Secure Your Slack Environment with Extensive SaaS Security

The Challenge

Used by more than 100,000 organizations, including 77 of Fortune 100 companies, Slack is one of the top apps for company communication. That's why ensuring its security is paramount. As more corporate enterprises adopt the tool and introduce additional apps and integrations, Slack's complexity and system administration grows. Managing organizations with numerous workspaces is complex. This is compounded as enterprise grid settings, guest users, and apps per workspace increase. Adding to the security challenge is users' lack of visibility into who can access what data, and what is occurring across the environment. Complicating matters, the security team may not have the same controls or insights as Slack administrators. Implementing a comprehensive security solution is crucial to minimize risks and protect your ecosystem.

BENEFITS

- Greater visibility over your Slack environment
- Reduced attack surface via prioritized alerts and insights
- Streamlined compliance and audit readiness
- Controlled organizational settings

KEY FEATURES

- Config and Posture Assessments
- Expert Insights
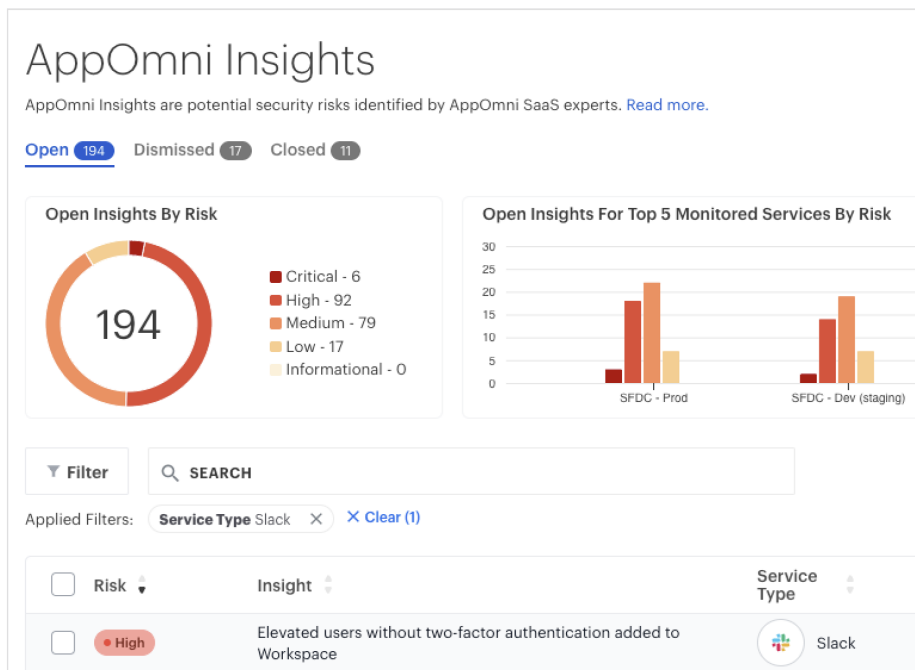- Continuous Monitoring
- OOTB Detection Rules

The Solution

AppOmni provides comprehensive security for Slack by continuously monitoring and protecting the entire platform. Our solution offers deep insights and visibility, helping you to understand, manage, and secure Slack more effectively. AppOmni delivers a detailed overview of risks in your environment, highlighting the criticality of each issue.

AppOmni also helps you quickly understand, monitor, and detect app scopes for the Slack app directory. By using AppOmni's baseline Slack policies, our out-of-the-box functionality helps you track and monitor the most critical app scopes, such as two-factor authentication changes, guest management, or externally shared channels management.

Our platform features more than 250 detection rules embedded with a powerful custom rule builder that detects and prioritizes SaaS threats, saving you precious time. AppOmni's patent pending streaming detection engine enhances detection accuracy and supports investigations with advanced telemetry analysis. With AppOmni's comprehensive security approach, your organization can safeguard sensitive data in the Slack ecosystem and beyond.

Figure 1: Surface key Slack alerts with AppOmni Insights.

Key Capabilities

Feature	Description	In action
Config and Posture Assessments	Use comprehensive SaaS security insights for risk-based posture prioritization.	An organization allows guest accounts with too many permissions. Through AppOmni, the company can limit permissions, strengthening its overall security posture.
Expert Insights	Gain context and recommendations to navigate the complexities of SaaS security.	A software company needed to establish baseline configuration policies that AppOmni created to reach an automated and continuously monitored security state in a matter of months.
Continuous Monitoring	Inspect, analyze, and monitor the security of SaaS and other applications via an ongoing basis.	A startup identified an unauthorized third-party app connected to its Slack environment through AppOmni's SaaS-to-SaaS access monitoring. Once identified, the company terminated the connection, preventing potential data leakage and securing sensitive customer data.
Detection Rules	Leverage detections with more than 250 pre-crafted rules and a powerful custom rule builder.	AppOmni's detection rules alerted a healthcare company about a employee that was attempting to take intellectual property (IP) from the organization before the last day of employment. By setting up custom rules, Slack administrators can set an alert when a large number of files are downloaded in a small time period.

Learn more about security for connected apps at appomni.com.

AppOmni