S&P Global
Market Intelligence

451 Research Market
Insight Report Reprint

SaaS security posture management, Part 1

Introduction to current trends

April 4, 2025

by Justin Lam

SaaS is increasingly preferred for application adoption. The discipline of SaaS security posture management overlaps with other disciplines in identity and access management, secure service edge, and data security. This first of a two-part series looks at SSPM's origination and current trends.

Introduction

For enterprises, SaaS is increasingly the preferred form factor for application adoption. For vendors deploying SaaS, the advantages to building competitive moats are meaningful, as network effects from consumption and the shared insights of user adoption guide more precise A/B testing and end-user enterprise agility. With the move to SaaS, security teams must provide different assurances against risk. Here we cover the security tools designed to assess and initiate remediations for deficiencies in SaaS security posture.

THE TAKE

The variety of operating approaches within SaaS makes enterprise security challenging. While there have been improvements in governing and controlling initial user authentication, accounting for and securing usage of sensitive data within SaaS applications is a distinct challenge that SaaS security posture management addresses. Yet challenges remain for SSPM vendors; SSPM controls are particularly dependent on integration with the SaaS environments they protect. Integrating with each SaaS vendor's APIs, given the variety of different operating approaches, forces SSPM vendors to be reactive to SaaS. SSPM vendors must choose to integrate with the SaaS providers that enable suitable API integration and are common enough to justify the integration expense. Enterprises still must account for, understand and protect the data they have, regardless of venue. A layered, resilient approach to security is needed even as integrations with SaaS vendors continue to evolve.

Context

According to 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Budgets & Outlook 2025 survey, 86% of all enterprises said that they used or were planning to use SaaS in the next 12 months, compared with 61% using IaaS public cloud infrastructure and just 40% using colocation or third-party datacenters. While the barriers to developing, deploying and hosting applications have fallen with the advent of cloud, the barriers to SaaS application adoption are even lower. Mission-critical applications in collaboration, human resource management (HRM), supply chain, enterprise resource planning (ERP) and customer relationship management (CRM) are delivered as SaaS. Even conventional tooling for core IT infrastructure is deployed as SaaS; source code control, development CI/CD pipelines, ITSM systems and even databases are delivered as SaaS, abstracting away many hosting, deployment and operational challenges. Business models and enterprise value of SaaS companies prize the customer loyalty and stickiness of recurring revenue.

Definitions, originations and characterizations

SSPM guides security teams, SaaS program administrators, developers and users in better understanding risks when using SaaS. To an extent, they also intervene to mitigate those risks. SaaS security risks are the combination of assets, threats, vulnerabilities and subsequent impacts when users or processes interact with these SaaS offerings.

SaaS vendors have narrowed the shared responsibility model with their customers. In general, the sole baseline integration IT task with SaaS is to specify which users will have access and how they will authenticate and access that SaaS service. Subsequent SaaS roles and permissions are configurations defined within SaaS, rather than attributes associated elsewhere within other infrastructures or platforms. Roles and permissions may be populated from users defined in identity platforms such as Microsoft Corp.'s Entra ID and they may leverage a single sign-on like Okta Inc.'s to access a given SaaS application with a single set of credentials. For example, consider the general customer journey to adopt a SaaS-based CRM. Enterprises select users or groups of users from their own identity platforms such as sellers and marketers.

The marketing campaigns, accounts and purchase transactions are examples of SaaS-specific data types. Subsequent permissions, roles or workflows and audited events are configurations defined by users and enforced by the SaaS platform. SaaS security leans heavily on the SaaS provider to furnish controlling features and is dependent on how often SaaS vendors update their API sets. SSPMs are at the mercy of the SaaS vendors' APIs.

Pure-play SSPM vendors unify the security risk posture for all SaaS adoption within an enterprise. Security administrators can integrate deeply into SaaS platforms and automate interventions that minimize risky user behaviors. For example, a Google Workspace item such as a Google Sheet may be easily shared with other users via a simple URL reference. SSPMs can understand how many Google workspace items have been shared, how long they have been shared and whether that sharing is active or dormant. SSPMs can further reduce risks, either overtly expiring dormant asset sharing or by prompting users to explicitly continue. While data loss prevention is the ultimate end goal, enterprises must actively account for their data. Data discovery and classification have been top initiatives and have fueled both the growth and consolidation in the adjacent DSPM segment. Specialist DSPM and broader data security suites are making plays themselves into SSPM.

While adjacent tools in IAM and security service edge (SSE) do not necessarily account for data within SaaS apps, they can control authentication and network access. For example, identity threat & response (ITDR) polices how users have accessed their SaaS applications. ITDR traces harm such as credential stuffing or exploits in faulty OAuth implementations to minimize account takeovers. SSE and preceding solutions such as cloud access secure brokerage (CASB) police all activities between users and the SaaS apps they access. CASB could be argued as a predecessor to SSPM offerings. Now, SSE solutions are integrating greater data loss prevention (DLP) tools. Both IAM and SSE approaches are perimeter-like controls in that they do not necessarily assess or harden the SaaS application or underlying data usage itself. SSE also limits "shadow SaaS" adoption that can incur additional risks.

Operational keys to success

While it may be overwhelming to consider all ingress and egress of data, it is also useful to employ phased approaches to progressively address risks, and to do so consistently whenever possible. For example, standardizing strong authentication and centralized identity and access management would allow greater enterprise control and reduce risks across all users. An additional basic step includes inventorying what SaaS is used, identifying any shadow SaaS usage. Yet reconciling app user accounts that were initially provisioned with their own sets of identities to a central IAM system may be a significant challenge. This is especially true for multiple SaaS solutions coupled together. Consider the use case of a seller accessing a CRM system with centralized SSO yet also leveraging LinkedIn Sales Navigator with their own individual account to better understand contacts within a key target account. Security teams must reconcile the identities of the SSO user and their externally or separately authenticated accounts.

Data, policy and behavior discovery within SaaS applications remain critical. Certain object types are well known and easier for both security and SaaS program administrators to account for. Structured items with obvious personally identifying information are natural candidates. Semi-structured or unstructured content items may require more analysis; within an HRM, ERP or CRM system, items may have multiple dependencies to discover and classify accurately. Additional discovery about events, permissions and policies must be made. Given an account takeover or insider attack, understanding what any given user or process has accessed and has access to is imperative to understanding and containing the harm.

SSPM consolidates and translates data, policy and behavior discovery into existing security operations. Even if security teams mastered the ins and outs of any given SaaS provider, they would still need to rationalize alert or remediation priorities. Some applications may have very good reasons to make their data more public than other applications, even if it is the same classification of data.

For larger or more complex organizations, other challenges remain, with no easy fixes. Enterprises that have grown by consolidation may have multiple instances of different ERP, collaboration or even IAM users to consolidate. If a complex supply chain management or ERP system is in scope for SSPM, many third-party SaaS apps will have to be considered. Additional challenges come from integration with legacy or proprietary systems, regulatory or data sovereignty requirements.

Other security posture management (DSPM, CSPM, ASPM, etc.) have various levels of remediation and SSPM is similar. In general, SSPM does not directly permanently alter or intervene in SaaS platforms to remediate weaknesses in security posture. Rather, suggestions are made for SaaS program managers to initiate more permanent policy fixes directly by the SaaS tool itself. Other SSPMs can make loose remediations — disabling excessive sharing of neglected items, for example — but they would not necessarily delete or redact sensitive information.

For security teams, the greatest challenge is understanding both the enterprise risk and rewards for any given SaaS application. Security teams can help promote or relegate any given SaaS app faster to boost agility, reduce risk and optimize SaaS spending. Overall, enterprises need clear understanding of their data. In 451 Research's Voice of the Enterprise: Customer Experience & Commerce, Merchant Study 2024 survey, managing the volume, variety and quality of customer data was the most significant inhibitor to growth for customer experience leaders who are economic buyers for CRM. Yet using more data for richer intelligent experiences and strong data security, consent and governance were their greatest initiatives. By understanding the specific concerns among lines of business about how data is used within SaaS, security teams can provide better support and proactive assurance.

Still early

For SSPM vendors, it is still early. In addition to the relative novelty of software delivered as a service, SaaS platforms themselves have undergone significant changes. Microsoft 365 has unified its substrate layers to consistently expose REST APIs and client libraries, to consistently access Microsoft 365 core services, Windows services, enterprise mobility and identity platforms like Entra ID.

Yet uncertainty remains, with cloud economics and the motivations for SaaS providers changing. An enabled product integration that drives platform consumption one day might become an indirect competitor the next. We will be publishing a subsequent report evaluating current trends and analyzing what may be next for SSPM.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html

S&P Global
Market Intelligence

451 Research Market Insight Report Reprint

SaaS security posture management, Part 2

The journey ahead

April 9, 2025

by Justin Lam

In the second report in this series, future trends for SaaS security posture management are considered. New challenges in trust, safety, architecture authenticity and shifting motivations for SaaS providers must be accounted for by enterprises to understand and anticipate future risks.

Introduction

SaaS security posture management faces profound challenges in aligning with shifting motivations and models within the broader SaaS ecosystem. We expect that generational industry changes in trust, safety, architecture and motivations will intertwine security and commercial risks as enterprises need to demonstrate with greater trust and confidence. In the first part of this series on SaaS security posture management, we covered current trends. In the second part, we evaluate future trends for SSPM given these industry changes.

THE TAKE

To understand SSPM's future direction requires understanding the current and future directions of SaaS. Currently, an SSPM vendor will support a specific SaaS platform only after it has gained critical mass in user acceptance. Yet there are thousands of emerging SaaS offerings that must be used safely and securely. Compliance automation has shown a way forward, with thousands of SaaS vendors achieving security compliance such as SOC 2 Type 2.

GenAI architectures and agentic approaches will likely transform existing SaaS vendors to become service-as-software vendors. Whereas SaaS has supported knowledge workers, service as software will perform knowledge work. As such, SSPM and technology vendors must establish trust and transparency, and guard against new harms, abuses or hallucinations. With potentially thousands of new emerging services that enterprises need to safely and economically onboard, these changes could drive the interests of SaaS vendors, SSPM providers and enterprise customers toward a shared destiny rooted in security, trust, service and outcomes.

Motivations

As SaaS vendors mature, they are motivated to reduce churn and improve net-new recurring revenue by integrating their offerings with as many other solutions as possible, maximizing an enterprise's dependence on them. The network effects and telemetry gathered from the consumption and integration build competitive moats; large SaaS platforms have created third-party marketplaces that drive platform consumption and achieve greater distribution to cross-sell and upsell more efficiently than their competitors. Underlying any given SaaS is the strength of its API set to drive integrations and, hence, platform dependence. SSPM exists because underlying SaaS APIs exist in the first place. These APIs allow for richer integration to the rest of the enterprise's technology stack.

SaaS APIs enable SSPMs to inspect and understand SaaS data and SaaS activities. Yet with any SaaS provider, an enabled production integration that drives platform consumption one day might become an indirect competitor the next. While Salesforce Inc. maintains APIs for third-party data management and backup, it also acquired Own (backup) and will fold its data management capabilities directly into its core platform. Most SaaS providers do not have the resources to indirectly compete with their technology partners, and third-party SaaS security's value is the ability to work across multiple SaaS apps.

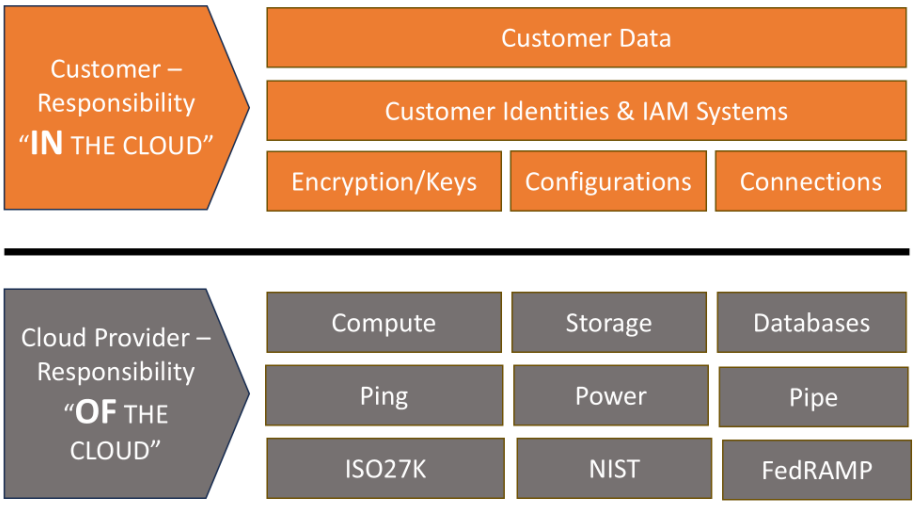
In the search for net-new recurring revenue, some tiered licensing has presented challenges to SSPM and security as a whole. So-called enterprise features have treated SSO integration as a premium feature. Additional detailed logs, roles and other functions may be deprecated in lesser product tiers and subsequently limit SSPM integration effectiveness.

Encouragingly, the SaaS industry is maturing in security, especially for business-to-business use cases. The rise of third-party risk, compliance automation and security questionnaires has SaaS vendors strategically designing security into core offerings. Atlassian Corp., a SaaS engineering tools platform, has required SOC 2 Type 2 compliance for any third-party SaaS vendor listed in its marketplace. Atlassian is motivated to drive consumption of its platform, and forces others in its orbit to follow. SaaS companies use compliance automation to demonstrate their security posture and designs to accelerate their own sales and distribution.

Compliance and risk management have matured, as have the responsibilities of SaaS developers and operators. The mere presence of documented controls in point-in-time audits is no longer sufficient. Operational security documented over time is mandatory for both risk management and to drive continued platform consumption. Compliance automation documents the SaaS vendor's security design and operations. SSPM documents the enterprise's security risk posture for its own usage of any given SaaS.

To that end, shared responsibility models are changing. In Figure 1, the first shared responsibility models clearly delineated responsibilities in the cloud compared with responsibilities of the cloud.

Figure 1: "Initial shared responsibility" — lift and shift circa 2008

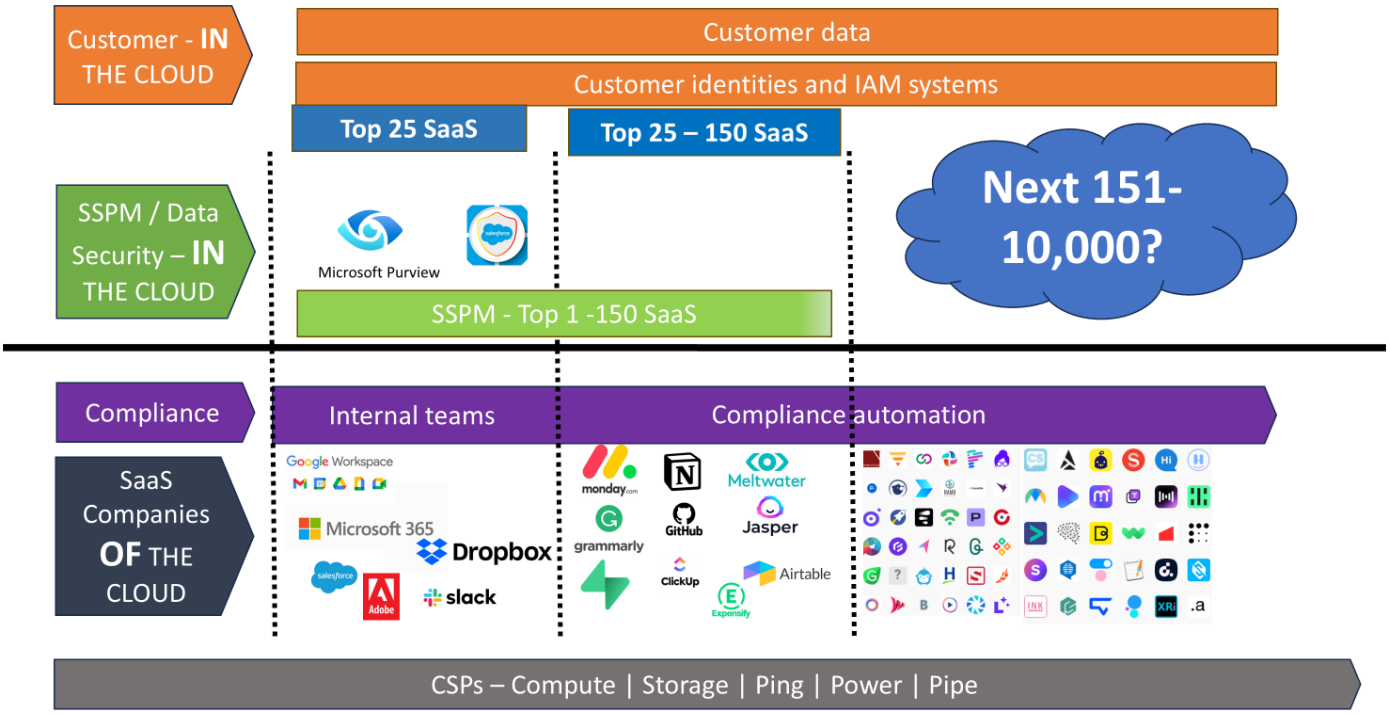


- Responsibilities defined by specific technologies and the operations thereof.
  - CSP makes a secure function (i.e., virtual networks).
  - CSP one-way delegates controls to tenants.
  - Only clients define and operate their virtual networks.
- Secure design and secure operation starting to converge, but remain distinct.
- Tenants inherit some risk management/compliance benefit from CSP.
  - Tenants have their own compliance mandates.

Source: S&P Global Market Intelligence 451 Research.

In Figure 2, responsibilities merge among customers, SSPMs, compliance automation, SaaS companies and the CSPs they are built on. From left to right, the tiering of SaaS providers shows the compliance and SSPM efforts for different SaaS provider sizes. Compliance shows responsibilities of the cloud and SaaS provider; SSPM and data security measures show responsibilities in the cloud. Compliance automation has democratized compliance standards for thousands of SaaS companies to document the secure design of their offerings. Can thousands of SaaS companies take the next step and ensure that their programs can be operated safely, and that the controls employed in the cloud can be taken by customers themselves?

Figure 2: "Converged destiny" — circa 2025 and beyond



Source: S&P Global Market Intelligence 451 Research.

The changing economics of SaaS to win repeat business and address new markets prevail. While SaaS's underlying APIs have been integral to enable SSPMs, more elements of SSPM might have to be undertaken by SaaS providers themselves if they are motivated to win repeat business and earn new customers with safer user operations. Generational shifts in the SaaS market are already happening, which should drive further convergence.

Architecture and authenticity

Over time, SaaS user experience and API sets have abstracted away the need to organize applications into different tiers, such as presentation, logic or data layers. Yet GenAI's integration into SaaS requires understanding a new layer — the model layer. Different algorithms and processes generate and alter outputs differently. Large public frontier models offer SaaS vendors simpler and faster integration with their pre-trained data sets, yet SaaS providers must still govern the inputs and outputs. Private models give SaaS providers greater control over both model parameters and hyper parameters, but could require greater data governance if any sensitive data is used for training. Yet data governance for GenAI lags. In 451 Research's Voice of the Enterprise: Data & Analytics, Data Architecture for AI 2024, among organizations that have adopted AI or have AI-related initiatives, 52% report engaging in AI governance practices.

Additional reasoning and automation functions within SaaS are driving agentic AI, where SaaS takes on actions previously left to individual users. More sophisticated prompting leads to LLMs acting as an agentic orchestration layer that can be assigned more sophisticated tasks and can take on more sophisticated, reasoned decisions.

While SaaS providers have long documented compliance for other layers within their offerings, documentation and transparency for model performance, customization, and how public or private models are used together remains to be seen. Providing assurances to enable users to safely operate any agentic AI also remains to be seen. Efforts to understand or "red team" GenAI applications are just beginning. While SSPMs today consider authenticated user activities, authentication of the agents and the tracking of their invoked activities also remain to be seen. Like nonhuman identity management, used to manage IoT or DevOps use cases, the agents' ephemeral identities must be accounted for.

New harms and risks also emerge, especially attacks on integrity, trust and safety. Removing bias or preventing abuses will also be challenging. Reality Defender, a pioneer of GenAI deepfake detection, still relies on evaluating deepfake artifacts themselves in focused use cases. Tracing or eliminating classes of deepfake sources remains a challenge for SaaS vendors and their customers.

Large vendors like Salesforce have built or facilitated SSPM and have accounted for the model layers among their agentic processes. Salesforce Shield and the Einstein Trust Layer highlight the investments larger SaaS companies can undertake. For the remaining ecosystem, controls and capabilities must be democratized further. While GenAI is lowering the barriers to entry for many SaaS startups, so much of the scale-up success around these new challenges must be co-invented with their customers.

Service as software

Software as a service has so far created trillions of dollars of investor value in the last generation. Its economics have removed opportunity cost from expensive licensed software, replacing it with per-seat or even consumption-based pricing. The largest SaaS vendors have created competitive moats around the data they have collected, and rely on network effects and superior distribution to drive platform consumption. Yet SaaS itself is going through generational changes. Software as a service could transform to service as software, and the disruptors from previous generations would become the disrupted incumbents.

The transformation from servicing knowledge workers to performing knowledge work would be profound. With more agents interceding within platforms, the services provided would likely perform more knowledge work, rather than simply augmenting knowledge workers. New model layers may remove competitive data layer moats that incumbent SaaS vendors have built. New consumption or subscription patterns would disrupt previous SaaS business models.

For SSPM vendors, existing SaaS providers, external auditing teams, compliance automation vendors and enterprises, aligning with current and future economic motivations remains essential. As stewards of last resort for the customer data and experiences entrusted to them, enterprises must lead the way forward. All players share a destiny to safely and economically discover, deploy, and eventually disperse SaaS and service-as-software offerings.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html