Industry Brief

Why Insurance Companies Need SaaS Identity Risk Management

grip

Table of Contents

Introduction

SaaS technology and artificial intelligence (AI) are revolutionizing the insurance industry. Today, AI and SaaS tools accelerate claims processing, provide personalized customer experiences, and monitor individual behaviors from driving to wellness habits, collecting data, and influencing insurance rates.

From administrative staff to field marketing offices and insurers, SaaS technology and AI tools boost productivity and drive outcomes. But while technology is fueling innovation, it's also introducing new risks and expanding the organization's attack surface. Previously, IT departments had control over software procurement and deployment, ensuring security measures were firmly in place. Now, SaaS and Generative AI technology have changed the game.

The Growth of SaaS, Identities, and Risks

In the past, IT environments were closely managed, with IT departments controlling software procurement and deployment. The rise of SaaS (Software as a Service) has significantly changed this dynamic. While core SaaS applications usually go through a formal purchase and security review process, many SaaS tools are now being adopted by individual employees on their own. SaaS applications are easy to acquire and deploy—employees can sign up and start using them with just an email and a few clicks, often bypassing traditional IT oversight.

When employees independently adopt SaaS tools, IT departments lose visibility into which applications are used, how they are used, and by whom. This occurrence, known as shadow IT, increases the risk of data breaches, as unvetted applications may not meet the organization's security standards or regulatory requirements.

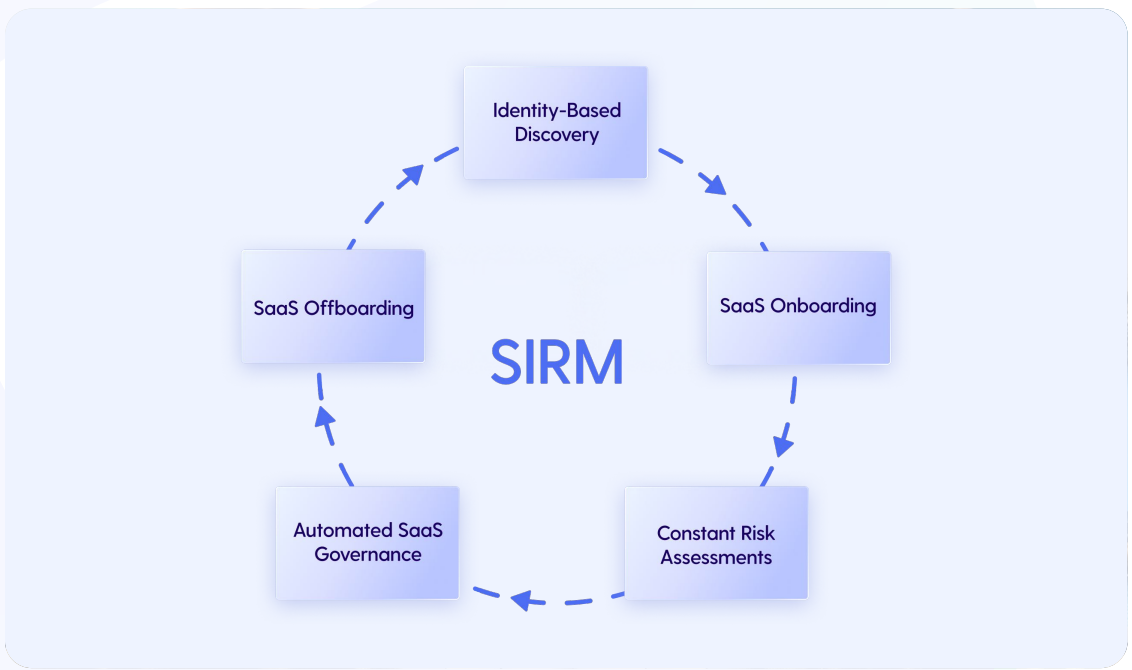
Each new SaaS application expands the organization's attack surface. Identity risks grow because each account can become a target for cybercriminals, who can use it to gain access to other corporate resources, leading to unauthorized access, data exfiltration, and other malicious activities. Recent high-profile breaches like Globe Life, Change Healthcare, and Medibank highlight the importance of protecting and securing identities and the costly consequences when compromised.

SaaS Identity Risk Management: A More Modern Approach

The shift from a closely governed IT environment to one where every employee can independently adopt technology requires rethinking SaaS security. To safeguard insurance companies effectively, the focus must be on enhancing visibility, control, and security compliance across all applications used within the organization. Enter SaaS identity risk management (SIRM), a strategic approach tailored to address the unique challenges posed by the widespread adoption of SaaS.

Traditional IT security frameworks fall short in a decentralized IT environment; however, SIRM provides a comprehensive framework designed to secure access, maintain compliance, and protect data within a decentralized and rapidly evolving IT ecosystem, ensuring that an organization can safely leverage the benefits of SaaS while mitigating the associated risks.

SaaS Identity Risk Management



The foundational elements of a SIRM program include:

- **Identity Lifecycle Risk Governance:** Establish and enforce policies for managing the digital identity lifecycle, including discovering and revoking user access to SaaS applications as necessary.

- **Access Management:** Involves implementing and managing secure access controls such as single sign-on (SSO), multi-factor authentication (MFA), and robotic process automation (RPA) to ensure that only authorized users can access SaaS applications.

- **Compliance Management:** Ensure adherence to relevant regulatory and industry standards, such as HITECH, HIPAA, NIST, SOC2, ISO27001, Gramm-Leach-Bliley Act (GLBA), NYDFS Cybersecurity Regulations, and others, particularly concerning securing access to applications and data.

- **Security Incident Management and Response:** Establishes comprehensive procedures for detecting, analyzing, and responding to security incidents affecting SaaS applications.

- **Enterprise Risk Management:** Evaluate and control risks posed by a SaaS application to the enterprise, distinct from assessing the risk profile of the SaaS vendor.

SaaS Identity Risk Management Outcomes

The objectives of a SIRM program are designed to address the unique challenges and risks associated with using SaaS and AI applications in an organization. These goals are critical for ensuring the security, compliance, and efficient management of identity-related aspects in a SaaS environment. The primary outcomes typically include:

- **Implementing Robust Access and Identity Risk Management:** Enforce strong access control mechanisms such as Multi-Factor Authentication (MFA) and Single Sign-On (SSO) to manage user access to SaaS applications securely. Efficiently manage the lifecycle of user identities from onboarding to offboarding.

- **Mitigating Risks Associated with SaaS Usage:** Identify and address security risks unique to SaaS environments, including those from shadow IT, where employees use unapproved but tolerated SaaS applications.

- **Ensuring Regulatory Compliance:** Align SaaS usage with regulatory and compliance requirements, ensuring organizational adherence to relevant standards and legal mandates.

- **Improving Visibility and Control:** Gain comprehensive visibility into SaaS application usage across the organization. Establish control over who accesses what applications, when, and how.

- **Adapting to Evolving Threat Landscape:** Develop the agility to quickly adapt to new threats and changes in the SaaS ecosystem to ensure ongoing protection and risk management.

- **Enhancing Operational Efficiency:** Streamline identity risk and access management processes for SaaS applications to improve operational efficiency and reduce administrative overhead.

SIRM takes a programmatic approach to discovering and managing risks from Gen AI services and SaaS applications. By focusing on identifying and mitigating threats related to identity sprawl, shadow IT, and shadow AI, SIRM supports regulatory compliance and ensures effective management of identity-related risks, providing the most comprehensive approach for securing SaaS applications.

HITECH, HIPAA, GLBA, & NYDFS (23 NYCRR 500) Compliance

Insurance operates in a highly regulated environment, and compliance with each regulation is essential to avoid costly penalties.

HITECH / HIPAA Compliance

Complying with Health Information Technology for Economic and Clinical Health (HITECH) requires insurance companies selling healthcare policies to implement comprehensive identity risk management across their SaaS applications. The HITECH Act update in 2024 significantly strengthens HIPAA compliance by imposing stricter penalties, extending HIPAA rules to business associates, enhancing enforcement and auditing capabilities, expanding patient rights, and promoting the adoption of secure systems. SaaS is crucial in this framework by providing scalable, secure, and efficient solutions that bolster compliance while maintaining operational efficiency.

Gramm-Leach-Bliley-Act

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, is a United States federal law enacted to regulate the collection, disclosure, and protection of consumers' personal financial information by financial institutions. SaaS has created numerous blind spots for compliance with the act's requirements since employees often use applications outside the internal IT purview. As employees work with business or distribution partners, consumer private information could be shared without providing the consumer an opt-out option, violating the company's privacy notices. One requirement under the Safeguards Rule mandates that insurance companies assess the risks to customer information and the effectiveness of the existing security controls.

NYDFS (23 NYCRR 500)

The New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500) imposes stringent requirements on insurance companies operating under NYDFS jurisdiction. The mandate to implement robust measures to protect nonpublic information is among its many requirements. Shadow IT is becoming a growing issue for insurance companies because it increases a company's attack surface and the likelihood of a data breach of nonpublic information.

Go deeper: Navigating 23 NYCRR 500 Shadow IT SaaS Provisions with Grip SSCP

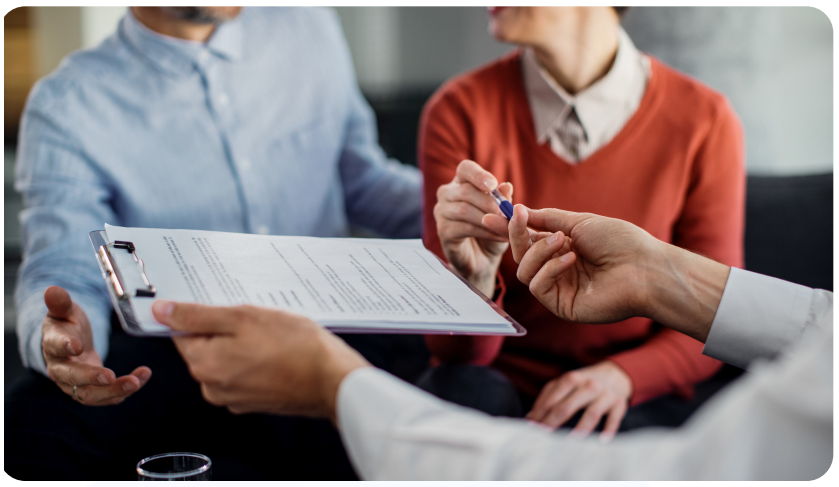
> "One of the significant challenges that companies have faced in complying with 23 NYCRR 500 is their tendency to prioritize traditional Software as a Service (SaaS) solutions while neglecting the critical issue of shadow IT SaaS."

Shadow SaaS and Shadow AI Jeopardize Compliance

Cybersecurity compliance standards often focus on known SaaS applications, but comprehensive discovery is crucial for identifying potential gaps and vulnerabilities that could lead to incidents. A SIRM approach helps organizations uncover both managed and unmanaged SaaS applications within their network, providing visibility into all applications in use, whether sanctioned or not. Once these applications are identified, the associated risks can be assessed and evaluated, considering factors such as data sensitivity, user access patterns, and the security practices of the SaaS providers. SIRM enables security teams to prioritize their efforts and address critical risks.

SIRM also supports risk mitigation by helping teams manage written policies and implement targeted security measures, such as enforcing multi-factor authentication (MFA) and securing dormant accounts. Additionally, SIRM can influence employee behavior by prompting them to modify actions that are out of compliance. For instance, employees using applications without MFA can be prompted to enable this feature.

Through continuous monitoring and automated compliance reporting, the SIRM framework has helped insurance companies adhere to HIPAA, HITECH, GLBA, and NYDFS requirements, improving their security posture, building customer trust, and ensuring that sensitive data remains secure and regulatory obligations are met.



Mitigating Workforce SaaS Identity Risks

Insurance companies face significant challenges in managing a complex and dynamic environment from a distributed workforce, the critical nature of their data, and stringent regulatory environments. Staff often work on personal devices and use online reference tools that the organization may not officially sanction. This diversity and fluidity create a challenging IT environment for several reasons:

- **Multiple Roles and Access Levels**: Each group within the workforce requires different levels of access to various systems and data. Insurers need access to medical records, administrative staff manage appointments and financial transactions, and contractors may need temporary access.

- **Changes in Staff:** Insurance environments experience high turnover rates and frequent role changes. Every staff and role change requires updates to access permissions. The workforce often comprises employees, contractors, or business associates working across various locations.

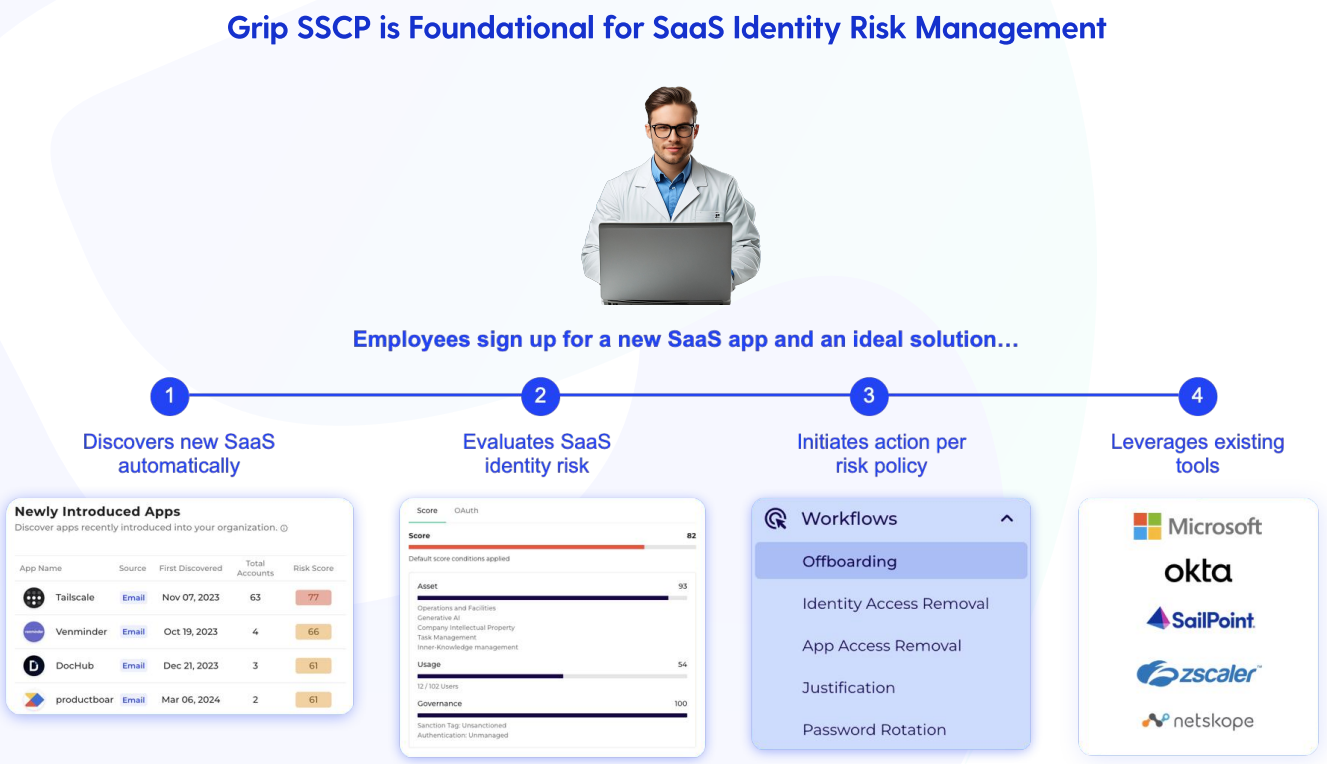
- **Distributed Access Needs:** Users often need to access internal systems and use external online resources to perform their duties onsite or from alternative locations. The use of personal devices is prevalent. This distributed access increases the complexity of ensuring secure and appropriate access controls.

HIPAA and GLBA require multi-factor authentication (MFA) to secure access to sensitive data. The HITECH Act update in 2024 significantly strengthens HIPAA compliance by imposing stricter penalties, extending HIPAA rules to business associates, enhancing enforcement and auditing capabilities, expanding patient rights, and promoting the adoption of secure IT systems. Shadow SaaS applications, which often store and process critical data, must also have MFA enabled to meet HIPAA, HITECH, and GLBA standards. However, this becomes more challenging with a diverse workforce due to varying roles, frequent changes, and widespread access needs. Without MFA, insurance companies risk falling short of essential cybersecurity protocols and exposing sensitive data to potential breaches.

The SIRM framework addresses these challenges by offering advanced identity risk management processes that ensure comprehensive visibility, detailed reporting, and access revocation when needed. With SIRM, insurance companies can maintain a secure and compliant IT environment, effectively protecting non-public data while supporting the operational needs of their dynamic workforce.

SIRM Platforms: Why Grip SSCP is the Best Solution for Insurance

As SaaS and AI adoption and reliance grow, the risks created must be addressed.
The Grip SaaS Security Control Plane (SSCP) is the industry's leading SIRM platform and has become essential for insurance organizations as they expand their SaaS usage. Grip SSCP provides actionable insights beyond what Cloud Access Security Brokers (CASB) and SaaS Security Posture Management (SSPM) can offer by supplying broader coverage, encompassing all SaaS applications, including those procured by individual users and used on unmanaged devices. Additionally, Grip SSCP is adaptable, including versatile integrations for diverse platforms and assessing risk based on the impact on the enterprise, which is critical for maintaining the security and integrity of sensitive healthcare data and patient privacy.



Supporting Regulatory Compliance

Grip SSCP is designed to meet stringent regulatory compliance standards, providing the tools necessary for comprehensive identity risk management across SaaS applications. Grip SSCP helps organizations navigate these complexities by:

- **Discovering Managed and Unmanaged Applications:** Grip SSCP identifies all SaaS applications within the network, whether officially sanctioned or not, ensuring no potential compliance gaps or security vulnerabilities are overlooked.

- **Assessing Risk**: It evaluates each application's risk based on data sensitivity, user access patterns, and the security practices of the SaaS providers. This risk assessment enables insurance companies to prioritize their security efforts effectively.

- **Mitigating Risks:** HIPAA and HITECH require covered entities to implement reasonable and appropriate administrative, technical, and physical safeguards to protect electronic protected health information (ePHI). Grip SSCP helps implement targeted security measures, such as enforcing multi-factor authentication (MFA) or securing dormant accounts, thus mitigating identified risks and enhancing overall security.

- **Continuous Monitoring and Reporting:** Automated compliance reporting and continuous monitoring ensure that insurance companies adhere to HITECH, HIPAA, GLB, and NYDF Cybersecurity Regulation (23 NYCRR 500), maintaining secure operations and protecting patient data.

The Future of SaaS Identity Risk Management in Insurance

Gartner projects that the adoption of SaaS and AI tools will continue to expand, with most tools being acquired outside of IT's purview. This means shadow IT and shadow AI risks will also increase, and breaches from compromised identities will persist unless these risks are proactively addressed. SaaS security is long overdue for modernization, and Grip is uniquely positioned to deliver the SIRM solution to address the evolving SaaS risks of today and tomorrow.

Grip SSCP's versatility allows seamless integration with a wide range of platforms, making it adaptable to the unique needs of any insurance organization. Its scalability ensures that as the organization grows and evolves, Grip SSCP can expand its capabilities by providing a future-proof solution that aligns with the ever-changing digital insurance landscape.

Grip SSCP also reduces the burden of manual compliance tracking and enables security teams to focus on core operations while ensuring continuous adherence to regulatory requirements. Grip's automation enhances security, provides real-time insights, and ensures that sensitive data is always protected.

About Grip Security

Grip Security is the industry leader in SaaS identity risk management, providing cutting-edge solutions to help enterprises navigate the security challenges of widespread SaaS adoption. Our platform enables companies to discover, prioritize, secure, and orchestrate SaaS risk mitigation. By leveraging identity as the central control point, we provide a comprehensive approach to securing all SaaS applications—including shadow SaaS and shadow AI—empowering organizations to adopt SaaS confidently and securely. Contact us to arrange a personal demo of the award-winning SaaS Security Control Plane.