The Secure Access Maturity Model

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

strongdm

Table of Contents

Introduction

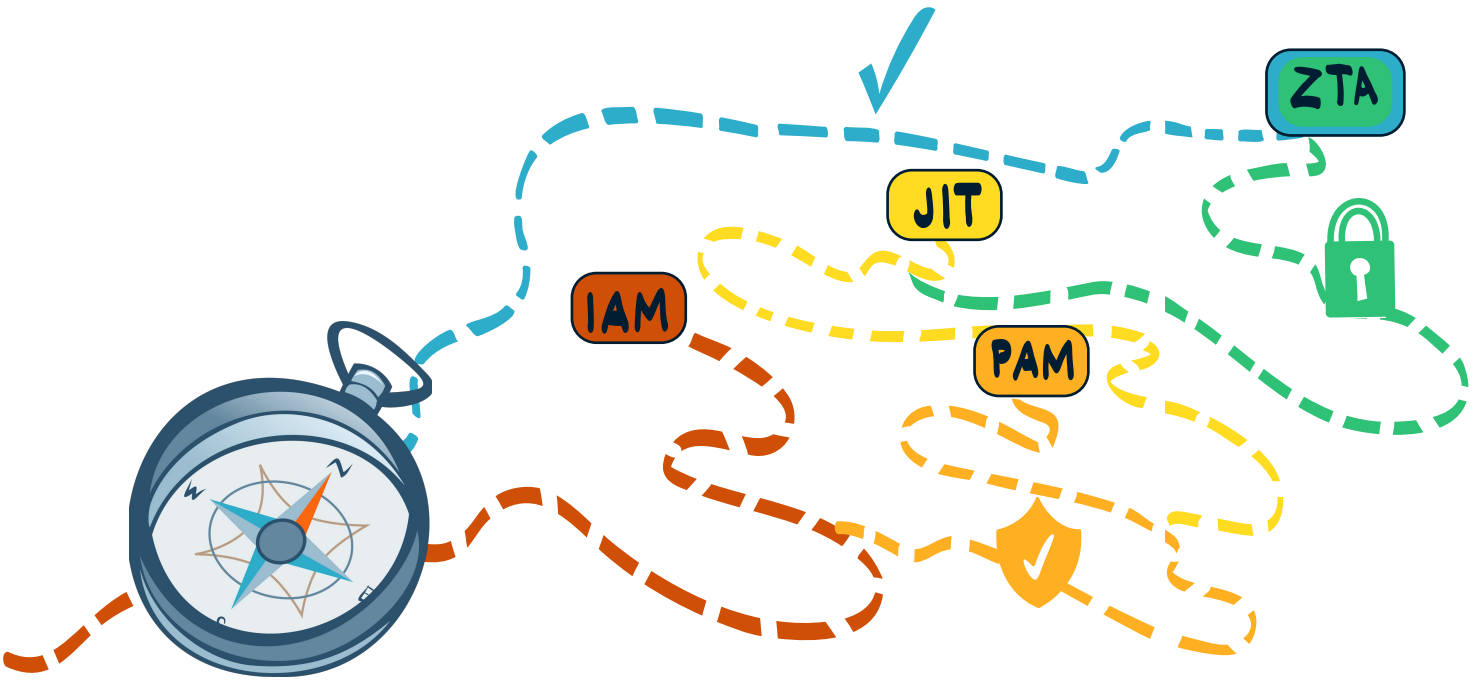
How we access systems has changed dramatically since the ball dropped in 2000. Data centers have become relics of the pre-cloud era. Just about anyone can work from anywhere at any given time. You no longer need a key to get into your office and get on the network.

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.

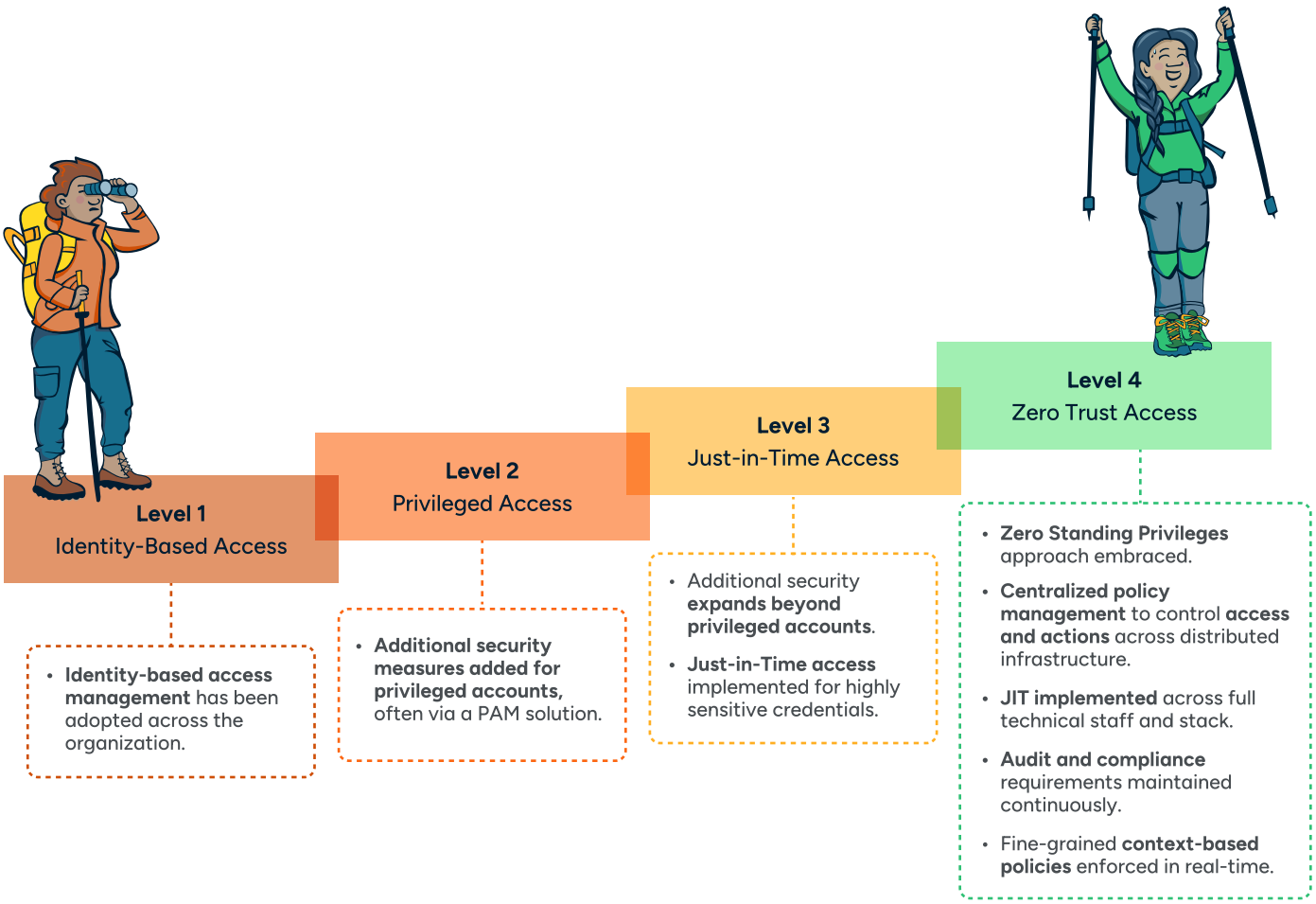
That's why we built the **Secure Access Maturity Model.** It provides an action-oriented approach to reducing the threat posed by all of those credentials, while keeping the end-user experience in mind, because all of the security layers in the world don't matter if your end users don't embrace them. 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 Zero Trust Access–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 Zero Trust Access. That's a fancy way of saying that each level builds on the prior level. However, for organizations just getting started with identity-based or privileged access management, it is possible to skip directly to Level 3: Just-in-Time access or Level 4: Zero Trust access.

The ultimate goal is for your access management to become as dynamic as your organization. As people, roles, and technology change, you should be able to adjust access dynamically to support those changes. The Secure Access Maturity Model provides a path from identity-based access to Zero-Trust 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	Zero Trust 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			✓	✓
Continuous Compliance			✓	✓
Access Insights and Analytics			✓	✓
Fine-Grained **Context-Based Policies** Enforced in Real-Time			✓	✓

Access Management Maturity

Understanding the Maturity Model

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

- **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, you can determine your current position on the Secure Access Maturity Model and identify the steps needed to level up.

It's important to recognize that different teams or parts of your technology stack may fall into different levels of the Secure Access Maturity Model—and that's perfectly okay. Each team or system within your organization may have unique requirements, constraints, and priorities influencing its current access maturity level. This variation is natural due to resource/data sensitivity, end-user onboarding, or differing security needs.

By acknowledging these differences, you can tailor your approach to improving access maturity in a more effective and pragmatic way. It allows you to allocate resources strategically, focusing on areas where enhancements will have the most significant impact or where risks are highest. Embracing this variability ensures that each part of your organization progresses at a pace that aligns with its specific context while contributing to the overall security posture. The goal isn't uniformity at all costs but rather a cohesive strategy that gradually elevates the entire organization's secure access maturity.

Level 1

Identity-Based Access

First and foremost, embracing Zero Trust 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 that specific individual's needs.

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.

Maturity Stage: Identity-Based Access

Level of Maturity	Identity-Based Access	Privileged Access Management	Just-in-Time Access	Zero Trust 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			✓	✓
Continuous Compliance			✓	✓
Access Insights and Analytics			✓	✓
Fine-Grained **Context-Based Policies** Enforced in Real-Time			✓	✓

Access Management Maturity

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 occurs.
Shared and Team Accounts	Access to critical or complicated technologies may be shared across teams or groups of individuals. This often means your organization cannot 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 typically required to enable each attribute. In this case, that includes an identity provider (IdP), a 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. However, it lacks protection for accounts with elevated permissions, and 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 technologies, such as Okta and Google Single Sign-On, to manage application access.
MFA	Your organization has started to use multi-factor authentication for criticalactivities. This may include using tools like Google Authenticator or Duo. 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? Access grants that don't exist when not in use can't be used against you.

Level 2

Privileged Access

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.

Maturity Stage: Privileged Access Management

Level of Maturity	Identity-Based Access	Privileged Access Management	Just-in-Time Access	Zero Trust 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			✓	✓
Continuous Compliance			✓	✓
Access Insights and Analytics			✓	✓
Fine-Grained **Context-Based Policies** Enforced in Real-Time			✓	✓

Access Management Maturity

Attributes of Level 2: Privileged Access

Privileged Access managed by PAM	Accounts with elevated privileges may have additional security measures in place, typically via a privileged access management (PAM) tool.

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 a 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 a breach. Common features of PAM solutions include **session recording** and **session management**, which enhance oversight and control over privileged sessions.

- **Session Recording**: This feature allows organizations to monitor and record activities performed during privileged sessions. By capturing detailed logs and video recordings of user actions, organizations can create an audit trail that is invaluable for compliance, forensic analysis, and detecting suspicious behavior.
- **Session Management**: PAM tools allow administrators to control and manage privileged sessions in real time. They can initiate, monitor, pause, or terminate sessions as needed. This level of control helps prevent unauthorized activities and enables immediate response to potential security incidents.

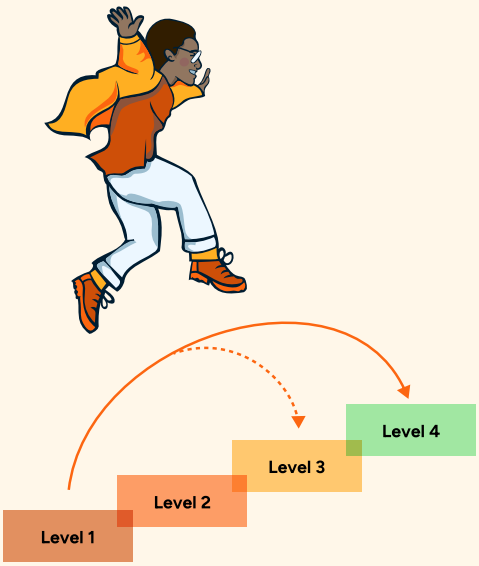
However, the biggest challenge is that the scope is very narrow—it only helps to protect privileged accounts, and in many cases, a limited set of resources.

Technologies Often Used as Part of Level 2

Privileged 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 many organizations, elevated privileges extend beyond traditional admin accounts. This includes developers, engineers with access to production data, and even marketing teams handling sensitive customer information or research teams handling patient data. By using StrongDM to manage privileged access, you broaden the scope of protected resources and users, ensuring that extra security measures are applied wherever elevated privileges exist. While this enhances security by covering more accounts and resources, it may still fall under Level 2 of the maturity model if JIT access has not been implemented.

Levels 3 and 4 of the maturity model will help to close this gap by introducing JIT access and more granular, context-aware policies. These advanced practices further reduce risk by ensuring that users have the minimum necessary access only when they need it.



Choose Your Own Adventure

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

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

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

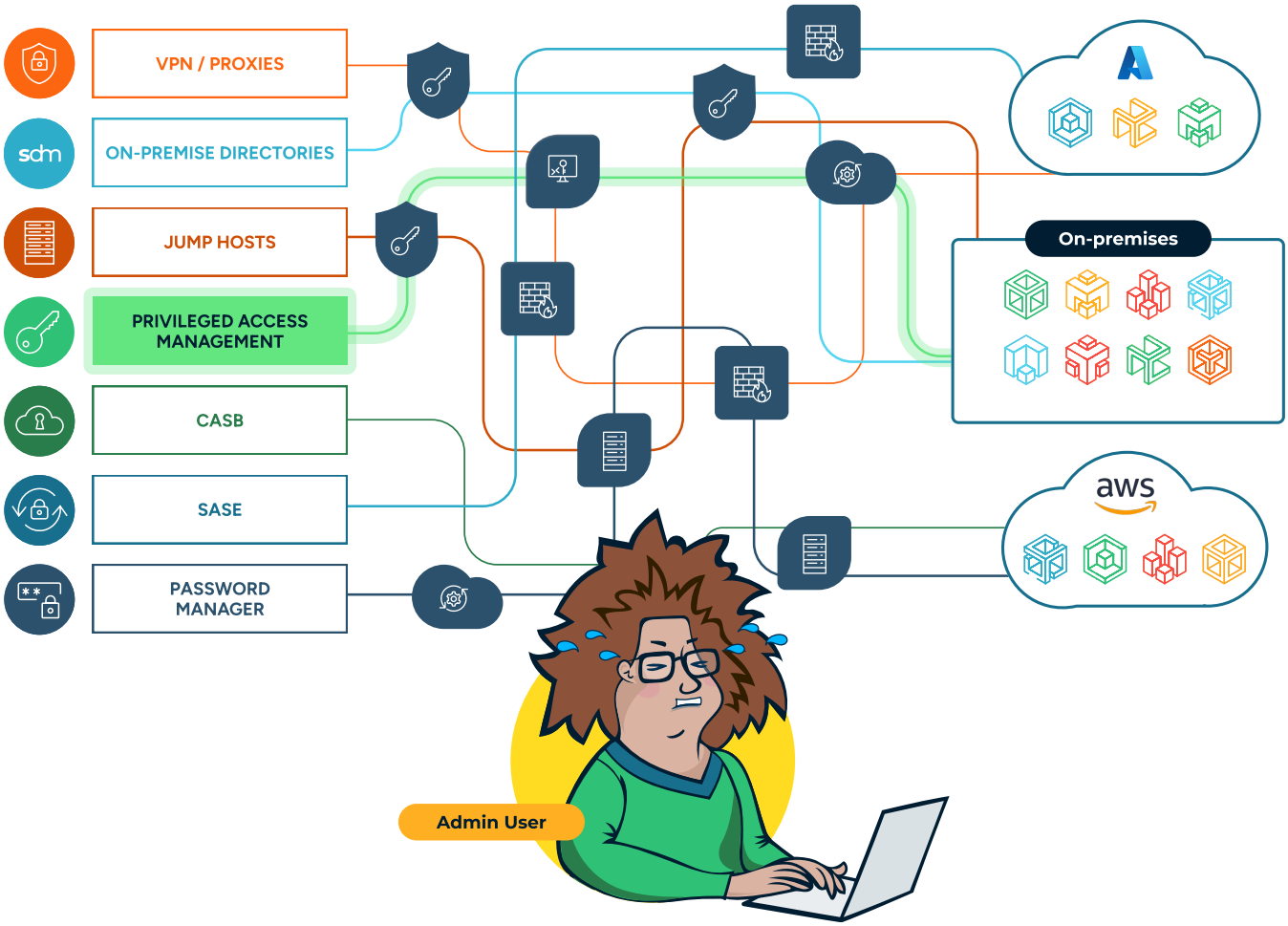
Like Level 1 of the maturity model, Level 2 has an "always on" lifecycle for credentials. This is defined as credentials being created when someone joins an organization or a new technology is adopted, and that credential exists in perpetuity until that individual leaves or the technology is retired.

From Privileged Access to Zero Trust Access

PAM (Privileged Access Management) tools have long been the gold standard for protecting access. This makes sense because if you can't protect everyone or every tool, protect the people and tools with the highest risk. But that just isn't the case anymore.

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

Traditional PAM environments leave critical gaps in your access management program, including cloud environments and new and modern tools. Zero Trust PAM tools address this by providing Just-In-Time access to every technical employee, and 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).

Maturity Stage: Just-in-Time Access

Level of Maturity	Identity-Based Access	Privileged Access Management	Just-in-Time Access	Zero Trust 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			✓	✓
Continuous Compliance			✓	✓
Access Insights and Analytics			✓	✓
Fine-Grained **Context-Based Policies** Enforced in Real-Time			✓	✓

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 to keep in mind that Just-in-Time access is a component of Zero Standing Privileges.

Just-in-Time access allows users to provision credentials when needed and de-provision them once they are no longer required. This approach minimizes the window of opportunity for unauthorized access and reduces the risk associated with long-lived credentials.

Benefits:

- **Reduced Attack Surface**: By limiting the time credentials exist, malicious actors have fewer opportunities to exploit them.
- **Improved Compliance**: Temporary access aligns with compliance requirements that mandate least privilege and access controls.
- **Operational Efficiency**: Automating access provisioning and deprovisioning can streamline workflows and reduce administrative overhead.

Zero Standing Privileges is an access management methodology that requires that no credentials exist in perpetuity; all access is provided in a Just-in-Time manner. It represents a more comprehensive adoption of JIT principles across the entire organization.

Benefits:

- **Maximum Security Posture**: Eliminating permanent credentials greatly minimizes the risk of credential misuse or theft.
- **Adaptive Access Control**: Access decisions are made in real-time based on current context and policies.
- **Simplified Credential Management**: Reduces the need to manage and rotate long-lived credentials.

Attributes of Level 3 Access

Limited-Scope JIT: Admin Accounts	Just-in-time access is typically prioritized for accounts with elevated privileges or access to sensitive or regulated data. Lower priority access may still be "always on," meaning credentials and accounts are primarily de-provisioned when an organizational change occurs.
Access Workflows Simplify Provisioning and Deprovisioning	End-users can request and obtain access quickly and efficiently, with the process being simple, fast, and automated where appropriate, enhancing productivity and security.

Regarding 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 supports 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 provide secure access to a wider range of tools and environments than traditional PAM (such as Clouds, 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 Zero Trust Access: Achieving Zero Standing Privileges and Enforcing Context-Based Policies

The ultimate goal for access management is **Zero-Trust access**, which prioritizes zero-standing privileges. Zero-trust access management means that no access exists except for the needed moments and only when the context surrounding the request deems it appropriate.

But it doesn't stop there. Zero Trust Access also incorporates **context-based policy enforcement** and **policy-based action control**, enhancing security by dynamically adjusting access permissions based on real-time contextual information and controlling the actions users can perform once access is granted.

Context-Based Policy Enforcement

Context-based policy enforcement ensures that access decisions are not solely based on static credentials or roles but also dynamic attributes such as:

- **User Identity and Role**: Verifies that the user's role aligns with the access request.
- **Time of Access**: Restricts access to specific times of the day or week.
- **Location**: Considers geographic location or network origin of the request.
- **Device Posture**: Checks the security status of the device being used (e.g., OS version, antivirus status).
- **Behavior Patterns**: Monitors user behavior for anomalies compared to established patterns.

By evaluating these factors (and any others you would like to include) in real-time, organizations can enforce fine-grained policies that grant access only when all contextual conditions meet predefined security criteria. For example, a user can access a resource only during business hours from a safe corporate device within the office network.

Policy-Based Action Control*

Policy-based action control goes beyond granting or denying access—it defines what actions a user can perform once access is granted. This includes:

- **Command Restrictions**: Limiting the commands or queries a user can execute.
- **Data Access Levels**: Allowing read-only access versus read-write permissions.
- **Session Controls**: Setting time limits on sessions or requiring re-authentication for sensitive actions.
- **Transaction Monitoring**: Tracking specific activities within a session for compliance and security.

By implementing these controls, organizations can minimize the risk of unauthorized activities, data exfiltration, or accidental damage. For instance, an engineer might have access to view production databases but cannot modify data without additional approval.

Bringing It All Together

Zero Trust access provides the resources and tools to simplify how your end-users interact with and request access while ensuring that all access is appropriate and secure. This approach:

- **Applies JIT Access Universally**: Extends Just-in-Time access to everyone in your technical stack, not just privileged users.
- **Enhances Audit and Compliance**: Keeps all access and activities easily available for audit purposes, meeting continuous compliance requirements.
- **Adapts in Real Time**: It enforces fine-grained, context-based policies and action controls dynamically, adjusting to changing conditions and threats.

By integrating context-based policy enforcement and policy-based action control, organizations fully embrace Zero Trust access. This comprehensive strategy ensures that access is granted only when necessary, under the right conditions, and with appropriate limitations on user actions—making access work for you in the most secure and efficient way possible.

*StrongDM supports action control for Postgres databases, with additional resource types coming in 2025.

Level 4

Zero Trust 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 they're 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 audibility of the access to your systems.

This approach delivers big benefits, eliminating the risk of always-on credentials, including specific attacks like credential stuffing.

Maturity Stage: Zero Trust Access

Level of Maturity	Identity-Based Access	Privileged Access Management	Just-in-Time Access	Zero Trust 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			✓	✓
Continuous Compliance			✓	✓
Access Insights and Analytics			✓	✓
Fine-Grained **Context-Based Policies** Enforced in Real-Time			✓	✓

Access Management Maturity

Attributes of Level 4: Zero Trust Access

Feature	Description
Zero Standing Privileges Embraced	No access rights persist beyond their immediate need; all credentials are temporary and provisioned on demand, minimizing the attack surface.
Centralized Policy Management	A unified system controls and enforces access policies and user actions across all distributed and hybrid infrastructures, ensuring consistency and compliance.
Just-in-Time Access Across Full Staff and Stack	Just-in-Time (JIT) access is implemented universally across the entire technical staff and technology stack, providing minimal necessary access precisely when needed.
Audit and Compliance Requirements Maintained Continuously	Real-time monitoring, logging, and reporting of all access events ensure continuous compliance and streamline audit processes, making it easy to answer "who did what, when, and where?"
Fine-Grained Context-Based Policies Enforced in Real-Time	Access controls dynamically adjust based on real-time context such as user identity, role, location, device health, and behavior patterns, enhancing security and compliance.
Always-On and Shared Accounts Fully Eliminated	Persistent credentials and multi-purpose accounts are removed, eliminating long-lived access and reducing security risks associated with shared accounts.
Access Management Extends to Full Tech Stack	Access across all technologies is simplified and streamlined, regardless of the heterogeneity of your tech stack, ensuring consistent security policies and practices.

Level 4 emphasizes enforcing **fine-grained, context-based policies in real-time**, dynamically adjusting access controls based on factors like user identity, role, location, device health, and behavior patterns. This ensures that access is granted only when appropriate and under the right conditions. Continuous monitoring, logging, and reporting are maintained to **meet audit and compliance requirements**, providing full visibility into all access events and actions performed by individuals while access existed. Additionally, eliminating always-on and shared accounts enhances security by removing persistent credentials and reducing risks associated with shared access. **Access workflows are streamlined**, simplifying provisioning and deprovisioning processes, allowing end-users to request and obtain access quickly and efficiently, often through automation.

Technologies Often Used as Part of Level 4	
Zero Trust Access Management	An access management solution that dynamically provides Just-in-Time, context-aware access to resources while eliminating persistent privileges and continuously verifying user identities to minimize security risks. Your security breach surface has shrunk dramatically, as system access becomes ephemeral.

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

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

Prioritizing Your Journey to Zero Trust Access

Implementing Zero Trust Access across your entire organization is a significant undertaking. Often, organizations get stuck at the very first step: creating a full inventory of all resources, teams, and roles. This exhaustive process can be time-consuming and may delay the implementation of critical security measures. Instead of aiming for completeness from the outset, a more pragmatic approach is to **start small and prioritize**.

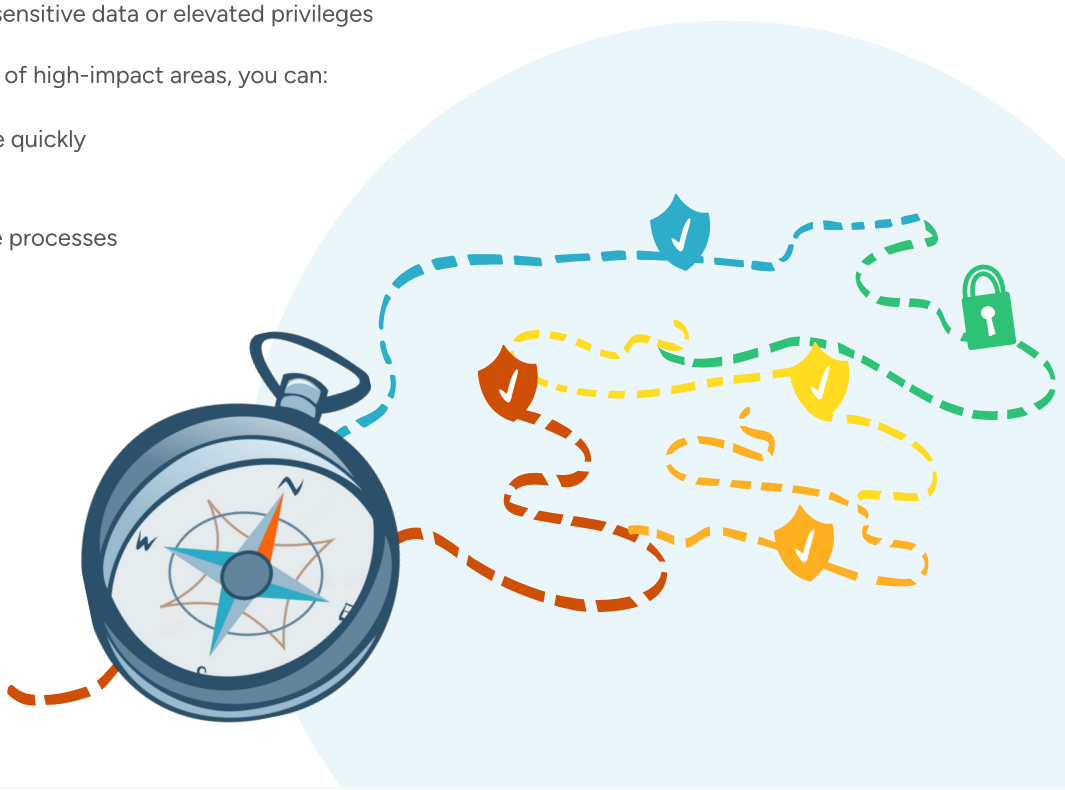
Start with a Manageable Scope

Begin your journey by identifying **1-3 resource types or teams** that:

- Are not yet covered by a Privileged Access Management (PAM) solution
- Have compliance gaps that need immediate attention
- Pose a higher security risk due to sensitive data or elevated privileges

By focusing on a manageable number of high-impact areas, you can:

- Implement Zero Trust access more quickly
- Gain immediate security benefits
- Gather valuable feedback to refine processes



Here's how StrongDM can help you navigate this journey:

1 **Identify High-Risk Resources and Critical Systems**

Begin by pinpointing the resources that pose the greatest risk to your organization if compromised. These typically include:

- **Production Databases and Servers**: Systems that store sensitive customer data or proprietary information.
- **Financial Systems**: Platforms that handle financial transactions, payroll, or budgeting.
- **Intellectual Property Repositories**: Codebases, design files, or research data critical to your business.
- **Infrastructure Management Tools**: Systems that control network configurations, cloud environments, or deployment pipelines.
- **Systems Outside of Current PAM Deployments**: Critical systems that are not managed by an existing PAM might also be a great place to start so you can benefit from control and auditing

Why Start Here?

Securing these resources first reduces the potential impact of a security breach and addresses compliance requirements for protecting sensitive data.

2 **Prioritize Teams with Elevated Privileges**

Focus on teams and individuals who have the most extensive access rights to those resources and, therefore, represent a higher security risk. These often include:

- **DevOps and Engineering Teams**: They require access to production environments and deployment systems.
- **IT Administrators**: They manage infrastructure and have broad access across systems.
- **Security Teams**: They need access to various systems for monitoring and response.
- **Third-Party Vendors and Contractors**: External parties that require temporary or limited access.

Why Start Here?

These users have permissions that, if misused or compromised, could lead to significant security incidents.

3 **Assess Access Patterns and Requirements**

Understand how these teams use their access:

- **Frequency of Access**: Do they need constant standing access, or is it periodic? (As the criticality of the resource increases, fewer standing access grants should exist.)
- **Type of Access Needed**: Are they accessing sensitive data, configuration settings, or performing administrative tasks?
- **Current Access Challenges**: Are there existing issues with over-permissioned accounts or shared credentials?

Why Is This Important?

This assessment helps tailor the Zero Trust Access implementation to meet users' actual needs without overrestricting them.

4 **Implement Zero Trust Access with StrongDM for Priority Areas**

Leverage StrongDM to transition the identified resources and teams to Zero Trust Access:

- **Just-in-Time Access**: Configure Access Workflows so that access is provisioned only when needed and deprovisioned immediately after use.
- **Zero Standing Privileges**: Eliminate persistent access rights to critical systems. (review the Standing Access Report in StrongDM to identify access grants that should be revoked)

- **Context-Based Policy Enforcement**: Set up policies that consider user context, such as role, location, and device health.
- **Audit and Monitoring**: Enable comprehensive logging to monitor all access requests and activities.

Why Use StrongDM?
StrongDM simplifies this process by providing a centralized platform to manage access dynamically, reducing complexity and administrative overhead.

5 **Gather Feedback and Refine Processes**
After initial implementation:

- **Collect User Feedback:** Understand any challenges faced by the teams during the transition.
- **Monitor Access Logs**: Analyze patterns to identify any policy adjustments needed.
- **Adjust Policies Accordingly:** Refine context-based policies to balance security and usability.

Why Is This Step Crucial?
Continuous improvement ensures that the Zero Trust Access model remains effective and user-friendly.

6 **Educate and Train Users**
Provide training and resources to help users understand:

- **The Importance of Zero Trust Access**: Emphasize how it protects both the organization and the users.
- **How to Request Access**: Demonstrate the simplified access request processes.
- **Best Practices for Security**: Reinforce policies on credential handling and reporting suspicious activities.

Why Invest in Training?
User buy-in is essential for the success of Zero Trust Access implementation.

7 **Establish Continuous Monitoring and Improvement**

- **Regular Audits**: Schedule periodic reviews of access policies and user privileges.
- **Policy Updates**: Stay up-to-date with evolving security threats and compliance requirements.
- **Scalability Planning**: Ensure that the access management system scales with organizational growth.

Why Is Ongoing Effort Needed?
Security is not a one-time task but an ongoing commitment to protect against emerging threats.

8 **Expand to Additional Teams and Resources**
With the initial phase refined:

- **Sequential Rollout**: Identify the next 3-5 resources or the next team you want to put on the journey to Zero Trust access. Gradually include other teams, such as development, QA, and business units.
- **Include Less Critical Systems**: Extend Zero Trust principles to systems that, while less critical, still benefit from enhanced security.
- **Automate Where Possible**: Utilize StrongDM's automation capabilities to streamline provisioning and deprovisioning.

Why Expand Gradually?
It allows your organization to adapt to new processes incrementally, ensuring stability and acceptance at each step.

How StrongDM Facilitates This Process

StrongDM simplifies the journey to Zero Trust Access by:

- **Centralizing Access Management**: Providing a single platform to manage access across diverse systems and teams.
- **Streamlining Onboarding**: Making it easy to add new resources and users without extensive setup.
- **Enhancing Visibility**: Offering comprehensive logging, monitoring, and reporting to keep track of all access events. Detailed reports help you uncover standing access grants that haven't been used, identify resources that no one is accessing, and detect roles that are over-privileged. These insights allow you to proactively clean up unnecessary permissions, reduce your attack surface, and tighten security policies.
- **Supporting Context-Based Policies**: Allowing you to define fine-grained access controls tailored to each team's needs.
- **Automating Workflows**: Reducing administrative overhead through automated provisioning and deprovisioning and JIT workflows.

Practical Tips for Getting Started

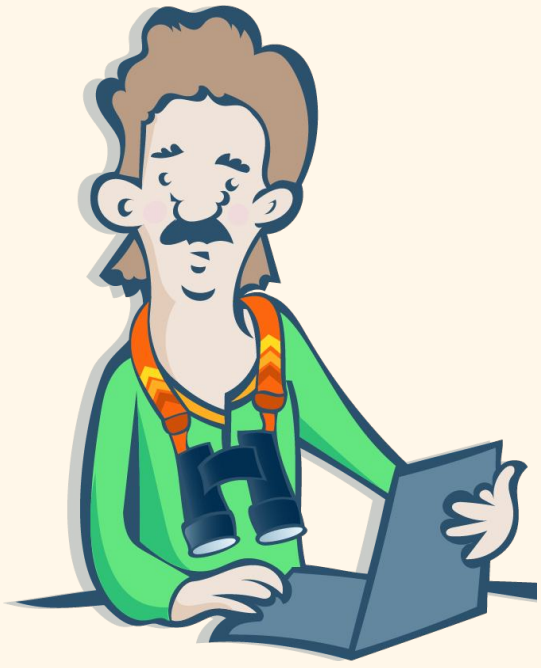
Engage Stakeholders Early
Involve team leads and key users from the selected groups to gain their support and input.

Communicate Clearly
Explain the benefits of Zero Trust access and how it will impact users' daily activities.

Provide Training and Support
Ensure users understand new processes and have resources to assist them during the transition.

Set Realistic Goals
Define clear objectives for what you aim to achieve with each group, such as reducing access provisioning time or eliminating shared credentials.

Measure and Report Progress
Track key metrics to demonstrate improvements in security posture and operational efficiency.



Example Implementation Plan

Week 1-2: Planning and Preparation

- Identify 3-5 high-priority resources that you want to move up the maturity curve.
- Inform relevant teams about the upcoming changes.
- Configure StrongDM for the selected resources if not already covered by the platform.

Week 3-4: Onboarding and Configuration

- Implement JIT access and Zero Standing Privilege workflows for these resources.
- Set up context-based policies tailored to each team's needs.
- Provide training sessions for users and administrators.

Week 5-6: Monitoring and Feedback

- Implement JIT access and Zero Standing Privilege workflows for these resources.
- Set up context-based policies tailored to each team's needs.
- Provide training sessions for users and administrators.

Week 7-8: Refinement and Documentation

- Adjust policies and workflows based on feedback.
- Document the process, including successes and lessons learned.
- Plan for the next group of resources or teams to onboard.

StrongDM Reports Help Measure Your Organization's Access Maturity Level

StrongDM also has reporting capabilities that can help you determine how your existing roles and access grants are being used. In the **Standing Access Report**, you will see three scores for your organization (or selected group of resources).

- **JIT Access Score** indicates what percentage of total access grants are temporary, JIT grants (vs. standing, permanent grants)
- **Role Utilization Score** indicates what percentage of total grants have been used during a time period
- **Overall Score** is the average of the JIT Access Score and Role Utilization Score

This report examines the grants created when a User or a Resource is assigned to a Role.

These permanent grants derived from Roles create a condition called standing access. The more standing access there is, the less secure your Resources are since one compromised User will expose many Resources to attack.

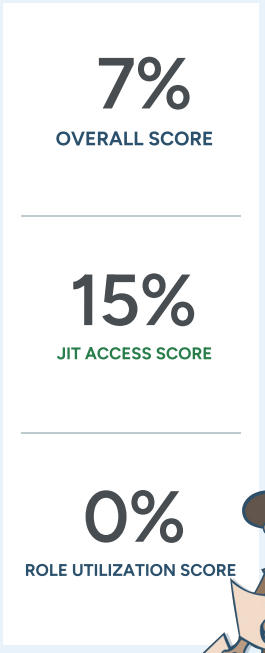
This report is meant to assist StrongDM administrators in minimizing the risk of standing access by helping migrate permanent grants from Roles into temporary grants from Workflow and Policies.

After reading this report, you will have a better understanding of your standing access status and an overview of remediation next steps.

Overall Score $\frac{\textit{JIT Access Score + Role Utilization Score}}{2}$

JIT Access Score $\frac{\textit{number of temporary grants}}{\textit{number of (temporary + permanent) grants}}$

Role Utilization Score $\frac{\textit{number of utilized permanent grants}}{\textit{number permanent grants}}$



The **JIT Access Score** evaluates all of your grants, and calculates the percentage of grants that provided access on a temporary basis versus the grants that derive from a Role. A **JIT Access Score** of 100% means your organization has no standing access because all of your grants provide access on a temporary basis.

The **Role Utilization Score** calculates the percentage of permanent grants where the User accessed the Resource. A **Role Utilization Score** of 100% means all of your permanent grants are utilized.

This report is compiled from grants and sessions from the previous 90 days.

Target Scores for Level 3: Just-in-Time Access

- **JIT Access Score: At least 25%–70%**. At this stage, JIT access is being implemented for most privileged accounts and potentially other high-risk or sensitive accounts. However, some non-critical accounts might still have standing access.
- **Role Utilization Score: 70%–85%**. This score reflects that the organization is actively monitoring role utilization, ensuring that privileges are granted when needed, but not yet consistently achieving 100% utilization across all accounts.
- **Overall Score**: An overall score (average of JIT Access Score and Role Utilization Score) of approximately **50%–75%** indicates that the organization is embracing JIT for most critical functions but still has room to grow in fully eliminating unnecessary access.

Target Scores for Level 4: Zero Trust Access

- **JIT Access Score: 71%–100%**. At Level 4, the goal is to eliminate all standing access, so JIT should be implemented for virtually every type of access across the organization, driving this score toward 100%.
- **Role Utilization Score: 85%–95%**. At this level, most access grants are used within their specified time frames, and any unused access is automatically de-provisioned. This indicates that access is tightly controlled and aligned with real-time needs.
- **Overall Score**: An overall score of **75%–100%** suggests that the organization is nearing complete adoption of dynamic, context-based access controls, with minimal standing privileges and real-time enforcement.

Conclusion

By starting with a focused set of resources and teams, you can make tangible progress toward Zero Trust access without getting bogged down in exhaustive planning. This iterative approach allows you to:

Improve Security Incrementally
Enhance your security posture step by step.

Adapt to Organizational Needs
Tailor the implementation to fit your unique environment.

Build Confidence and Support
Demonstrate the value of Zero Trust access to stakeholders.

StrongDM supports this journey by providing the tools and capabilities needed to implement Zero Trust principles effectively, enabling you to protect critical assets while maintaining operational efficiency.

To learn more or request a demo, please visit www.strongdm.com/get-a-demo.

strongdm

StrongDM is a Zero Trust access platform that centralizes and simplifies access management for all technical users across every resource in your infrastructure, whether on-premises or in the cloud. By embracing Zero Standing Privileges and implementing Just-in-Time (JIT) access across your full tech stack, StrongDM provides fine-grained, context-based policy enforcement in real-time.

Security teams gain complete visibility and control over access and actions with advanced reporting and analytics, helping to identify unused access grants, unaccessed resources, and over-privileged roles to enhance security and compliance postures. End users enjoy fast, intuitive access to the resources they need when they need them, improving productivity and operational efficiency.

Connect with us on LinkedIn, X (formerly Twitter), Facebook, YouTube or head to www.strongdm.com to learn more.