Solution Brief

Modern SaaS Security for Managing Generative AI Risk

Modern SaaS Security for Managing Generative AI Risk

The technological landscape is undergoing a seismic shift with the integration of Generative Artificial Intelligence (Gen AI) into Software as a Service (SaaS) platforms. This integration offers unprecedented capabilities in many areas including automating content creation, data analysis, and personalized user experiences. Employees are rapidly adopting these Gen AI applications, and the decentralized procurement of these applications by employees occurs without going through the standard security checks. While Gen AI apps herald a new era of SaaS functionality and innovation, they also introduce a spectrum of risks that the Grip SaaS Security Control Plane (SSCP) is uniquely positioned to help manage.

Generative AI Risk is Not Only in New SaaS Apps

Gen AI is not a new category of applications but rather a technology that is being incorporated into a wide range of software applications. This integration occurs in two main forms: apps specifically designed for Gen AI use cases and existing SaaS platforms that are becoming Gen AI-enabled. Despite the different origins and purposes of these applications, both types of Gen AI integrations introduce significant security risks that organizations must carefully manage.

Some applications are built from the ground up with Gen AI technology at their core. They are designed to leverage the power of AI for generating content, automating tasks, analyzing data, and more. Examples include AI-driven content creation tools, design applications, and predictive analytics platforms. While these tools offer innovative capabilities, they also pose security risks related to data management, privacy, and the potential for generating misleading or inaccurate content.

Many existing SaaS applications are integrating Gen AI capabilities to enhance their offerings, improve user experience, and introduce new functionalities. This can range from adding natural language processing for better customer service interactions to implementing AI-driven analytics for enhanced data insights. The availability of these powerful AI capabilities in existing platforms requires companies to revisit their initial risk assessment about data security, user privacy, and the integrity of AI-generated outputs.

Generative AI Risk Management with Grip SaaS Security Control Plane

Grip SaaS Security Control Plane (SSCP) provides an identity-focused approach to managing the risk of Gen AI apps being adopted in the enterprise. By leveraging identity as the key control point, it can discover and address a range of risks that extend beyond what traditional controls can handle. It enables a programmatic SaaS Identity Risk Management (SIRM) approach to implement a variety of strategies and tools specifically designed to address the risks associated with the use of Gen AI SaaS applications. The SIRM approach is essential for ensuring the security and compliance of an enterprise's Gen AI risk program.

The primary elements include:

- **Gen AI app Discovery:**

  Identity-based discovery that ties Gen AI SaaS usage directly to individual users with clear identification of the business owner.

- **Gen AI Risk Lifecycle Management:**

  Establishes and enforces policies for managing the adoption of Gen AI apps, including identifying and revoking user access to those that are deemed to be out of compliance.

- **Gen AI Access Control:**

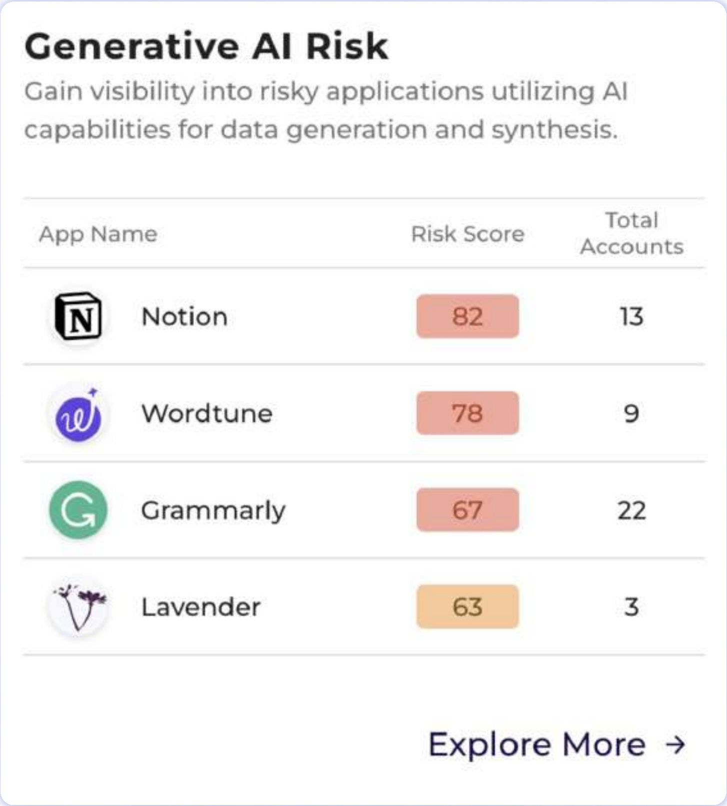
  Recommends the use of Single Sign-On (SSO) and Multi-Factor Authentication (MFA), providing a layer of access control that works for unmanaged devices and newly discovered SaaS apps.

- **Gen AI Risk Measurement:**

  Evaluates apps to identify existing apps in the SaaS portfolio that are Gen AI-enabled to trigger a review of the apps risk and compliance issues.

To address the unique and evolving Gen AI app risks enterprises face, Grip SSCP offers capabilities as standard features within the platform. This offers companies immediate, effective risk mitigation strategies without the need for extensive custom configuration, ensuring that businesses can manage Gen AI-related risks from the moment they deploy the Grip SSCP.

Figure 1 shows the standard Gen AI risk tile that is part of the Risk Management dashboard on Grip SSCP. The tile highlights the riskiest Gen AI apps based on an enterprise specific risk score. This risk score is not based on the security certifications achieved by the vendor but on a dynamic calculation that considers variables such as the number of app users, the growth of these users, frequency of usage, the type of data processed, and the authentication methods employed. This enterprise-centric view offers a more accurate reflection of the risk to the enterprise.



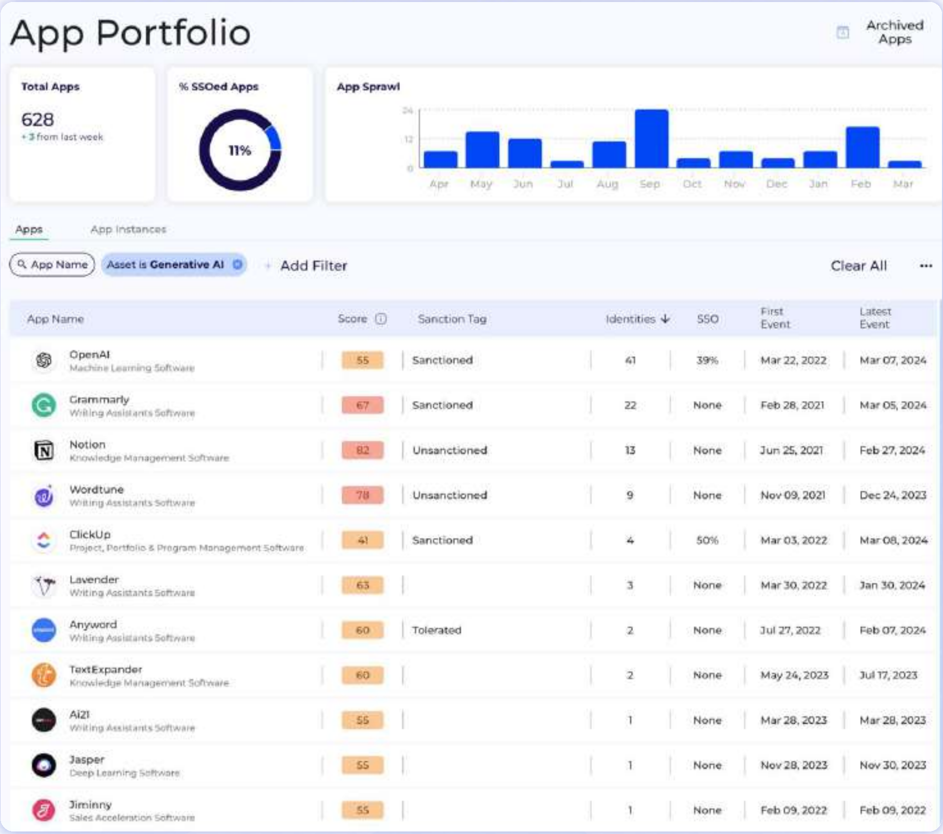
Generative AI Risk

Gain visibility into risky applications utilizing AI capabilities for data generation and synthesis.

App Name	Risk Score	Total Accounts
Notion	82	13
Wordtune	78	9
Grammarly	67	22
Lavender	63	3

Figure 1 : Gen AI Risk Dashboard Tile

The Grip SSCP also provides a portfolio view of all Gen AI SaaS apps being used in a company. The information includes pertinent information such as sanction status, number of users, SSO usage, and SaaS event dates. This view includes applications that are part of the SaaS portfolio that have been Gen-AI enabled as well as newer apps whose capabilities are based entirely on Gen AI.



App Name	Score	Sanction Tag	Identities	SSO	First Event	Latest Event
OpenAI Machine Learning Software	55	Sanctioned	41	39%	Mar 22, 2022	Mar 07, 2024
Grammarly Writing Assistants Software	67	Sanctioned	22	None	Feb 28, 2021	Mar 05, 2024
Notion Knowledge Management Software	82	Unsanctioned	13	None	Jun 25, 2021	Feb 27, 2024
Wordtune Writing Assistants Software	78	Unsanctioned	9	None	Nov 09, 2021	Dec 24, 2023
ClickUp Project, Portfolio & Program Management Software	41	Sanctioned	4	50%	Mar 03, 2022	Mar 08, 2024
Lavender Writing Assistants Software	63		3	None	Mar 30, 2022	Jan 30, 2024
Anyword Writing Assistants Software	60	Tolerated	2	None	Jul 27, 2022	Feb 07, 2024
TextExpander Knowledge Management Software	60		2	None	May 24, 2023	Jul 17, 2023
Ai21 Writing Assistants Software	55		1	None	Mar 28, 2023	Mar 28, 2023
Jasper Deep Learning Software	55		1	None	Nov 28, 2023	Nov 30, 2023
Jiminny Sales Acceleration Software	55		1	None	Feb 09, 2022	Feb 09, 2022

Figure 2 : Gen AI Portfolio View

Harnessing the Power of Gen AI and Minimizing Risk

The integration of Generative AI into SaaS platforms presents a complex challenge, blending immense potential with significant security considerations. The incorporation of Gen AI technology into a broad range of applications is revolutionizing SaaS offerings. From native Gen AI applications to traditional SaaS solutions enriched with AI capabilities, the security implications are profound. The Grip SSCP is an essential platform to provide organizations the tools and strategies needed to navigate the Gen AI risk landscape with confidence.

The platform's automatic discovery, risk lifecycle management, secure access controls, and incident response mechanisms provide a comprehensive and dynamic approach to SaaS security. The risk management dashboard and portfolio view furnish organizations with real-time insights and actionable data, transforming how enterprises approach Gen AI security.

Gen AI will continue to be an integral part of the SaaS risk landscape. Organizations using the Grip SSCP are not just reacting to the risks but proactively managing them, enabling safer and more effective use of Gen AI technologies. This strategic advantage ensures that businesses can harness the full potential of Gen AI innovations while maintaining the highest standards of security and compliance, ready to meet the demands of the modern digital world.

About Grip Security

Grip Security is a pioneer in SaaS identity risk management, providing innovative solutions to help enterprises address the security risks associated with widespread SaaS adoption. The company's SaaS Security Control Plane platform helps companies discover, prioritize, secure and orchestrate the mitigation and remediation of risks. The innovative approach of leveraging identity as the key control point allows companies to secure all SaaS applications and empowers enterprises to embrace SaaS adoption securely.

Contact us to arrange for a personal demo of the award-winning Grip SaaS Security Control Plane platform.