Threat & Anomaly Detection

Telemetry and tools to identify, prioritize, and respond to SaaS security threats

The Challenge

Detecting and responding to SaaS threats is increasingly complex. SaaS logs are inconsistent, difficult to analyze, and fragmented across applications, making it harder to connect related events and distinguish threats from noise. Without centralized visibility, detections are often incomplete or delayed, creating security gaps.

Effective SaaS threat detection requires deep telemetry, near real-time insights, and seamless integration into existing workflows to drive confident response.

The Solution

AppOmni normalizes and structures SaaS logs across applications with different formats, naming conventions, and event types. By creating a unified data model, AppOmni enables security teams to correlate related events across applications, improving detection fidelity and reducing investigation time.

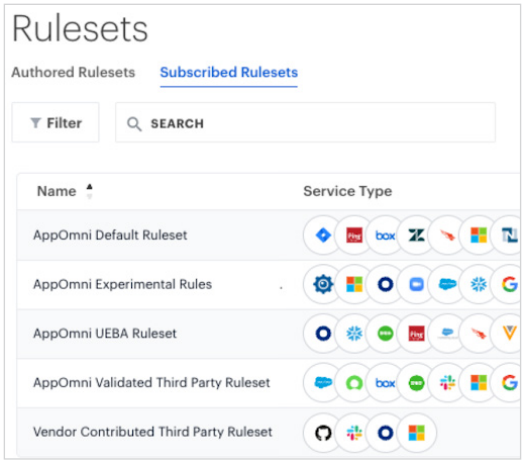
The threat detection engine applies over 250 out-of-the-box rules while allowing teams to build custom detections tailored to their SaaS environment. User and Entity Behavior Analytics (UEBA) strengthens detections by identifying anomalous access patterns, privilege misuse, and mass data exfiltration, helping teams distinguish normal behavior from true risk, like dormant accounts being reactivated or excessive permission changes in a short timeframe.

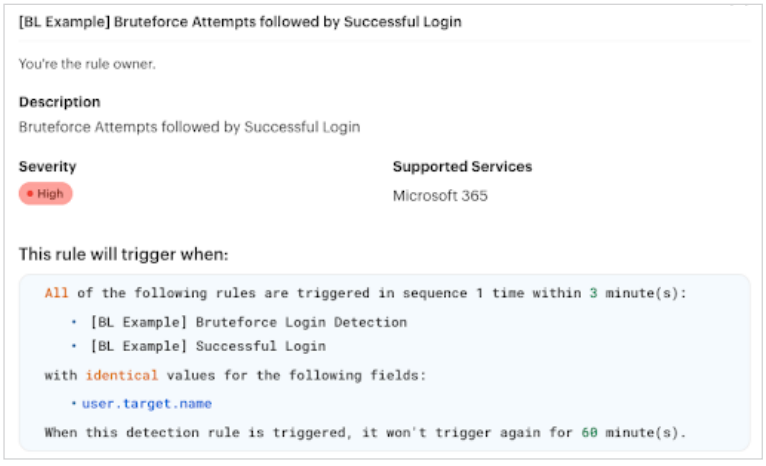
BENEFITS

- **Correlate identity, access, and activity data** to improve detection.
- **Detect threats across SaaS apps** with complete event correlation.
- **Accelerate detection and investigation** with prioritized alerts.
- **Reduce alert fatigue** by filtering out noise.
- **Optimize log ingestion** to lower costs and improve visibility.

KEY FEATURES

- Cross-SaaS Threat Correlation
- User & Entity Behavior Analytics (UEBA)
- Custom Detection rules
- SIEM & SOAR integrations
- Event Source Management





With near real-time processing and SIEM/SOAR integrations, security teams can triage, investigate, and respond within their existing workflows—eliminating the need for manual log parsing and fragmented analysis.

How It Works

Feature	Description	Security Impact
Cross-SaaS Threat Correlation	Detects threats like OAuth token abuse and excessive permission changes by correlating data across multiple SaaS applications.	Uncovers hidden attack paths that would be missed if analyzing applications in isolation
User & Entity Behavior Analytics (UEBA)	Detect high fidelity, low false positive detections from anomalous activities in your SaaS environment.	Distinguishes abnormal from expected behavior, reducing false positives and improving response time
Custom Detection Rules	Security teams can use 250+ pre-built rules or create their own to match specific organizational needs.	Adapts threat detection to unique SaaS risks, ensuring organizations catch what matters most
SIEM/SOAR Integrations	Send SaaS detections and alerts directly to a SIEM or SOAR for triaging and investigation.	Improves operational efficiency by reducing time spent switching between tools
Event Source Management	Users gain granular control over which security event collection, which improves s are collected, optimizing detection accuracy and reducing unnecessary log volume.	Cuts unnecessary log volume, helping teams focus on critical security signals while lowering costs

> AppOmni has allowed us to be more proactive in addressing security challenges. By providing complete visibility into our SaaS environment and automating critical processes, it's another tool in our security armory to automate and orchestrate our response capabilities.
>
> **Information Security Director, Legal Services**

About AppOmni

AppOmni, the leader in SaaS Security, helps customers achieve secure productivity with their applications. Security teams and owners can quickly detect and mitigate threats using unmatched depth of protection, continuous monitoring, and comprehensive visibility. Trusted by the world's largest enterprises, AppOmni specializes in securing diverse SaaS environments.

Learn more about SaaS threat detection at appomni.com/use-case/threat-detection/.