ADAPTIVE SHIELD

The Ultimate SaaS Security Posture Management Checklist

2023 Edition

Contents

Intro

The ease with which SaaS apps can be deployed and adopted today is remarkable, but it has become a double-edged sword. On one hand, apps are quickly onboarded, employees can work from anywhere, and there is little need for operational management. However, security teams are now burdened with the responsibility of monitoring every app, user, configuration, and device across the organization to ensure that they do not pose a risk.

SaaS Security Posture Management (SSPM) solutions enable security teams to handle the ever-growing challenges brought on by the new SaaS app landscape by continuously assessing security risks and managing the SaaS app security posture. If purchasing an SSPM solution is on your radar, here's a checklist for what to look out for when evaluating different vendors.

Background

The top pain points that stem from the explosion of SaaS app usage can be explained by the "3 V"s:

Volume

Each app can have hundreds of global settings, such as which files can be shared, whether MFA is required, or whether recording is allowed in video conferencing. Multiply this number by thousands – or tens (or even hundreds) of thousands – of employees. Security teams must first be able to discover all the users who are using each application, as well as familiarize themselves with every application's specific set of rules and configurations, and ensure they are compliant with their company's policies.

Visibility

With this incredibly high volume of configurations, user roles and permissions, devices and SaaS-to-SaaS access, security teams need multi-dimensional visibility to monitor them all, identify when there is an issue, and remediate it swiftly.

Velocity

The speed of change that SaaS apps bring are incredibly hard to govern. SaaS apps are dynamic and ever evolving — apps' settings need to be modified on a continuous basis from security updates and app feature enhancements to employees added or removed, and user roles and permissions set, reset, updated, etc. There are also continuous, compliance updates to meet industry standards and best practices (NIST, SOC2, ISO, MITRE, etc.) that need to be checked and modified.

Named by Gartner as a MUST HAVE solution in the "4 Must-Have Technologies That Made the Gartner Hype Cycle for Cloud Security, 2021," SaaS Security Posture Management (SSPM) solutions come to answer these pains to 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 solution can significantly improve security-team efficiency and protect company data.

As one might expect, not all SSPM solutions are created equal. The Misconfiguration Management use case sits at the core of SSPM. However, there are more advanced use cases that tackle the emerging and growing challenges existing in the SaaS landscape.

Misconfiguration Management

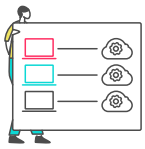
Deep visibility and control of all configurations, settings, and built-in security controls across all SaaS apps for all users.

SaaS-to-SaaS App Access

Monitoring and management of all third-party apps connected to the company's core SaaS stack.

Identity & Access Management Governance

Consolidation and validation of User Identity and Access, enabling attack surface reduction, efficient SecOps programs, and operational integrity (for example, identifying dormant accounts or external users with administrative access).



Device-to-SaaS User Risk Management

Manage risks stemming for the SaaS user's device based on the device hygiene score.

This checklist will help security teams identify all the areas they need to oversee in this complex, ever-changing SaaS environment.

Misconfiguration Management

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 responsible for knowing every app, user, and configuration to ensure they comply with industry and company policy.

Visibility & Insights

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

Breadth of integrations

SSPM solutions must have the ability to integrate with SaaS apps across the organization in all departments (Sales, Marketing, HR, R&D, etc.). Each SaaS app has its platform-specific configurations; if there is access to user's and the company's systems, it should be monitored by the organization. Any app can pose a risk, even non-business-critical apps. It is often smaller apps that serve as gateways for an attack.

Look for an SSPM system that can integrate with the SaaS apps in use by your organization and that can run checks on every data type to protect against misconfigurations.

Comprehensive & deep security checks

Another vital component of an effective SSPM is the expanse and depth of the security checks, where you gain context to the security alerts and gain answers to questions like: who are these users that are subject to a certain misconfiguration? Are they admins? How much do they "use" this access method? The SSPM should provide insights into user behavior as well as context for these affected users, giving the security team full visibility and the information needed to make access decisions for these users. Built-out IAM Governance capabilities are recommended for any SSPM solution.

SaaS vendors provide robust settings to protect the SaaS environment, yet it's the SSPM solution that ensures every configuration, user and permission adheres to corporate security policies. These are the domains and configurations that the SSPM should track and monitor:

- **User context:** Check which users are accessing systems without authentication, whether they are admins, and how frequently they use back-door access points.
- **Access control for external users:** Check that external users are verified and trusted and grant them limited access and permissions while enabling them to do their job.
- **Identity and access management governance:** Gain visibility into MFA, SSO, third-party user access, domain authentication, and legacy authentication protocols as they 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 specific processes.
- **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:** Run checks to compliance frameworks with 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 every configuration and enable you to monitor and set up alerts easily. This way, vulnerabilities are managed before threat actors can exploit them. SSPM vendors provide 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 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.

Non-intrusive

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

Role-based access

Collaboration between stakeholders is a key design principle. Often the business owner of the SaaS application sits outside of security, and the SSPM can offer limited access to 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.

SaaS-to-SaaS App Access

In an effort to improve productivity, employees often extend the functionality of their primary SaaS applications by connecting them to a secondary SaaS app, or otherwise known as 3rd-party app access. Interconnectivity is quick and easy and can be done in seconds with just a few clicks. Today's workforce depends on business-critical apps that easily connect with other applications.

However, users rarely realize they've handed over significant permission rights to the new 3rd-party application. These rights include the ability to read, create, update, and delete corporate or personal data not to mention, that the app itself could be malicious. This access is granted in seconds, usually far outside the view of the IT and security teams, and significantly increases an organization's attack surface.

These 3rd-party applications, which can number in the thousands for larger organizations, all must be monitored and overseen by the security team.

Effective SaaS-to-SaaS Access security solutions identify connected applications, review the permissions granted to the apps, classify their access levels and permissions across multiple primary apps in a consistent manner, and send alerts or notifications when permissions exceed company policy. The solution should also validate that the third-party app has a Privacy Policy and Terms of Use.

Visibility & Insights

Track and monitor all SaaS-to-SaaS access through comprehensive security checks to have a full understanding of your exposure.

Discovery of SaaS-to-SaaS apps

SaaS-to-SaaS App Access solutions must be capable of discovering and integrating with all primary and secondary SaaS apps. It is a critical piece of 3rd-party vendor risk management, and ensures that third-party risk management activities are more than a one-time pre-procurement exercise.

Risk can come from any application, even a non-business-critical application. When users authorize applications to access their system, threat actors have a new entranceway into the organization's environment.

Like with the traditional core SSPM solution capabilities, SaaS-to-SaaS access security systems should be capable of discovery across the full breadth of primary apps and create a consistent, cross referenced baseline for apps, such as a scheduling app, that are connected to M365, Salesforce and Google Workspace. The solution should seamlessly support as many apps as possible, preferably within your existing SSPM security solution.

- **Baselining Apps:** Set baselines for all third-party applications along with their access permissions
- **Access Reviews:** Review accessed data and scope sensitivity, number of users, and apps privacy policy and terms of service
- **Volume of Access:** Review third-party access based on the number of scopes, platforms being accessed, and number of accessed user accounts

SaaS-to-SaaS App Continuous Monitoring & Control

To prevent secondary apps from providing an unauthorized gateway into your environment, your SSPM solution should be equipped with the following third-party monitoring tools.

Automated discovery

Automatically and continuously discover 3rd-party app access across multiple SaaS platforms, including Microsoft 365, Google Workspace, Salesforce, Slack, and Github

Settings detection

Detect built-in, default access approval settings from the primary SaaS app and their recommended state, such as access approval by admins only

Consolidate API clients

Identify and consolidate API clients that are used by the same vendor across multiple SaaS environments, such as Microsoft 365 clients who use Slack and Salesforce

Scope breakdowns

Provide a granular, consistent breakdown of all access scopes or authorizations that are used by each third-party app API client, so you can measure access across multiple primary apps (e.g. review only apps with 'sensitive' access to any primary app)

Identification

Identify each authorization and consent type, such as admin or designated user, and the user details that authorized or consented to each 3rd-party app client

Create a standardized system

Baseline 3rd-party apps access scopes across multiple SaaS environments. Create a unified and measurable system to compare and benchmark their access levels, access sensitivities, and access type, such as all apps with high sensitivity access

User context

Attain details relating to individual users, such as their organizational context, permissions, or risk (based on other misconfigurations that they are subject to)

Installation dates

Identify 3rd-party app clients' install dates

Certification status

Identify whether 3rd party apps have a SaaS provider certification

Third-party enrichment

Provide additional external enrichment, such as 3rd-party provider description, purpose, website, and logo

Reporting

Generate reports of 3rd-party apps with high access levels used by privileged users, benchmarking and comparing 3rd-party access between different and distinct SaaS environments

Device-to-SaaS User Risk Management

Even before employees were routinely working from home, user devices posed a risk to corporate networks. Security teams had no visibility into the owners of different devices and couldn't ensure that the devices were secure.

Personal devices are susceptible to data theft and can inadvertently pass on malware that was downloaded for personal use into the organization's environment. Lost or stolen devices can also provide a gateway for criminals to access the network. When individuals with advanced privilege levels use devices that are unsecured, they expand the attack surface with what amounts to an open gateway.

IT security departments require effective solutions that allow them to correlate the user, application, and device. More privileged users, such as admins or executives, present a higher risk level, and their end devices must be more secure. Once the security team has a strong understanding of the user and their access level, they can effectively evaluate the level of risk a personal device poses.

Visibility and Insights

Make sure the SSPM solution you are evaluating is capable of integrating with endpoint protection platforms, unified device management platforms, or vulnerability management platforms in order to track and monitor corporate-owned or corporate-registered devices and the device hygiene score accessing your SaaS environment.

Associating Devices with Users

End user device posture is a critical component in any SSPM program. Most existing endpoint protection and device management platforms lack SaaS and user context, impeding the security team's ability to assess device posture risk.

Your SSPM tool should include the following features to limit the exposure from user devices.

User information

Details relating to access privileges, apps they use, and the devices they access the network with.

Risk scoring

Device manageability and security posture.

Device discoverability

Discover end-user corporate-owned and BYOD devices and their user association.

Reporting

Provide multiple reports such as corporate and BYOD end-user devices that access SaaS platforms and their compliance level, devices used by privileged users and their compliance level, and unmanaged devices used by admins.

Device posture data

Provide end-user device posture data, such as critical vulnerabilities, through integrations with endpoint protection platforms and vulnerability management solutions.

Operating system verification

Identify users connecting to SaaS platforms using outdated operating systems, such as Windows XP and Vista.

Device-to-user correlation

Correlate end-user device details such as the operating system version or HD encryption status with the user's SaaS access level, and identify when a user is at high risk with a low device security score coupled with privileged roles and permissions.

Identity & Access Management Governance

Over time, the number of users with access to different parts of an enterprise's system increases. These user lists include active employees and partners but also may include inactive users, former employees, and vendors who are no longer providing services.

While these users may have moved on, they remain in the system and retain the same privileges that they had. Threat actors or disgruntled associates of the company can use these credentials to gain access to unauthorized areas of the system.

Security teams need a tool to identify and disconnect these users from multiple environments and applications within the company.

Visibility and Insights

Identify all users with access to any system or application within the corporate environment.

Identifying users

Detecting dormant or orphaned user accounts is an important step in ensuring that accounts don't provide access to the organization's environment. Once detected, security teams need to review the account's user state and de-provision access as indicated.

Your SSPM tool should also provide the following functionalities:

- **User Discovery:** Discover all users that are provisioned to the monitored SaaS platforms, including de-provisioned users that are reported by the platform
- **User Classification:** Automatically classify each user's affiliation as an internal or external user
- **Guest Status:** Identify guest and user invitation settings' state
- **Privileged users:** Identify privileged users from external domains
- **Full Employee Visibility:** Combine and present internal user descriptions, including department and title, from multiple platforms

Continuous Monitoring and User Authorizations

Your IAM Governance solution is critical in monitoring SaaS logins and ensuring that user activity meets security guidelines.

- **SSO:** Analyze single sign-on state in all accessed platforms
- **MFA:** Track multi-factor authentication in all accessed platforms, including for each user
- **Password Management:** Assess password complexity and expiration settings
- **Authentication Protocols:** Identify open legacy authentication protocols, such as POP3, SMTP, MAPI, and the users capable of leveraging these protocols. Monitor and gain context to the measurements for actual usage of such protocols.
- **Video Conferencing**: In conferencing systems like Zoom and Cisco Webex, identify the state of guest participants' access control and identification

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 that extends beyond Misconfiguration Management to cover SaaS-to-SaaS Access, Device-to-SaaS User Risk levels, and Identity & Access Management Governance. Our solution integrates 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

Misconfiguration Management

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 80 integrations
- [ ] Ability to easily add more SaaS apps
- [ ] Ability to capture user behavior

Comprehensive & Deep Security Checks

These are the domains and configurations to track and monitor.

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

Continuous Monitoring & Remediation

Enable security team to stay informed, communicate effectively, quickly shut down vulnerabilities, and protect your system.

- [ ] 24/7 continuous monitoring
- [ ] 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
- [ ] Non-intrusive
- [ ] Role-based access

SaaS-to-SaaS App Access

Track and monitor all SaaS-to-SaaS app access through comprehensive security checks to have a full understanding of your exposure.

Discovery of 3rd-Party Apps

- [ ] Ability to easily discover secondary SaaS apps
- [ ] Baselining apps
- [ ] Access reviews
- [ ] Volume of access

Continuous Monitoring & Control

To prevent secondary apps from providing an unauthorized gateway into your system, your SSPM solution should be equipped with the following third-party monitoring tools.

- [ ] Automated discovery
- [ ] Settings detection
- [ ] Consolidate API clients
- [ ] Scope breakdowns
- [ ] Identification
- [ ] Create standardized system
- [ ] User context
- [ ] Installation dates
- [ ] Certification status
- [ ] 3rd-party enrichment
- [ ] Reporting

Device-to-SaaS User Risk Management

Track and monitor all device-to-SaaS user risk to eliminate surprise vulnerabilities.

Associating Devices with Users

- [ ] User information
- [ ] Risk scoring
- [ ] Device discoverability
- [ ] Reporting
- [ ] Device posture data
- [ ] Operating system verification
- [ ] Device to user correlation
- [ ] Device posture data

Identity & Access Management Governance

Identify all users with access to any system or application within the corporate network.

User Authorizations

Your IAM Governance solution is critical in monitoring SaaS logins and ensuring that user activity meets security guidelines.

- [ ] SSO
- [ ] MFA
- [ ] Password management
- [ ] Authentication protocols
- [ ] Video conferencing

Identifying Users

- [ ] User discovery
- [ ] User classification
- [ ] Guest status
- [ ] Privileged users
- [ ] Full employee visibility
- [ ] User risk level
- [ ] Platform context
- [ ] Dormant accounts
- [ ] Administrative permissions
- [ ] Reporting
- [ ] Unique permission identification
- [ ] Oversight
- [ ] Unauthorized users