AppOmni

PARTNER SERVICES

Partner Opportunities

As companies look to deploy SaaS security solutions to protect their SaaS platforms, they will need partners who can provide services to help them. AppOmni is committed to working with our partners to develop services that help customers assess, remediate, and ultimately reduce their risk within SaaS environments. These services will help you differentiate yourself in the crowded value-added reseller market.

AppOmni Is Here To Support You In Your Services Journey

- SaaS Risk Assessment
- Implementation & Remediation
- Managed SaaS Security Operations

SaaS Risk Assessment

The SaaS Risk Assessment provides a point-in-time automated scan, either as a one-time scan or on a recurring basis. This enables you to help customers assess the security posture for their SaaS platforms and review their security gaps. Powered by the AppOmni platform, the Risk Assessment makes it easier to review configuration, data exposure, and regulatory risk.

Implementation & Remediation

AppOmni partners can offer end-to-end design, implementation, and remediation services for risks uncovered by the AppOmni platform. Use the AppOmni Insights engine to identify the risk, the criticality of the risk, and the steps to remediate. These findings are based on SaaS industry best practices, as well as best practices for specific SaaS platforms. The services you offer customers can include SaaS application configurations, integrations, and security settings management.

Managed SaaS Security Operations

Provide your customers the ultimate services experience by managing their security operations. The AppOmni platform provides continuous monitoring, alerting, and reporting on SaaS security posture, making it easier for you to proactively manage your customers' security. Take it a step further and enhance the experience using the AppOmni Monitoring & Detection engine and SDLC processes.

Key SaaS Security Challenges

- According to Gartner, 99% of cloud security failures through 2023 will be the customer's fault[1]
- Default security settings are not secure and can be an open door to confidential data
- SaaS application permissions change thousands of times per month in the average organization
- SaaS applications have sophisticated security processes that require expertise to understand and address security risks
- Security and IT teams may not be aware of all 3rd party apps that are connected to their enterprise environment—on average, customers have 42 3rd party apps connected to their environment[2]

[1]Gartner Innovation Insight for CSPM, ID G00377795.
[2]Source: AO Labs Risk Assessment, 2020.

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