Solution Brief

SaaS Identity Risk Management is Essential for Modern Cybersecurity

SaaS Identity Risk Management Goals

SaaS Identity Risk Management (SIRM) is a cybersecurity category designed to address the unique challenges and risks tied to managing identities within an enterprise's Software as a Service (SaaS) portfolio. This new category takes a programmatic approach to the discovery and management of risks across SaaS services and web applications, focusing identifying and mitigating threats related to identity sprawl and the use of unsecured or unsanctioned SaaS solutions. By delivering a comprehensive solution for securing SaaS applications, SIRM ensures compliance and effective management of identity-related risks.

Distinguishing SIRM from CASB and SSPM

SIRM sets itself apart from established categories such as Cloud Access Security Brokers (CASB) and SaaS Security Posture Management (SSPM) in several ways:

- **Broader Coverage:**

  While CASB discovers SaaS risks through network data, and SSPM assesses the security posture of a limited set of known SaaS applications, SIRM encompasses the entire set of SaaS applications. Most SaaS in the enterprise is procured by individual users and bypass official procurement process, resulting in a high volume of SaaS apps. They are often used on unmanaged devices, which mean their risks cannot be discovered through network traffic monitoring. SIRM manages all SaaS used on managed or unmanaged devices without the need to integrate to APIs or proxies for network traffic monitoring, offering control measures beyond the scope of CASB and SSPM.

- **Identity-Centric Approach:**

  SIRM leverages identity as a critical control point rather than the network or endpoint, which is different from CASBs and SSPMs. This allows SIRM to address issues like identity sprawl—where employees have access to numerous unmonitored and potentially unsecured SaaS accounts even if they are accessing them on unmanaged devices.

- **Comprehensive Risk Management:**

  Unlike CASB and SSPM that operate in silos for specific security functions, SIRM takes a more integrated approach. It deals with the interconnected nature of SaaS environment risks and the domino effect of a breach in one area, such as generative AI applications can impact multiple systems and services.

- **Adaptability and Integration:**

  Designed to adapt to a wide range of SaaS applications and services, SIRM offers versatile integrations and solutions for managing identity risks across diverse platforms. New applications are identified from day one, and the risk is assessed based on how much risk the application poses to the enterprise rather than focusing on the risk of the SaaS vendor. The risk information can be viewed and resolved in the SIRM platform or pushed into other systems used by security and risk operations.

- **Automated Detection and Mitigation:**

  SIRM includes capabilities that automatically detects shadow IT, rogue cloud accounts, and other unsanctioned SaaS-related risks. It also streamlines the prioritization and mitigation of these risks in an automated fashion.

- **Dynamic Access Control:**

  SIRM responds to risks from based on the SaaS vendor and user risk profiles. It goes beyond the static inputs of certifications and data types to measure the usage growth, functions of the users, and frequency to respond with access controls that can be applied to managed and unmanaged devices

SaaS Identity Risk Management Components

SIRM provides an identity-focused approach to managing security across the SaaS ecosystems, successfully, addressing a range of risks that extend beyond what traditional CASB and SSPM can handle. With a programmatic SIRM approach enterprises can leverage a variety of strategies and tools specifically designed to address the risks associated with the use of SaaS applications. These elements are essential for ensuring the security and compliance of an organization's digital identity infrastructure. The primary elements include:

- **Identity Lifecycle Management:**

  Establishes and enforces policies for managing the digital identity lifecycle, including identifying 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) that automatically rotates passwords, providing an layer of access control that works for unmanaged devices and unmanaged SaaS apps.

- **Compliance Management:**

  Ensures adherence to relevant regulatory and industry standards, such as NIST, SOC2, ISO27001 and regulations such as GDPR, HIPAA, and others, particularly concerning securing access to applications and data.

- **Security Incident Management and Response:**

  Establishes comprehensive procedures for the detection, analysis, and response to security incidents affecting SaaS applications.

- **Enterprise Risk Management:**

  Evaluates and controls risks posed by a SaaS application to the enterprise, distinct from assessing the risk profile of the SaaS vendor

SaaS Identity Risk Management Benefits

SIRM has strategic and operational benefits that address the unique challenges and risks associated with the proliferation of SaaS usage within the modern enterprise. These benefits are crucial for ensuring the security, compliance, and efficient management of identity-related aspects in SaaS environments, including:

- **Robust Access and Identity Risk Management:**

  Enforce and measure the effectiveness of strong access control mechanisms such as MFA and SSO to securely manage user access. Efficiently manage the lifecycle from onboarding through offboarding.

- **Mitigating Risks Associated with SaaS Usage:**

  Identify and mitigates security risks unique to SaaS environments, including 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 industry standards and legal requirements.

- **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 swiftly adapt to new threats and shifts within the SaaS ecosystem, ensuring continuous 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.

SaaS Identity Risk Management—Essential for Modern Cybersecurity

In the landscape of modern enterprise technology, where the surge in SaaS application use is both a boon and a potential security pitfall, SIRM stands out as an essential strategy. It offers a comprehensive solution to the complex web of identity-related challenges that expanded after the SaaS revolution. What sets SIRM apart is its identity-centric approach and its capability to weave together comprehensive risk management with the flexibility to address the rapid evolution of SaaS usage and threats.

As organizations navigate the complexity of securing their SaaS portfolios, the SIRM framework provides a beacon for managing risks in a cohesive, integrated manner. It avoids the siloed approach of traditional models, instead offering a panoramic view of the organization's security posture. With its focus on automating detection and simplifying mitigation processes, SIRM exemplifies a proactive, forward-thinking approach to SaaS security that not only identifies shadow IT and rogue accounts but also empowers organizations to anticipate and adapt to risks. The strategic significance importance of a SIRM program extends into the core of operational integrity and business continuity. By fostering robust access and identity risk management and improving the visibility of SaaS application use, SIRM enables organizations to harness the full potential of SaaS without compromising security or efficiency.

grip

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.

Contact Us

✉ info@grip.security
in @GripSecurity
🌐 grip.security

SOC 2 Type II Certified

AICPA SOC

As the SaaS environment becomes increasingly complex, the insights provided by a SIRM program can help organizations stay ahead of the curve. For those looking to delve deeper into the world of SaaS security, exploring the nuances of SaaS Identity Risk Management can reveal new avenues for protecting and optimizing their digital ecosystems. It's not just about safeguarding assets; it's about enabling innovation, growth, and competitive advantage in an ever-changing digital landscape.

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.

grip

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.

Contact Us

info@grip.security
@GripSecurity
grip.security

SOC 2 Type II Certified

AICPA SOC