vijilan
IT Security: Enabled

10 QUESTIONS FOR SSPM VENDORS

What to Ask Before Choosing a SaaS Security Posture Management Provider

Making the Right SaaS Security Decision

Organizations rely heavily on SaaS platforms like Microsoft 365, Google Workspace, and Salesforce to support daily operations, but these tools can introduce security risks such as misconfigurations, excessive permissions, and risky third-party integrations. SaaS Security Posture Management (SSPM) solutions help identify and manage these risks, making it important for organizations to ask the right questions when evaluating vendors to ensure the solution provides the visibility, monitoring, and security support they need.

THE QUESTIONS

Which SaaS Applications Do You Support?

1 Ensure the vendor supports the applications your organization relies on today and can expand coverage as new SaaS platforms are adopted. Common platforms include Microsoft 365, Google Workspace, Salesforce, Slack, and other collaboration or business applications.

How Do You Detect SaaS Misconfigurations?

2 Ask how the platform identifies security gaps. A strong SSPM solution should continuously evaluate SaaS configurations against industry security best practices and identify policy violations.

Do You Provide Continuous Monitoring or Periodic Scans?

3 Some tools only perform periodic configuration assessments. Continuous monitoring helps identify configuration changes and potential risks in near real time.

How Do You Identify Risky User Permissions?

4 Excessive privileges and role misconfigurations are common security risks. The solution should provide visibility into privileged accounts, administrative roles, and permission changes.

Can You Monitor Third-Party Applications?

5 OAuth applications and integrations can introduce hidden risks. Ask whether the platform can detect connected applications, evaluate permissions, and identify suspicious activity.

How Are Security Alerts Investigated?

6 Many SSPM tools generate alerts but require internal teams to investigate them. Understanding whether the vendor provides investigation support or security expertise can help determine operational impact.

Does the Platform Provide Threat Detection?

7 Configuration monitoring alone may not detect active threats. Ask whether the solution can identify suspicious behavior such as abnormal logins, unusual data access, or privilege escalation.

How Do You Support Compliance Requirements?

8 Organizations often need to demonstrate security controls for frameworks such as HIPAA, GDPR, or SOC 2. SSPM tools should provide reporting and visibility that supports compliance initiatives.

What Deployment and Integration Options Are Available?

9 The solution should integrate easily with existing security tools, logging platforms, or security operations workflows without creating operational complexity.

What Operational Support Do You Provide?

10 Some SSPM platforms are fully self-managed, requiring internal teams to monitor alerts and manage configurations. Others provide managed services or expert support to help investigate risks and respond to threats.

vijilan
IT Security: Enabled
vijilan.com
info@vijilan.com
+1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN