Reco
SaaS Security

CISO Guide To SaaS Security

In today's digital landscape, the role of a Chief Information Security Officer (CISO) is becoming more and more important as the dynamic landscape of cybersecurity threats has come to affect almost all aspects of business. This guide seeks to give an overview of the current security threat environment and introduce the key steps that CISOs can take in selecting an SSPM vendor and creating a comprehensive security defense plan.

Overview of Current SaaS Security Environment

As the majority of companies use cloud solutions – public, private, or a combination of both – Software as a Service (SaaS) has become an integral part of modern business operations. Across all industries, SaaS platforms provide unmatched scalability and flexibility and have quickly become the go-to solutions that enhance collaboration, productivity, and efficiency. However, as SaaS environments expand in complexity and use, that also means that a wide array of sensitive information also gets moved to the cloud, which renders critical the importance of securing these environments.

The year 2023 has seen an increase in attacks of all kinds. The Cloud Security Alliance reports that 55% of the 1130 organizations surveyed in 2023 reported a breach in the past two years, and another 12% also confirmed the possibility of having been breached (p. 3).[1] Additionally, IBM Security pinpoints the cost of a data breach in 2023 at USD 4.45M, a 2.3% hike from the 2022 Numbers (p. 5).[2] Verizon also signals a concerning upward trend in attacks, noting that "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering," while 83% of 2022-23 breaches involved an external actor perpetrating an attack from outside the organization (p. 8).[3]

In this context, for the past few years, Security Service Posture Management (SSPM) has emerged as a cornerstone of present and future cloud security, strengthening both proactive and reactive security capabilities. A subset of the broader cloud security framework, SSPM is an API-based solution that connects to a company's SaaS applications and investigates misconfigurations, access and account identity, while providing malware and ransomware protection.

[1] *State of SaaS Security: 2023 Survey Report*. (n.d.). CSA. Retrieved December 14, 2023, from https://cloudsecurityalliance.org/artifacts/state-of-saas-security-2023-survey-report/

[2] *Cost of a data breach 2023* | IBM. (n.d.). www.ibm.com. Retrieved December 14, 2023, from https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258

[3] Verizon. (2023). 2023 *Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

While SSPM helps companies analyze data, ensure continuous monitoring, identify patterns, and react to anomalies, it also helps them be proactive and prepare for future attack scenarios. To reduce the attack surface and minimize the future possibility of a breach, SSPM also provides an inventory of best practice solutions for regulatory compliance and a record of tactics, techniques and procedures (TTPs) to create security policies. In addition, to make both proactive and reactive decisions efficiently, the security team has quick access to dashboards and reports. As a result of all these advantages, SSPM has been constantly growing in importance for the past few years and has become a must-have for companies that want to have a solid risk-management strategy and a real-time overview of their SaaS environment and of all their connected applications, including third-party ones.

At its core, SSPM modernizes cloud protection and ensures a future where risk is manageable. SSPM represents an investment, but it also represents an insurance policy, where companies are making an investment in their SaaS applications to decrease their attack surface and reduce the likelihood of future exposure. An SSPM investment is worth the upfront cost when taking into account long-term breach costs.

In their 2023 report, IBM Security traces a direct correlation between cost and length of days before discovering a security breach. Automation is part of the offerings of many SSPM solutions. For example, SSPM is most effective when it includes AI solutions and advanced threat analytics that use deep learning to identify and analyze anomalies, where people and machines behave in unexpected/atypical ways. Extensive use of AI security solutions has proven very effective in identifying and containing data breaches. For example, IBM Security estimates that an organization using AI and automation through several tools that are integrated at the operational level saves about 108 days experiencing an attack, by discovering it faster (p. 51).[4] This translates to savings of approximately USD 1.8M for these companies, an almost 40% difference when compared with companies that did not use any AI or automation (p. 52).[5]

The year 2023 has witnessed an intensified focus on SSPM, not only due to the escalating sophistication of cyber threats, but also due to increased regulatory scrutiny. As a result, companies are grappling with achieving a delicate balance between satisfying their users' requirements for convenience and simplicity, and the implementation of stringent security protocols, such as the ones related to personally identifiable information (PII) (p. 19).[6] Overall, compliance frameworks and regulations governing data protection are shaping the direction of SSPM strategies. In addition, as data sovereignty and privacy concerns become paramount, companies are compelled to tailor their SSPM practices to align with regional and global regulatory requirements.

[4] *Cost of a data breach 2023* | IBM. (n.d.). www.ibm.com. Retrieved December 14, 2023, from https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258

[5] Ibid.

[6] Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[7] Cost of a data breach 2023 | IBM. (n.d.). www.ibm.com. Retrieved December 14, 2023, from https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258

SaaS Security Questions and Answers for Forward-Looking CISOs

As cloud environments have a complex and constantly-changing threat landscape, CISOs can build SSPM solutions into their present and future business strategy by drawing on the following lessons learned from past SaaS security.

A few helpful questions and answers to consider are:

Where does a SaaS security journey begin?

The SaaS security journey typically begins with a comprehensive assessment of an organization's current security posture and of potential risks associated with adopting or already using SaaS applications. This initial phase involves identifying the types of SaaS applications in use, understanding data sensitivity, and evaluating existing security measures.

What is a SaaS security's end goal?

Due to the dynamic nature of cloud environments, a company's SaaS security needs to be adaptable and scalable to match a company's current and future needs that are determined by the constantly evolving nature of threats. The end goal of SaaS security should significantly decrease a company's risk exposure and attack surface.

Has SaaS changed or have security priorities changed?

The landscape of SaaS security is continuously evolving. Growing cloud adoption and development of public, private or hybrid cloud solutions definitely triggered SaaS security changes, but most importantly, security priorities have changed as well, especially through and since the pandemic. As the world shut down, the majority of the workforce became remote. This brought to the forefront the urgency of securing remote connectivity and of accelerating robust identity and access management solutions, as well as implementing multi-factor authentication. Remote employees also gave rise to data privacy and compliance concerns, while the exponential adoption of collaboration tools overnight catapulted security risks associated with these tools to the top of security concerns.

How to align SaaS security strategy with the broader business objectives of a company?

SaaS security used to be relegated to the IT team. However, SaaS security has come to affect many aspects of a company's growth, some softer ones, such as influencing customer trust, reputation and brand, or other ones with direct impact, such as costs associated with disrupting operations or supply chains, raking up insurance costs, losing intellectual property, or forsaking partner and investor confidence. These aspects make it so that the responsibility and the benefits of an effective SaaS security is shared, which in turn, requires that CISOs have a seat at the table when making decisions about business priorities, objectives, and the respective allotted budget.

Should an investment in AI be part of SaaS security strategy?

If a company faces complex threats and operates at scale, investing in AI upfront is the best investment move that will guarantee a return on investment per the most recent IBM Security report. Their survey revealed that companies that used AI and automation managed a much faster response to detecting and managing a breach. They were 108 days faster than similar companies, not using AI (p. 53)[7], and this translated in significant cost reductions. Hence, an upfront investment in AI will pave the way for future savings and a successful, proactive SaaS security.

[7] *Cost of a data breach 2023* | IBM. (n.d.). www.ibm.com. Retrieved December 14, 2023, from https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258

SSPM Key Features: Selecting the Best SSPM Solution

SSPM stands at the forefront of SaaS security. It offers companies a strategic approach to fortify their security postures and manage risk effectively. It also ensures the seamless integration of SaaS applications within a secure and compliant framework. An effective SSPM solution helps a company gain key insights to identify misconfigurations, control over-permissions, stay alert to anomalous and risky user behavior, quickly pinpoint compromised accounts, and monitor third-party apps continuously including those connected by both human interaction and machines. With new market entrants competing with more established providers, selecting the best SSPM solution involves careful consideration of various factors. An effective solution needs to help companies establish a discover-control-protect framework. Here are a few must-have characteristics to look for in the selection process:

Effective SaaS application discovery

Does every company know every SaaS app being used in their environment? SSPM solutions connect to the SaaS environment and discover connected applications, including third-party ones. They index sanctioned applications and reveal unsanctioned ones that have been connected by a human or machine. The key to adequate protection is continuous monitoring of the posture of SaaS applications at the metadata level to provide alerts to exposure. So, while human expertise remains invaluable, SSPM solutions allow companies to optimize their security team's time and effort in monitoring third-party applications through prioritized alerts and real-time data, so they can undertake the remediation of threats faster.

Configuration management

SSPM helps the security team keep up to date with monitoring and security updates of SaaS applications, identities, and data within the Security infrastructure. Once a security baseline is established, SSPM solutions will help the security team oversee configuration settings and will enable them to get alerts as to any deviations from the baseline in order to monitor and control configuration drifts and detect any other configuration-related vulnerabilities. Configuration drifts occur when changes are made to the system outside of the established processes, and it can occur for various reasons. Manual posture checks across complex systems is slow, takes a lot of time and is prone to human error. So, possibly the most appealing aspect of SSPM solutions is that it includes AI and automation for continuous configuration checks. With AI, configuration management can be automated to correct configurations when deviations are detected, or to revert them back to the baseline.

Identity, permission and SaaS application monitoring

With an SSPM solution, companies can monitor identities to see who has access to what applications. The question to ask is whether users have the adequate permission level, or whether they benefit from permission privileges above their level. Overall, SSPM best practices require the implementation of least privileged access, which ensures that users get the access they need, but not more because uncontrolled access usually exposes the company to additional and unnecessary risk. Additionally, with SSPM, companies can also identify connected, unsanctioned third-party applications and remove them, or they can discontinue subscriptions to unused applications, which can trigger significant cost savings. Finally, anomalous user behavior and patterns are quickly spotted and prioritized alerts sent to the security team, so they can quickly take steps to remedy various situations, such as an employee downloading sensitive information because leaving the company.

Ready-to-use policies based on TTPs

Reputable SSPM solutions will have a library of ready-to-use policies created based on real-world cyber attack scenarios that use various ransomware, account takeover, and insider threats TTPs. Additionally, effective SSPM solutions will be able to push prioritized alerts to the security team, which will speed up the detection of any threats. Prioritized alerts provide the ability to develop responses to insider threat, account takeover, or ransomware. They also facilitate the development of an incident response plan specific to SaaS applications that should outline the steps to be taken in the event of a security breach, including communication protocols and mitigation strategies. From there on, continuously updating the plan based on the nature of the prioritized alerts received should be easy.

Integration with an Existing SIEM or SOAR solution

Integration between SSPM, SIEM and SOAR enhances an organization's ability to detect, respond to, and mitigate security threats effectively. For example, SIEM systems can use SSPM-generated data to enrich the information used by security analysts regarding security events. In correlation with data from other events, SSPM data can also help with establishing risky behavior from various personas and can aid in setting up and triggering automated or semi-automated alerts. In turn, SOAR platforms can integrate with SSPM to create automated responses to certain security events for which they can apply set rules according to established policies, and they can also initiate set remediation processes when SSPMs identify misconfigurations.

Adherence to compliance frameworks

In the aftermath of the pandemic, industry regulations and data protection laws have become even more stringent than before. In particular, industries, such as healthcare or finance that sometimes have the burden of many legacy systems, have more than ever come under compliance scrutiny. An SSPM solution can help companies achieve and maintain compliance with regulatory requirements over time, with a SaaS security program that is automated and updated regularly. To establish a SaaS governance or assurance plan that implements security measures to reduce the risk associated with SaaS applications, SSPM solutions can continuously check SaaS security posture against built-in compliance policies, frameworks, and due diligence best practices, such as HIPAA Security Rule, NIST Cybersecurity Framework, HITRUST CSF, ISO/IEC 27001, or CIS, SOX and SOC 2, FFIEC Cybersecurity Assessment Tool, PCI DSS, SWIFT Customer Security Controls Framework and GLBA.

Data privacy

A state-of the art SSPM solution will not increase your attack surface because it does not get access to your actual, proprietary data, but only ingests and analyzes your metadata. Examples of metadata are identification data about your assets and devices and their physical location on the network, user access permissions, or data about the settings of devices and applications and the infringement of set rules and policies that may indicate high-risk behavior from various internal or external actors.

Fast connection via API

API-based SSPM solutions offer greater efficiency gains because no integration is required.
Your security team can do in a few hours what they used to accomplish with manual check-ups in a month.

Automation capabilities

With the persistent evolution of the threat landscape, security professionals are adopting proactive approaches to SSPM, emphasizing real-time monitoring, adaptive controls, and threat intelligence integration. Automation is key, where topmost companies leverage artificial intelligence and machine learning to detect anomalous activities and respond to potential security incidents with utmost expediency. Of vital importance is the automation of the monitoring of incorrectly configured SaaS-based applications that expose applications and identities to external parties.

Scalability

Companies need to select an SSPM partner that can grow and evolve with them. Robust SSPM solutions take into account how a company's application footprint will grow and they allow the company to scale ahead.

Select a Partner for the Road Ahead

As companies continue to innovate and adapt, the synergy between SaaS adoption and robust SSPM practices will continue to shape the future of cloud security. Companies need to strive to match the versatility of cyber attackers by reducing their attack surface with the help of SSPM solutions. With this long-term view in mind, when selecting an SSPM solution, companies need to look for a partner not only for today, but for the road ahead. In order to achieve this, there are a few factors to consider beyond technical prowess. While not exclusive, here are a few steps to follow.

Start a request for proposal process

Before investing in a new solution, companies typically put out an RFP to evaluate vendors and capabilities. However, even before getting to this step, CISOs should do a thorough security assessment to understand the limitations of their infrastructure and security and to set goals for the new tool that they are looking to purchase.

Evaluate reputation

To a certain extent, an SSPM's vendor reputation directly correlates with their reliability, and as the best SSPM partnerships are long-term – reliability is one of the key features a company should look for in a vendor.
As part of the RFP process, companies should research the finalists' reputation by looking at their experience, customer reviews, and their commitment to regular updates and improvements.

Rate customer support

A company that puts its customers at the heart of its development, growth and operations is one that will not only stay ahead of the competition, but also that will be around for a long time. Happy customers equal growth and reliability. So, a few factors to consider when researching finalist vendors are not only knowledge and expertise, but also availability of customer service, open transparency and communication, including service-level agreements (SLAs) for response times and escalation processes, abundant documentation and training materials that are user-friendly, as well as a user-friendly platform, among other things.

Take advantage of demos and trial periods

All vendors will offer free demos. While you can definitely get a feel for a product during a demo, especially when it is given by one of the finalists of a rigorous RFP-selection process, nothing beats the hands-on trial of a product. Testing the solution in their environment allows a company to assess its performance and suitability for their exact needs. Vendors that offer this option are confident in the strength of their product and can make the top of a company's short list.

In conclusion, the process of selecting a Security Posture Management (SSPM) vendor is a serious endeavor that requires planning and meticulous evaluation. While the process may seem complicated and even daunting, the choice of an SSPM solution that fits a company's present and future needs will be a worthy investment with a high return. What is required in the selection process is a holistic assessment of technical capabilities, integration potential, scalability, and alignment with a company's unique security objectives. Fit is important beyond technological capabilities. Vendor reputation is crucial. In this respect what to look for are great customer support reviews that prove that the vendor is committed to customer success and a track record that indicates that the vendor has successfully solved similar challenges to the ones the company is experiencing or projecting.
As companies embark on their unique SaaS security journey, the selected SSPM vendor should not merely meet current needs but serve as a strategic partner that is able to evolve with the company in a constantly shifting cybersecurity landscape. After all, this partner will contribute to the long-term resilience and security posture of the company, and inherently, to its current and future growth and success.

Reco

Reco is a leading SaaS security solution that is redefining the way enterprises secure their SaaS environment by taking an identity-first approach to SaaS Security Posture Management (SSPM). Connecting in minutes via API, Reco discovers every app, its users, and their actions to seamlessly prioritize and control the risks in the SaaS ecosystem.

Reco can help CISOs to provide the right tools to their security, engineering, and IT teams to prevent the risk of exposure to breaches, by understanding their SaaS applications and identities, while controlling access and permissions. Reco uses advanced analytics around persona, actions, interactions and relationships to other users to identify suspicious human behavior patterns. It also enables alerts on exposure from misconfigurations, over-permission users and compromised accounts.

With Reco, security teams have the insight they need to take swift action to mitigate risk and the right advisors that can accompany you on your growth path.

You can learn more or book a demo at www.reco.ai

Reco SaaS Security Checklist for CISOs

Reco created this checklist to help CISOs establish, implement, and continually improve their SaaS security posture while staying informed about updates and emerging threats.

Starting point

Asking questions constitutes the foundation of your plan to build out your security strategy. As cloud environments have a complex and constantly-changing threat landscape, a few helpful questions to consider as you start investigating an SSPM solution are:

- □ Where does my SaaS security journey begin?
- □ What is my SaaS security's end goal?
- □ Has SaaS changed or have security priorities changed?
- □ How do I align my SaaS security strategy with the broader business objectives of my company?
- □ Should I invest in AI as part of my SaaS security strategy?

Middle of the Road

Comparing and contrasting SSPM vendors paves the way to finding an effective solution that will help you create a discover-control-protect security framework for your company. Here are a few must-have characteristics to look for in the selection process:

Effective SaaS application discovery

- □ Sanctioned connected applications
- □ Unsanctioned connected applications
- □ Third-party applications
- □ Shadow applications
- □ Installation dates and end user analytics
- □ Authorized apps
- □ Monitoring of incorrectly configured SaaS-based applications
- □ 24/7 continuous monitoring

Identity, permission and SaaS application monitoring

- □ Monitor identities
- □ Monitor permission privileges
- □ Discovery of permission access level
- □ Advanced analytics for additional context
- □ Implement least-privilege access
- □ Identify anomalous user behavior patterns

Configuration management

- □ Baseline configuration settings
- □ Detection of configuration drifts
- □ Automated detection of misconfigurations
- □ Automated continuous configuration checks and corrections
- □ Measure SaaS security posture and risk reporting over time
- □ IT audit readiness

Ready-to-use policies based on TTPs

- □ Extensive library of ready-to-use, dynamic policies created and maintained by experts
- □ Prioritized alerts

Integration with SIEM or SOAR

- □ Aggregated and normalized SaaS activity events
- □ Data-based analysis of risky behavior personas
- □ Automated or semi-automated alerts based on personas
- □ Automated response to security events
- □ Apply set rules according to event
- □ Guided remediation

Adherence to compliance frameworks

- □ Establish An industry-specific SaaS governance or assurance plan
- □ Built-in compliance frameworks, and due diligence best practices that support your industry and territory requirements

Data privacy

Access only to metadata such as:

- □ Location
- □ Implement least-privilege access
- □ Analysis of settings of devices and applications

System functionality

- □ Quick deployment via API
- □ Guided onboarding process
- □ Integrations for secure onboarding
- □ Low false positives
- □ Scalability

Automation capabilities

- □ Real-time monitoring
- □ Adaptive controls
- □ Threat intelligence integration

The Road Ahead

When selecting an SSPM solution, you need to look for a partner not only for today, but for the road ahead. Beyond looking for technical prowess, here are a few other factors to consider and steps to follow:

Start a request for proposal process

- □ Thorough security assessment of needs
- □ Understand limitations of infrastructure and security
- □ Set security goals for tools needed

Evaluate reputation

- □ Customer reviews
- □ Experience
- □ Communications
- □ Frequency of updates and improvements

Rate customer support

- □ Availability of customer service
- □ Open transparency and communication
- □ SLAs for response times and escalation processes
- □ User-friendly training offerings
- □ User-friendly platform

Take advantage of demos and trial periods

In conclusion, a comprehensive Security and Service Performance Management (SSPM) solution checklist serves as a vital tool for CISOs in their search to fortify their cybersecurity and optimize service delivery. On this journey, Reco can serve as your advisor and partner.