

Why standing access keeps causing breaches

A practical guide to continuous least privilege

Organizations are facing more breaches each year, and identity continues to be at the center of the problem. The 2025 Verizon DBIR saw its highest number of confirmed breaches to date. And the cost is real.



IBM's 2025 Cost of a Data Breach Report puts the average breach at

\$4.44 million



With malicious insider incidents closer to

\$4.92 million

Most didn't rely on sophisticated exploits. They relied on something much simpler: access privileges that shouldn't have been there in the first place.

Attackers are still successfully using valid credentials, misconfigurations, and old permissions that never got cleaned up.

What ties these incidents together is an access management gap. If access controls evolved as quickly as the environments they protect, a large share of these breaches could be avoided. Continuous least privilege is designed to solve exactly this gap, and we will break down what that means.

What this guide will help you understand

- Why identity-driven breaches continue to rise in modern, cloud-native environments
- Why traditional least-privilege models can't keep pace with dynamic infrastructure and fast-moving engineering teams
- How continuous least privilege keeps access aligned with real usage across humans and NHIs
- How continuous least privilege lays the foundation for Zero Standing Privilege
- How automation and context make least-privilege guardrails practical and scalable
- A clear framework for reducing breach risk without slowing down engineering velocity

Why identity keeps driving modern breaches

When you break down identity-related incidents, the root causes fall into a few predictable patterns.



Excessive access

Permissions tend to spread. A team member gets temporary access for a project, and it never gets removed. A contractor changes roles, but their authorization stays the same. These small exceptions accumulate over months and years, and when one of those identities is compromised, the attacker inherits far more power than they should ever have had.



Always-on privileges

Standing access remains one of the most reliable paths attackers use. A stolen password or API key is dangerous enough on its own. Combine it with privileges that are available all the time, and the attacker can move quietly with very little resistance.



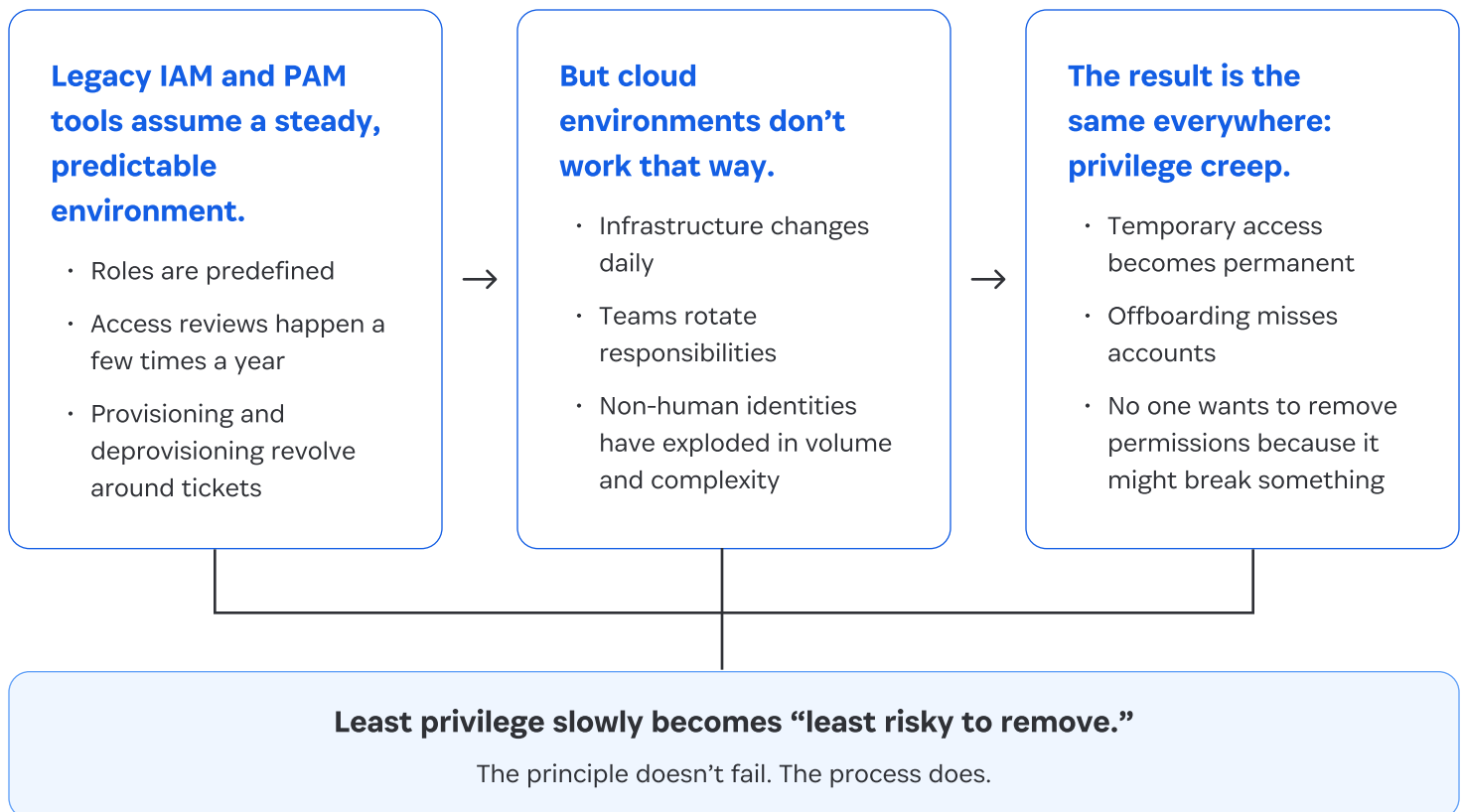
Drift and JML gaps

Cloud environments evolve constantly. Identities move roles. Resources get created and deleted. But access often stays frozen in its original form. Wildcards show up, roles expand, entitlements pile up, and joiner/mover/leaver (JML) processes struggle to keep access aligned with reality. Attackers look for these gaps because they're easy to exploit.

None of this is surprising. These issues occur naturally in environments that move fast, where access management is still mostly manual.

Why traditional least privilege falls short

Least privilege is one of the most well-known principles in security: identities should only have the minimum access needed to perform their job.



What continuous least privilege brings to the table

Continuous least privilege **builds on the goal of restricting identities to only the necessary access**. But it then goes the extra step and treats it as an **ongoing activity rather than a cleanup project**.



Continuous reduction of excessive privileges

Instead of waiting months for reviews, access is corrected as it becomes outdated. This keeps exposure windows shorter and prevents yesterday's exception from becoming tomorrow's breach path.



Context-aware rightsizing

Not all permissions are equal. Some enable routine tasks; others touch critical production systems or sensitive data. Continuous least privilege adjusts permissions based on real usage, risk, and changing responsibilities. When context shifts, access shifts with it.



Automation to prevent drift excessive privileges

Manual processes almost guarantee oversight gaps. Automated provisioning and deprovisioning realign access with actual needs and prevent old permissions from lingering indefinitely.

Continuous least privilege keeps organizations aligned with the principle of least privilege. Not just the intention.

How continuous least privilege leads to zero standing privileges

Once privileges are reduced continuously, the next step is addressing how long they remain available. This is where Zero Standing Privilege (ZSP) comes in.

Zero Standing Privileges bring together two principles: **Just-in-Time access** to restrict the window of privilege, and **Just-Enough access** to restrict the breadth of that privilege.

ZSP eliminates permanent privileged access. Instead of privileges sitting around unused but available:

1. Access is requested when needed
2. Approvals can be required for sensitive actions
3. Privileges expire automatically
4. Each elevation is logged and attributable



Continuous least privilege **reduces what identities can do**.



Zero Standing Privileges reduce **when they can do it**.

Together, they dramatically shrink the attack surface and lower the risk of both accidental and intentional misuse.

How 1Password Privileged Access enables teams to implement least privilege

1Password Privileged Access turns least privilege from a periodic cleanup project into a continuous, automated control. Instead of relying on static roles or manual reviews, 1Password Privileged Access keeps access aligned with real usage across fast-moving cloud and hybrid environments.

1Password Privileged Access helps teams achieve this by:



Continuously analyzing entitlements to uncover privilege sprawl and unnecessary access



Mapping effective permissions to real behavior, resource sensitivity, and downstream risk



Neutralizing excessive privileges safely through reversible quarantines or Just-in-Time elevation

The result is a practical, maintainable least privilege posture that reduces exposure without disrupting workflows.



Automated privilege reduction

1Password Privileged Access continuously identifies unused or risky permissions across human users and non-human identities and provides pragmatic remediation options.



An adaptive access engine

1Password Privileged Access's policy engine adjusts as environments, resources, and responsibilities change. It incorporates business context, identity context, and risk signals to keep privileges aligned with actual needs.



Just-in-time access

Privileged access is granted only when needed and only for the duration of the task. Sensitive access can require approval; lower-risk access can be self-served with auditability built in.



Unified identity coverage

1Password Privileged Access applies continuous least privilege to everything—users, contractors, service accounts, pipelines, API keys, and more. Least privilege only works when it covers the entire identity landscape.



Ephemeral roles that disappear

Instead of relying on static IAM roles that persist forever, 1Password Privileged Access creates temporary roles dynamically. Once the access window closes, those roles vanish. That means attackers can't misuse roles that no longer exist.



Continuous monitoring and logging

Every request, approval, and privileged action is logged. This helps with compliance frameworks like SOC 2, ISO 27001, and HIPAA, and gives teams visibility into who did what, when, and why.

Preparing for what comes next: AI-driven identities

Identity is evolving. Human access still dominates today. Non-human identities are accelerating. And Agentic AI systems are approaching quickly.

The position for 1Password Privileged Access is simple.

Zero Standing Privilege for every identity, human or not. 1Password Privileged Access is most mature in human access today and expanding deeply into non-human identities. Our adaptive access engine is built to extend naturally into AI-driven identity models the moment they hit production scale. You get meaningful risk reduction now with a clear path to securing whatever identity types your organization adopts next.

Quick self-assessment

Take a moment to ask yourself where you stand on continuous least privilege with these high-level questions:

Continuous least privilege checklist

- ☐ Do you know how many identities currently have admin rights?
- ☐ Are unused permissions being removed automatically?
- ☐ Do any identities still retain standing privileged access?
- ☐ Are JML processes keeping access aligned with changing roles?
- ☐ Can users request temporary access without waiting on tickets?
- ☐ Are privileged actions logged and attributable across all identities?
- ☐ Do access policies adapt as cloud environments shift?



Want a deeper benchmark?

Our **ZSP checklist** outlines the top indicators that standing privileges may be putting your environment at risk.

Conclusion: guardrails for a moving environment

Most access failures aren't dramatic. They're the slow accumulation of permissions that no one revisited. Continuous least privilege provides a practical way to keep access aligned with reality and reduce exposure without slowing work down. Zero Standing Privilege builds on that by removing the always-on access attackers depend on.

If you're exploring how to bring these guardrails into your environment, our team can walk you through what effective implementation looks like in practice.

[See how 1Password Privileged Access works in practice](#)