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, laaS tenants, Snowflake instances, and all associated user accounts. As a result, a complete and continuously updated inventory is created.

	Tetral Appo IL SSGed	Appr	App Sprawl							
	653 - Hore had even	3	-		-			a di se		
	App States									
	Snowflake Account Management									
	0, App Norre + Add Fitter 1									
	App Name	88	Ann filter							-
	Structure Construction Constructi	24	Organization (D	Account ID	Antione Line	er .teto	First storegiest	Unit	United West	
			HENHEDZ	H814802.08V1	5-6,56777		May 8, 2028	44	16	
		0	HEMIROX	HEMBOZ-SNC2	953460201	· Accient	Jan 17, 2004	32	16	
			HEHRER	HEMEDIC COM	S20420939	· Annual	309 25, 2524	34	4	
		۵	weinenstesz	HEMBORICUST	81.139900	· Active	Feb 9, 2124	**	14	
		æ	300H00	HEHEDZ-HHT	L0584022		Har 75, 2024		1	
		6	HEMISCIE	HEMBOLINE	5/134040	• Action	May A 2026	Υ.	1.16	
		8		optives-mat.00.3		Distance	June, 2026	3	1.1	
				putuoe-om.ped		1 tables	3058.2024	40	1.14	
			Riveriti Shoving	25 👻 renatis per pige	Name	Account ID	Tenant Status	Employ	se Name	Employee Email
					Snowflake	opbvoss-cust_db_3	Shadow	Jon Sno	w	jon.snow@got.com
					Snowflake	opbyoss-cust db 3	Chadaus	Sansa S	and a local data	sansa.stark@got.com

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.



Main	Events V	Vorkflows			
Score	r.	64	64		
Defau	t score conditions app	lied			
Ast	set	83			
	Management onfigurations				
Usi	age	34			
5/1	07 Users				
Go	vernance	75			
	ction Tag: Untagged				

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.

Review Required 1974 Under Review 25	Received 0					
11 High-Bisk Ummanaged Apps Supporting SSD -	56 Unimanaged Apps Supporting MFA	ş	51 Managed Apps V			
				Snowflak Data Warehouse	e « Software	
9, App Name is Snowflake 0 Score is between	47 - 100 0 SSO is not in use 0 +1 + Add	Filter		thenistew		
App Name Score: ()	Identitae GAMI, + SSO	MFA Support	MFA E			
Snowfake Extra Manhage Suffrage	5 Ves None	. Yes	Unkno	Request GP admin for		Send P
Tresults out of 1974 Showing 25 v result	o per poge			Other Additiona Required Primary Con		Serred P
				Override identified M Mark as no further at		Edit MEX Mark As Re
				0 11/2		
				Rick Score	STATE OF	
				Derection		
				Primary Constant.	Tysen Lannistar 🛛 🛩	*
				Inter-Others	5	
				Data Automy	DB Wanaperson IT Configuration	70
		_	_	0= Login Helhod		
				850	None	
				save. topponent?	Prodisidents, Driedine, Goools, Miscanalt, Concores, Data, Autral o Jury Cloud	840.

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 laaS landscape.

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