access users have to critical business data in your SaaS applications.

Once clear Roles have been defined in your SaaS applications - whether there are five roles or fifty - AppOmni can be connected to representative user accounts in each of those roles. From there, AppOmni's automation is able to scan and model the effective access of each role and compare it to your described, intended state.

AppOmni's automation platform helps you take your RBAC strategy from intention to implementation and then keep it there. All you need to do is describe the appropriate permissions and access for each role in your RBAC strategy. From that information AppOmni is able to continuously monitor your SaaS applications and alert on any deviations. Alerts can be sent to you for evaluation, to a security incident response team for tracking, and to an IT work system for resolution. All without the need for your intervention.

HELP IS HERE

AppOmni helps security teams Scan, Secure, and Monitor their SaaS applications. Our patented technology deeply scans SaaS APIs and configurations, identifying data leaks in minutes. Apply consistent access controls and data governance across your cloud applications with our policy engine. Continuously monitor your SaaS applications for security events, and integrate detection and response capabilities with your existing workflow.