TAGCYBER

A PRIMER ON SAAS SECURITY SOLUTIONS

DAVID NEUMAN, SENIOR ANALYST TAG INFOSPHERE

nudge

A PRIMER ON SAAS SECURITY SOLUTIONS

DAVID NEUMAN

As the SaaS security market begins to take shape, TAG Cyber developed this primer to help stakeholders make informed decisions on securing their SaaS environments. This guide was commissioned by Nudge Security.

INTRODUCTION

As the digital revolution continues to reshape the business landscape, organizations of all sizes and sectors have embraced cloud-delivered infrastructure (IaaS), platforms (PaaS), and software applications (SaaS) to drive efficiency, agility, and innovation. But this rapid and often decentralized adoption of SaaS applications (by both business units and individual employees) has meant new challenges in managing security risks, maintaining compliance, optimizing costs, and ensuring that these tools genuinely deliver on their promise of transforming business operations.

This guide underscores the growing importance of SaaS security and governance platforms. These tools provide the visibility, control, and automation needed to manage and secure an organization's SaaS environment effectively, but their value extends beyond mere risk mitigation. By providing a single source of truth for all SaaS applications, a SaaS security platform can also identify redundant applications, underused licenses, and opportunities for better integration and leveraging of these tools to optimize cost and operational efficiency.

The critical differentiating capabilities of SaaS security platforms—including comprehensive visibility, automated compliance monitoring, threat detection and response, risk management, access control and identity management, integration capabilities, and actionable insights and reporting—make them essential tools for navigating the complex and rapidly evolving SaaS landscape. The adoption and effective use of SaaS security is not solely the domain of IT departments as it involves diverse stakeholders: CIOs, CFOs, CISOs, IT managers, compliance officers, risk managers, procurement managers, business unit leaders, data privacy officers, R&D, and DevOps teams. It even includes individual employees who become citizen admins for the tech they introduce to the SaaS environment. Each of these roles brings a unique perspective and set of concerns, and each stands to benefit in different ways from the insights and controls provided by a SaaS security platform.

The opportunity here, and the central premise of this guide, is that by using the SaaS security platform as both a system of record and a tool for partnership and collaboration, these stakeholders can address the challenges of SaaS adoption and unlock its full potential for driving business success. By ensuring that SaaS applications are used securely, efficiently, and in a manner that supports rather than impedes business objectives, organizations can truly leverage the transformative power of SaaS.

So whether you're a CIO looking to manage your organization's SaaS landscape, a compliance officer tasked with maintaining regulatory compliance and frequent access reviews, a business unit leader seeking to drive efficiency and innovation, or any of the other roles involved in managing and using SaaS applications, this guide is designed to help you understand the value of SaaS security platforms and navigate the process of selecting and implementing the right solution for your organization.

ADVANTAGES OF SAAS ADOPTION

Embracing SaaS carries many benefits that resonate with an organization's technical- and business-minded leaders. These advantages often drive SaaS adoption and are worth considering when selecting a SaaS security platform. Let's explore them in more detail.

Agility and Scalability to Meet Business Demands. SaaS platforms are designed for agility, making businesses nimble in fluctuating market conditions and customer needs. They allow for the swift deployment of new technology, eliminating the need for lengthy installations or substantial upfront investments in infrastructure, enabling businesses to scale their SaaS usage based on real-time demands, a crucial factor for growth opportunities and navigating market changes.

Cost Efficiency and Resource Optimization. SaaS platforms present a cost-efficient solution, operating on a subscription model that typically incurs lower initial costs than traditional software. In addition, the subscription often encompasses updates, maintenance, and customer support, facilitating predictable budgeting. Further, SaaS adoption lightens the load on IT teams, freeing them from tasks such as software installation, updates, and troubleshooting and allowing them to concentrate on strategic initiatives. This leads to enhanced operational efficiency.

Innovation for a Competitive Edge. SaaS can fuel innovation and provide a competitive advantage. SaaS providers regularly roll out new features and capabilities, giving businesses access to the forefront of technological advancements. This fosters the ability to quickly leverage new tools and features, a significant advantage in delivering exceptional customer experiences, streamlining operations, and keeping pace with market trends.

Flexibility and Accessibility for a Modern Workforce. Flexibility and accessibility are hallmark advantages of SaaS applications. As cloud-based solutions, they can be accessed anywhere with an internet connection, a vital feature in supporting today's increasingly remote and mobile workforce. Because SaaS is designed to be frictionless for any individual to use and learn, most often without requiring any specialization or certification, it also promotes collaboration among geographically dispersed teams and can often "go viral" by encouraging users to invite collaborators to use the technology.

Disaster Recovery and Business Continuity. This flexibility extends to business continuity and disaster recovery, allowing operations to persist regardless of the accessibility of physical office locations. Many SaaS applications are also designed to integrate with other business systems in no-code and low-code manners, simplifying the creation of a unified, flexible technology ecosystem that caters to diverse business needs. They also shift the shared responsibility model as functions such as system updates and vulnerability patching are now the responsibility of the SaaS provider.

RISKS ASSOCIATED WITH SAAS ADOPTION

Business units often turn to SaaS applications out of a need for agility, efficiency, and customizability, which traditional IT departments may need specific domain expertise to address. In this sense, adopting SaaS applications can be a proactive and innovative approach to solving business problems. There is also no inherent risk associated with SaaS that doesn't also apply to owned IT.

However, this doesn't diminish the fact that uncontrolled or uncoordinated use of SaaS applications can introduce security risks and compliance issues. This is where the concept of SaaS security becomes critical. An effective SaaS security and governance strategy allows organizations to embrace the benefits of SaaS while mitigating the associated risks and providing the necessary visibility and control over SaaS use across the organization.

With SaaS applications, data is typically stored on the provider's servers, which may be located anywhere in the world. This can raise *data privacy and protection* issues, particularly if the provider still needs robust security measures. Additionally, unauthorized individuals could access data if user access controls are not correctly implemented and managed.

Maintaining *compliance can be challenging*, particularly for organizations subject to regulations like GDPR, CCPA, or HIPAA. SaaS providers may store and process data in locations or ways that are not compliant with these regulations, potentially exposing the organization to penalties. Therefore, organizations must understand their compliance obligations and ensure their SaaS providers can meet them.

Application sprawl is the use of duplicative software and systems, including SaaS applications, without the knowledge or approval of the IT department. This can lead to a proliferation of unmanaged, potentially insecure applications, and can drive excessive costs, create significant security risks, and make it difficult to maintain an accurate inventory of the organization's software assets.

Access control and identity management with SaaS applications are critical. Managing who has access to what data and ensuring access is revoked when no longer needed can be complex and nuanced. Without proper access control and identity management, there's a risk of unauthorized access or inappropriate sharing of sensitive information.

Relying on *third-party vendors* for critical applications can be risky if the vendor experiences downtime, goes out of business, or fails to deliver the expected service. Moreover, if the vendor is breached, it could expose the customers' data to risk.

SaaS providers face *data loss and recovery* issues just like any organization. While SaaS providers typically have measures to prevent data loss, there's always a risk that data could be lost or corrupted due to a technical issue, cyberattack, or human error. And while some providers offer data recovery services, these may only sometimes be sufficient to recover all lost data.

Many SaaS providers offer APIs and support OAuth to allow for integration with other systems. These integration points could provide attackers with a potential entry point if they are not adequately secured. Therefore, OAuth and *API security* will continue to be a risk that must be addressed.

OAuth and API tokens are integral components of SaaS application integration, ensuring secure data exchanges without revealing user credentials. However, they could be exploited, giving unauthorized access to sensitive data. Therefore, it's essential to prioritize robust OAuth and API token management to safeguard your data against potential cybersecurity threats.

BUSINESS STAKEHOLDERS IN SAAS SECURITY

Let's delve deeper into the various business personas who would find value in a SaaS security and governance platform. Each persona plays a critical role in adopting and managing SaaS applications and their associated security posture within an organization. They each have unique responsibilities and perspectives that influence their understanding of the value that a SaaS security platform can bring. Their relevance lies in the extraordinary impact they can each have on the successful selection and implementation of a SaaS security platform.

Chief information officer (CIO): The CIO oversees an organization's IT strategy and implementation. As SaaS adoption increases, the CIO must ensure that these applications align with the organization's IT strategy and are properly managed and secured. In addition, a SaaS security platform can provide the tools needed to manage the SaaS landscape effectively, so a guide that helps them choose the right solution would be valuable.

Chief information security officer (CISO): The CISO primarily manages cybersecurity risks. As such, they would be interested in SaaS security platforms that can provide comprehensive visibility into the organization's SaaS attack surface, supply chain risk, security policies, compliance, and threats such as signs of an account takeover. A buyer's guide can help them understand the required security features and capabilities in a SaaS security platform.

IT manager: IT managers oversee day-to-day IT operations, including managing SaaS applications. They would be interested in SaaS security platforms that simplify SaaS management tasks, such as access control, identity management, user lifecycle management, and incident response. A buyer's guide could help them identify platforms that offer these capabilities.

Compliance officer: Compliance officers must ensure that the organization uses SaaS applications to comply with relevant regulations and standards. They would be interested in SaaS security platforms that monitor compliance, generate compliance reports, and automate compliance tasks, such as conducting regular SaaS access reviews. A buyer's guide would help them understand how different platforms can support specific aspects of their compliance programs.

Procurement manager: Procurement managers are responsible for purchasing decisions. They would be interested in the cost-effectiveness of different SaaS security platforms and their scalability, reliability, and vendor support. A buyer's guide could give them the information they need to evaluate and compare options.

Business unit leaders: Business unit leaders use SaaS applications to drive business operations and results. They would be interested in SaaS security platforms that can ensure the availability and performance of these applications without impeding productivity. It can help them understand the adoption and use of the SaaS they administer, so they can plan and budget accordingly.

Data privacy officers: Data privacy officers ensure an organization complies with relevant data protection laws and regulations. They oversee data privacy policies, conduct privacy impact assessments, and serve as the point of contact for individuals whose data the organization processes. With the rise in SaaS applications, data privacy responsibility extends to the cloud. Data privacy officers must ensure that sensitive data stored or processed in SaaS applications is adequately protected and that the organization's SaaS use complies with privacy laws such as GDPR, CCPA, or HIPAA.

DevOps team: DevOps teams are responsible for developing, deploying, and managing software applications, including SaaS applications. They aim to deliver high-quality software quickly and reliably while ensuring security is embedded in the development and deployment process, a practice often called DevSecOps. DevOps teams must ensure that customizations and integrations with other systems are done securely in the context of cloud infrastructure and SaaS applications.

Individual employees: All employees benefit from understanding (1) what sanctioned tools are already being used across the organization and which citizen administrator can provide access; (2) the extent and details of their own SaaS footprint; and (3) what their own SaaS security posture looks like relative to the organization's IT and security policies, as well as guidance on how to support those policies and use SaaS applications responsibly.

DIFFERENTIATING CAPABILITIES AND ADVANTAGES OF A SAAS SECURITY PLATFORM

As digital transformation becomes the norm across industries, the security of software systems has taken center stage. A SaaS security and governance platform offers unique capabilities and advantages in addressing these concerns. Its fundamental differentiation comes from its cloud-native structure, offering comprehensive, scalable, and agile security solutions. These platforms present a paradigm shift in cybersecurity, blending security and governance. This section discusses the distinct capabilities and advantages of a SaaS security platform, highlighting how it can help organizations maintain security, agility, and resilience in the face of ever-evolving security threats.

Comprehensive Discovery and Visibility. A SaaS security platform provides a continuous overview of your entire SaaS application landscape as it changes. This unified view lets you see which applications are used, who uses them, and how they are configured, enabling effective management and control over your SaaS environment.

> **Key considerations**: Highly distributed organizations, especially those with flexible and remote work options, should evaluate vendors' discovery capabilities based on their ability to look beyond the network perimeter and corporate-managed devices to discover SaaS use. Not all SaaS discovery solutions provide the same breadth of discovery, and buyers should consider how deployment is performed. For example, agents or browser plug-ins require an additional level of effort for IT teams. Additionally, the ability to inventory applications already in use before deployment is essential. Finally, the continuous discovery of new applications versus having to provide a list of applications in use is an important differentiator.

Automated Compliance Monitoring. This is an important function that not only safeguards your data but also ensures that your system adheres to the latest compliance regulations. It simplifies the complex and time-consuming process of compliance reporting. SaaS security platforms can automate compliance checks across all SaaS applications, which is crucial in adhering to regulatory standards, such as GDPR, HIPAA, or SOC 2, helping your organization avoid potential fines and reputational damage.

> **Key considerations**: The ability to automate user access reviews such as those required for SOC 2 certification is an important function of SaaS security platforms. In addition, platforms should support the identification and grouping of applications that are in scope for different compliance regulations, ensuring that the right governance policies are applied to those apps. Real-time tracking capabilities that provide continuous monitoring and immediate alerts on any compliance deviation can mitigate risks before they develop into serious threats.

Threat Detection and Response. SaaS security platforms should use advanced analytics and machine learning to detect unusual or suspicious behavior that could indicate a security threat. Once a potential threat is identified, the platform can take predefined actions to respond or alert your security team for manual intervention. Some platforms can even alert you to breaches of the SaaS providers you use and those in the digital supply chain of your providers. This is becoming more important as threat actors like Lapsus$ have demonstrated the ability to move across the SaaS supply chain toward high-value targets.

> **Key considerations**: Consider the platform's ease of integration with existing security systems and technology, such as security information and event management (SIEM) and security orchestration, automation, and response (SOAR). Additionally, an effective SaaS security platform should provide real-time threat detection capabilities. This means the system continuously monitors for any suspicious activities or anomalies and generates immediate alerts when potential threats are identified.

Risk Management. SaaS security platforms use advanced technologies like artificial intelligence and machine learning to identify and evaluate potential risks before they become issues. Some can collect information about a SaaS provider's security program, compliance attestations, breach history, and other relevant factors to assess potential risks and speed up vendor security reviews. This proactive approach allows businesses to effectively evaluate risks and implement preventive measures, thereby reducing the likelihood and potential impact of security incidents.

> **Key considerations**: SaaS security platforms can identify risks in applications or between applications. This is particularly true when examining OAuth grants. They can also identify risks in applications and cloud services that exist outside central governance, which might not have appropriate security controls applied.

Access Control and Identity Management. SaaS security platforms often include features for managing user identities and access controls across your SaaS applications. This can consist of identifying which apps and accounts are (or are not) enrolled in single sign-on (SSO) or multifactor authentication (MFA), identifying app-to-app integrations via OAuth, and leveraging user behavior analytics, all of which contribute to securing user access.

> **Key considerations**: The SaaS security platform should seamlessly integrate with your existing identity and access infrastructure and other SaaS applications. It should support standard protocols to ensure compatibility and minimize operational disruptions during implementation. A platform that offers prebuilt integrations or APIs can further streamline the integration process. As your organization grows or evolves, the platform should be scalable to accommodate an increased number of users, applications, and data. It should also offer flexibility to handle diverse user roles and complex access policies. The ability to scale and adapt in response to your business needs is critical to maintaining robust and effective access control and identity management over time.

Actionable Insights and Reporting. SaaS security platforms provide detailed, audit-ready reports for compliance requirements for attestation such as SOC 2, as well as actionable insights on your SaaS security posture. These insights can include highlighting updates to framework controls such as CIS or ISO, assessing MFA and SSO coverage across applications, and documenting user access reviews. These insights can help guide decision-making and security strategy and demonstrate compliance to stakeholders or auditors.

> **Key considerations**: Look for a platform that provides customizable reporting options, allowing you to adapt reports to meet your unique needs and export them in the format you need for compliance and other reporting requirements. This can include tailoring the metrics and data presented, the report format, and the frequency of report generation. The ability to customize reports can help you focus on the information that matters most to your organization, aiding in efficient decision-making. Furthermore, the platform should offer the capacity to generate compliance reports based on specific standards like CIS or ISO to simplify the auditing process. A beneficial feature of SaaS security platforms is their ability to provide intelligent insights which should not only identify current vulnerabilities and compliance gaps but also predict future risks based on trends and patterns. This proactive approach allows for early mitigation of potential threats and enhances strategic planning.

Collaboration. Use insights from the SaaS security platform to engage with business units, understand their needs and challenges, and discuss potential risks associated with their SaaS applications. This collaborative approach encourages business units to be part of the solution rather than viewing IT as a barrier.

> **Key considerations**: A critical consideration for promoting collaboration is the ease of use of the platform. A user-friendly interface encourages business units to interact with the platform, enabling them to understand their security postures. This, in turn, facilitates informed discussions about potential risks and mitigation. Platforms that offer clear dashboards and intuitive tools promote higher engagement and foster a collaborative environment. The platform should allow for controlled access across different departments or business units to enable various stakeholders to view and understand the security status relevant to their operations. Such transparency can drive proactive discussions and shared responsibility for security, positioning IT as a partner rather than a barrier. The platform should offer fine-grained access control to ensure users can only view and modify data relevant to their roles.

Empowerment. By providing business units with the tools and information they need to manage their SaaS applications securely, they can take greater responsibility for their SaaS security posture with oversight. This might include training on secure usage practices, providing access to the SaaS security platform for self-service security checks, triggering prompts to request that end users take specific actions, and establishing clear SaaS adoption and use guidelines.

> **Key considerations**: An effective SaaS security platform should offer the ability to point users to educational resources and training modules to help them understand security best practices and how to use the platform effectively. This could include short tutorials or just-in-time guidance. Empowering users with the necessary knowledge and skills at the optimal time encourages greater ownership of security responsibilities and promotes a culture of security awareness throughout the organization. The platform should offer user-friendly, self-service capabilities so users can conduct security checks and manage their security settings. For instance, users should be able to view the security status of their applications or adjust security settings. This kind of user empowerment allows for quicker responses to security issues and a more decentralized, yet secure, control over the SaaS applications.

Eliminating Redundancies. A SaaS security platform's visibility into all SaaS applications across the organization can identify redundant applications. By consolidating these applications, the organization can reduce unnecessary costs.

Key considerations: The platform should provide a broad view of all the SaaS applications being used across the organization, along with categorization to identify redundant applications. It should also include information on the use of each application, which can further assist in determining which applications are essential and which are superfluous. Moreover, the platform should provide actionable recommendations for consolidating applications and reducing unnecessary expenses. It would be beneficial if the platform can also estimate potential cost savings of removing certain applications.

A UNIFIED APPROACH

In light of the emerging nature of SaaS security solutions, the focus should be on selecting tools that align with your organization's primary objectives and desired state for SaaS security and governance. This process begins with understanding the risks associated with SaaS adoption and establishing a vision of how you want to manage those risks. From there, an inventory of existing technologies, such as IAM/IdP solutions, can be leveraged to integrate with the selected SaaS security solution, ensuring seamless functionality and maximum utility.

In this strategic approach, practitioners and business leaders come together to balance the equation of risk management and operational efficiency. The ultimate aim is to empower business units with the right SaaS tools that foster innovation while maintaining security and compliance, essential in today's intricate digital ecosystem. A culture of shared responsibility becomes integral, where every stakeholder understands their role in maintaining security protocols.

By prioritizing their primary objectives and harmoniously integrating new SaaS security solutions with existing technology, organizations can enhance their security posture, maintain compliance, and optimize costs associated with SaaS applications. This strategic approach not only addresses immediate security needs but also contributes to the organization's long-term financial health and sustainability.

CONCLUSION

The rapid adoption of SaaS applications across various sectors and industries has brought new challenges in managing security risks, maintaining compliance, optimizing costs, and ensuring that these tools deliver on their promise of transforming business operations. SaaS security platforms offer a solution to these challenges. By providing a centralized view of an organization's SaaS applications, SaaS security platforms offer the visibility, control, and automation necessary to manage and secure the SaaS environment.

Beyond mitigating security risks and ensuring compliance, SaaS security platforms offer cost optimization and operational efficiency opportunities by identifying redundant applications, underused licenses, and opportunities for better integration and leveraging of SaaS tools. Thus, the critical differentiating capabilities of SaaS security platforms make them essential tools for navigating the complex and rapidly evolving SaaS landscape.

Finally, adopting and effectively using a SaaS security platform requires diverse stakeholders, including CIOs, CISOs, IT managers, compliance officers, risk managers, procurement managers, business unit leaders, data privacy officers, and DevOps teams. Each of these roles holds a unique perspective and set of concerns, and each stands to benefit from the insights and controls provided by a SaaS security platform. Therefore, organizations must work collaboratively to ensure the SaaS security platform is optimized for all stakeholders' needs, contributing to better security, compliance, cost optimization, and operational efficiency.

ABOUT NUDGE SECURITY

We at TAG Cyber strongly recommend that organizations explore the benefits of Nudge Security's SaaS security solution. Nudge Security's platform offers comprehensive capabilities to help organizations manage and secure their SaaS environment.

In particular, Nudge Security deploys without any browser plugins, agents, network proxies, or changes to employee behavior. It simply requires read-only API access to Microsoft 365 or Google Workspace. With this easy, one-time configuration, their platform discovers the machine-generated emails sent by SaaS platforms to confirm account creation, addition of users, and other security-relevant events. This patented approach provides a complete and immediate inventory of all SaaS in use, even for accounts unmanaged by IT, and outside the purview of billing records (such as free tools).

Another aspect we appreciate is the enrichment of this SaaS inventory with security and risk insights for SaaS providers, which is essential for risk assessments and vendor security reviews. This context includes auto-categorization, data locality, breach disclosure histories, security attestations, and supply chain data, as well as OAuth risk analysis. The data can also be leveraged to trigger automated workflows that nudge employees to take simple, yet impactful steps to help secure SaaS accounts (e.g., by enabling MFA). Automating employee engagement alleviates the burden on IT security teams while also creating opportunities for every employee to participate positively in the security program.

Overall, Nudge Security is essential for organizations seeking to manage and secure their SaaS environment effectively. Its advanced capabilities, comprehensive features, and actionable insights make it a powerful solution for navigating the complex and rapidly evolving SaaS landscape. Therefore, we strongly encourage organizations to explore the benefits of Nudge Security's SaaS security solution and discover how it can help them transform their SaaS environment into a secure, compliant, and efficient digital workspace.

ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner's perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: DAVID NEUMAN

Publisher: TAG Cyber, a division of TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.

Citations: Accredited press and analysts may cite this book in context, including the author's name, author's title, and "TAG Cyber." Non-press and non-analysts require TAG Cyber's prior written permission for citations.

Disclaimer: This book is for informational purposes only and may contain technical inaccuracies, omissions, and/or typographical errors. The opinions of TAG Cyber's analysts are subject to change without notice and should not be construed as statements of fact. TAG Cyber disclaims all warranties regarding accuracy, completeness, or adequacy and shall not be liable for errors, omissions, or inadequacies.

Disclosures: Nudge Security commissioned this book. TAG Cyber provides research, analysis, and advisory services to several cybersecurity firms noted in this paper. No employees at the firm hold any equity positions with the cited companies.

TAG Cyber's forecasts and forward-looking statements serve as directional indicators, not precise predictions of future events. Please exercise caution when considering these statements, as they are subject to risks and uncertainties that can affect actual results. Opinions in this book represent our current judgment on the document's publication date only. We have no obligation to revise or publicly update the document in response to new information or future events.