Beyond Identity
SECURE DEVOPS

Snowflake Boosts Developer Productivity with Beyond Identity Secure DevOps

OVERVIEW

Snowflake, the AI Data Cloud company, looked for ways to streamline developer productivity, which involved creating a more seamless security experience.

For a company like Snowflake, protecting the integrity of the software development lifecycle (SDLC) is a top priority. But like many fast-moving software companies, they focused on enhancing their build pipeline workflows, while maintaining robust security, without slowing down developers.

By implementing Beyond Identity's Secure DevOps product, Snowflake eliminated static credentials, established greater verified code commit coverage, and saved thousands of developer hours annually.

This case study outlines the solution Snowflake implemented to streamline workflows across security, productivity, and compliance.

Highlights

METRIC	IMPACT
Developer Onboarding	From ~1 hour / developer spent during onboarding to setup SSH keys and access tokens to near-zero, saving thousands of engineering hours annually on credential management.*
Static Credential Risk	Teams adopting this workflow have meaningfully reduced reliance on static SSH keys and personal access tokens on developer endpoints.
Code Integrity	Successfully implemented verified, signed commits across all in-scope repositories. Research shows the industry average is just 10%.
Access Revocation	Real-time revocation with developer offboarding, helping reduce the risk of unauthorized code pushes with SSH keys.

*Based on internal estimates across participating Snowflake engineering teams

The Challenge

SECURING THE SOFTWARE SUPPLY CHAIN

At the core of the problem was how to validate developer identity. Specifically, how to confirm that the person committing code is who they say they were.

Traditional methods, like SSH keys, do not always provide the level of validation needed because they can only prove possession of a credential, not the identity of the user. A compromised SSH key is indistinguishable from a legitimate one, creating the potential for an attacker to impersonate a developer.

> Historically, the industry has relied on static SSH keys, which validate possession but don't inherently verify developer identity.
>
> As supply chain risks have continued to evolve, Snowflake took a forward-looking approach to identity assurance in the development workflow. By addressing areas where commit authenticity and attribution matter most, the team further raised the bar against risks such as commit spoofing and unauthorized code changes.
>
> Gaurav Singodia, Senior Manager of Cloud DevOps & SRE at Snowflake

The Challenge

BALANCING DEVELOPER EXPERIENCE WITH SECURITY

Snowflake aims for high developer productivity because developer velocity is directly tied to business value and the speed of innovation. However, security controls often add friction and slow down work. The process of managing SSH keys, from setup to rotation, was a clear example of this friction.

The challenge was finding a security solution that removed friction for developers. The goal was to remove security roadblocks, not create new ones.

> There is a sweet spot between security and user experience. You want everything to be secure, but at the same time you don't want the user experience to be affected.

MEETING COMPLIANCE DEMANDS

Snowflake operates within a regulatory environment that includes rigorous compliance and audit standards such as SOC, FedRAMP, and the SLSA framework. This requires proof of who has control over their development process.

This meant they needed a solution that could provide a verifiable audit trail to prove the authorship and integrity of every code change.

> Every line of code committed in our repository needs proof of control. So auditability becomes a matter of policy that must be enforced in the CI/CD pipeline.

The Solution

To meet these challenges, Snowflake chose Beyond Identity's Secure DevOps product. The solution authenticates developers by cryptographically binding their identities to their devices, creating a clear chain of custody for every code commit.

Secure DevOps uses public key cryptography to sign code within developers' Git workflows without disrupting it. This change eliminates the friction from manual key management, encryption, and rotation.

The Solution

To meet these challenges, Snowflake chose Beyond Identity's Secure DevOps product. The solution authenticates developers by cryptographically binding their identities to their devices, creating a clear chain of custody for every code commit.

Secure DevOps uses public key cryptography to sign code within developers' Git workflows without disrupting it. This change eliminates the friction from manual key management, encryption, and rotation.

> What stood out to me was the ability to cryptographically bind developer identities to trusted devices. Secure DevOps provides hardware-backed, ephemeral credentials tied to the active session, giving us strong assurance of authenticity for every interaction in the development workflow.

Secure DevOps provides Snowflake with a verifiable record of code changes, helping to ensure every line of code came from a trusted developer on a secure device that is compliant with their corporate security policies. This ultimately forms a critical part of how Snowflake secures their software supply chain and gives them the proof of control needed for compliance audits.

> The question for me is, how can I take this friction away from developers so they can operate with fewer interaction points in their journey, while making sure that our code base is secured in the way that continues to meet our standards of code integrity?
>
> With Secure DevOps, identity and security verification happen as part of the workflow. The repository only accepts code from authorized users and compliant devices, creating a much more seamless experience.

The Results

GAINS IN DEVELOPER PRODUCTIVITY

By adopting Secure DevOps, Snowflake saved thousands of engineering hours. The time spent on security setup for new developers, which was about an hour, was cut to near-zero.

Productivity improved in other areas too. Developers no longer had to deal with key rotations and encryption, letting them focus on their work. Offboarding also became simpler. When an employee leaves, their access is quickly cut off, which reduces the security risk of unauthorized code pushes after a developer is offboarded.

The Results

> If I have 5,000 engineers, that is 5,000 hours saved. I basically eliminated the onboarding time for SSH keys. It's reduced to near-zero with Secure DevOps. This represents hundreds of productive engineering hours. And revoking access occurs in real-time because as soon as you revoke the identity, you revoke the ability for them to push code. There are no zombie SSH keys.

SECURING THE SOFTWARE SUPPLY CHAIN

With the implementation of Secure DevOps, some business units within Snowflake saw a near-complete reduction in static SSH keys and personal access tokens on developer devices.

Snowflake increased GitHub commit verification to specific business units and development workflows, a significant jump from the reported industry average of only 10% for signed commits. This provides a high level of code integrity.

This verifiable chain of custody helps ensure that every line of code is tied to a trusted developer on a secure device, giving Snowflake confidence in their software's integrity.

> The basic element that everyone wants to know is who is writing, what is writing, and on which device they're writing it on. If you have answers to these questions, you can better prevent bad actors from getting into the codebase and this is what we consider to be our immutable ledger of trust. Today, we have achieved verified signed commits across all in-scope repositories in GitHub.

COMPLIANCE AND AUDITING

With Beyond Identity, Snowflake can support compliance efforts aligned with frameworks like SOC and FedRAMP. The platform provides a complete audit trail for every code commit, linking it to a verified identity and device. This simplifies the audit process and provides auditors with the strong assurances they need.