Solution Brief

Snowflake Security Incident: A Wake-Up Call for CISOs and CIOs

Recent large-scale data breaches at Ticketmaster and Santander Bank may have resulted from a fundamental failure to secure access to data on a third-party cloud service properly. While the details surrounding the recent security incident are still emerging, numerous reports point to a concerning trend. Although Ticketmaster and Santander have not disclosed the identity of the third-party cloud service, several security analysts have identified the provider as Snowflake, a prominent cloud-based data platform. Snowflake, along with CrowdStrike and Mandiant, issued a joint statement asserting that they found no evidence of a vulnerability, misconfiguration, or breach of Snowflake's platform itself. Instead, they suggest this incident is a targeted campaign against single-factor authentication users.

How the Snowflake Incident Happened

The details of the Snowflake incident are still unfolding, but it appears to have occurred when threat actors leveraged credentials previously obtained through info-stealing malware. Though the reports at the time of this publication aren't definitive, Snowflake found evidence that a threat actor gained access to demo accounts belonging to a former Snowflake employee. These demo accounts, while not containing sensitive data, were not protected by Okta or Multi-Factor Authentication (MFA), unlike Snowflake's corporate and production systems.

Actions Recommended Following the Snowflake Incident

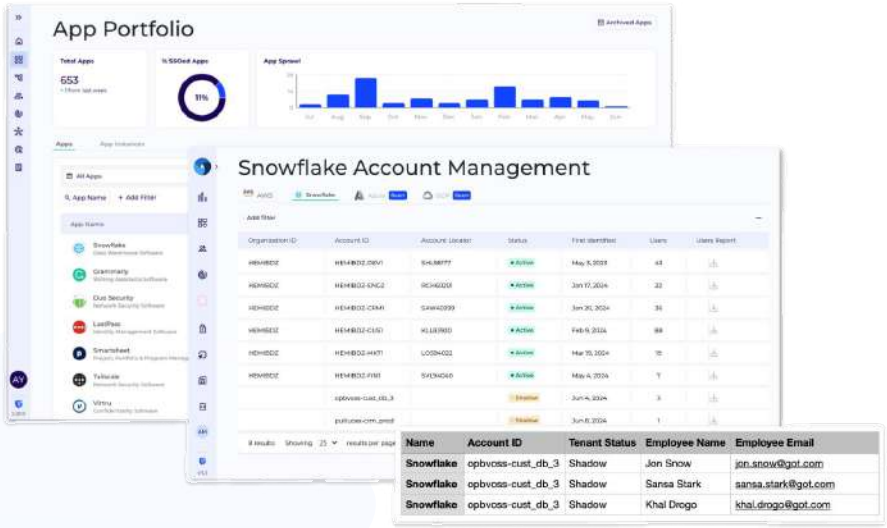
Snowflake recommends that organizations immediately enforce MFA on all accounts, establish Network Policy Rules to only allow authorized users or traffic from trusted locations (such as VPNs or Cloud workload NATs), and reset and rotate Snowflake credentials for impacted organizations.

Preventing Similar Security Incidents with Grip

Grip pioneered a comprehensive strategy for managing SaaS risks- SaaS Identity Risk Management (SIRM) to address the changing SaaS landscape and emerging risks. Companies with a modern and robust SIRM program can avoid breaches like the one unfolding with Snowflake. Though SIRM principles are extensive and comprehensive, we can apply specific aspects to this type of breach.

Discovery of all Snowflake Instances and Accounts

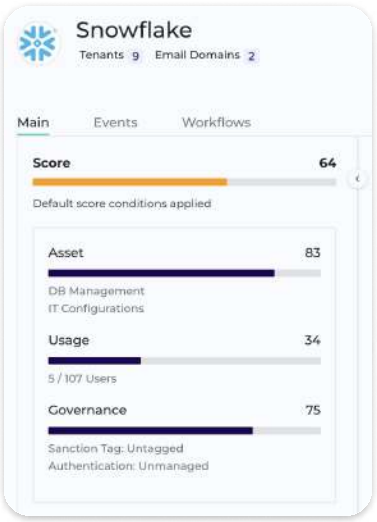
The first step is to discover all SaaS applications, including all Snowflake instances and accounts within an organization. This includes unmanaged accounts that employees may have created without proper oversight from IT and security teams. Grip provides full visibility across your SaaS ecosystem, identifying gaps and cataloging managed and unmanaged SaaS, IaaS tenants, Snowflake instances, and all associated user accounts. As a result, a complete and continuously updated inventory is created.



App, Account, and User Discovery:
Grip discovers all Snowflake instances and accounts

Evaluating SaaS Identity Risks

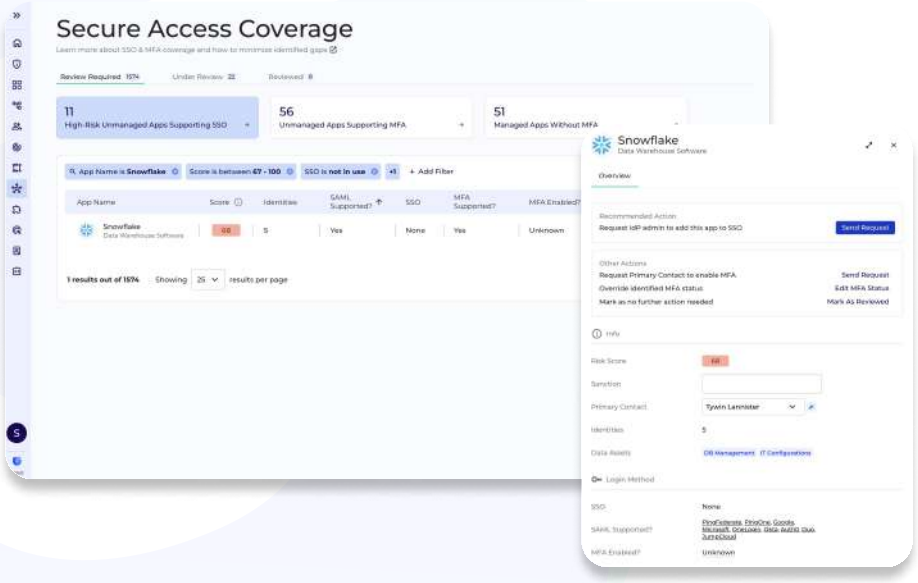
Next, Grip evaluates the "SaaS Identity Risks" of each application, looking beyond traditional vendor risks such as certifications and data protection policies. Grip uncovers more indicative risk factors such as asset risks, usage risks, and authentication risks, collectively known as "SaaS identity risks." From there, Grip assesses whether applications are inherently risky or benign, if users authenticate to apps with SSO or MFA, and if the apps are managed or unmanaged. The Grip SaaS identity risk platform provides an easy-to-understand risk score and assessment for each app, helping you to prioritize which risks to address first.



SaaS Risk Score:
Grip evaluates Snowflake's SaaS Identity Risks and presents a holistic risk score.

Mitigating Risks Prescriptively

Finally, Grip helps reduce your SaaS risks effectively and efficiently. Once Grip has discovered SaaS instances and accounts and evaluated them for risk, it recommends the best course of action. Should your security team find an app useful and should be allowed, Grip helps secure access more broadly, including Single Sign-On (SSO) and Multi-Factor Authentication (MFA) with built-in recommendations and actions, such as contacting the Identity Provider (IdP) admin or business owner to enable SSO/MFA with instructions and context.



Secure Access Coverage:
Grip finds opportunities to secure Snowflake with SSO and MFA, initiating requests with IdP admins and business owners.

If an app is deemed too risky, Grip can revoke access to credential-based apps by rotating passwords, ensuring former employees can no longer access sensitive data and mitigating breaches by forcing a password reset.

Centralized Control of Shadow SaaS and IaaS Assets

In addition to shadow SaaS, users also create accounts in IaaS tenants and other assets such as Snowflake. Grip finds opportunities to bring these assets under centralized control where admins can apply security policies and controls. By providing details on tenants, instances, and user accounts, Grip makes it easy for security teams to contact the right people and incorporate their accounts and assets into an established security program.

Breaking the Cycle of Security Breaches

Despite the lack of detailed breach information, the Snowflake incident highlights a recurring pattern seen with other organizations that have been hacked: the absence of protection by SSO or MFA, dangling access, and exploitation of former employees' demo or production accounts. Grip helps organizations cover all bases by identifying and mitigating SaaS identity risks through a holistic SIRM program. The Snowflake security incident is just one example of the threats that Grip can potentially prevent while ensuring robust security measures are in place across your entire SaaS and IaaS landscape.

Book time with our team to learn more about the Grip platform and how we can help secure your SaaS landscape.