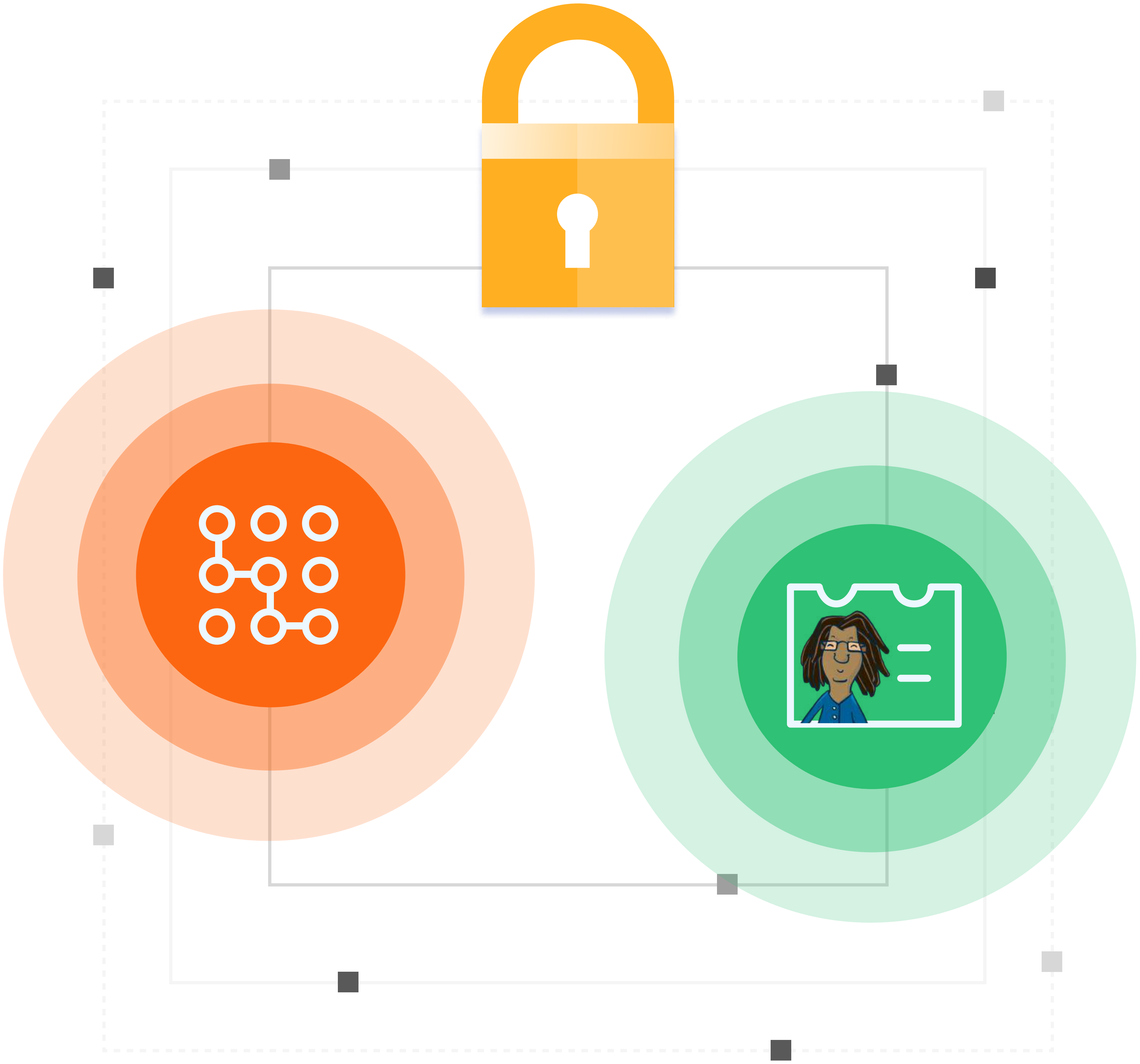
strongdm

REPORT

The Broken Promise of Least Privilege

How unused access, permissions, and resources are increasing your attack surface

Least Privilege: A Failed Promise



The Principle of Least Privilege. It's the idea that every person or thing in your environment should only be granted the baseline access and permissions required to do their jobs.

Logically, that makes sense. Why would you provide permissions or access beyond what an individual needs? Especially when the outcome can be catastrophic. In fact, 61% of all breaches involve using credentials to gain access to sensitive systems—so of course you'd want to limit the access to those systems.

Furthermore, an analysis of real-world access management and permission usage across 225 companies, ranging from small startups to large enterprises shows:

- 85% of credentials with privileges have not been used in the last 90 days
- Nearly 1 in 3 users with access to systems have not used that access in the last 90 days.
- 15% of resources available have not been accessed in the last 90 days.

The problem? The inability to audit, track, and understand how permissions are being used (or if they're used at all) has been non-existent. Until now. The findings are clear: organizations need visibility into privileged access and its usage to fully understand and address their total attack surface.

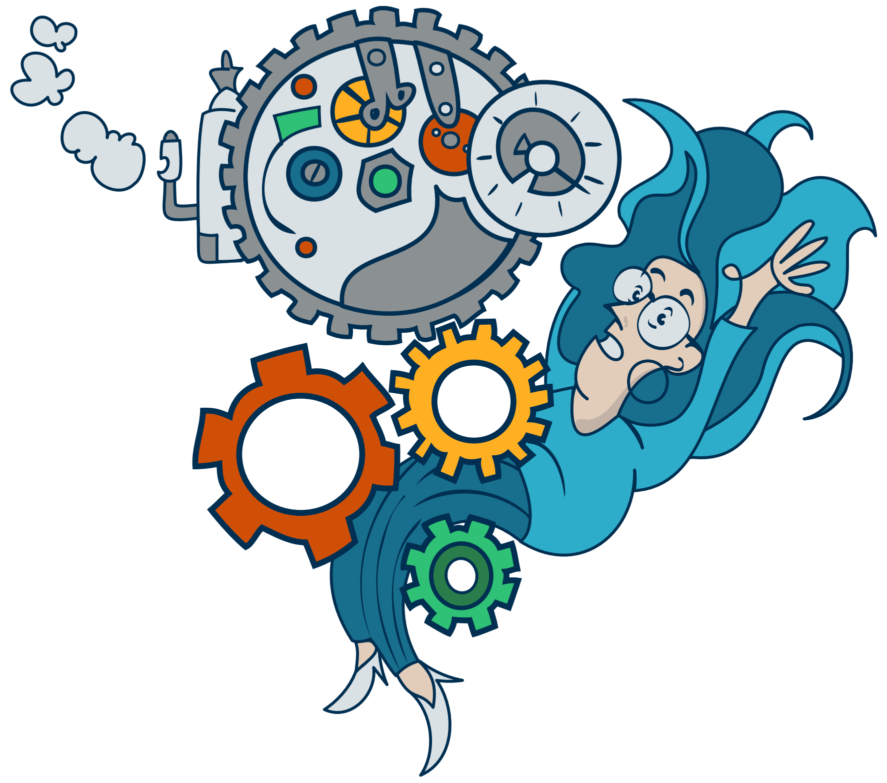
Breaking Down Access: Users, Resources, & Privileges

Users

Identities that have access to a particular system.

Resources

Infrastructure accessed by users.



Privileges

Identities with standing elevated permissions to specific resources.

This report breaks down access across three dimensions: users, resources, and privileges. Each is defined below, and helps to paint the broader picture—that the gaps in visibility into permission usage creates a significant attack surface for virtually every organization.

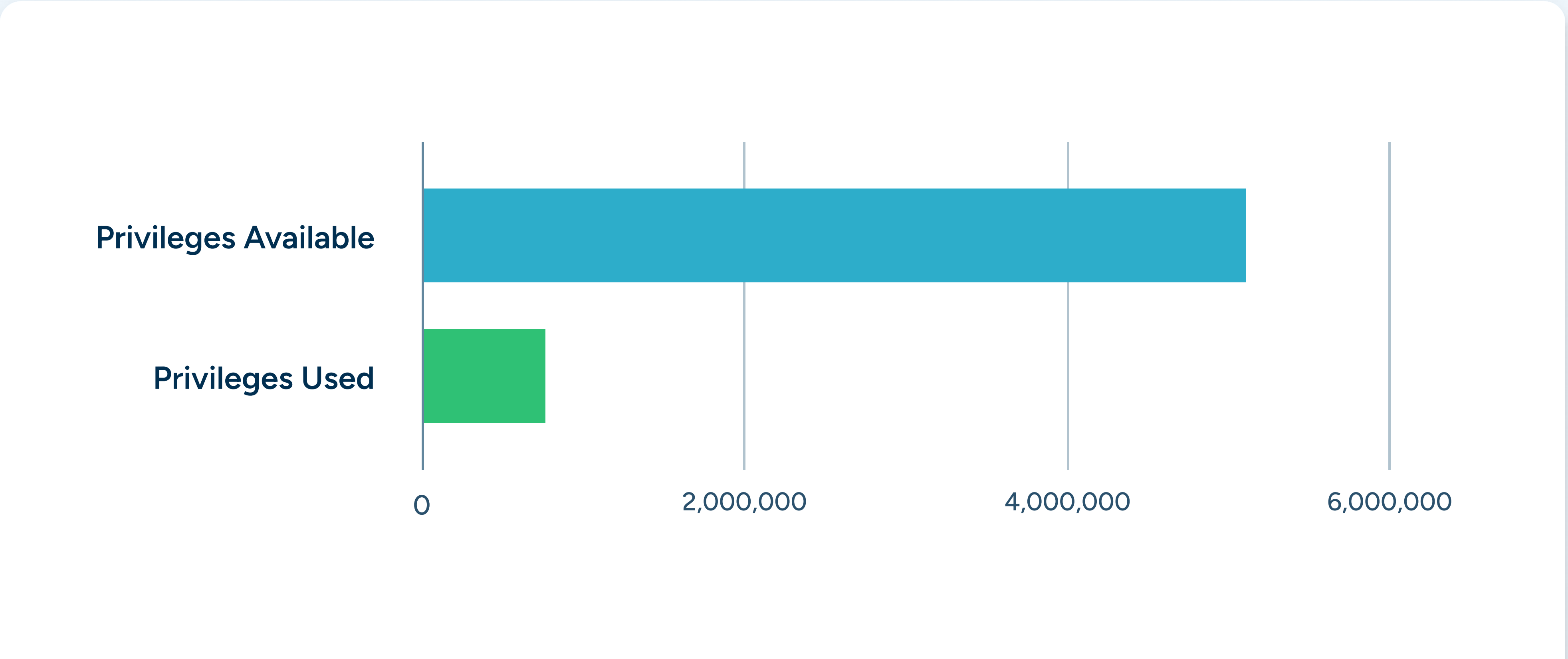
Unused Privileges, Unnecessary Risk

Privileges are a critical source of risk for every organization. Every user or identity that has elevated privileges can be a target for credential theft, credential stuffing, or ransomware, among others. It's no wonder that credentials are involved in nearly two-thirds of all breaches.

Even worse, the analysis shows that **85% of credentials with privileges have not been used in the last 90 days**. These are privileges that are available, unused, and ripe for the picking for bad actors. And this raises an obvious question: if the privileges have not been used in the last 90 days, are they even needed? Deprovisioning unused credentials with privileges is a substantial opportunity for security teams to reduce their overall attack surface.

The principle of least privilege requires that credentials have the bare minimum privileges possible to be productive—and yet 85% of privileges go unused. Not having visibility into privileges use across the entire stack has prevented security teams from taking remedial actions, and enabling them to truly take a least privilege approach. It's virtually impossible for security teams and admins to know which permissions are actually needed, and this type of visibility provides a data-driven approach to managing permissions based on real-world usage.

Existing Privileges Used in the Last 90 Days



85% of privileges have **not** been used in the last 90 days

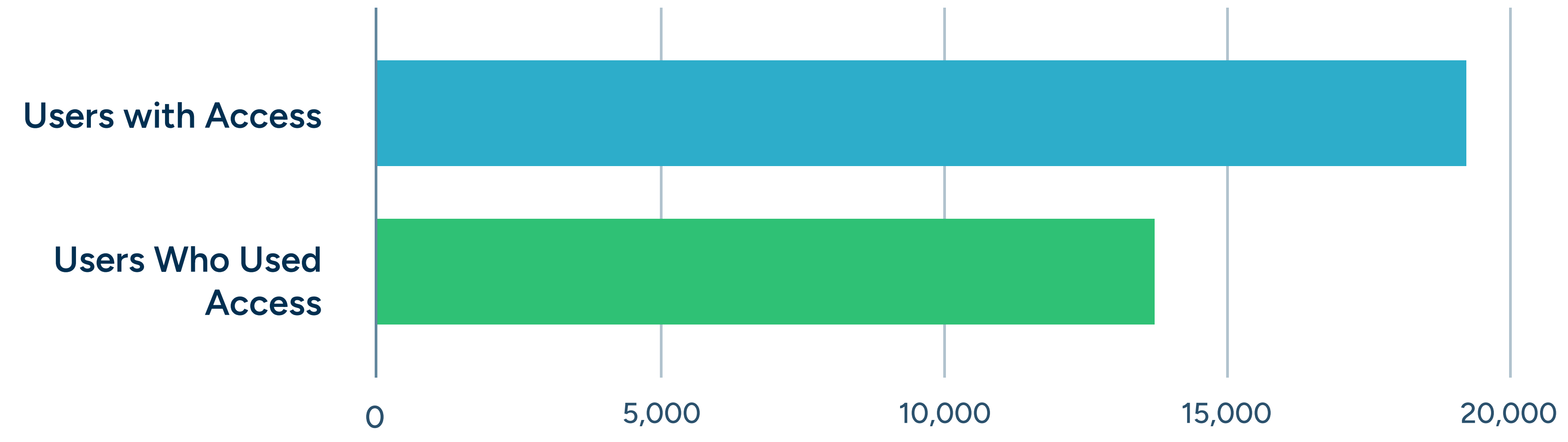
The Impact of Over Provisioning

It's not just privileges that go unused. In many cases, the complexity of provisioning access on an identity-based level results in users being over-provisioned, and having access they may not need.

In fact, the analysis shows that nearly **1 in 3 users have access to systems that they have not used in the last 90 days**. The heterogeneous nature of modern technology stacks has made it extremely difficult for security teams to track which credentials are being used, what systems are being accessed, and by whom. This lack of visibility has resulted in access to systems living in perpetuity, but not being used, and creating unnecessary risk.

Users having unnecessary access is the antithesis of least privilege, and presents a tangible opportunity for security teams to audit access usage across teams, and deprovision access that exists, but is not being used.

Access Used in the Last 90 Days



29% of users have not used their access in the last 90 days and could be an attack target

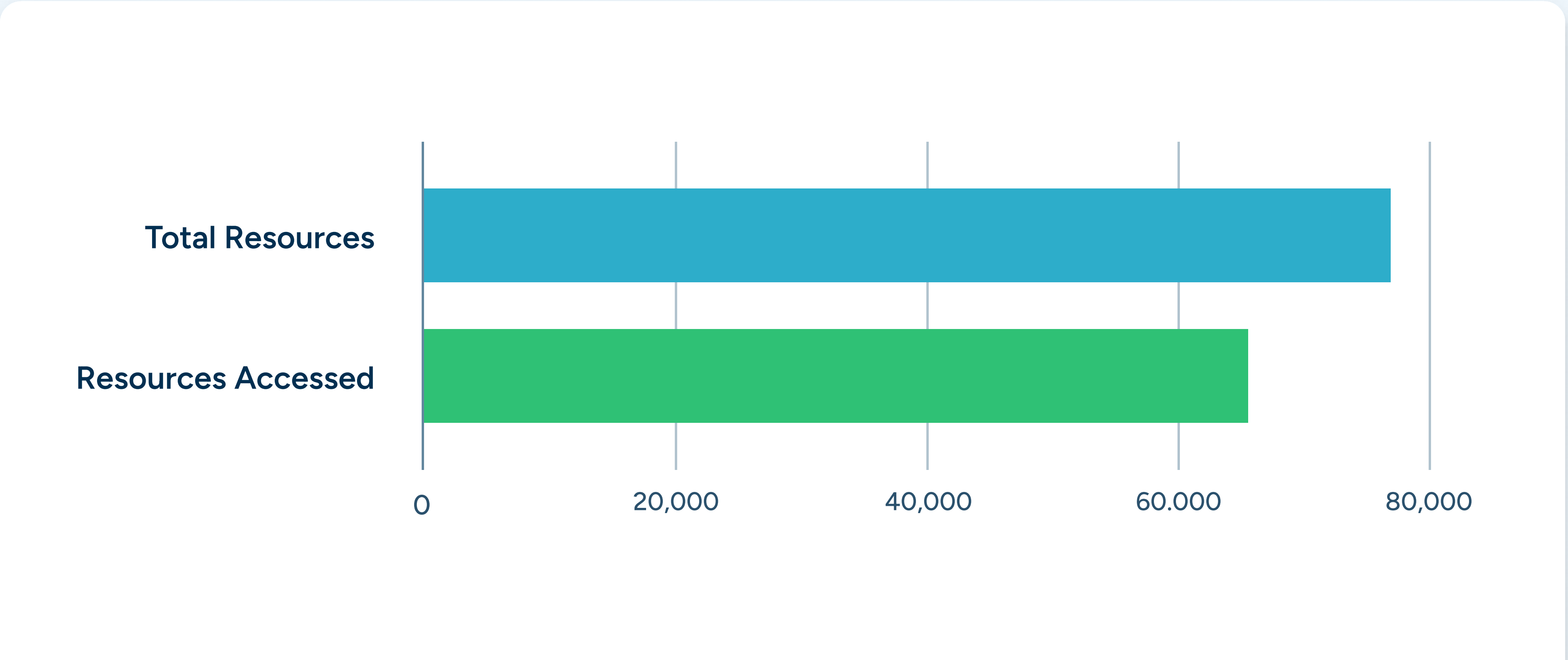
The Risk & Costs of Unused Resources

Getting visibility into access and usage extends beyond reducing risk. In this case, the analysis has shown that **15% of resources available have not been accessed in the last 90 days**.

Resources includes everything in your stack—databases, servers, cloud resources. These unused resources are not just a security risk, they may also be systems that can be deprovisioned or moved to a cheaper service to free up budget for other uses. Similar to unused privileges, the question at hand is, "If these resources haven't been touched in 90 days, do we still need them?"

In the case of the principle of least privilege, it's not only credentials to be concerned about, it's the systems that can be accessed by those credentials. Getting visibility into system usage gives security teams an opportunity to reduce their overall risk, while also **reducing costs by identifying unused resources.**

Resources Available in the Last 90 Days



15% of resources have **not** been accessed in the last 90 days

The Impact of Visibility on Least Privilege

The principle of least privilege is not a flawed methodology. It's just a methodology that has been impossible to embrace due to the inherent challenges by modern technology.

The challenge of getting visibility into access, privilege, and resource usage across your entire tech stack is daunting. But the benefits of doing so can be immense:

- Lower risk by removing unnecessary privileges
- Reduced attack surface by right-sizing user access
- Cost savings and reduced attack surface by deprecating unused resources

Your ultimate goal when implementing least privilege should be to effectively get to zero: zero unused privileges, zero over provisioning, and zero unused resources.

You should also aspire to have zero credentials exposed either to the end user or end-user system. This ensures that even where credentials may be over provisioned or have unnecessary access, the human element of risk is removed.

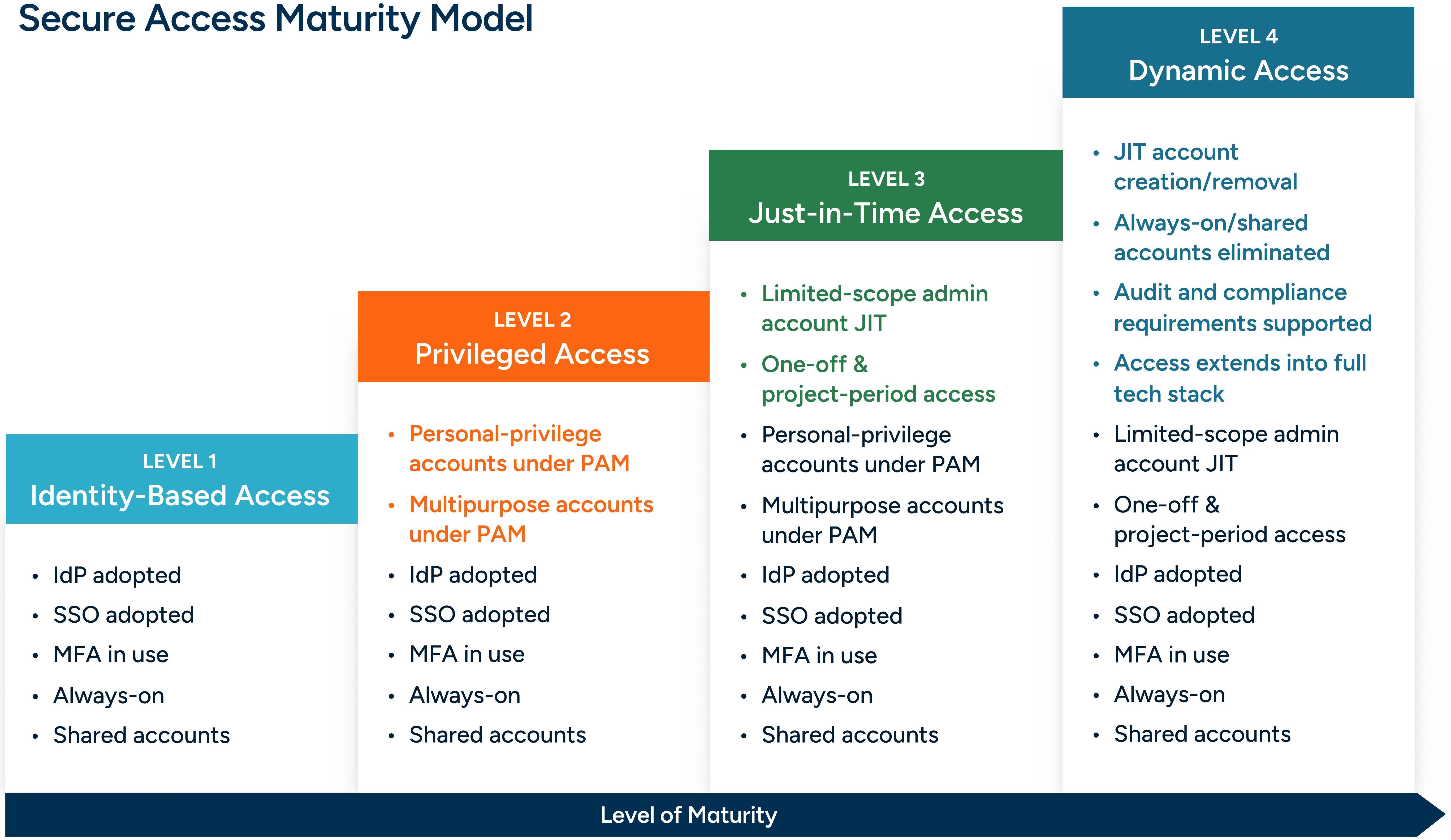
Getting to Least Privilege: StrongDM

When it comes to access management, least privilege is a critical stepping stone on your journey towards achieving zero standing privileges and dynamic access. But historically, it's been extremely difficult to get the visibility you need in order to implement least privilege as it was meant to be realized.

That's where StrongDM comes in. StrongDM provides the visibility you need to not only implement least privilege, but also enable you to progress on the Secure Access Maturity Model, a model designed to help you go from identity-based access to dynamic access management.

These changes don't happen overnight. Achieving true dynamic access is a journey, and being able to reduce risk, limit access to sensitive systems, and understand systems not being used, is an important milestone. StrongDM can help you get there.

Secure Access Maturity Model



LEVEL 1
Identity-Based Access

- IdP adopted
- SSO adopted
- MFA in use
- Always-on
- Shared accounts

LEVEL 2
Privileged Access

- Personal-privilege accounts under PAM
- Multipurpose accounts under PAM
- IdP adopted
- SSO adopted
- MFA in use
- Always-on
- Shared accounts

LEVEL 3
Just-in-Time Access

- Limited-scope admin account JIT
- One-off & project-period access
- Personal-privilege accounts under PAM
- Multipurpose accounts under PAM
- IdP adopted
- SSO adopted
- MFA in use
- Always-on
- Shared accounts

LEVEL 4
Dynamic Access

- JIT account creation/removal
- Always-on/shared accounts eliminated
- Audit and compliance requirements supported
- Access extends into full tech stack
- Limited-scope admin account JIT
- One-off & project-period access
- IdP adopted
- SSO adopted
- MFA in use
- Always-on
- Shared accounts

Methodology

This ebook was produced by StrongDM. It is an analysis of the real-world access patterns of 225 companies, ranging from small and medium organizations to large enterprises.

About StrongDM

StrongDM provides a dynamic access platform that gives every business secure, dynamic access controls that people love to use. Trusted by the Fortune 500 to fast-growing businesses like SoFi, Chime, Yext, and Better, StrongDM gives businesses the control and visibility they need at the speed they want, with one platform that works for every environment. Connect with us on LinkedIn, Twitter, Facebook, YouTube or head to www.strongdm.com to learn more.

Sign up today