AppOmni

DATASHEET

Threat Detection

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

The Challenge

With 78% of organizations[1] storing sensitive data in SaaS applications, ensuring security is crucial, yet challenging. SaaS logs are complex and time consuming to analyze. To add to the challenges, there is a lack of consistency in SaaS events and audit logs between applications. This complicates data consolidation and integration into security operations tools, resulting in fragmented detections and delayed incident response. And further, there are limited insights on the posture, identities, and connections of each application, leaving next-steps unknown. Effective SaaS threat detection requires advanced telemetry, seamless integration, and comprehensive coverage to protect critical business data.

The Solution

Securing SaaS applications necessitates swift and precise detection mechanisms that are consumable, actionable, and prioritized.

AppOmni's Threat Detection provides the essential context needed to combat SaaS threats more efficiently by combining advanced detection capabilities with posture management and identity analysis. Our platform delivers high fidelity, low false positive UEBA detections and cross SaaS product threat detection for a unified view of applications. By integrating seamlessly into existing SIEM and SOAR tools, AppOmni works where you work, streamlining workflows and enabling actionability.

Utilizing AppOmni's SaaS expertise, over 250 detection rules with a powerful custom rule builder have been built to detect and help your teams prioritize SaaS threats. Patent pending streaming detection engine further aids in enhancing detection accuracy and investigations with advanced telemetry analysis. AppOmni's holistic approach to threat detection empowers organizations to maintain a proactive stance and respond to threats efficiently with greater precision and speed.

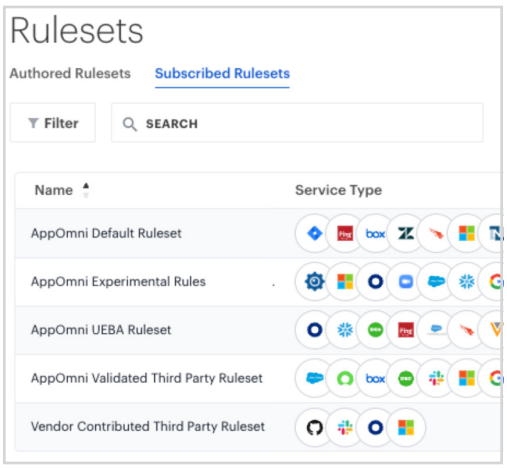
BENEFITS

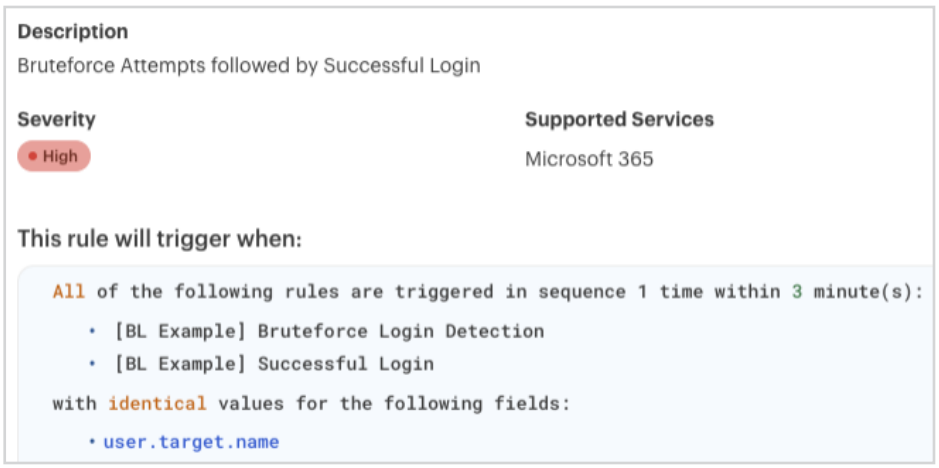
- Clear and actionable context
- Comprehensive detection coverage
- Faster response, containment, and investigation of SaaS threats
- Reduce alert fatigue
- Streamline SaaS detection workflows

KEY FEATURES

- Log and event normalization
- Identity and posture enhanced threat detection
- UEBA
- 250+ Out-of-the-box rule-based detections
- SIEM & SOAR integrations

[1] DevSquad - SaaS Statistics and Trends for 2024





Feature	Description	In Action
Log normalization	Identify event gaps, group detections, and correlate events across multiple apps.	A multinational company unifies logs from various SaaS applications, providing a single view for all security events and compares logging capabilities to prioritize which apps need additional monitoring or custom rules.
UEBA	High fidelity, low false positive detections from anomalous activities in your SaaS environment.	Detection of brute force login. An attacker tried to brute force access to an executive's account. AppOmni detected the pattern and alerted the security team, preventing unauthorized access and potential data theft.
Detection rules	Guide detections with 250+ pre-crafted rules and powerful custom rule builder.	A media company created custom rules to detect unusual data access patterns, preventing unauthorized content leaks by setting up alerts for large data downloads or access from unusual locations.
Integrations	Send SaaS detections and alerts directly to a SIEM or SOAR for triaging and investigation.	A cybersecurity firm sends AppOmni data to Splunk to automate rule updates, continuously refining their detection logic based on new intelligence and attack patterns.

Learn more about SaaS threat detection at appomni.com

About AppOmni

AppOmni is the leader of SaaS Security, enabling customers to achieve secure productivity with their SaaS applications. AppOmni prevents SaaS data breaches and secures mission-critical data from attackers and insider threats. Over 25% of the Fortune 100 and enterprises across industries trust AppOmni to secure their SaaS applications.

For more information, please visit appomni.com