strongdm

REPORT

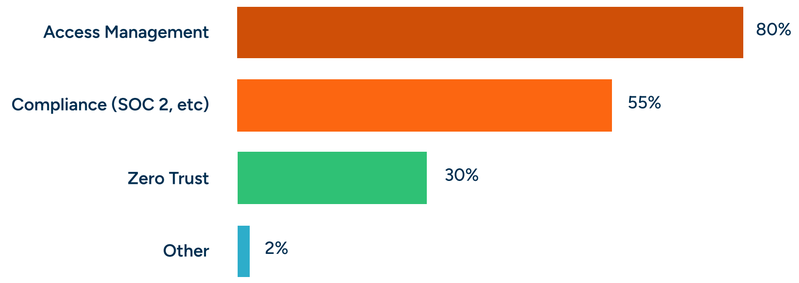
2023: The Year of Access

Why the road to modern security starts with access.

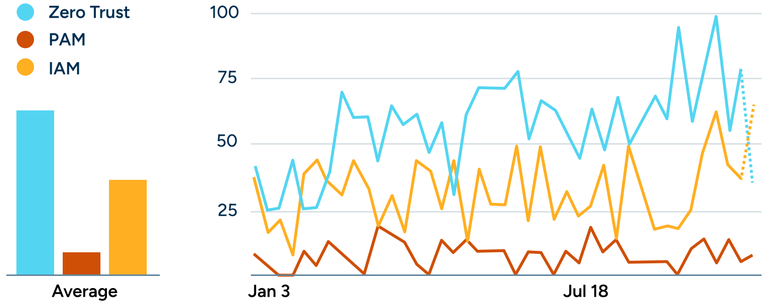
Zero Trust is Aspirational. Access is Addressable.

Taking a modern approach to security is a top priority for Security and DevOps teams. In many cases, that includes embracing new methodologies such as Zero Trust. The idea that you can “never trust and always verify” all access to your infrastructure will go a long way towards improving your overall security posture. But similar to DevOps, Zero Trust isn’t something you buy–it’s a methodology that you embrace. And when done well, it can even improve how you deliver access to your infrastructure.

In fact, in **a recent podcast**, Gartner analyst John Watts named access and identity as the critical starting points for adopting Zero Trust. It’s no surprise that as Zero Trust gains steam, 80% of organizations are including Access Management as a critical initiative over the next 12 months.



Which of the above are strategic initiatives for your organization over the next 12 months?



Interest Over Time

Source: Google Trends; Jan. 1, 2010–Oct. 15, 2021

State of Infrastructure Access Management: At a Glance

Access to infrastructure has snowballed out of control...

93% of organizations (with technical staff) that have access to sensitive infrastructure

And has become untenable, growing beyond human scale.

53% take hours to weeks for access to infrastructure to be granted

88% require 2+ people to grant and approve access

25% require 4+ people

That's across the entire stack.

Organizations with access challenges for these systems:

60% Cloud providers

57% Databases

57% Data centers and servers

This makes organizations less secure and less compliant...

65% use team or shared logins

41% name gathering evidence for compliance as a top challenge

42% use shared SSH keys

And the problem isn't going away. It'll only get worse.

Broad adoption of Kubernetes has barely started, and already **1 in 3** name Kubernetes as the most difficult technology to manage.

This is why Access Management has become a critical initiative.

80% name Access Management as a critical initiative over the next 12 months, laying the foundation for organizations to embrace Zero Trust

Survey Results

strongdm

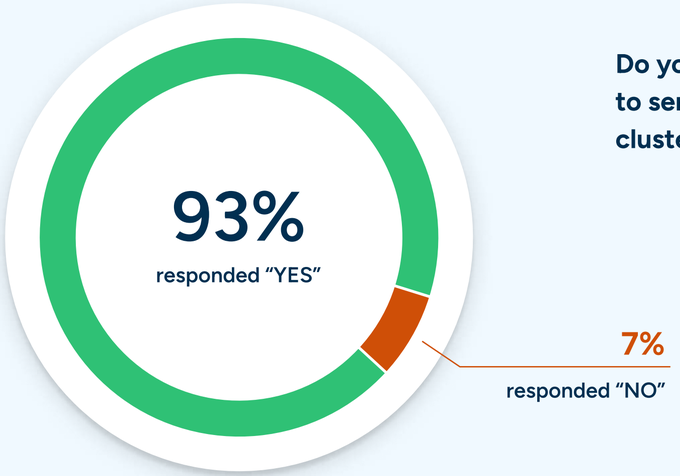
Infrastructure Access is Out of Control.

Innovation. Democratized access to data. Company growth. New Tools. These are just a few of the items driving more employees to gain access to a business's critical systems—and they're a major reason why Infrastructure access is snowballing out of control.

This leaves businesses with two critical problems:

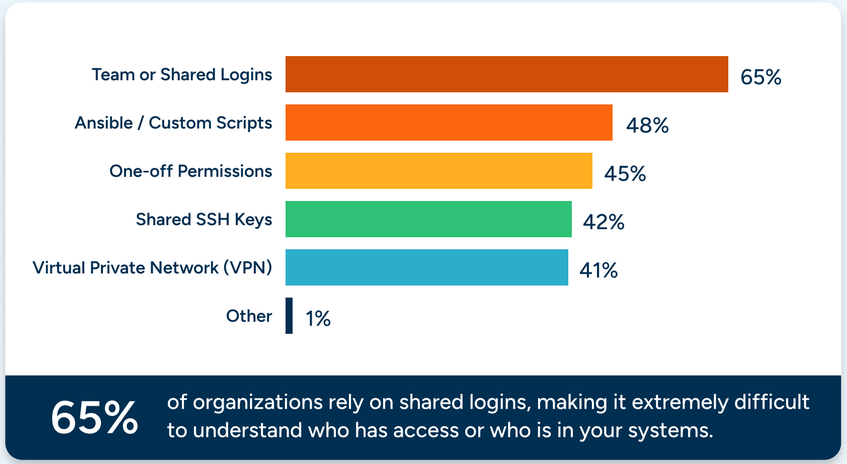
Access issues prevent developers from meeting business demands, and everyday workflows put the business at risk.

Existing workflows and processes involve old school methods that don't scale and are non-compliant.



Do you have technical staff that has access to sensitive infrastructure (e.g. servers, clusters, databases, cloud APIs, etc.)?

How are you currently managing infrastructure access today?



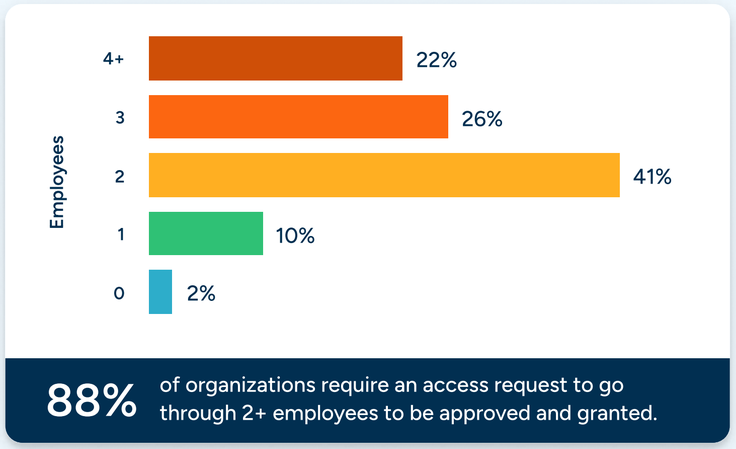
65% of organizations rely on shared logins, making it extremely difficult to understand who has access or who is in your systems.

Current Approaches to Infrastructure Access: Broken & Untenable

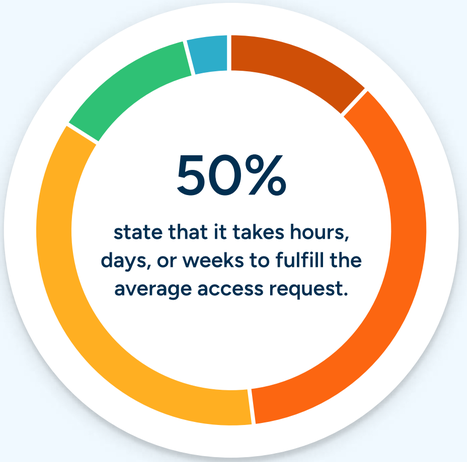
Accelerating the development process is the core of DevOps. But when developers struggle to gain timely access to the systems they need, it's clear that something isn't working. **If one of the main tenets of DevOps is agility, then it's clear these workflows are fundamentally broken.**

More than 1 in 5 organizations require 4+ people to be involved.

On average, how many staff members are involved in approving and granting an access request?



88% of organizations require an access request to go through 2+ employees to be approved and granted.



How long does it typically take for an access request to be routed, approved and granted?

- 12% Seconds
- 36% Minutes
- 36% Hours
- 12% Days
- 5% Weeks

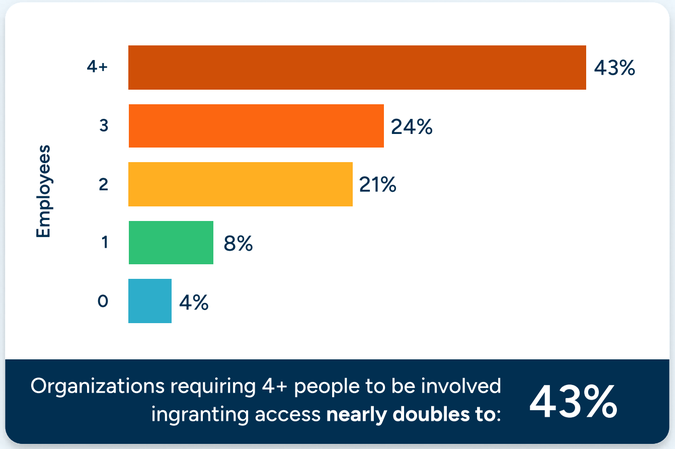
Current Approaches to Infrastructure Access:
Complexity Grows as Organizations Scale

Facilitating access quickly exceeds human scale by the time a company becomes mid-sized. When a company grows to 1,000+ employees, it is impossible to manage manually without error. All of this complexity amounts to wasted time for technical staff and significant overhead for everyone involved.

Approximately 60% listed “the time it takes to request/grant access to systems or data” as one of their biggest challenges

ENTERPRISE

On average, how many staff members are involved in approving and granting an access request?



How long does it typically take for an access request to be routed, approved, and granted?

- 4% Seconds
- 38% Minutes
- 29% Hours
- 21% Days
- 8% Weeks

Existing Approaches, like Privileged Access Management (PAM) are too Narrow and Just Aren’t Working.

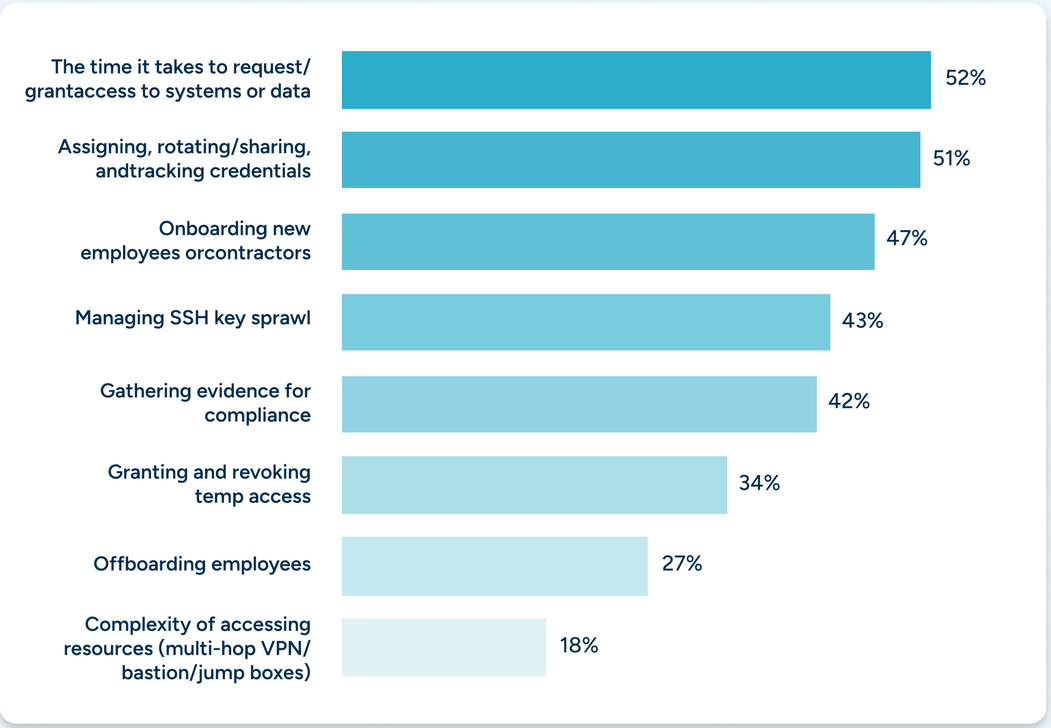
While the PAM market has existed for a while, those tools do not solve the complete access challenge. The same problems they claim to solve are still the primary challenges companies face, and others—such as onboarding and compliance—go well beyond privileged access. For example:

- **More than 50%** of all companies surveyed struggle with assigning, rotating, and tracking credentials
- Another **47%** struggle with onboarding employees and contractors
- **52%** of organizations continue to face challenges with the time required to simply grant access to critical systems

Furthermore, these tools are poorly adopted because they slow down developers and add complexity to their workflows. Gartner reports PAM market growth at a modest 12% from 2019 to 2020.*

*Source: Gartner Magic Quadrant for Privileged Access Management, July 2021

What are your team’s biggest challenges in regard to accessing critical infrastructure?

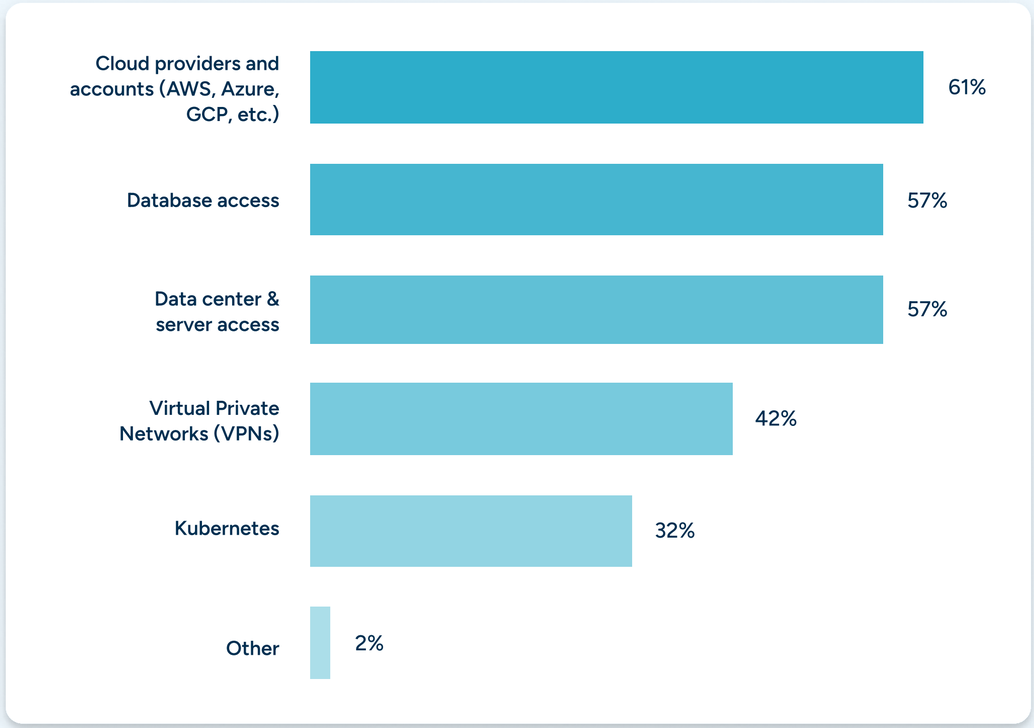


Infrastructure Access: An Evolving Challenge

Infrastructure access will only get more complex as organizations grow and continue to embrace new technologies and the cloud. For example, if every new technical employee needs access to 15 systems, that's 15 credentials that must be managed.

Only 32% of teams list Kubernetes as one of the most difficult technologies to manage in terms of access—a number that is likely to increase as adoption of this new and upcoming technology continues. That means the difficulty inherent in managing access to ephemeral infrastructure has not been fully realized yet.

Which technologies are the most difficult to manage in terms of access (time, cost, complexity)?

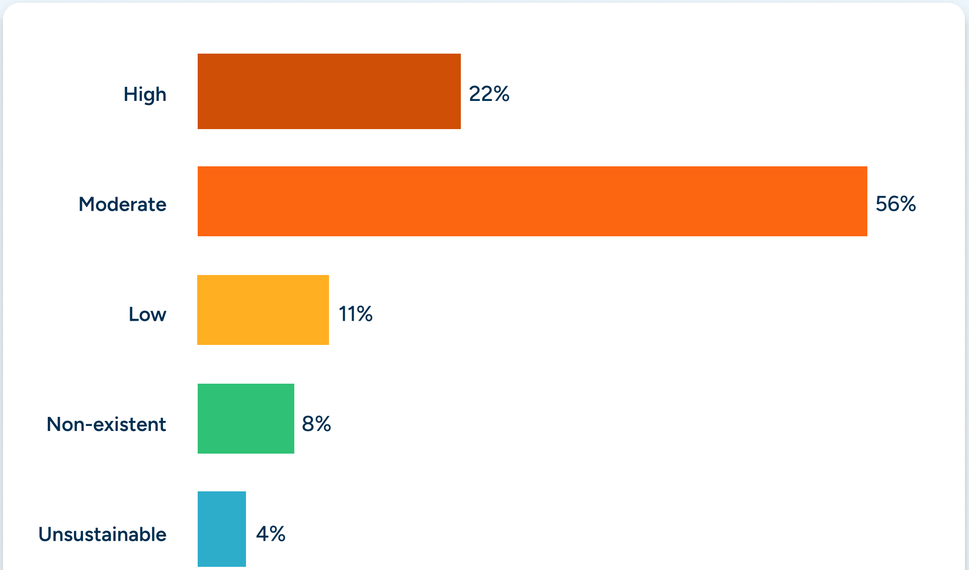


Infrastructure Access: Accumulating Technical Debt

This challenge is **additive**. Access to every new technology or system must be managed in addition to all existing systems and technical debt. The more organizations grow, innovate, and use new technologies, the harder this problem gets.

In fact, nearly 80% claimed that the technical debt associated with their current approach to access is moderate to unsustainable.

How would you classify technical debt of your current access methodologies?



Nearly 80% claimed that the technical debt associated with their current approach to access is moderate to unsustainable

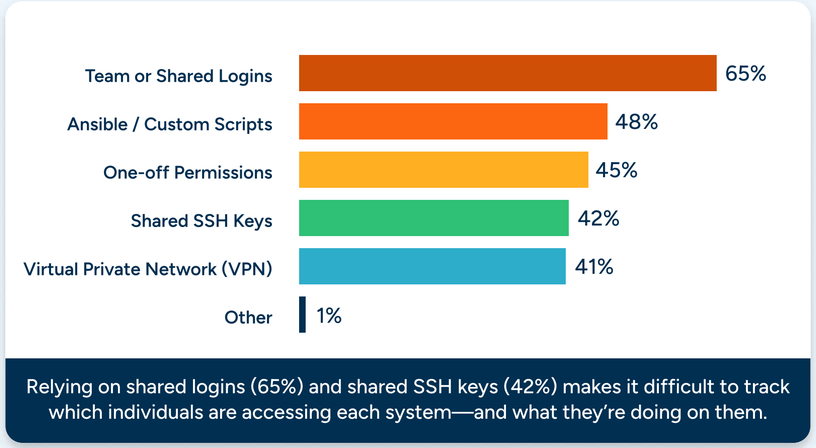
Ignoring Access Issues? Not an Option. Access Ignorance Invites Security Issues and Auditing Woes.

There is currently an over-reliance on legacy and insecure approaches to access that are driving business risk.

Shared logins and over-provisioning are tangible examples of the access challenges that organizations must overcome to fully achieve Zero Trust.

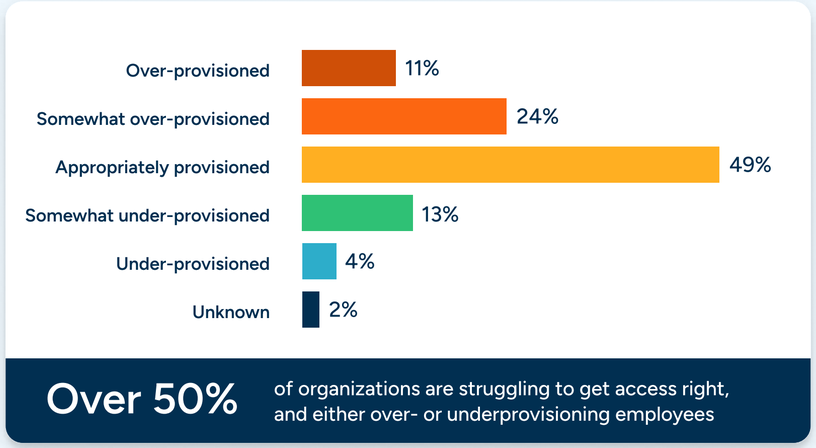
1 in 3 organizations over-provision employees, indicating that adoption of Least Privilege is still a work in progress.

How are you currently managing infrastructure access today?



Relying on shared logins (65%) and shared SSH keys (42%) makes it difficult to track which individuals are accessing each system—and what they're doing on them.

When it comes to alignment or roles to access, do you find employees tend to be:



Over 50% of organizations are struggling to get access right, and either over- or underprovisioning employees

Infrastructure Access Doesn’t have to be Painful.

Despite how ubiquitous infrastructure access challenges are, organizations that address them are seeing tangible benefits, including higher productivity, reduced costs, improved security and compliance, and even improved peace of mind.

Below are three examples of real companies that solved the challenge and the benefits each received.

Challenge

With 250+ databases, Yext dealt with frustrating on-/off-boarding processes. They also needed detailed auditing to pass SOC 2, which was estimated in the millions to implement.

Improve Infrastructure Access

- Simplified access with one control plane
- Cut provisioning time from two days to one hour
- Delivered significant cost and time savings to implement SOC 2-compliant auditing
- Detailed audit trails for every query

Read the case study ›

Challenge

Coveo needed an easier way to manage secure access to over 100 multi-regional databases, with 100 usernames names and passwords per employee.

Improve Infrastructure Access

- Delivered one credential to access everything
- Reduced the need to manage passwords
- Enabled a more efficient auditing process
- Provided peace of mind with visibility of every query

Read the case study ›

Challenge

Better was managing access manually and had a compıex and lengthy provisioning process. Auditing also suffered due to inadequate logging.

Improve Infrastructure Access

- Simplified access and audit controls
- Cut provisioning time from one week to minutes
- Enabled real-time revocation
- Ensured every change and query is automatically logged and accessible

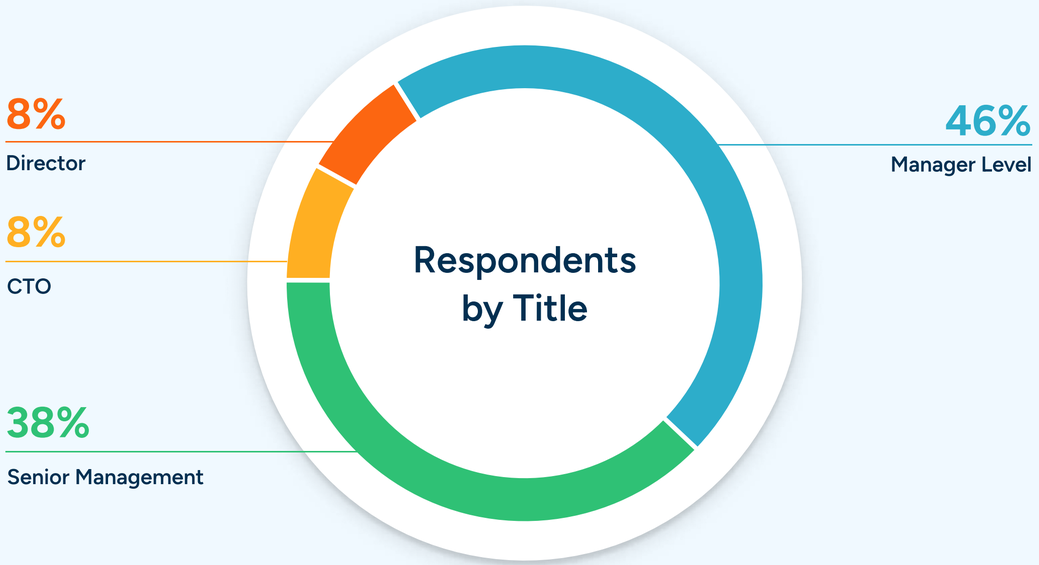
Read the case study ›

Method and Demographics

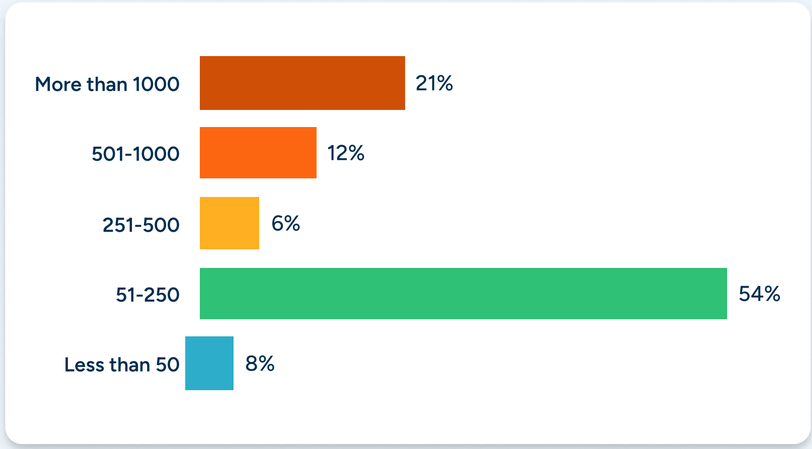
The 2023: Year of Access report was produced by StrongDM.

The data is a result of an online survey of DevOps professionals conducted by Pollfish.

A total of 600 recipients from all over the United States, representing organizations for virtually every size, responded to the survey in September and October 2021.



Respondent Size of Organization



strongdm

StrongDM is a Dynamic Access Management platform that puts people first by giving technical staff a direct route to the critical infrastructure they need to be their most productive. End users enjoy fast, intuitive, and auditable access to the resources they need. Administrators gain precise controls, eliminating unauthorized and excessive access permissions. IT, Security, DevOps, and Compliance teams can easily answer who did what, where, and when with comprehensive audit logs. It seamlessly and securely integrates with every environment and protocol your team needs, with responsive 24/7 support.