

Whitepaper

The Configurations That Cost Millions: Why SaaS Is the New Breach Frontier

Author

Ashish Kumar Mishra (Tech Mahindra)



Executive Summary

In many cases, enterprises have zero visibility into their Salesforce environments, OAuth connections, and Microsoft 365 tenants. This visibility gap between security programs and SaaS applications is creating a new frontier for cyber risks. A few notable breaches from the recent past highlight the severity of these blind spots. A misconfigured Salesforce community site leak, a compromised OAuth token granting access to GitHub repositories, and unauthorized access to 38TB of Microsoft's internal data underscore the business impact of unmanaged SaaS risks. ^{1, 2, & 3}

SaaS security posture management (SSPM) precisely addresses this oversight challenge and provides the visibility, context, and control needed to secure modern SaaS environments. What follows is a practical blueprint for understanding SaaS risks, evaluating SSPM capabilities, and operationalizing SSPM across the enterprise.



Table of Contents

1.	The Current Landscape of Enterprise Security	04
2.	Three Incidents That Exposed the SaaS Security Gap	05
	▪ The Salesforce Story	05
	▪ The GitHub Incident	06
	▪ The Microsoft Case	07
3.	Tackling SaaS Risks with SSPM	08
4.	Building a SaaS Security Program	10
5.	The Compliance Case for SSPM	11
6.	The Final Word	12

The Current Landscape of Enterprise Security

Today, enterprises have essential security controls in place, but their defenses often stop at the infrastructure, identity, and endpoint layers. Teams often rely on CSPM to monitor cloud infrastructure, identity platforms to manage access, and endpoint tools to protect devices across the network. However, the SaaS application layer falls outside the purview of these controls.

Unlike cloud transformation, SaaS adoption is decentralized and shaped by the assumption that security accountability rests with the provider. Moreover, SaaS applications are adopted across the enterprise to meet various business needs. Salesforce may be introduced by the sales team, Slack by the product team, and GitHub by the development team. By the time these applications become critical business systems, they are already outside the perimeter of traditional security programs.

A recent study from AppOmni illustrates this distinct security blind spot. Among respondents who used Microsoft 365, 49% reported having fewer than 10 applications connected to their tenant. However, the study found that the average number of connections exceeded 1000.⁴ This unaccounted visibility gap in SaaS exposure makes it difficult for security teams to assess risk and prioritize remediation.

The following diagram denotes where traditional security controls end and the SaaS security blind spots begin.

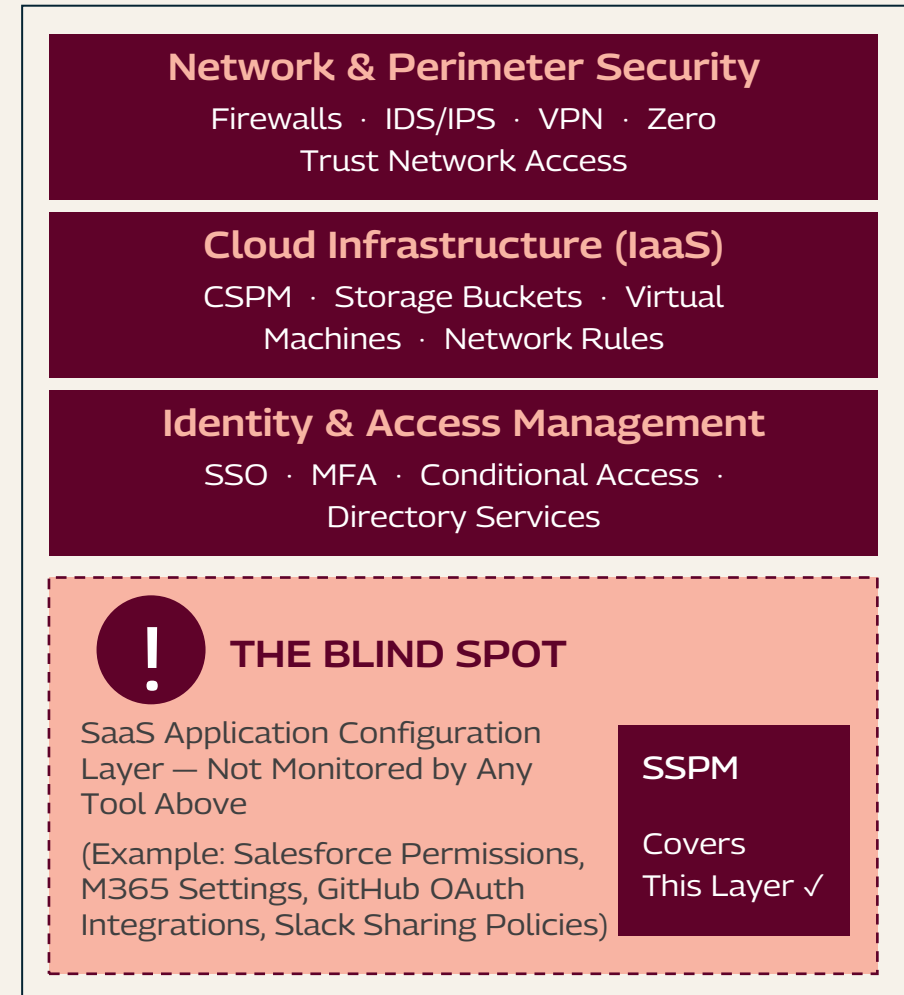


Figure 1: The SaaS Security Blind Spot and the Role of SSPM

Three Incidents That Exposed the SaaS Security Gap

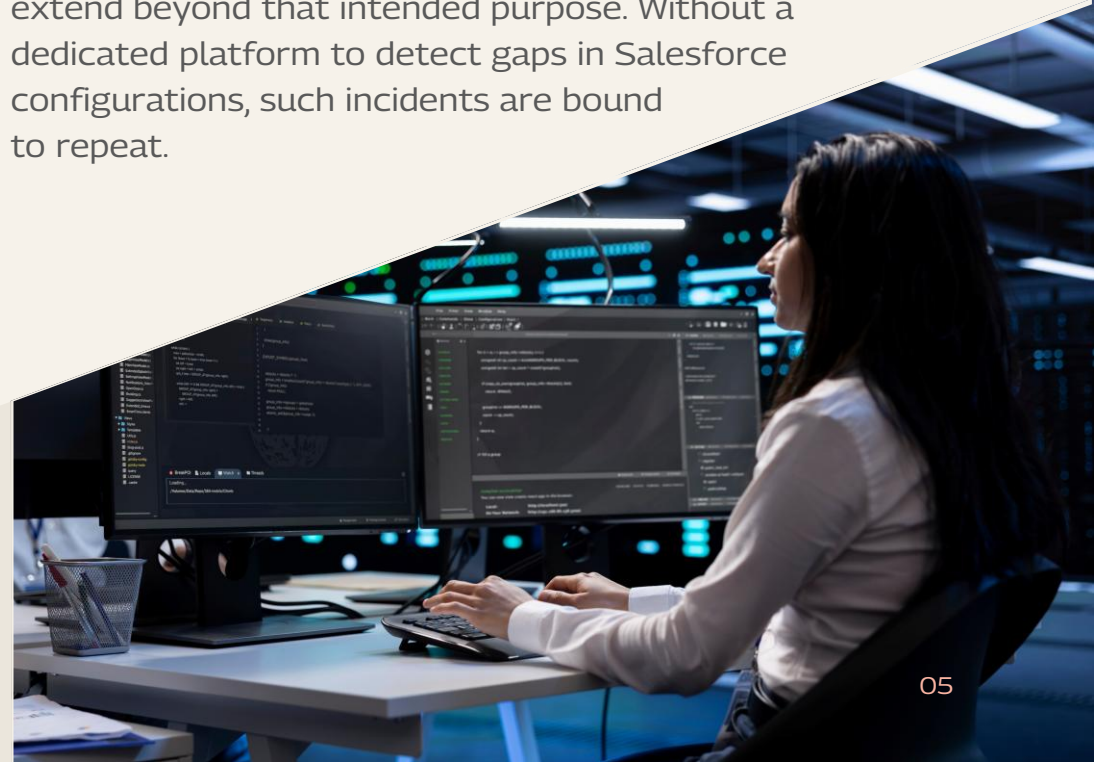
1) The Salesforce Story

In April 2023, KrebsOnSecurity broke the story that Salesforce community websites suffered a major data breach exposing critical data from government agencies, banks, and healthcare providers.¹ The attack exploited a blind spot in the API endpoint and a misconfigured guest user profile. This breach exposed records, including Social Security numbers, account details, and personal addresses. The Salesforce team responded that the attack was not due to a platform vulnerability but rather to a misconfigured guest access policy that had slipped past the security teams.

Guest user profiles in Salesforce communities allow users to access data records. If administrators set the permissions too broadly, unauthenticated external users can access data through the API. The breach highlighted this issue after researchers identified the misconfigurations across multiple public-facing Salesforce sites.

Typically, such exposures follow a similar pattern. Configurations are made under time pressure, defaults are set slightly too permissively, and oversight is limited. Over time, SaaS applications accumulate these exposures, creating persistent access paths that can be exploited.

The technical significance lies in the API surface available through Salesforce Experience Cloud. The functionality of a guest user profile is a documented feature. Administrators use it intentionally to allow the public to access certain content. Risk emerges when permissions extend beyond that intended purpose. Without a dedicated platform to detect gaps in Salesforce configurations, such incidents are bound to repeat.





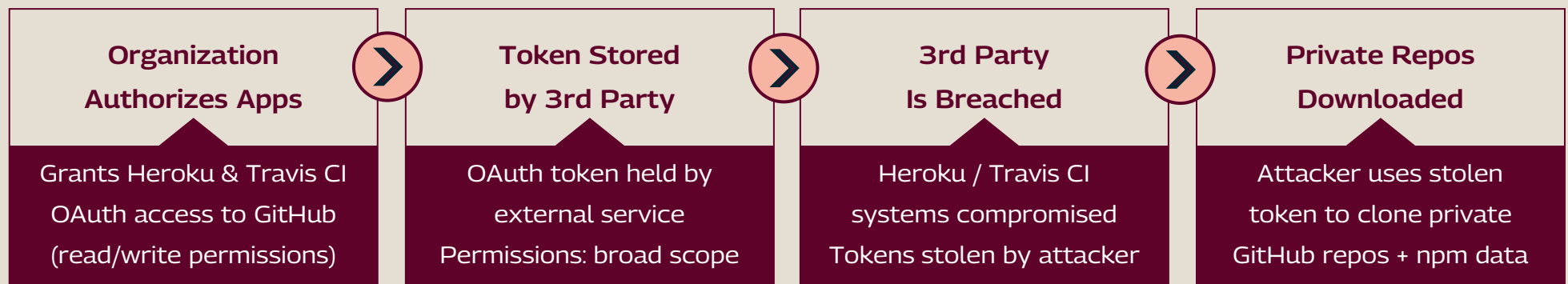
2) The GitHub Incident

In April 2022, GitHub disclosed an investigation that uncovered an attack. The breach abused OAuth tokens issued by Heroku and Travis CI to download data from dozens of organizations, including npm.² The investigation revealed that GitHub systems were not exploited. The tokens were traced to compromised third-party applications and their account authorization.

The entry point for the attack was through the CI/CD tools. The organizations had used the tools to connect to GitHub and other platforms, granting broad read and write permissions, which were never revisited.

This demonstrates the OAuth risk. Once organizations authorize third-party applications, the application's vulnerability extends to the data and functions covered by the granted permissions, creating an exploitable path into the connected SaaS environment. Most security programs fail to address these risks or lack specialized tools for oversight.

How OAuth Token Abuse Led to the GitHub Breach (2022)



Key Lesson: GitHub was never compromised directly. The access came through a third-party integration the organizations had authorized — and never reviewed again.



What SSPM Would Have Caught: Stale OAuth integrations with over-broad permission scopes → flagged for review → revoked before the breach window opened.

Figure 2: The 2022 GitHub Breach Chain



3) The Microsoft Case

In September 2023, Wiz Research reported that Microsoft's AI team had inadvertently exposed 38TB of internal data, private keys, passwords, and 30,000+ Teams messages to the public.³ The exposure resulted from a misconfigured Azure access token that was intended to share a single training dataset on GitHub but instead granted access to the entire storage account.

To put it succinctly, this access signature token is a credential that grants scoped access to Azure storage systems. With it, teams can specify which resources the token can access, which actions it permits, and how long it remains valid. Used correctly, it is a valuable tool. However, in this case, the token's scope was set too broadly, granting access to the entire storage account. Adding to the complexity, the token was also embedded in a GitHub repository, making it discoverable to the entire public.

The case underscores the need to apply least-privilege principles to access credentials and continuously monitor how they are configured, shared, and used. It also shows how sensitive application data can move beyond its original platform through backups, repositories, and connected cloud services.

Tackling SaaS Risks with SSPM



For security teams serious about addressing SaaS-related risks, the first step is to establish complete visibility across the SaaS estate. This requires identifying and assessing every application, user, integration, and configuration. Manual reviews cannot sustain this level of oversight at an enterprise scale. Therefore, security teams need centralized, continuous monitoring to identify gaps as they emerge.

SSPM effectively addresses the need. It connects SaaS applications through their native APIs and continuously evaluates deviations against security baselines, established policies, vendor guidance, Center for Internet Security (CIS) controls, and compliance frameworks. When anomalous activity is detected, it immediately alerts security teams, enabling them to investigate potential threats, contain attacks, and initiate remediation.

The following diagram maps SSPM capabilities across the SaaS security lifecycle.



Figure 3: Key Capabilities of SSPM

Building a SaaS Security Program

Compliance often provides the most direct business case for implementing an SSPM. Regulatory standards such as System and Organization Controls (SOC 2) require evidence of access reviews, configuration monitoring, and remediation. An SSPM can continuously deliver this and support ongoing security oversight and corrective measures.

However, before implementing SSPM, the leadership team should address the following.

- Which SaaS applications are in use across the enterprise?
- Who is accountable for each application?
- What data and systems can each application access, and who can change them?

Determining these factors early will help organizations deploy SSPM effectively. Three central operational practices guide teams in this endeavor:

▪ SaaS Estate Discovery

Enterprise procurement records miss a significant portion of actual SaaS usage. This is because developers use free tools, business units buy isolated tool subscriptions, and OAuth integrations accumulate without any formal process. Therefore, organizations need to unify procurement records, single sign-on (SSO) logs, network data, and OAuth audit information to map SaaS usage and identify risky applications.

▪ Establishing Secure Configuration Baselines

Once the critical applications are identified, teams need to record deviations and define correct configurations. Vendor security guides, CIS benchmarks, and compliance frameworks help teams in this process. With this baseline established, teams can create the foundation for the SSPM to detect and monitor configuration drift.

▪ Continuous Access Review

SaaS permissions change on a day-to-day basis, making annual reviews insufficient. Hence, organizations should conduct regular privileged-access reviews and use automated detection to identify dormant, excessive, or orphaned accounts.

The Compliance Case for SSPM

Security leaders need to justify SSPM investment to key stakeholders. Regulatory risks provide a compelling basis to secure this investment because the same SaaS misconfigurations that create security risks also result in compliance violations and financial penalties.

Consider the Salesforce 2023 exposure.¹ Organizations that were significantly impacted included healthcare and financial institutions. The breach constituted a major violation of the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA).

This case reflects a broader compliance challenge across SaaS environments. Organizations must address applicable regulations and assurance requirements, including:

- **Gramm-Leach-Bliley Act (GLBA)**

Designed specifically for financial institutions, the framework requires organizations to implement safeguards to protect customer financial information. The obligation extends to all relevant systems, including SaaS platforms.

- **General Data Protection Regulation (GDPR)**

The framework explicitly requires institutions to protect customers' personal data and identity. Additionally, it also requires 72 hours' notice in the event of any breach. The challenge with SaaS exposures, however, is that misconfigurations are often discovered by external researchers, which delays containment and complicates regulatory responses.

- **SOC 2**

A voluntary attestation for organizations that manage customer data. It assesses controls such as access management, configuration drift detection, timely remediation, and third-party integrations. In SaaS environments, frequent changes make such assessments increasingly complex.

SSPM plays a pivotal role in addressing these requirements. By continuously monitoring SaaS configurations and generating audit-ready artifacts, it helps organizations promptly achieve control effectiveness and compliance.

The Final Word

The three incidents examined in this paper reveal a critical security weakness in SaaS environments. Serious exposure can occur even without a sophisticated cyberattack. Misconfigurations, excessive permissions, and ungoverned integrations are already laying the groundwork for compromise.

In this volatile environment, security teams need a reliable model built around continuous oversight and timely remediation. SSPM emerges as a comprehensive control layer that makes SaaS a defined and governed part of enterprise security.

The bottom line is clear. SaaS is not going away, and neither is the configuration complexity that comes with it. Organizations navigating this reality must reinvent their security strategies and prioritize SaaS governance as a survival imperative.

References

Krebs, B. (2023, April 27). Many public Salesforce sites are leaking private data. Krebs on Security. <https://krebsonsecurity.com/2023/04/many-public-salesforce-sites-are-leaking-private-data/>

Hanley, M. (2022, April 15). Security alert: Attack campaign involving stolen OAuth user tokens issued to two third-party integrators. GitHub Blog. <https://github.blog/news-insights/company-news/security-alert-stolen-oauth-user-tokens/>

Ben-Sasson, H., & Greenberg, R. (2023, September 18). 38TB of data accidentally exposed by Microsoft AI researchers. Wiz Blog. <https://www.wiz.io/blog/38-terabytes-of-private-data-accidentally-exposed-by-microsoft-ai-researchers>

AppOmni. (2024, August 27). AppOmni State of SaaS Security Report 2024 finds that the security of enterprise SaaS applications is still far from ideal. AppOmni. <https://appomni.com/press-releases/new-state-of-saas-security-report-2024/>





Ashish Kumar Mishra

Group Manager Service
Delivery, CSRM
Tech Mahindra

About the Author

Ashish Mishra is a seasoned IT professional and author with over 20 years of experience in the industry. He has a strong grasp and command of the IT (Information Technology), IS (Information Security), and Cyber Security domains. Ashish is also experienced in managing large IT and IS operations, strategy building, transformation journeys, project and program management, and service delivery. His expertise includes Public Cloud, Private Cloud, Cloud Security, Network Security, SASE, and Zero Trust. With the thought process of 'continuous learning is the key to success,' he has obtained more than 150 professional certifications across various technologies and platforms related to public and private cloud, cloud security, information security, cybersecurity, compliance, infrastructure management, leadership, project management, and many more.

About **Tech Mahindra**

Tech Mahindra (NSE: TECHM, BSE: 532755) offers technology consulting and digital solutions to global enterprises across industries, enabling transformative scale at unparalleled speed. With 146,000+ professionals across 90 countries, Tech Mahindra provides a full spectrum of services including consulting, information technology, enterprise applications, business process services, engineering services, network services, customer experience & design, AI & analytics, and cloud & infrastructure services. It is the first Indian company in the world to have been awarded the Sustainable Markets Initiative's Terra Carta Seal, which recognizes global companies that are actively leading the charge to create a climate and nature-positive future. Tech Mahindra is part of the Mahindra Group, founded in 1945, one of the largest and most admired multinational federation of companies.. For more information on how TechM can partner with you to meet your Scale at Speed™ imperatives, please visit <https://www.techmahindra.com/>.



www.techmahindra.com

www.linkedin.com/company/tech-mahindra

www.x.com/Tech_Mahindra

Copyright © Tech Mahindra Ltd 2026. All Rights Reserved.

Disclaimer: Brand names, logos, taglines, service marks, tradenames and trademarks used herein remain the property of their respective owners. Any unauthorized use or distribution of this content is strictly prohibited. The information in this document is provided on “as is” basis and Tech Mahindra Ltd. makes no representations or warranties, express or implied, as to the accuracy, completeness or reliability of the information provided in this document. This document is for general informational purposes only and is not intended to be a substitute for detailed research or professional advice and does not constitute an offer, solicitation, or recommendation to buy or sell any product, service or solution. Tech Mahindra Ltd. shall not be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. Information in this document is subject to change without notice.