AppOmni Developer Platform
Secure Any Standard or Custom SaaS App

The AppOmni Developer Platform
Leverage the functionality and depth of AppOmni’s SaaS security platform to ensure universal coverage of all SaaS applications.

- Common security controls layer
- Support for any app with a normalized control framework
- Ability to expand authentication, UI, and APIs to create custom monitored service types and ingest posture data
- Automatic support for policies, compliance mapping, reports, and more
- Rapid integration with the AppOmni platform

Organizations Worldwide Trust AppOmni to Secure Their SaaS Data

“AppOmni provides a real partnership around securing my cloud footprint. I hadn’t seen a tool do what they do with configuration management and it’s a real differentiator. It’s a killer app for large enterprises and SMB companies. I’m looking forward to adding more apps to our AppOmni footprint because I love what the tool does.”

— Bob Genchi, Vice President of Information Technology and Security at Scale Venture Partners

There are thousands of SaaS applications that require security coverage, including custom applications built for specific enterprise needs. There’s no doubt the SaaS app footprint and distribution of data will only grow. Through an easy develop-and-deploy approach, the AppOmni Developer Platform extends our SaaS security expertise, insights, and continuous monitoring to any SaaS or modern business application.

**Understand Your Organization’s Comprehensive Risk Profile**
Implement a common security framework with a consistent set of policies and controls, and clearly understand risk across your entire SaaS ecosystem.

**Improve Security Controls Monitoring**
Map application security posture information from authentication, UI, and APIs to AppOmni to easily monitor and receive alerts when changes occur, and secure critical configurations, user permissions, and 3rd party applications.

**Detect Configuration Drift**
Monitor the security of your SaaS applications from one security solution so your team can quickly identify misconfigurations or drift to close security gaps and drive compliance across the entire enterprise application footprint.

**Utilize Deep SaaS Expertise**
Harness our deep experience as security practitioners and leaders at respected SaaS vendors, cybersecurity, and technology companies. AppOmni delivers unprecedented depth of security controls analysis, data access and permissions modeling, 3rd party application assessment, and advanced threat detection for SaaS.
Minimal Effort for Maximum SaaS Protection

The process flow below details the necessary steps to extend AppOmni’s coverage to custom and in-house SaaS apps. The AppOmni APIs are very well documented and we provide extensive walk-through-support for this process. This process essentially entails developing an ETL pipeline between the custom app and the AppOmni Platform.

**STEP 1**
Start with identifying a target SaaS app that AppOmni does not currently provide coverage for.

**STEP 2**
Develop a data ingest and transformation script – low technical expertise required and support available.

**STEP 3**
Extract the data.

**STEP 4**
Transform the data.

**STEP 5**
Ingest the data from the custom app into the AppOmni Platform.

Custom SaaS application (Ex: Miro)

**Ingestion of custom app data via automation built by customer**

Ingest collected data via AppOmni Developer Platform Endpoint

Immediate SaaS App Security Coverage

Once the app has been integrated into the AppOmni Platform you get all of the existing features that you typically receive with AppOmni’s flagship apps, including:

- Policies
- Rulemaking
- Posture Explorer
- Universal Insights (Q3)
- Threat Detection (Q3)
Importance of Understanding Security Objectives

The only challenging facet in this process is understanding what value do you want to derive by extending AppOmni’s coverage to a custom or in-house application. At face-value this sounds easy but it can prove challenging.

This process requires research to see what insights you want to get out of that SaaS app. There may also be challenges on the capability and quality of the given apps. Note: The nature of the API may limit what data you are able to pull.

It’s important to start with simple data points like the number of end-users is key before building out depth or posture management granularity.

Product Features Coming Soon:

1. Python SDK
   - Wrapper API
   - Automatic Pagination & Serialization
   - Data Model Validation

2. Threat Detection

3. Universal Insights & Reports - Immediate out-of-the-box value