Solution Brief

Modern SaaS Security Risk Management

Modern SaaS Security Risk Management

In today's rapidly evolving digital landscape, where Software as a Service (SaaS) applications have become ubiquitous across business operations, the risk to the enterprise is undergoing a seismic shift. Traditional risk assessment models are increasingly proving inadequate, as they are unable to accommodate the unique and dynamic nature of SaaS usage within a company. A modern program requires a tailored approach to assess the risk that reflects the distinct realities of each enterprise's SaaS utilization. A modernized risk evaluation framework is imperative for an accurate reflection of the SaaS identity risk landscape, considering the specific variables that characterize an individual company's use of a SaaS app.

The crux of the challenge resides in acknowledging that the true risk factors for SaaS adoption within a company are linked to the organization itself. Variables such as the number of app users, the growth of users for an app, the frequency of app use, the nature of data used, and the users' authentication methods, all paint a more precise picture of potential vulnerabilities. These factors are not uniform; they differ markedly from one enterprise to another, thus necessitating a bespoke risk assessment model for each company.

The industry's SaaS risk standards have not kept pace with the fluid character of SaaS adoption in businesses. In today's digital workplace, employees frequently subscribe to and utilize a vast array of SaaS applications to fulfill their job requirements, outside of the purview of IT supervision. Conventional security tools often assess the risk associated with the SaaS vendors, disregarding the risk to the enterprise using the SaaS app acquired through a dispersed model.

A review of significant SaaS data breaches underscores the inadequacy of depending solely on industry certifications for a comprehensive risk evaluation. These SaaS companies, despite having advanced, mature security operations and being compliant with multiple industry standards, were not impervious to substantial breaches that garnered widespread media attention. The impact on the companies who relied on their apps differed and depended on specific enterprise usage factors unique to each customer. This highlights the critical need for an in-depth understanding of the distinct risk factors pertinent to an individual company. It reinforces the point that companies should take an enterprise-centric view of SaaS risk assessment rather than relying on vendor-centric risk evaluations.

SaaS Company	SOC2	SOC3	ISO/IEC27001	PCI DSS	Data Breach
Microsoft	✓	✓	✓	✓	✓
slack	✓	✓	✓	✓	✓
Dropbox	✓	✓	✓	✓	✓
Uber	✓		✓	✓	✓
LastPass	✓	✓	✓	✓	✓
HubSpot	✓	✓	✓	✓	✓

Data Breaches of Mature SaaS Vendors

Grip SaaS Security Control Plane Redefines Risk

SaaS Identity Risk Management (SIRM) emerges as a modern, programmatic approach that tailors the measurement of risks associated with widespread SaaS use. SIRM emphasizes the importance of understanding specific risk contributors such as the number of application users, the acceleration in user growth, the frequency of app usage, the sensitivity of the data involved, and the robustness of user authentication mechanisms. By employing precise metrics to evaluate these variables constantly and over time, SIRM delivers the monitoring of key enterprise specific risk indicators and informing cybersecurity strategies. This approach enables organizations not only to react to threats but also to anticipate and prepare for them, ensuring a secure SaaS environment.

With a unique identity-centric approach to risk, the Grip SaaS Security Control Plane (SSCP) stands out as the premier product for organizations aiming to implement SIRM. The platform is engineered to provide a comprehensive understanding of the enterprise-centric risk factors and provide the relevant context to act. Grip SSCP systematically measures the impact of multiple metrics such as user activity, growth trends, usage patterns, data classification, and authentication methods. By offering continuous oversight and actionable intelligence, it enables businesses to move from a defensive to a proactive stance in their SaaS security operations. This proactive edge positions the Grip SSCP not just as a tool but as a foundational platform to implement SIRM.

The following sections discuss some of the key factors the Grip SSCP measures to help companies assess their risks. These risk factors and others are synthesized into an overall SaaS app risk score that is specific to an enterprise's risk tolerance.

Sanction Status:

- **Metric:** Approval status of a SaaS application by IT with categories such as sanctioned, unsanctioned, tolerate, or pending review.
- **Risk:** The use of unsanctioned apps (often referred to as "shadow SaaS") poses a significant risk, as these applications may not adhere to the organization's security, compliance, and governance standards. Unsanctioned apps can lead to data leaks, breaches, and compliance violations due to the lack of oversight and control.

Number of Users:

- **Metric:** Total count of active users of a SaaS app.
- **Risk:** A higher number of users increases the potential attack surface of an enterprise. Each user account could potentially be compromised, acting as an entry point for unauthorized access.

Growth in Number of Users:

- **Metric:** User growth rate calculated over a specific time period (weekly, monthly, quarterly, annually).
- **Risk:** Rapid growth of new, unsanctioned apps indicates widespread adoption and raises the priority for IT and security to evaluate whether the app meets the guidelines and policies of the company. Without user management and oversight there is a higher potential for lapses in security protocols.

Inactive Accounts:

- **Metric:** Number of apps with inactive accounts
- **Risk:** Inactive accounts can become vectors for security breaches or compliance issues. They can be overlooked during security monitoring and any data stored in the app can be compromised and go unnoticed for a longer period.

User Authentication Methods:

- **Metric:** Type of authentication method used (local password, single sign-on, MFA/lack of MFA, etc.).
- **Risk:** Using local passwords for apps that process or store sensitive or regulated data increases risk due to potential data breaches or compliance violations.

Gen AI Capability:

- **Metric:** Flag indicating apps that incorporate artificial intelligence into their features and capabilities.
- **Risk:** The integration of AI models introduces risks that need to be evaluated. AI-driven actions might not always align with expected user behavior patterns or outputs. Other risks the company becomes exposed to include risks related to data management, privacy, and the potential for generating misleading or inaccurate content.

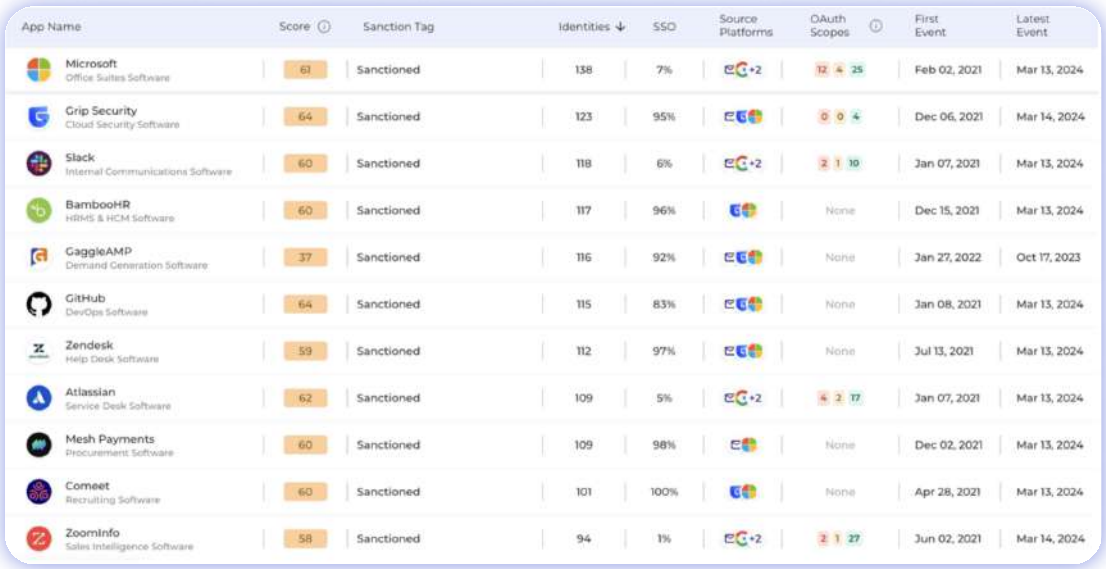
OAuth Scopes

- **Metric:** Number of OAuth grants approved categorized by risk level for each app and the frequency a particular scope is used.
- **Risk:** Overly broad or improperly granted scopes to third-party applications could indicate data exposure or misconfiguration that provides privileges beyond what is needed for the necessary functionality.

Data Type

- **Metric:** Type of data that is expected to be stored or used in a SaaS application based on the intended use.
- **Risk:** The more sensitive the data type, the greater the risk of a data leak or breach. This could lead to legal penalties, financial loss, and reputational damage.

The following screenshot from the Grip SSCP risk dashboard shows how the platform provides a quick and actionable assessment of a company's SaaS portfolio. Information such as the overall number of users, percentage of users authenticating with single sign-on, and OAuth grants are quickly displayed. The overall risk score of each app is also prominently shown. Each of these columns can be sorted, and the user can drill down to the relevant details with a few clicks.



App Name	Score	Sanction Tag	Identities	SSO	Source Platforms	OAuth Scopes	First Event	Latest Event
Microsoft Office Suites Software	61	Sanctioned	138	7%	+2	12 4 25	Feb 02, 2021	Mar 13, 2024
Grip Security Cloud Security Software	64	Sanctioned	123	95%		0 0 4	Dec 06, 2021	Mar 14, 2024
Slack Internal Communications Software	60	Sanctioned	118	6%	+2	2 1 10	Jan 07, 2021	Mar 13, 2024
BambooHR HRMS & HCM Software	60	Sanctioned	117	96%		None	Dec 15, 2021	Mar 13, 2024
GaggleAMP Demand Generation Software	37	Sanctioned	116	92%		None	Jan 27, 2022	Oct 17, 2023
GitHub DevOps Software	64	Sanctioned	115	83%		None	Jan 08, 2021	Mar 13, 2024
Zendesk Help Desk Software	59	Sanctioned	112	97%		None	Jul 13, 2021	Mar 13, 2024
Atlassian Service Desk Software	62	Sanctioned	109	5%	+2	4 2 17	Jan 07, 2021	Mar 13, 2024
Mesh Payments Procurement Software	60	Sanctioned	109	98%		None	Dec 02, 2021	Mar 13, 2024
Comeet Recruiting Software	60	Sanctioned	101	100%		None	Apr 28, 2021	Mar 13, 2024
ZoomInfo Sales Intelligence Software	58	Sanctioned	94	1%	+2	2 1 27	Jun 02, 2021	Mar 14, 2024

Grip SSCP SaaS Risk Dashboard

Modern SaaS Security: Decentralized Acquisition, Centralized Risk Management

The modern IT landscape demands a redefined approach that goes beyond the scope of traditional models to guard against the complex risks of the rampant SaaS adoption enterprises face today. SIRM provides this by focusing on risk metrics that reflect the actual use of SaaS within an enterprise. This modern approach enables a more detailed and organization-specific analysis of potential vulnerabilities.

The Grip SSCP has established itself as an essential platform to implement SIRM, providing the necessary analytics and oversight. It assesses a range of factors from user activity to the sanction status of applications, offering enterprises a comprehensive view of their SaaS security posture. As organizations strive to safeguard their SaaS environments, the proactive capabilities of Grip SSCP ensure that they can not only respond to threats as they arise but also anticipate and mitigate them effectively. This positions Grip SSCP as an essential component in the modern enterprise's cybersecurity toolkit, facilitating a robust and proactive SaaS identity risk assessment and management strategy.