AppOmni

The SaaS Security Buyer's Guide

Five Key Considerations, a Checklist, and an RFP Template for Evaluating Your SaaS Security Solution

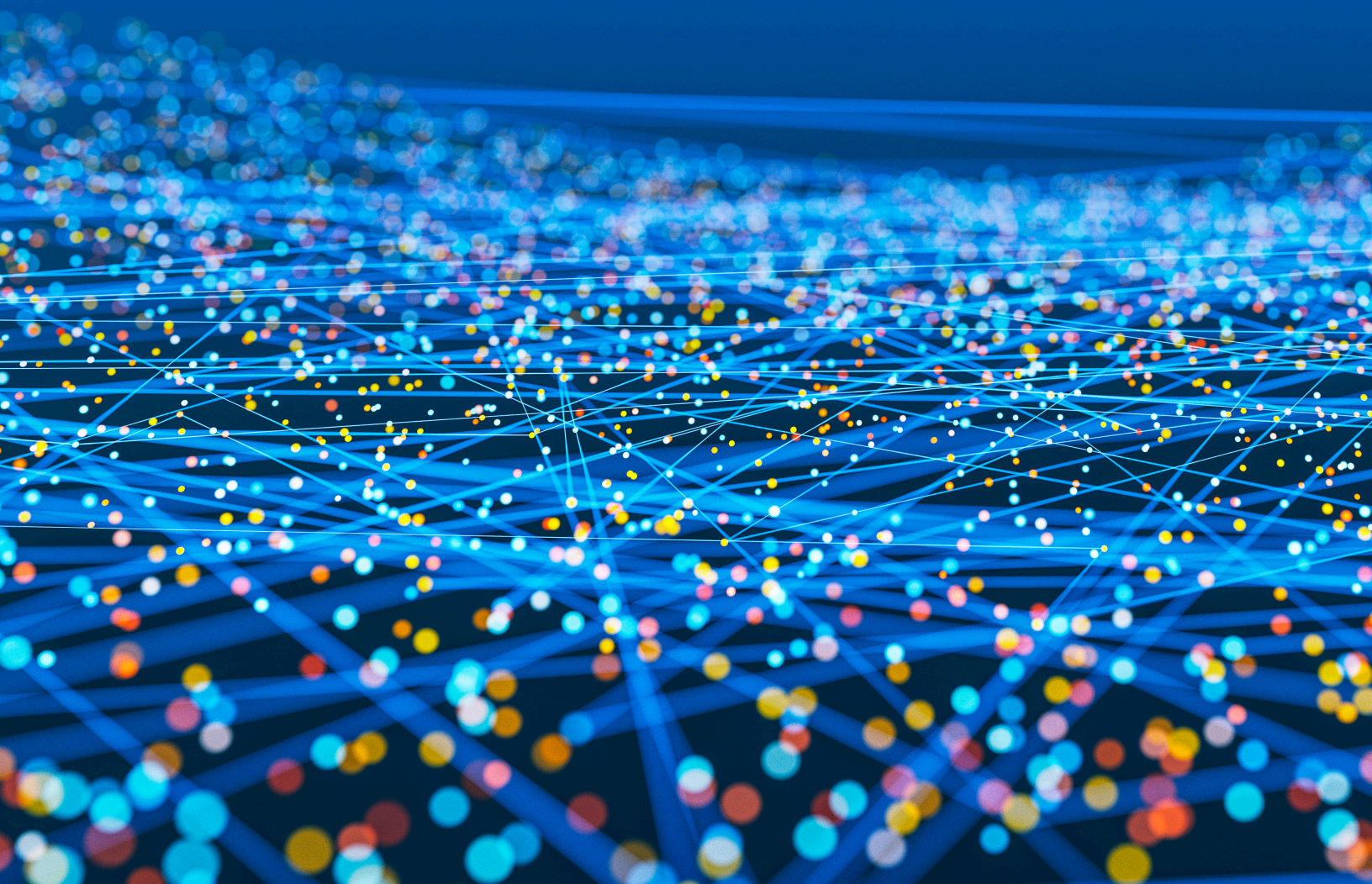

TABLE OF CONTENTS

Executive Summary

Key Takeaways

- Large enterprises typically use over 200 SaaS apps to streamline processes, enhance collaboration, and drive innovation.[1] But those SaaS apps, when not properly secured, can cause data breaches that cost organizations an average of $4.45M in 2023.[2]
- Securing SaaS apps requires a risk-based, collaborative strategy that enterprises cannot achieve by only leveraging traditional tools such as CASBs, SASE, SWGs, and CSPM.
- To protect SaaS data at the enterprise level, organizations need a robust SaaS security posture management (SSPM) solution that provides the risk prioritization and depth of coverage needed to ensure the confidentiality, integrity, and availability of business-critical data.

Why Now?

Businesses increasingly depend on critical SaaS applications such as Microsoft 365, Salesforce, Workday, and ServiceNow to drive their operations. And due to the rapid rate of SaaS adoption, SaaS now constitutes the fastest-growing cloud attack surface.

But there is a fundamental gap between how traditional cybersecurity is managed and how SaaS applications must be secured. Traditional network-based cybersecurity controls such as cloud access security brokers (CASBs) fail to protect SaaS applications from the sophisticated attacks that halt business operations and expose sensitive data. And due to the extensive blast radius and costs associated with SaaS data breaches, SaaS security is mission-critical.

To protect their sensitive SaaS data, maintain correct configurations and permissions, and prevent data access exposure, enterprises require a solution that addresses the nuances of SaaS security — SaaS security posture management (SSPM). SSPM solutions equip enterprises with the visibility and control they need to manage and secure their entire SaaS stack.

As leaders evaluate SSPM platforms, it's important that they find a platform that provides the depth of coverage, flexibility at scale, and security expertise that they'll need to build out a comprehensive SaaS security program.

This guide provides a framework to help leaders evaluate SSPM solutions and choose the right vendor for their specific organization's needs.

200+

SaaS Apps Typically Used by Large Enterprises[1]

$4.45M

Average Cost Resulting From Data Breaches Caused by Poorly Secured SaaS Apps[2]

[1] State of SSPM report, 2023
[2] IBM Cost of a Breach 2023 Report

SaaS Security Challenges

SaaS applications introduce unique security challenges that complicate traditional IT and security models, requiring that enterprises adopt new strategies to protect their data, maintain business operations, and remain compliant. Here are the four most common challenges that enterprises face as they secure their SaaS apps.

Four Common SaaS Security Pitfalls

Limited Visibility Into the SaaS Attack Surface

Historically, IT and security teams had complete oversight of on-site applications and data. But the move towards SaaS applications has resulted in rapid organic SaaS adoption that does not include full IT or security oversight.

Custom Features Breed Misconfiguration Risks

SaaS apps give enterprises the flexibility needed to adapt configurations to meet their specific needs, but that flexibility also adds complexity to SaaS environments and increases the likelihood of misconfigurations. With large enterprises typically using several business-critical SaaS apps — each with their own unique customization features — maintaining consistently applied, secure configurations across the entire SaaS estate becomes impossible.[3]

Dynamic App Usage Results in Configuration Drift

Not only are SaaS apps highly customizable, they're also highly dynamic. SaaS companies regularly update capabilities for their customers, and these updates can affect security settings. Enterprises also change constantly, adding new users or adjusting user privileges and access rights as needed.

Security teams and administrators want to embrace Zero Trust guiding principles that, by default, deny all users, applications, workflows, data flows, and requests for access. But this can hamper the pace of productivity. And it's not always clear to app owners when and how they should adjust user access rights or other data access policies. This confusion breeds identity risks and configuration drift — a phenomenon introduced when SaaS apps deviate from intended configurations.

Third-Party SaaS App Risks Broaden the Attack Surface

Third-party app integrations — such as Github connections to Salesforce or grammar checker apps connected to M365 — provide significant business value but also expose enterprises to additional risk. For example, these SaaS-to-SaaS connections enable unsanctioned third-party apps to access user groups, settings, and data in the primary SaaS application. What's worse, some of these apps can also read, write, and delete sensitive data.

Without an SSPM platform, enterprises can't get the visibility they need to understand which third-party SaaS apps are in their environments, what permissions those apps have, and who has the access required to connect those apps.

[3] State of SSPM report, 2023

What Is SSPM?

A SaaS security posture management (SSPM) platform manages and secures an organization's SaaS applications. With SSPM, security leadership and app owners get a consolidated view into the enterprise's entire SaaS estate and can proactively identify and mitigate SaaS security risks.

The Pareto principle — i.e. 80% of the consequences come from 20% of the causes — drives the concept of SSPM and illustrates how enterprises must address their SaaS security. Because an enterprise's SaaS-associated risks are concentrated in the core SaaS apps that its employees use on a daily basis, securing its apps with SSPM is the most efficient way to reduce the SaaS attack surface.

With SSPM, enterprises can mitigate the effects of SaaS security issues such as configuration drift, misconfigurations, unauthorized access, and noncompliance. Given the increasingly complex and expanding SaaS attack surface, a robust SSPM platform is a critical component of any comprehensive SaaS security program.

Legacy Cybersecurity Tools Weren't Designed for SaaS Security

Robust SaaS security requires a nuanced understanding of both the evolving cybersecurity threat landscape and the highly dynamic nature of SaaS applications. While cybersecurity tools like cloud access security brokers (CASBs), secure access service edge (SASE), secure web gateways (SWGs), and cloud security posture management (CSPM) shaped initial network-based SaaS access security or IaaS cloud security strategies, they are limited in their ability to secure SaaS environments.

Cloud Access Security Brokers (CASBs)

CASBs monitor and control the use of cloud services and SaaS applications. Because CASBs primarily inspect network traffic, they cannot offer the deep visibility or control over user activity — such as fine-grained access controls or real-time activity monitoring — that is needed to detect potential vulnerabilities that can frequently hide in the complex and dynamic ecosystem of SaaS applications.

Secure Access Service Edge (SASE)

While SASE offers a broad range of security services, its primary focus is network security and connecting users to applications from the corporate network or VPN. Therefore, it does not offer the functionality that enterprises need to secure their activity and data within SaaS applications themselves.

Existing cybersecurity tools rely on network-centric controls to secure access to SaaS applications. However, they are limited in their ability to secure against modern SaaS security challenges.

Secure Web Gateways (SWGs)

Because SWGs were designed to monitor and control web traffic, they protect against threats and enforce policy compliance but lack valuable SaaS-specific features such as application-level security, data loss prevention (DLP) within the application, and user behavior analytics. Additionally, traditional SWGs are typically not equipped to handle the dynamic, distributed nature of cloud environments, where users can access SaaS applications from anywhere, thereby bypassing the traditional network perimeter.

Cloud Security Posture Management (CSPM)

CSPM tools and their evolution to CNAPP (cloud-native application protection platforms) focus on identifying security issues in the IaaS based applications, their infrastructure, code, and workloads but do not scan for potential misconfigurations or security risks associated within SaaS applications.

Developing a Multifaceted Security Strategy

While the solutions outlined above do not adequately protect your SaaS data, they are still important components of a comprehensive cybersecurity strategy. When enterprises combine SSPM with other security solutions, they reduce the overall attack surface of their cloud and SaaS applications.

Together, these solutions provide a layered security approach and ensure that enterprises can safeguard their business operations against evolving threats while maintaining compliance and enhancing operational efficiency.

A Multi-Faceted SAAS Security Strategy Is Needed.

CASBs, SASE, SWGs, CSPM do not adequately protect your SaaS data. But when combined with SSPM, a layered security approach ensures enterprises can safeguard their business operations from evolving threats.

Getting Started With SaaS Security

Security teams, app owners, and their business stakeholders must forge a robust partnership if they wish to cultivate a company culture that prioritizes SaaS security. Cross-organization collaboration is critical to address common SaaS security challenges for several reasons.

To start, awareness and education ensure that everyone, from IT teams to end-users, understand the potential risks and best practices associated with SaaS usage. Security teams must keep an eye on emerging SaaS threats, while business stakeholders must understand the security implications of their SaaS-related decisions.

Additionally, the allocation of necessary resources — of both personnel and time investments across different teams — is vital as the organization rolls out a comprehensive SaaS security program. This cross-team effort should be integrated into the organization's broader cloud security strategy, leveraging insights and expertise across departments. The goal is to create a seamless approach to security that accounts for all cloud environments and SaaS applications and is tailored to the organization's specific needs and risks.

Adopting SSPM and SaaS security at the enterprise scale requires a risk-based approach that involves a cross-organization collaborative effort to identify, assess, and prioritize SaaS app risks. With this approach, enterprises can prioritize the most critical security threats and establish security guardrails and practices that are aligned with the enterprise's risk tolerance.

By assessing the current and anticipated risks associated with SaaS solutions — all while taking each specific team's feedback and requirements into account — security teams can allocate their resources more effectively, ensuring that critical assets receive the highest level of protection. A risk-based approach also enhances the organization's resilience against threats and ensures compliance with evolving regulatory requirements.

Five Key Components of an SSPM Solution

To get the risk prioritization and depth of coverage needed to secure their SaaS data, enterprises should look for an SSPM platform that includes the five following capabilities:

Configuration and Drift Management

Configuration management involves reviewing and updating the settings and policies needed to maintain policy baselines, security, and access controls. By controlling configuration drift, configuration management solutions protect enterprises against unintentional data access exposure and make it challenging for attackers to exploit vulnerabilities.

SSPM platforms mitigate configuration drift by optimizing settings and aligning them with the enterprise's security standards. The ultimate goal is to ensure that the right people have access to the right resources, with the right settings, at the right time.

What to look for	Questions to ask
SaaS security guardrails	☐ Does the solution provide a snapshot of my enterprise's ideal state?
	☐ Can we easily build guardrails to avoid straying from our ideal state?
Individual stakeholders across the organization can remediate issues	☐ If we identify misconfigurations or configuration drift, can individual stakeholders easily fix those issues?
Proactively enforces permissions	☐ What is the level of granularity in how the platform identifies policies and configurations?

SSPM Component #1

Configuration and Drift Management: Review and update the settings necessary to maintain policy baselines, security, and access controls.

Data Access Exposure

Data access exposure identifies vulnerabilities where an enterprise's information might be compromised, e.g. data is exposed to the public internet. An SSPM solution can assess such misconfigurations before data is exposed, thereby protecting the confidentiality, integrity, and availability of data while also paving the way for secure and reliable operations.

What to look for	Questions to ask
Risk prioritization that accounts for risks associated with posture, configuration, identities, and connected application	☐ How does the solution monitor for SaaS data access exposure?
	☐ Does the solution flag the most common misconfigurations that lead to data exposure?
	☐ Does the solution provide numerous baselines and include a rule customization feature?
Exposure controls	☐ What does access control monitoring look like on the platform?
	☐ Does the vendor enable my enterprise to prevent users from bypassing
Dynamic alerts and remediation	☐ Does the platform give me the insights my teams need to remediate issues quickly?

SSPM Component #2

Data Access Exposure: Identify vulnerabilities that can compromise sensitive data.

Threat Detection

Threat detection identifies and analyzes potential threats within an enterprise's applications. This process includes collecting activity and event logs, normalizing those logs, and structuring the data for analysis to include ordering events. The SSPM solution then applies out-of-the-box and custom rule sets to identify anomalies and potential threats. Once those threats are identified, the solution provides triage guidance to the end user.

What to look for	Questions to ask
Complete SaaS activity monitoring	☐ Can the platform generate normalized event logs?
	☐ Are the normalized event logs' underlying data model details documented?
Continuous alerting	☐ Can teams configure detections that are specific to their unique environments?
	☐ Can the threat detection solution handle out-of-order events?
Application-specific and cross-cloud detections	☐ Does the platform provide both out-of-the-box and custom detection rules?
Alert-specific context and guided remediation	☐ Is guided remediation provided?
	☐ Does the platform provide event JSON, MITRE mapping, triggering logic, and questions to help your team investigate alerts?
	☐ Is the threat detection logic clearly documented by the vendor?
Specificity and depth of detection	☐ Do the detection results offer specificity and avoid redundancy with the output from my existing security tools?
SOC Integrations	☐ Does the SSPM platform integrate with SIEM, SOC tools, and security data lakes?

SSPM Component #3

Threat Detection:
Identify and analyze anomalies and potential threats in event logs.

SaaS-to-SaaS Security

SaaS-to-SaaS connections — also known as the integrations and data exchanges between different SaaS apps — enable businesses to streamline their operations by allowing various cloud-based services to communicate with each other, share data, and automate workflows across different platforms without the need for manual intervention.

For example, a company might use a customer relationship management (CRM) SaaS application to manage customer data and interactions. This CRM could be connected to an email marketing SaaS platform, allowing for automated sending of targeted emails based on customer behavior tracked in the CRM. In this example, the email marketing platform is considered a third-party app connection because of its relationship to the CRM, and any apps connected to the email marketing platform would be considered fourth-party app connections.

The threat researchers at AppOmni have discovered that, on average, over 256 distinct SaaS-to-SaaS connections are installed in a single SaaS instance within enterprise companies. Of those 256 SaaS-to-SaaS connections, an average of 100 have not been used in the last 6 months — yet they retain the ability to access data via these connections.[4]

Securing these third and fourth-party apps — including both sanctioned and unsanctioned applications — is a critical but oftentimes overlooked component of SaaS security. Getting visibility into third-party connections to their SaaS apps enables enterprises to proactively protect their attack surface, reduce data leaks, maintain compliance, and understand their exposure to third-party risk.

What to look for	Questions to ask
Visibility into and monitoring of third-party connections to SaaS apps	☐ Am I getting the visibility I need to understand how third and fourth-party apps contribute to my SaaS attack surface?
Granular visibility into app privileges	☐ Can I identify if a specific app has create, read, update, and delete (CRUD) privileges?

[4] AppOmni Blog: How SaaS-to-SaaS Apps Can Compromise the Security of SaaS Environments

SSPM Component #4:

SaaS-to-SaaS Security: Get visibility into third-party connections to SaaS apps and protect the attack surface.

Compliance

Manual compliance audits for SaaS apps are time-intensive and complex, given the disparate configurations, policy models, and log conventions used by different SaaS vendors. For example, new country-level regulations for data security and privacy — in addition to new regulations such as the Securities and Exchange Commission (SEC) rules targeting SaaS — introduce additional considerations and workflows for overworked compliance teams.

The lack of consistent log files also makes it hard to analyze events or compliance violations. Without an SSPM, compliance tasks become so complex and time-intensive that they cannot be performed on demand.

What to look for	Questions to ask
On-demand compliance assessments and reporting	☐ Can I monitor my SaaS apps by a specific compliance framework?
Identifies and addresses misconfigurations that lead to non-compliance	Can I produce audit reports by monitored service (e.g., Workday)?
Out-of-the-box enterprise policy templates with continuous monitoring	☐ Can I track my compliance reporting by SaaS app over time?

The Business Case for SaaS Security

Given the mission-critical role of SaaS applications in modern business operations, companies that gain secure productivity with SaaS will have a competitive edge. The ever-increasing threat of nation-state adversaries, ransomware, and even insider threats means that SaaS security and productivity are inherently connected as two sides of the same coin.

Disruptions caused by SaaS breaches and firefighting incidents that lead to data loss and reputation damage will be costly for organizations and will distract them from the business priorities that SaaS was designed to help. Addressing SaaS security isn't just about the security of SaaS apps — it's about the integrity of your enterprise.

SSPM Component #5:

Compliance:
Streamline compliance and reporting with on-demand compliance assessments.

Request for Proposal Template

Choosing the right SSPM vendor is a critical step in your SaaS security journey. This request for proposal (RFP) template will streamline your evaluation of potential providers, ensuring that you select a comprehensive and robust SSPM platform.

SSPM Infrastructure and Deployment

Requirement	Vendor Response
SaaS-delivered SSPM solution (i.e. there is no infrastructure to be deployed)	Yes ☐ No ☐
No inline components, network, or infrastructure changes needed for SSPM deployment	Yes ☐ No ☐
Connects to SaaS applications in minutes	Yes ☐ No ☐
Connects to Custom SaaS applications	Yes ☐ No ☐
Guided SaaS on-boarding process	Yes ☐ No ☐
Out-of-the-box SaaS security best practice policies are available and ready to be deployed in minutes	Yes ☐ No ☐
Provides instant visibility into SaaS security drifts	Yes ☐ No ☐
Single solution for SaaS security monitoring (SFDC, M365, Zoom, Box, Slack, Github etc)	Yes ☐ No ☐
Provides continuous SaaS Posture Security monitoring (i.e. SaaS configuration drift detection)	Yes ☐ No ☐
Provides continuous SaaS Data Access monitoring (i.e. SaaS data access drift detection)	Yes ☐ No ☐
Provides continuous SaaS functionality monitoring (i.e. notifies on missing SaaS permissions)	Yes ☐ No ☐
SSPM vendor is SOC2 Type II certified	Yes ☐ No ☐

Identity and Access Management

Requirement	Vendor Response
Role-based access control (RBAC) for users managing the SSPM platform	Yes ☐ No ☐
Restricts user access to specific SaaS application environments	Yes ☐ No ☐
Supports automatic user provisioning for SAML	Yes ☐ No ☐
Define global session expiration for users	Yes ☐ No ☐
Create and manage access and refresh API tokens for integrations to other systems	Yes ☐ No ☐
User authentication supports in-built two-factor authentication using time-based one time passwords (TOTPs)	Yes ☐ No ☐

SSPM Security and Compliance Reporting

Requirement	Vendor Response
Built-in and always-on SaaS Security reporting	Yes ☐ No ☐
Built-in and always-on compliance reporting (SOC2, ISO 27001, NIST 800-53, NIST-CSF, SOX) for each monitored SaaS application	Yes ☐ No ☐
Ability to create groups of reports and schedule them for regular delivery to specific email addresses	Yes ☐ No ☐
Generate reports based on a specific framework (e.g. NIST CSF, ISO 27001, SOC2) across all monitored SaaS applications	Yes ☐ No ☐
Display compliance trending information with up to 90 days worth of historical trends	Yes ☐ No ☐
Availability of executive level summary reports for management	Yes ☐ No ☐

SSPM Event Monitoring and Detection

Requirement	Vendor Response
SaaS audit/event log normalization	Yes ☐ No ☐
SaaS audit/event log monitoring via out-of-the-box detection rules that alert on suspicious SaaS activities	Yes ☐ No ☐
Ability to create custom SaaS threat rule detections with custom sequences of events	Yes ☐ No ☐
Create custom event sinks that integrate with a data receiver, such as Splunk, Sumologic or any other HTTP based data receiver. Delivery formats supported must include JSON and/or Splunk HEC	Yes ☐ No ☐
Generated events can be sent to the event sink in Full or Condensed ECS format	Yes ☐ No ☐
Ability to turn on or off event processing on an individual SaaS application basis in order to reduce noise	Yes ☐ No ☐
Includes a user interface that manages detection alert workflow and enables the user to define "Open", "In Progress" or "Closed" alerts. Closed alerts can be marked with requisite comments and categorized as malicious or benign.	Yes ☐ No ☐
Event alerts are supplemented with MITRE ATT&CK tactic and technique mapping, trigger logic, triage questions as well as instructions on how to trigger the rule for testing purposes.	Yes ☐ No ☐
Detection rules apply across SaaS applications (e.g. ability to detect simultaneous cross-cloud SaaS login failures)	Yes ☐ No ☐

SSPM Policy and Posture Monitoring

Requirement	Vendor Response
Can create custom SaaS security policies	Yes ☐ No ☐
Policy scans can operate autonomously and on a variable frequency basis, down to the granularity of one scan per 1 hour	Yes ☐ No ☐
Policies can monitor multiple instances of the same SaaS application type (e.g. monitor Prod, Pre-prod, Dev, UAT environments via a single consistent policy)	Yes ☐ No ☐
Policy violations can be immediately routed to predefined email addresses and/or integrations (e.g. ticketing system, SIEM, SOAR, etc.)	Yes ☐ No ☐
Individual policy rules can be customized with the ability to define specific values to rules (e.g. session timeout must be X minutes or greater, where X can be any valid, configurable value)	Yes ☐ No ☐
Individual policy rules can be mapped to compliance controls of any framework, in order to report on compliance	Yes ☐ No ☐

SSPM Data Classification and Risk Assignment Capabilities

Requirement	Vendor Response
SaaS data classification or mapping engine	Yes ☐ No ☐
Multi-vector approach for risk assignments for SaaS security findings (e.g. the ability to define custom risk ratings)	Yes ☐ No ☐

Incident Investigation and Response Management

Requirement	Vendor Response
Always on and point-in-time SaaS incident response investigation capabilities	Yes ☐ No ☐
Central console for cross-SaaS configuration review and analytics	Yes ☐ No ☐
Central view of all policy issues with the ability to filter on the SaaS application, risk severity, policy, issue class, issue subclass and compliance framework	Yes ☐ No ☐
Ability to export issues in XLSX, JSON and CSV formats for off-line processing	Yes ☐ No ☐

SSPM Third-Party Application Coverage

Requirement	Vendor Response
Discovers and provides a central view of all third-party applications and integrations	Yes ☐ No ☐
Automatically rates the third-party application risk based on criticality of scope and/or permissions granted	Yes ☐ No ☐
Ability to submit and crowdsource publisher information, risk rating and comment for each third-party app	Yes ☐ No ☐
Approve / Unapprove third-party apps for investigation	Yes ☐ No ☐

SSPM Data Leakage and Exposure Detection

Requirement	Vendor Response
SSPM solution has the ability to automatically detect data leakage or exposure	Yes ☐ No ☐
Detect bulk or mass download actions	Yes ☐ No ☐
Ability to model data access based on the user role, in order to track and remediate over-privileged access	Yes ☐ No ☐

SSPM Configuration Management

Requirement	Vendor Response
Compare configuration changes between two points in time	Yes ☐ No ☐
Compare configuration differences between two access roles	Yes ☐ No ☐

General Attributes

Requirement	Vendor Response
Ability to generate audit logs of activity in the SSPM platform	Yes ☐ No ☐
Local sales and presales representatives for responsiveness and account support	Yes ☐ No ☐