BEYOND IDENTITY | snowflake®

Case Study

SNOWFLAKE AND BEYOND IDENTITY

Securing Critical SaaS Resources With Passwordless, Risk-Based Authentication

Contents

Executive Overview

Snowflake chose Beyond Identity to restrict access to critical SaaS applications for only company-issued or secure, authorized devices — without adding additional friction or complexity for their workforce. In this case study, you will find:

- A review of the challenges facing Snowflake in securing critical SaaS applications
- The legacy solutions that failed Snowflake
- Snowflake's needs and evaluation criteria
- Why Snowflake chose Beyond Identity to perform strong, passwordless multifactor authentication (MFA) for their critical SaaS applications and resources

About The Global Disruptor in Cloud Data

Founded in 2012 in San Mateo, California, by Benoit Dageville, Thierry Cruanes, and Marcin Żukowski, Snowflake has many accomplishments. Credited with disrupting and innovating the data warehouse industry, Snowflake wowed the market on entry by being the first to separate data storage from data queries.

Rather than store data on-premise, Snowflake offers the ability to warehouse vast volumes of data in the cloud and make it queryable for cloud-based hardware and software. This functionality informs business insights that improve business productivity and performance across the globe.

In 2018, Snowflake reached "unicorn" status with a valuation of $1.5 billion, and in September 2020, Snowflake broke records, debuting on the NYSE at $120 per share and skyrocketing to $300 per share on the first day of trading.

Their debut on the exchange was the largest software company to IPO in U.S. history, raising $3.4 billion at their initial public offering and becoming the largest company to ever double in value on its opening day, reaching a market cap of close to $75 billion.

02

Snowflake's Authentication and Security Challenges

Like the innovative company they are, Snowflake addressed their security challenges head on. They deployed systems to secure access to critical cloud resources on all company-issued laptops, ensuring that access would only be gained by secured, known devices. But at home, employees were accessing Snowflake's SaaS applications on personal laptops and other unmanaged devices that were unsecured and unmonitored by these tools.

The use of insecure personal devices at home allowed employees to circumvent MFA, SSO, and MDM controls and access Snowflake's cloud resources, potentially exposing the business to the threat of unauthorized access and data exfiltration.

Snowflake's team refers to its customers' data as the "Holy of Holies" and works exceedingly hard to protect customers from data compromise. Their customers include U.S. government agencies, financial institutions, and businesses of all sizes across all sectors. Snowflake processes more than 515 million transactions and manages over 250PB of data daily.

Snowflake strives to continuously improve how they safeguard customer data. Although they deployed MFA, SSO, and MDM on organizational laptops, they still had to address the remaining challenge of stopping unauthorized access from unsecured or unregistered devices.

"What immediately became clear to me was how Beyond Identity could solve a lot of the challenges in accessing SaaS applications in the cloud"

Mario Duarte, VP of Security, Snowflake

CHALLENGES:

1 Enforcing Security Policies on Unmanaged Devices

Snowflake manages company-owned Mac and Windows laptops, but an MDM alone could not offer actionable insight into unmanaged devices or restrict resource access in real-time. The alerts would be useless if access to critical resources had already been granted.

2 Stopping Unsecured Devices from Accessing SaaS Company Resources

Snowflake chose to use a single sign-on (SSO) and a built-in, legacy MFA solution to centralize control of access to apps and simplify provisioning of users. SSO helped improve the productivity for users and improved the login experience for their workforce because now there was just one username and password for all of their apps.

The goal was to support a layered approach to preventing unauthorized access to cloud resources.

However, these identity solutions lacked security controls. SSO uses one password for access to every connected application, a critical security vulnerability that allows account takeovers and data breaches. Additionally, they lack the ability to prevent unauthorized access from unsecured devices and to stop lateral movement.

CHALLENGES (Continued):

"Anyone can use any computer to connect to SaaS applications - Workday, Salesforce, GitHub, and download stuff onto their personal machines. We wanted to only have Snowflake laptops or approved devices to have the ability to connect to Okta."

Mario Duarte, VP of Security, Snowflake

3 Securing Cloud Services and Resources

As work from home exploded at the beginning of 2020, Snowflake quickly realized that VPNs — though great for a few hundred persons remotely accessing resources on-premise — were woefully inept at protecting SaaS resources from unauthorized access.

VPN introduced vulnerabilities and inefficiencies in the form of:

- Complicated configurations and provisioning, and even easier to leverage for unauthorized access
- Slowed traffic that impacted Snowflake's productivity, as VPNs were not created to facilitate SaaS-intended traffic
- No way to validate or deny access based on the security posture of the device at the time of request for resource access

For Snowflake, this meant forcing their entire workforce onto their VPN and burdening them with a slow, friction-filled experience for the sake of "security," even though the VPNs themselves were a risk.

4 Checking the Security Posture of Devices Before Authorizing Access

Snowflake's CASB implementation lacked automated and actionable contextual assessment of both user and device identity and security. CASBs, though created to secure SaaS access and the movement of data within those applications, were unable to ensure the security posture of the device nor authenticate the user and allow access from public and temporary devices.

This deficiency in capability left Snowflake open to potential threats like:

- Rooted devices which significantly alter their security posture and can expose enterprise applications to attacks and malicious applications
- Access via unsecured or compromised network access like public wifi that bad actors could leverage for credential or data theft
- Temporary and personal devices that may be infected or compromised with malware or by keyloggers

Snowflake needed a solution to secure remote access, authenticate users with a high level of assurance, and check the security of each device before authentication.

03

Why Snowflake Chose Beyond Identity

Snowflake chose Beyond Identity to ensure that only known devices tied to a user's identity that adhere to device security policies are granted access to their organization's resources.

Before Beyond Identity, Snowflake had no way of knowing if the personal devices that their employees were using should be trusted and given access to their company's data. Beyond Identity gave them the ability to restrict access to cloud resources only to authorized devices, removing the top security vulnerability associated with cloud resources by:

Imposing Device Access Restrictions and Enforcing Granular Device Security Policies

Restricting enrollment to Beyond Identity and access to SaaS applications and data only on corporate-issued laptops

- Restricting and rejecting unauthorized enrollment attempts on virtual machines
- Checking managed or registered status of Mac and Windows devices using API from JAMF and Microsoft Intune
- Ensuring that all devices accessing resources have a biometric or pin enabled, encryption enabled, anti-virus enabled before gaining access to cloud resources
- Customizing the employee self-enrollment process, forcing corporate device use, SSO authentication, and MFA at initial enrollment for all users
- Displaying all devices registered with a specific identity

Enhancing The Current Stack With Advanced, Cloud-Based Passwordless MFA Technology

- Creating customizable rules to restrict cloud resource access and allow user exceptions for unmanaged and multiple devices
- Streaming all logs to Snowflake SIEM, including successful and unsuccessful login, registration, and migration attempts
- Integrating Beyond Identity with their existing legacy SSO, MFA, and IdP to protect against unauthorized access and remove user friction at each login

Removing Vulnerabilities and Complexities of Legacy Solutions

- Making sure credentials could not be copied from one device to another
- Securing cloud resource access without causing unnecessary user friction
- Being able to de-provision enrolled users and devices from Beyond Identity Portal

In addition, Beyond Identity is a cloud-native solution. Snowflake was confident that Beyond Identity could offer the reliability, availability, and scalability to support large numbers of users and any spikes in authentication requests.

> "We can now enforce policies to say your device has to be clean before you come in"
>
> Mario Duarte, VP of Security, Snowflake

04

A Look At Snowflake's Results, What Beyond Identity Delivered

To begin, Snowflake set up a proof of concept to roll out Beyond Identity to a sample set of 200 users. Impressed by the solution, Snowflake allowed the entire company, all 2,800 employees, to enroll, with over a quarter of them doing so within 24 hours.

After implementing Beyond Identity, Snowflake was able to control access to cloud resources by adhering to device security posture, a requirement for login without impacting their employees' productivity. For Snowflake, Beyond Identity helped fill the security gaps left by traditional authentication and access control solutions.

Beyond Identity ensures strong authentication, verifies device identity, and enforces device security posture as a condition of access for Snowflake. The removal of passwords from the authentication workflow prevents MFA circumvention and unsecured device access for Snowflake.

2,800 Employees Enrolled Remotely

100% Adoption Rate

750 Users Enrolled in the First 24 Hours

Strong authentication to protect critical company data

Snowflake can recognize unauthorized persons or devices circumventing the access controls, protecting their critical resources in real-time. They have ensured users' strong authentication and protected access to critical cloud resources with Beyond Identity's immovable, cryptographically proven, device-bound identities securely stored in the TPM hardware of enrolled devices. There are no passwords to steal or compromise now, effectively securing Snowflake's Saas resources and customer data repositories against unauthorized users and credential-based intrusions.

Risk-based authentication controls for all devices

Snowflake can deploy rule-based access via customizable policies within Beyond Identity and force unmanaged devices to adhere to Snowflake device security policies. Devices, either managed or unmanaged, that attempt access without a device-bound identity are rejected from access — a needed capability missing from Snowflake's security stack when using VPNs or CASBs.

Passwordless MFA their workforce actually loves

Snowflake's workforce was thrilled with Beyond Identity's passwordless authentication experience. They didn't have to waste their time picking up their phones to retrieve one-time passcodes for authentication anymore. Instead, Beyond Identity turned Snowflake's laptops and subsequently enrolled devices into multi-factor cryptographic authenticators. Snowflake laptops are now a cryptographically proven factor, removing the need for second devices and all of the friction and hassle used to go with them.

Conclusion

Snowflake needed to secure access for their corporate users accessing SaaS apps, especially when these applications and cloud resources are accessible from any device. Snowflake chose Beyond Identity to protect their critical resources from unauthorized attack because of the strong authentication and enforced device security policy on any device their employees use.

About Beyond Identity

Beyond Identity provides the most secure authentication platform in the world. Breaking down barriers between cybersecurity, identity, and device management, Beyond Identity fundamentally changes the way the world logs in by eliminating passwords and providing users with a frictionless multi-factor login experience. Beyond passwordless, the company provides the zero-trust access needed to secure hybrid work environments, where tightly controlling which users and which devices are accessing critical cloud resources has become essential. The advanced platform collects dozens of user and device risk signals during each login, enabling customers to enforce continuous, risk-based access control. The innovative architecture replaces passwords with the proven asymmetric cryptography that underpins TLS and protects trillions of dollars of transactions daily. Customers turn to Beyond Identity to stop cyberattacks, protect their most critical data, and meet compliance requirements.

The company was founded by Jim Clark and TJ Jermoluk, who helped ignite the commercial internet with Netscape and @Home Networks. The dynamic duo assembled an all-star team and created the world's most advanced passwordless identity platform at a time when digital transformation is impacting every business, and cyberattacks have become a top risk. The company raised $105M from premier investors Koch Disruptive Technologies (KDT) and New Enterprise Associates (NEA). Beyond Identity is headquartered in NYC with offices in Boston, Dallas, Miami, and London.

Ready to Have Beyond Identity Solve Your Authentication Challenges?

GET A DEMO

beyondidentity.com

info@beyondidentity.com

BEYOND IDENTITY