vijilan
IT Security: Enabled

SSPM VENDOR COMPARISON

Evaluating SaaS Security Posture Management Solutions

Choosing the Right SSPM Platform for Your Organization

As organizations increasingly rely on SaaS applications such as Microsoft 365, Google Workspace, Salesforce, and Slack, maintaining secure configurations across these platforms becomes more complex. Misconfigurations, excessive permissions, and third-party integrations can expose sensitive data and create new attack surfaces.

SaaS Security Posture Management (SSPM) solutions help organizations identify security gaps, enforce best practices, and monitor SaaS environments for misconfigurations and risks.

This guide provides a side-by-side comparison of common SSPM capabilities to help organizations evaluate solutions and select the right platform.

Core SSPM Capabilities

Effective SSPM platforms should provide visibility, risk detection, and continuous security monitoring across SaaS applications.

Configuration Monitoring
Continuously scans SaaS environments for security misconfigurations and policy violations.

User and Access Visibility
Identifies privileged users, excessive permissions, and risky access patterns.

Third-Party Application Monitoring
Detects risky OAuth apps and unauthorized integrations connected to SaaS platforms.

Security Benchmarking
Compares SaaS configurations against industry best practices and security standards.

Automated Alerts and Remediation Guidance
Generates alerts and provides recommendations to correct identified security issues.

Vendor Capability Comparison

Capability	Typical SSPM Tools	Security Monitoring Providers
SaaS Configuration Scanning	✓	✓
Risk and Misconfiguration Detection	✓	✓
Continuous Monitoring	Limited	✓
Threat Detection	Limited	✓
Security Operations Response	×	✓
Investigation and Incident Response	×	✓
24/7 Security Monitoring	×	✓
Expert Security Analysts	×	✓

Many SSPM tools focus primarily on identifying configuration risks but may not provide ongoing threat monitoring or incident response capabilities.

Key Evaluation Considerations

When selecting an SSPM solution, organizations should evaluate more than just configuration scanning.
Important factors include:
Continuous Visibility
The ability to monitor SaaS environments in real time rather than periodic scans.

Threat Detection Capabilities
Detection of suspicious behavior such as account compromise, privilege abuse, or unusual access patterns.

Integration with Security Operations
Ability to feed alerts into a security monitoring platform or SOC for investigation.

Coverage Across SaaS Platforms
Support for the applications used across the organization.

Operational Support
Whether the solution includes managed security expertise or requires internal teams to manage alerts.

The Importance of Continuous SaaS Security Monitoring

While SSPM tools are valuable for identifying misconfigurations, they are most effective when combined with continuous security monitoring and expert analysis.

Organizations benefit from solutions that provide:

- Continuous monitoring of SaaS environments
- Detection of suspicious user behavior
- Investigation of security alerts
- Rapid incident response
- Visibility into third-party application activity

Combining SaaS posture management with active security monitoring helps organizations quickly detect and respond to threats targeting cloud applications.

Making the Right Security Decision

Choosing the right SSPM approach depends on organizational needs, internal security resources, and the complexity of SaaS environments.

Organizations that combine posture management with active security monitoring and expert analysis gain stronger protection against both configuration risks and real-world threats.

DELIVERING CONTINUOUS VISIBILITY AND THREAT DETECTION ACROSS MODERN CLOUD ENVIRONMENTS.

vijilan.com
info@vijilan.com
+1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN