AppOmni (a Solutions+ Partner)

Cisco Partner
https://cs.co/1page

AppOmni is a SaaS Security Posture Management (SSPM) set of tools 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.

Benefits:

Visibility: Provides visibility into SaaS applications, including configurations, permissions, and risks across all your SaaS apps in real time.

Detect and Respond to Threats: Identify insider and outsider threats, compromised accounts, and unusual user behavior early.

Efficiency: Simplifies SaaS security management with actionable data and minimal training

Security posture: Provides a comprehensive security posture for SaaS deployments, including continuous monitoring and risk prioritization

Automate Compliance: Helps teams maintain compliance with out-of-the-box compliance frameworks. Easily generate reports and stay aligned with SOC 2, GDPR, and HIPAA.

Data access management: Provides centralized visibility and data access management for SaaS applications

Security control: Provides security control for SaaS applications, including critical apps like Microsoft 365, Salesforce, and Workday

FAQs:

Q: Is AppOmni available on Cisco's GPL?
A: Yes! Portfolio sellers are compensated and AppOmni is part of the SSE family.

Q: How is AppOmni licensed?
A: By user count and app count. Please contact your AppOmni sales contact or cisco@appomni.com for assistance with quoting.

Q: What does a typical PoC look like?
A: Typically, a 21-day process focusing on 1 or 2 core apps i.e., Salesforce, M365. The key is to ensure they are well qualified first.

Q: My customer has a CSPM solution, why do they need SSPM?
A: CSPM tools are specifically for continuous monitoring of IaaS like Azure, AWS and GCP. SSPM tools like AppOmni is exclusively focused on continuous monitoring of business-critical SaaS like M365, Salesforce, ServiceNow etc.

Common Apps Supported:

Microsoft 365, Google Workspace, Veeva, salesforce, servicenow, workday, iManage, snowflake

Use Cases:

Configuration Management:
SaaS environments are complex with widely varying configurations, ownership, and access patterns. AppOmni prevents SaaS misconfigurations, configuration drift and reduces your SaaS attack surface, enhancing visibility, and simplifying SaaS compliance.

Data Exposure:
AppOmni automates and consolidates monitoring and management of SaaS, ensuring robust protection of critical data in your applications.

Threat Detection:
Each SaaS application has different schemas, connections, and data, making it difficult to build detections or remediate threats effectively. AppOmni provides the telemetry and tools, combined with posture and identity centric analysis to efficiently prioritize and respond to security threats.

Connected Apps:
SaaS environments are more interconnected than ever, exposing risk from connected applications. AppOmni identifies and discovers 3rd and 4th party impacts enhancing visibility of non-human identities and SaaS risks.

Positioning SSPM: [1]

	AppOmni	PANW	Netskope	Zscaler
Connected Applications	40+	90+	14	29
IAM	Yes	Not in SSPM	Limited	8 apps
Posture Mgmt. & Drift	Yes	Limited	Limited	Limited
Data Exposure / Leakage Detection	Yes	Limited	Limited	Limited
Third Party Application Visibility	Yes	Limited	30 Apps	Yes
Threat Detection	Yes	Limited	Yes	Limited
Compliance Benchmarking	Yes	Yes	Limited	Limited
SaaS Threat Intelligence	Yes	Limited	No	No
Customization (custom rules w/in policy)	Yes	Limited	Yes	Limited

[1] *Refer to AppOmni for additional comparative details*

Resources:

Cisco & AppOmni
Order Guide
Glossary
AppOmni Blogs
Use Cases
Questions
Demo Request
AppOmni.com

Example SKU: ***APPOMNI-ENT-IN-1***