AppOmni

MONITOR & DETECTION OVERVIEW

# Enhanced Visibility for SaaS Application Environments

Constantly evolving business and market requirements are driving transformation across the modern enterprise. Teams are leveraging Software as a Service (SaaS) as new systems of record for everything from customer data to proprietary code. The sensitive nature of this data requires a new type of management where security teams can put purpose-built technologies to work and keep that data secure.

However, many security teams are unaware of the security posture, configuration, and management practices of all the SaaS applications used by their companies. This prevents security teams from creating a holistic threat map of their SaaS environment and delays the development of programs to protect it.

At a tactical level, lack of or limited visibility creates unnecessary pain points in deploying access control principles and responding to incidents, creating gaps in threat hunting capabilities.

AppOmni removes the burden from security teams by providing monitoring and detection capabilities across business-critical SaaS applications. It combines cross-cloud event normalization, customizable risk classifications, and actionable alerts, along with seamless integration into existing security technologies.

## SIGNATURE-BASED DETECTION

- User Impersonation
- User Enumeration
- Cross-Cloud Login Failures
- Brute Force/Password Spraying Attempts
- High Volume Data Reads
- Mass Download Actions
- Mass Resource Deletions
- Resource Permissions Updates

## MONITOR

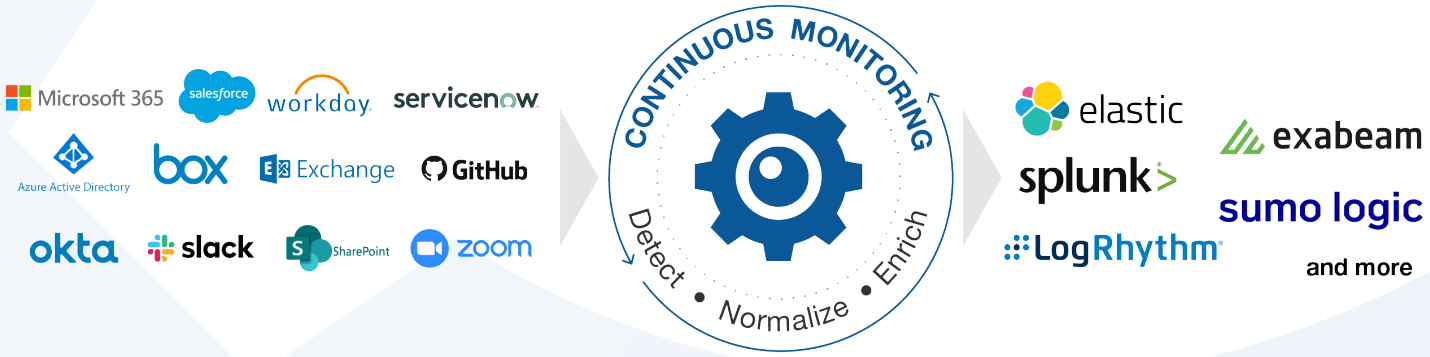
Cross-cloud event normalization provides log aggregation across monitored SaaS applications. The platform parses and structures logs into a common format, Elastic Common Schema (ECS), for ingestion into existing security tooling. This helps security teams maintain consistency and standardization across all SaaS log data sources.

## DETECTION

AppOmni's signature-based detections align to the MITRE ATT&CK Matrix for Enterprise and provide security teams with actionable alerts. This allows security teams to easily map data to existing runbooks and processes for consistency during response.

## SEAMLESS INTEGRATION

Through SIEM integrations, AppOmni provides security and IT teams with the capabilities and configurations to send actionable SaaS alerts to tools already in use. Through this integration, new information and enriched events empower teams with the ability to make informed response decisions and take quick action.




To learn more, email us at **info@appomni.com** or visit **appomni.com**.

AppOmni is a leading provider of SaaS Security Management software. Its patented technology scans APIs, security controls, and configuration settings to compare the current state of enterprise SaaS deployments against best practices and business intent. AppOmni makes it easy for security and IT teams to protect and monitor their entire SaaS environment, from each vendor to every end-user.

AppOmni