# The Secure Access Maturity Model

It's time to level up your access management plan.

strongdm

# Table of Contents


## Introduction

How we access systems has changed dramatically since the ball dropped in 2000. Data centers have become relics of the pre-cloud era. Just about anyone can work from anywhere at any given time. You no longer need a key to get into your office and get on the network.

Why does this matter? It means how we manage access needs to change dramatically too.

61% of all breaches involve using credentials in order to gain access to sensitive systems. If someone told you, "3 out of 5 breaches happen because of credentials," you'd probably think to yourself, "We should probably re-evaluate how we're managing access."

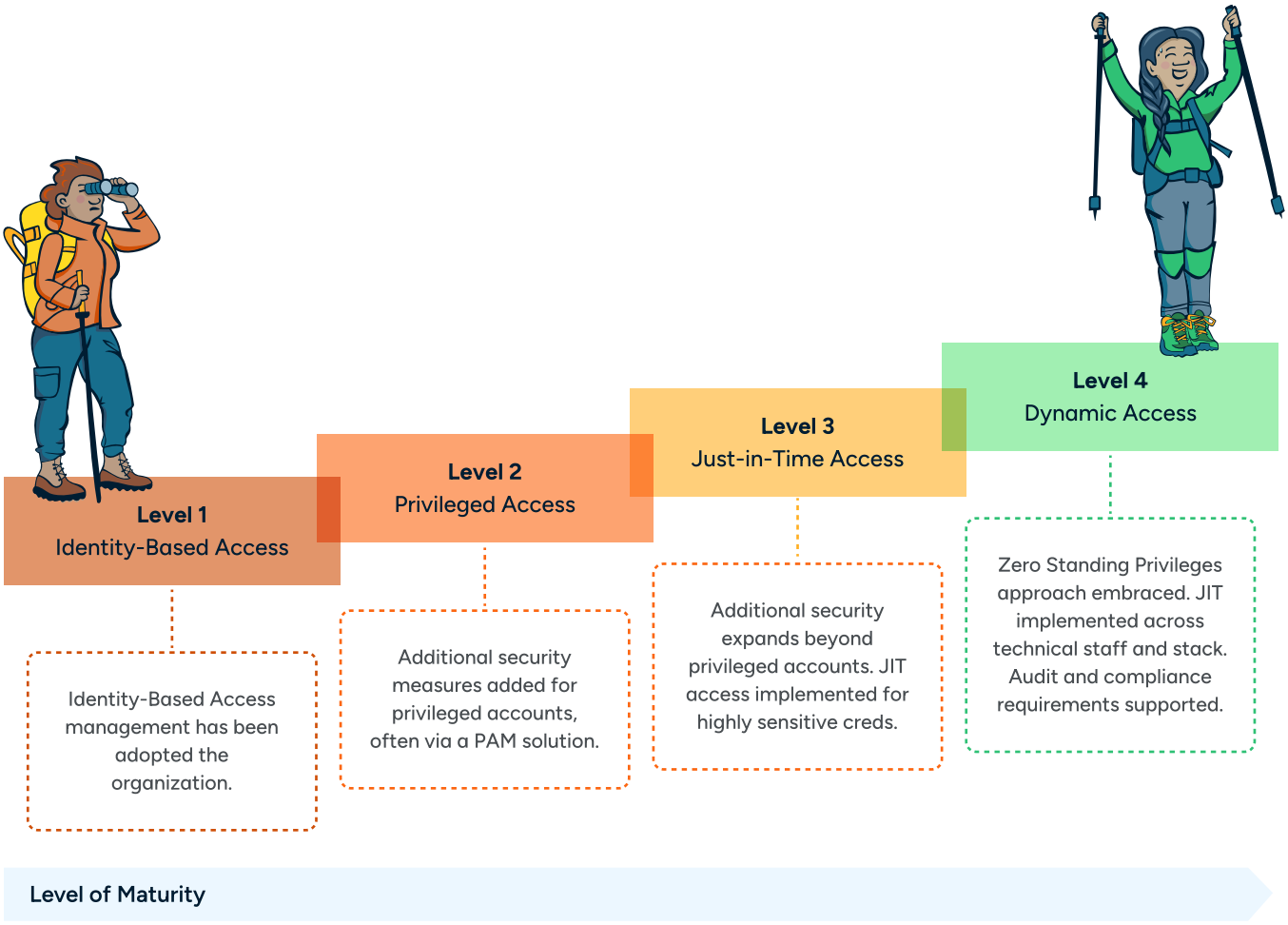
But when implementing additional layers of security requires your teams to take extra steps, it's easier said than done.

That's why we built the **Secure Access Maturity Model (SAMM).** It provides an action-oriented approach to reducing the threat posed by all of those credentials, while keeping the end-user experience in mind, because all of the security layers in the world don't matter if your end users don't embrace them. The model also provides a path that makes access secure while being easy to use for end users. It embraces the idea that security and the user experience are not mutually exclusive.

# The Secure Access Maturity Model

The Secure Access Maturity Model provides a logical progression for adopting and becoming more mature with your infrastructure access. Each stage contains critical pieces of access security that build on each other, to ultimately enable Dynamic Access Management–the ability to easily manage access to your entire stack in a safe, audible, and secure way.

Each of the four levels represents a significant benchmark in your access management journey (see image below).




The Secure Access Maturity Model is an additive approach to achieving Dynamic Access Management. That's a fancy way of saying that each level builds on the prior level. There is however, one exception—and that's the possibility to skip Level 2.

The ultimate goal is to have your access management become as dynamic as your organization. As people, roles, and technology change, you should have the ability to adjust access dynamically in order to support those changes. The Secure Access Maturity Model provides a path from identity-based access through to Dynamic Access and includes a breakdown of key components across the journey.

## Secure Access Maturity Model

| Level of Maturity | Identity-Based Access | Privileged Access Management | Just-in-Time Access | Dynamic Access Management |
|---|---|---|---|---|
| Shared Accounts | ✓ | ✓ | Eliminated | Eliminated |
| Always-On Access | ✓ | ✓ | Mostly Eliminated | Eliminated |
| MFA in Use | ✓ | ✓ | ✓ | ✓ |
| SSO Adopted | ✓ | ✓ | ✓ | ✓ |
| IdP Adopted | ✓ | ✓ | ✓ | ✓ |
| Privileged Accounts Protected | | ✓ | ✓ | ✓ |
| Time-Bound Access | | | ✓ | ✓ |
| Full-Stack Secured | | | ✓ | ✓ |
| Granular Auditing | | | | ✓ |
| Access Insights and Analytics | | | | ✓ |
| Identity Secured Across Entire Lifecycle | | | | ✓ |

Access Management Maturity

## Understanding the Maturity Model

The following sections break down each level of the Secure Access Maturity Model into:

- **Access Lifecycle:** The lifecycle of credentials typically seen at that level
- **Attributes:** The characteristics of access associated with that level
- **Technologies:** The common technology categories needed to support each level

By understanding these three dimensions, and where your organization fits within them, it's possible to find where you exist on the Secure Access Maturity Model, as well as identify the steps needed to level up.

## Breaking down the Secure Access Maturity Model

| Level of Maturity | Identity-Based Access | Privileged Access Management | Just-in-Time Access | Dynamic Access Management |
|---|---|---|---|---|
| Shared Accounts | ✓ | ✓ | Eliminated | Eliminated |
| Always-On Access | ✓ | ✓ | Mostly Eliminated | Eliminated |
| MFA in Use | ✓ | ✓ | ✓ | ✓ |
| SSO Adopted | ✓ | ✓ | ✓ | ✓ |
| IdP Adopted | ✓ | ✓ | ✓ | ✓ |
| Privileged Accounts Protected | | ✓ | ✓ | ✓ |
| Time-Bound Access | | | ✓ | ✓ |
| Full-Stack Secured | | | ✓ | ✓ |
| Granular Auditing | | | | ✓ |
| Access Insights and Analytics | | | | ✓ |
| Identity Secured Across Entire Lifecycle | | | | ✓ |
| | Access Management Maturity | | | |

## Level 1: Identity-Based Access

First and foremost, embracing Dynamic Access requires an identity-based approach to access management. This means that access to systems is defined at the individual or employee level, and access is provisioned based on the needs of that specific individual.

The criticality of this approach cannot be overstated. Without foundationally basing access on what each individual person in your organization needs, it becomes impossible to dynamically adjust access when turnover, role changes, or new technology adoption occurs.

| Attributes of Level 1 Access | |
|---|---|
| Always-On Access | Access tends to be "always on"—meaning credentials and accounts are primarily de-provisioned when an organizational change happens. |
| Shared and Team Accounts | Access to critical or complicated technologies may be shared across teams or groups of individuals. This often means your organization is unable to identify who is using each technology, complicating audits and other compliance requirements. |
| MFA... Sort of | Multi-factor authentication is required for some users and tools, but may not be required holistically. |

Level 1 is accompanied by a specific set of technologies that are typically required to enable each attribute. In this case, that includes an identity provider (IdP), single-sign on provider (SSO), and a tool to enable multi-factor authentication.

The combination of these technologies results in an access experience that is aligned to an identity and makes it simple to access web-based or custom applications, but is lacking when it comes to protecting accounts with elevated permissions, and that simplicity continues to be non-existent for accessing backend infrastructure or cloud service providers (CSPs).

| Technologies Often Used as Part of Level 1 | |
|---|---|
| IdP | Your organization has embraced an identity-based approach to access, using an identity provider to manage individuals. This can include technologies like MS Active Directory. |
| SSO | You're currently using single-sign on to manage access to applications. These technologies can include Okta and Google Single Sign-On. |
| MFA | Your organization has started to use multi-factor authentication for critical activities. This may include using tools like Google Authenticator or Duo.<br><br>Note: At Level 1, MFA adaptation may not be pervasive across the organization yet. |

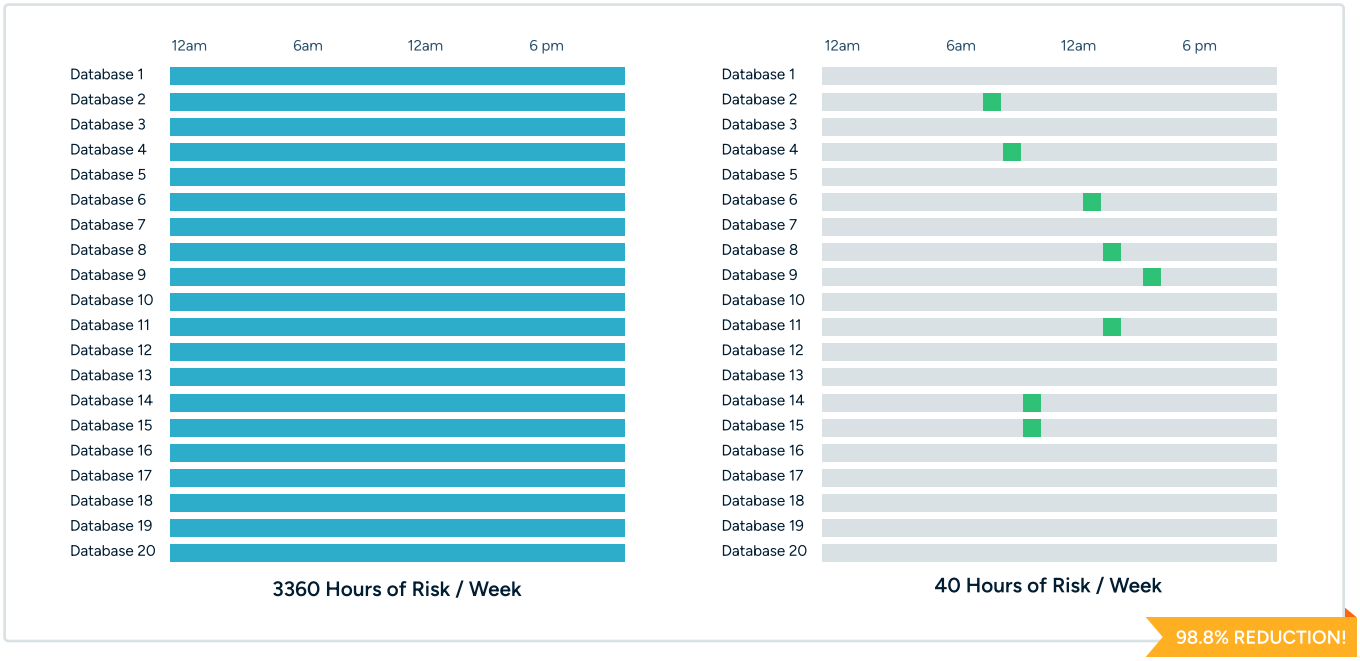
## Access Lifecycle: Always On

Organizations at Level 1 of the maturity model typically have an "always on" lifecycle for credentials. This is defined as credentials being created when someone joins an organization, or a new technology is adopted, and that credential exists in perpetuity until that individual leaves or the technology is retired.

## Why go from Identity-Based Access to Just-in-Time Access

The case for Just-in-Time Access is a question of risk. Credentials that exist in perpetuity can represent a substantial attack surface for organizations. The more that credentials are available, the higher the risk that they may be used as an entry point into your organization (see image below).

## Moving from Standing to JIT Access Greatly Reduces Risk




Maturing from standing to just-in-time access represents a significant reduction in your potential attack surface. Why? Credentials that don't exist when not in use can't be used against you.

## Level 2: Privileged Access

First and foremost, embracing Dynamic Access requires an identity-based approach to access management. This means that access to systems is defined at the individual or employee level, and access is provisioned based on the needs of that specific individual.

The criticality of this approach cannot be overstated. Without foundationally basing access on what each individual person in your organization needs, it becomes impossible to dynamically adjust access when turnover, role changes, or new technology adoption occurs.

## SAMM: Privileged Access Management

| Level of Maturity | Identity-Based Access | Privileged Access Management | Just-in-Time Access | Dynamic Access Management |
|---|---|---|---|---|
| Shared Accounts | ✓ | ✓ | Eliminated | Eliminated |
| Always-On Access | ✓ | ✓ | Mostly Eliminated | Eliminated |
| MFA in Use | ✓ | ✓ | ✓ | ✓ |
| SSO Adopted | ✓ | ✓ | ✓ | ✓ |
| IdP Adopted | ✓ | ✓ | ✓ | ✓ |
| Privileged Accounts Protected | | ✓ | ✓ | ✓ |
| Time-Bound Access | | | ✓ | ✓ |
| Full-Stack Secured | | | ✓ | ✓ |
| Granular Auditing | | | | ✓ |
| Access Insights and Analytics | | | | ✓ |
| Identity Secured Across Entire Lifecycle | | | | ✓ |
| | Access Management Maturity | | | |

Level 2 of the Secure Access Maturity Model is primarily focused on adding additional security measures for the most sensitive credentials. These typically include credentials with admin-level privileges or those with elevated privileges–basically any account that has direct access to sensitive data or settings.

### Attributes of Level 2 Access

| | |
|---|---|
| Privileged Access managed by PAM | Access tends to be "always on"—meaning credentials and accounts are primarily de-provisioned when an organizational change happens. |

## Privileged Access Management

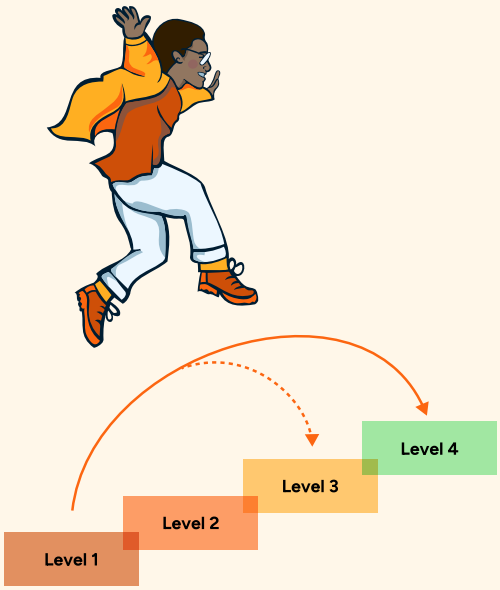
The main characteristic of Level 2 is the adoption of security measures that ensure accounts with elevated privileges have extra protections. This practice encompasses an entire technology category: Privileged Access Management (PAM).

PAM solutions establish policies and practices that ensure the security of sensitive data through the close management of administrative accounts. The idea is to add additional security layers for those accounts that represent the most risk in the case of a breach. The biggest challenge, however, is that the scope is very narrow–it only helps to protect privileged accounts, and in many cases, a limited set of resources.

| Technologies Often Used as Part of Level 2 | |
|---|---|
| Privilege Access Management Tool | Your organization has a PAM tool that secures and manages privileged accounts. In some cases, this may include tools that help on-board/off-board users and supports audits. |

In most organizations, elevated privileges exist beyond admin accounts. This could be a developer or engineer with access to production data, or even marketing teams with access to sensitive customer data. Levels 3 and 4 of the maturity model will help to close this gap.

In fact, it's possible to skip Level 2 of the maturity model altogether.




### Choose Your Own Adventure:

## Did you know you can skip Level 2? Here's how.

If your organization has achieved Level 1, but has not yet implemented a PAM solution, it's possible to jump directly to Level 3 or 4.

**Here's how:**

Requirement: No PAM solution implemented

Skipping Level 2: It's possible to avoid a privileged access approach entirely by making the upfront decision that all technical access is potentially privileged. That means accounting for all employees and their access by default, and skipping the step of only protecting privileged accounts.

## Access Lifecycle: Always On

Similar to Level 1 of the maturity model, Level 2 has an "always on" lifecycle for credentials. This is defined as credentials being created when someone joins an organization, or a new technology is adopted, and that credential exists in perpetuity until that individual leaves or the technology is retired.

## From Privileged Access to Dynamic Access

PAM has been the gold standard for protecting access for a long time–and it makes sense, because if you can't protect everyone or every tool, protect the people and tools that carry the highest risk. But that just isn't the case any more.

Modern organizations must extend protection of access to all employees and all tools. Any less and you're leaving yourself open to risk.

## Cloud Environments

## On-Premises

Traditional PAM

Not Supported by Traditional PAM

Traditional PAM environments leave critical gaps in your access management program, including cloud environments and new and modern tools. Dynamic Access Management (DAM) addresses this by providing just-in-time access to every technical employee, every tool in your stack, and ensuring that every action taken is logged and kept available for audits and investigations.

## Level 3: Just-In-Time (JIT) Access

Level 3 of the maturity model is where the temporal aspect of the access lifecycle begins to come into play. This is where organizations begin to adopt Just-in-Time Access (JIT), ultimately paving the way for Zero Standing Privileges (ZSP).

## SAMM: Just-in-Time Access

| Level of Maturity | Identity-Based Access | Privileged Access Management | Just-in-Time Access | Dynamic Access Management |
|---|---|---|---|---|
| Shared Accounts | ✓ | ✓ | Eliminated | Eliminated |
| Always-On Access | ✓ | ✓ | Mostly Eliminated | Eliminated |
| MFA in Use | ✓ | ✓ | ✓ | ✓ |
| SSO Adopted | ✓ | ✓ | ✓ | ✓ |
| IdP Adopted | ✓ | ✓ | ✓ | ✓ |
| Privileged Accounts Protected | | ✓ | ✓ | ✓ |
| Time-Bound Access | | | ✓ | ✓ |
| Full-Stack Secured | | | ✓ | ✓ |
| Granular Auditing | | | | ✓ |
| Access Insights and Analytics | | | | ✓ |
| Identity Secured Across Entire Lifecycle | | | | ✓ |
| | Access Management Maturity | | | |

## Defining Just-in-Time Access & Zero Standing Privileges

Often, there is confusion between Just-in-Time Access and Zero Standing Privileges. The easiest way to delineate between them is keep in mind that Just-in-Time Access is a component of Zero Standing Privileges.

- **Just-in-Time Access** – the ability to provision credentials the moment they're needed, and deprovision those credentials once they are not needed.
- **Zero Standing Privileges** – access management methodology that requires that no credentials exist in perpetuity, and all access is provided in a Just-in-Time manner.

In other words, you must have implemented Just-in-Time Access in order to fully embrace Zero Standing Privileges. This evolution is one of the key pillars of Level 4, Dynamic Access.

### Attributes of Level 3 Access

| | |
|---|---|
| Limited-Scope JIT: Admin Accounts | Just-in-Time access has started to be embraced, and is typically being prioritized for accounts with elevated privileges.<br><br>Lower priority access may still be "always on"—meaning credentials and accounts are primarily de-provisioned when an organizational change happens. |

When it comes to Level 3, it is key to remember that Just-in-Time access also represents an expanded scope in the types of accounts supported. Where privileged access only supported critical accounts, Just-in-Time access begins to lay the foundation for dynamic access across your technical teams.

| Technologies Often Used as Part of Level 3 | |
|---|---|
| Modern PAM or Cloud PAM | Your organization has adopted tools that enable dynamic provisioning and de-provisioning of credentials, and also provide secure access for a wider access of tools and environments than traditional PAM (such as CSPs, Kubernetes, etc.). |

### Access Lifecycle: Mixed

Level 3 has a combination of always-on access and just-in-time access. Fundamentally, it is a middle step on the path towards dynamic access, where you're ensuring that the credentials that pose the biggest risk in the case of a breach are provisioned dynamically, and credentials with less risk continue to exist in perpetuity.

### From JIT to DAM: Achieving Zero Standing Privileges and Making Access Work for You

The ultimate goal for access management is zero standing privileges. It's the idea that no access exists, except for the moments that it's needed. This is what Dynamic Access Management is all about.

But it doesn't stop there. DAM also focuses on providing the resources and tools you need to simplify how your end-users interact with and request access; keeps all access and activities easily on hand for audit and compliance purposes; and represents applying JIT access to everyone in your technical stack. Here's how you get there.

## Level 4: Dynamic Access

Level 4 is the pinnacle of access management. It embraces Zero Standing Privileges, the concept that credentials and access should only exist in the moments that it's needed. In other words, your access becomes dynamic. As people join and leave your organization, or technology is implemented or retired, you have full visibility, control, and auditability of the access to your systems.

The benefits of this approach are momentous, as it essentially eliminates the risk posed by always-on credentials, including specific attacks like credential stuffing (if no credentials exist, what do you stuff?).

## SAMM: Dynamic Access

| Level of Maturity | Identity-Based Access | Privileged Access Management | Just-in-Time Access | Dynamic Access Management |
|---|---|---|---|---|
| Shared Accounts | ✓ | ✓ | Eliminated | Eliminated |
| Always-On Access | ✓ | ✓ | Mostly Eliminated | Eliminated |
| MFA in Use | ✓ | ✓ | ✓ | ✓ |
| SSO Adopted | ✓ | ✓ | ✓ | ✓ |
| IdP Adopted | ✓ | ✓ | ✓ | ✓ |
| Privileged Accounts Protected | | ✓ | ✓ | ✓ |
| Time-Bound Access | | | ✓ | ✓ |
| Full-Stack Secured | | | ✓ | ✓ |
| Granular Auditing | | | | ✓ |
| Access Insights and Analytics | | | | ✓ |
| Identity Secured Across Entire Lifecycle | | | | ✓ |

**Access Management Maturity**

## Technologies Often Used as Part of Level 1

| | |
|---|---|
| Just-in-Time Account Creation and Removal | Access to key systems only exists at the moment it's needed, and is deprovisioned as soon as work is complete. |
| Always On and Shared accounts fully eliminated | Credentials that live in perpetuity are eliminated, and the organization no longer uses multi-purpose accounts. |
| Audit and compliance requirements supported | Reporting and auditing is streamlined, making it easy to ask "who did what, when, and where?" |
| Access management extends to full tech stack | Access across technologies is simplified and streamlined, regardless of the heterogeneity of your tech stack. |
| Access workflows simplify provisioning and deprovisioning | The ability for end users to request access is simple, fast, and can be automated if appropriate. |

Level 4 requires the capability to provision and deprovision access to infrastructure in real time, the ability to understand if a particular individual actually needs that access, and the ability to monitor everything that individual did while that access existed.

| Technologies Often Used as Part of Level 4 | |
|---|---|
| Dynamic Access Management | Simply put: Access that is as dynamic as your organization.<br><br>It is easy to provide, revoke, and manage access across your employee base and tech stack. Your security breach surface has shrunk dramatically, as access to systems becomes ephemeral. |

## Access Lifecycle: Just-in-Time & Zero Standing Privileges

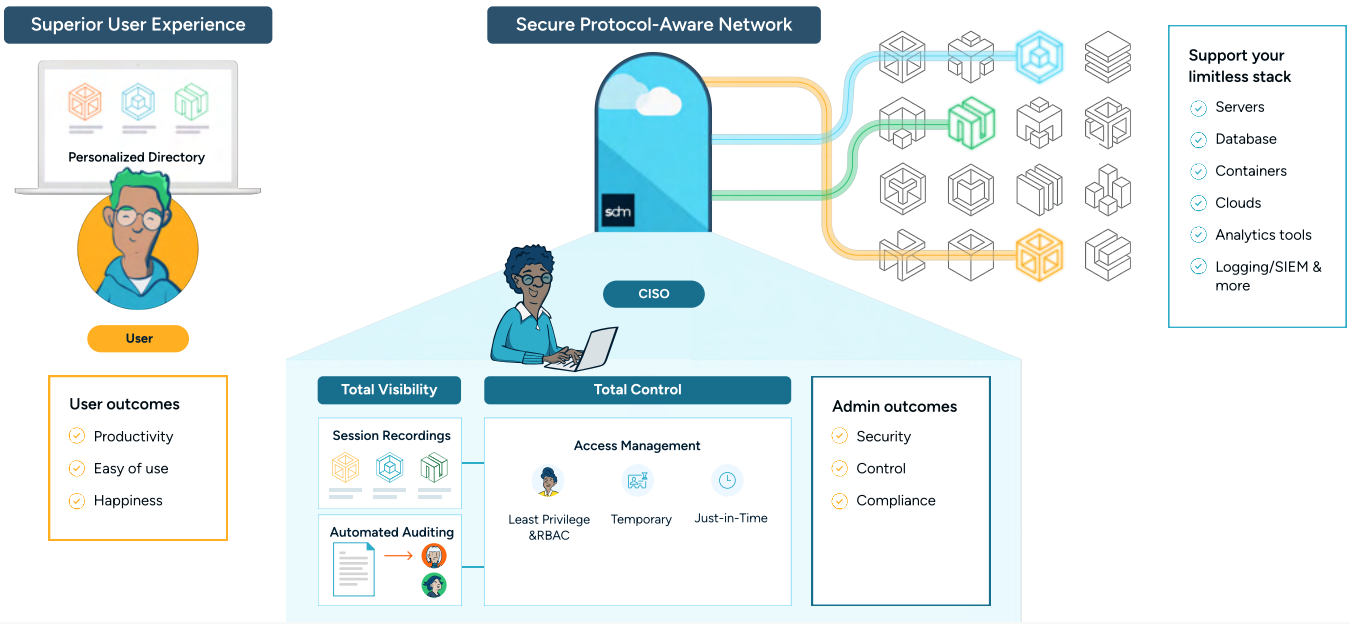
Level 4 requires that access is only provided using Just-in-Time policies, and always-on credentials are fully eliminated. That means credentials *only* exist on a temporary basis, are hidden from users, and activity on systems is tracked closely.

# StrongDM: Helping You Achieve Dynamic Access Management

There's no trick or secret to reaching Level 4 and Dynamic Access. It just requires re-evaluating your current approaches to infrastructure access, and then updating it to account for modern challenges, such as hybrid, multi-cloud, and remote work.

One of the biggest challenges you'll face on this journey is the inability to streamline access across backend infrastructure and cloud service providers. That's because every tool in your stack is focused on doing what it does best—for example, databases are focused on managing data, not necessarily ensuring that they have access workflows that provide simplicity to end users and organizations.

That's where tools like StrongDM come in. They take the hard work you've done at Level 1–moving to an identity-based approach to access–and extend it to your infrastructure and cloud environments. They make accessing infrastructure as simple as using an SSO provider for any technical employee that needs access to your stack.



StrongDM provides a number of benefits for your organization, across teams:

- **DevOps:** DevOps teams can provision and deprovision access to specific instances, servers, or databases, in a matter of clicks.
- **Security & Compliance:** Security and compliance teams can gain full visibility into "who did what when" on each system, including video playback of what individual users have executed on specific systems. For compliance, full records are kept of "who was in each system and what were they doing" at any given point in time.
- **Admins:** Access to critical infrastructure can be granted and revoked quickly and easily, greatly simplifying user onboarding and offboarding, provisioning for third parties, and the ability to provide access for a specified period of time. Users, roles, and access are easily managed via an Admin UI (CLI available as well).

These benefits are the result of addressing the access issues created from all of the different technologies, different roles, different levels of permissions, and evolving technologies in your stack. StrongDM removes the need to manually address each of these challenges, giving you a clear path to achieving Level 4 and Dynamic Access. To learn more or request a demo, please visit www.StrongDM.com/get-a-demo.

## Conclusion

61% of all breaches involve using credentials in order to gain access to sensitive systems.

The days of badging into an office in order to get onto the corporate network are long gone. And as the technologies we embrace continue to evolve, the ways we access these technologies will need to follow suit. That's the only way that it becomes possible to reduce that 61%, and ensure that access to systems is as dynamic as your organization.

strongdm

StrongDM is a Dynamic Access Management platform that centralizes privileged access for all technical users to every resource in your infrastructure on-premises and in the cloud. Security teams have complete visibility into every keystroke to enhance security and compliance postures and end users enjoy fast intuitive access to resources they need. Connect with us on LinkedIn, X (formerly Twitter), Facebook, YouTube or head to www.strongdm.com to learn more.