ADAPTIVE SHIELD

The Ultimate SaaS Security Posture Management (SSPM) Checklist

Contents

Introduction

Cloud security is the umbrella that holds within it: IaaS, PaaS and SaaS. Gartner created the SaaS Security Posture Management (SSPM) category for solutions that continuously assess security risk and manage the SaaS applications' security posture. With enterprises having 1,000 or more employees relying on dozens to hundreds of apps, the need for deep visibility and remediation for SaaS security settings is only getting more critical.

The top pain points for SaaS security stem from:

Lack of control over the growing SaaS app estate

Lack of governance in the lifecycle of SaaS apps: from purchase, to deployment, operation, and maintenance

Lack of visibility of all configurations in the SaaS app estate

Skills gap in ever-evolving, accelerating, complex cloud security

Laborious and overwhelming workload to stay on top of hundreds to thousands (to tens of thousands) of settings and permissions

The capability of governance across the entire SaaS estate is both nuanced and complicated. While the native security controls of SaaS apps are often robust, it falls on the responsibility of the organization to ensure that all configurations are properly set — from global settings, to every user role and privilege. It only takes one unknowing SaaS admin to change a setting or share the wrong report for confidential company data to be exposed. The security team is burdened with knowing every app, user, and configuration to ensure they are all compliant with industry and company policy.

Effective SSPM solutions come to answer these pains and provide full visibility into the company's SaaS security posture, checking for compliance with industry standards and company policy. Some solutions even offer the ability to remediate from within the solution. As a result, an SSPM tool can significantly improve security-team efficiency and protect company data by automating the remediation of misconfigurations throughout the increasingly complex SaaS estate.

As one might expect, not all SSPM solutions are created equal. Monitoring, alerts, and remediation should sit at the heart of your SSPM solution. They ensure that any vulnerabilities are quickly dealt with before they are exploited by cyberattackers. When comparing SSPM options, here are some key features to look out for.

Visibility & Insights

Run comprehensive security checks to get a clear look into your SaaS environment, at all the integrations, and all the domains of risk.

Breadth of Integrations

First and foremost for an SSPM solution, is the SSPM's ability to integrate with all your SaaS apps. Each SaaS has its own framework and configurations, if there is access to users and the company's systems, it should be monitored by the organization. Any app can pose a risk, even non-business-critical apps. Point of note is that often smaller apps can serve as a gateway for an attack.

Look for an SSPM system with a **minimum of 50 integrations** adaptable and able to run checks on every data type to protect against misconfigurations.

Even more, a solution should be able to support as many apps as possible that are within the SaaS IT stack, in a **seamless out-of-the box way**.

Comprehensive & Deep Security Checks

The other vital component of an effective SSPM is the expanse and depth of the security checks. SaaS vendors provide robust settings to protect the SaaS environment, yet it's the SSPM solution that ensures that every configuration and permission is correctly configured. These are the domains and configurations that the SSPM should track and monitor.

Identity and access management. Visibility into MFA, SSO, third-party user access, domain authentication, and legacy authentication protocols as these are among the most common attack vectors currently being exploited.

Malware protection. Enforce the configurations that protect against social-engineering attacks including spoofing, phishing, and spam, and prevent client-side attacks.

Data leakage protection. Ensure correct configuration to protect against data leakage from any user account.

Auditing. Provide digital forensics, control the level of specificity, and in regulated industries, provide logs for certain processes.

Access control for external users. Check that external users are verified and trusted and grant them limited access and permissions while still enabling them to do their job.

Privacy control. Control visibility between co-workers and service providers and create better separation between what people are sharing personally vs. professionally.

Compliance policies, security frameworks and benchmarks. Checks that are run to test compliance levels to industry standards and best practices.

Continuous Monitoring and Remediation

Combat threats with continuous oversight and fast remediation of any misconfiguration

Remediating issues in business environments is a complicated and delicate task. The SSPM solution should provide deep context about each and every configuration and enable you to easily monitor and set up alerts. This way vulnerabilities are quickly managed before they are exploited by cyberattackers. SSPM vendors provide you with these tools, which allow your security team to communicate effectively, shut down vulnerabilities, and protect your system.

24/7 continuous monitoring

For a clear picture of risk and vulnerability, your dynamic environment demands 24/7 visibility.

Activity monitoring

Track privileged user activities and activities of interest across your SaaS estate. Simplify forensic and retrospective investigations for cross-platform (e.g. user creation) and platform-specific activities.

Alerts

Set alerts to immediately detect any configuration drifts or potential risks. Integrate these alerts with your company's change control processes to enable the security team to monitor everything from a single pane of glass.

Ticketing

Open and share tickets across the security team, detailing the vulnerability and describing the steps needed to remediate the issue.

Remediation

Gain full context of the security risk including extent and severity of exposure as well as stakeholders impacted. See exactly how to fix the SaaS misconfigurations either directly from the system or easily share issues when more advanced intervention is required.

Posture over time

Snapshots aren't enough to view network changes. Look for a system that provides a timeline view of your SaaS environment, so you can detect changes and see how your system has evolved over time.

System Functionality

Integrate a strong and smooth SSPM system, without extra noise.

Your SSPM solution should be easy to deploy and allow your security team to easily add and monitor new SaaS applications. Top security solutions should integrate easily with your applications and your existing cybersecurity infrastructure, to create a comprehensive defense against cyber threats.

Self-service wizards

With new SaaS applications being added to networks all the time, you need an interface that allows anyone in the organization to easily connect their latest applications.

Robust APIs

Connect your SSPM solution to SIEM and other vulnerability platforms.

Low false positives

False positives desensitize security teams to real alerts while wasting resources on investigating non-issues. By eliminating false positives, your security team can focus on real vulnerabilities rather than chase phantom positives.

Non-intrusive

Look for an out-of-band management solution that uses APIs rather than proxy your service.

Tiered use

Often the business owner of the SaaS application sits outside of security, and the SSPM can offer limited access for the business owner's apps. That way, the business owner can have visibility into their owned apps and remediate issues right away, saving the security team time and effort.

Final Thoughts

The right SSPM solution PREVENTS the next attack

At Adaptive Shield, we liken SSPM to brushing one's teeth. It's a foundational requirement that creates a state of preventive protection. We work hard to ensure Adaptive Shield is a best-of-breed SSPM solution that provides organizations continuous, automated surveillance of all SaaS apps, alongside a built-in knowledge base to ensure the highest SaaS security hygiene.

Using Adaptive Shield, security teams will deploy best practices for SaaS security, while integrating with all types of SaaS applications—including video conferencing platforms, customer support tools, HR management systems, dashboards, workspaces, content, file-sharing applications, messaging applications, marketing platforms, and more.

Adaptive Shield's framework is easy to use, intuitive to master, and takes five minutes to deploy.

Learn more about how you can secure your company's SaaS security now.

Request a Demo

Printable Checklist

Visibility & Insights

Run comprehensive security checks to get a clear look into your SaaS estate, at all the integrations, and all the domains of risk.

Breadth of integrations

- [ ] Minimum of 50 integrations
- [ ] Ability to easily add more SaaS apps

Comprehensive & Deep Security Checks

These are the domains and configurations that the SSPM should track and monitor.

- [ ] Identity and access management
- [ ] Malware protection
- [ ] Data leakage protection
- [ ] Auditing
- [ ] Access control for external users
- [ ] Privacy control
- [ ] Compliance policies, security frameworks and benchmarks

Continuous Monitoring & Remediation

The SSPM should allow your security team to stay informed, communicate effectively, quickly shut down vulnerabilities, and protect your system.

- [ ] 24/7 continuous monitoring
- [ ] Data leakage protection
- [ ] Activity Monitoring
- [ ] Alerts
- [ ] Ticketing
- [ ] Remediation
- [ ] Posture over time

System Functionality

Integrate a strong and smooth SSPM system, without extra noise.

- [ ] Self-service wizards
- [ ] Robust APIs
- [ ] Low false positives
- [ ] Non-intrusive
- [ ] Tiered use