strongdm

Table of Contents

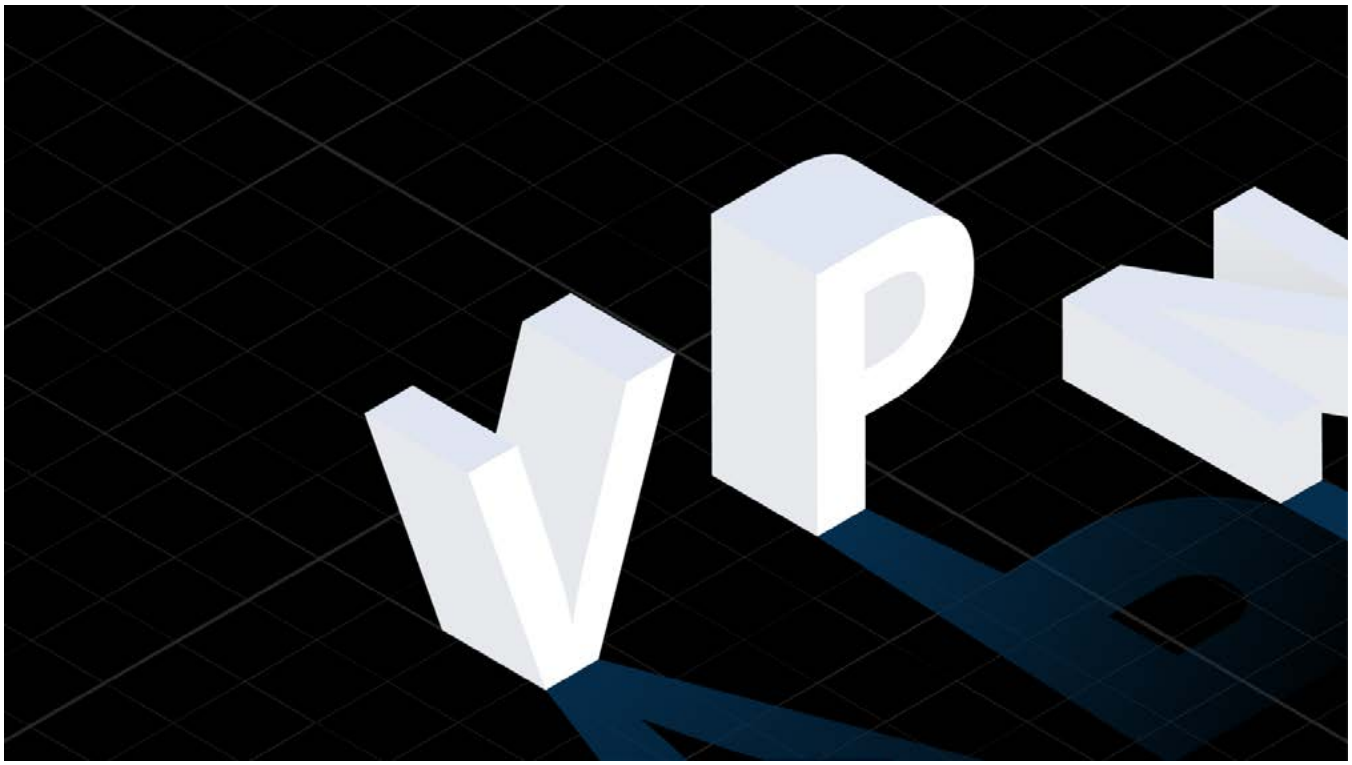
TL;DR

This article will introduce several robust VPN alternatives to help you secure remote access using the infrastructure you already have.

You'll see how teams of all sizes—from three-person startups to large organizations like Peloton—have replaced outdated VPN architecture with secure, scalable, auditable solutions built for modern computing.

- These VPN alternatives will:
- Fill security gaps left by your VPN.
- Scale with modern infrastructure.
- Provide an audit trail and logs.
- Manage access without disrupting workflow.
- Enforce least privilege.

But first, let's take a look at the problem.



01

What is a Virtual Private Network

A virtual private network (VPN) lets you transmit data across the internet as if you were directly connected to a private network. This was sufficient when only a few people needed access. Infrastructure connection was managed by somebody walking into an office, or into the colo down the street...and then Cloud came.

Suddenly, teams are deploying legacy systems like Oracle and Sybase alongside Memcached, multi-cloud Kubernetes, cloud CLIs, and most of it doesn't speak the same language. Plus, you have an entirely distributed workforce that includes contractors and third-party vendors—**lots of people that need access to lots of things in lots of places.**

This complicates things. Now you can't track user activity. You don't know who connected or from where. And the person managing network access—their fingers are bleeding. They're running dedicated circuits, adding more VPNs, writing scripts to hold it all together—this just isn't feasible in modern environments.

> "You see this at conferences all the time, where people get up and talk about what they're doing at their companies. And you're like, 'wow, my environment's crap. I wish I could build something like that.' And the person next to you says, 'Yeah, me too.' When you look at their badge and they work at the same company as the speaker."
>
> **Corey Quinn** | Screaming in the Cloud

VPNS WERE GOOD, BUT THEY DON'T TELL THE WHOLE STORY

VPNs leave gaps in your security, providing all-or-nothing access rather than Zero Trust. They fail to enforce least privilege and other policies that protect credentials. And they typically provide no audit trail beyond logging connection times.

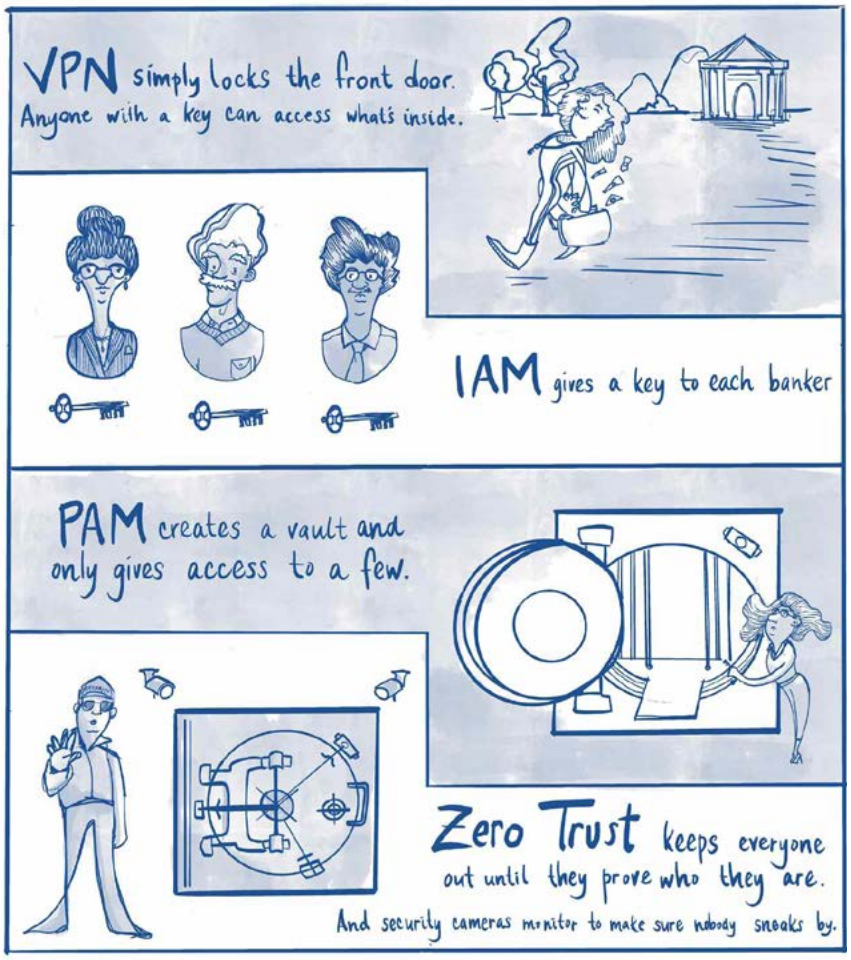
02
Manage VPN Security Risks with IAM

Modern computing forced us to redefine access. It's no longer enough for admins to simply secure the network. They need role-based access control (RBAC). That is—access should depend on who you are, not just the network you happen to be on.

Think of it like this: A bank doesn't just lock its front door. That would be the equivalent of a VPN getting you onto some sort of network. There's also a bank vault, plus security cameras to see what somebody is doing. Identity Access Management (IAM or IdAM) solutions attempt to lock that bank vault, ensuring that the right users have exactly the intended access to technology resources.

IAM tools manage accounts for all of the users in your network. However, a good VPN alternative must simplify onboarding and offboarding, manage vendor access, and provide authentication for humans as well as service accounts.

This is where PAM comes in.



03

PAM: A Better Access Solution

A VPN alternative is only effective if it can manage access to everything. IAM eases friction for everyday users, but what about privileged accounts, critical systems, and third-party vendors? Privileged Access Management (PAM) builds on the advantages of IAM by protecting the accounts that need privileged access to sensitive data.

PAM helps you:

- Manage passwords and authentication.
- Enable secure communication between systems.
- Audit and monitor privileged accounts and actions.
- Enforce least privilege policies for sensitive accounts.

Traditional PAM solutions manage access to resources inside your network but may not extend to cloud environments. Modern PAM solutions have responded to this need by adopting a Zero Trust Model.

STRENGTHENING PAM WITH ZERO TRUST

Zero Trust is founded on a "never trust, always verify" principle. With Zero Trust, administrators only grant access to what is required. Every device and user, whether inside or outside of the private network, is monitored and managed. This includes everyday users, privileged accounts, and third-party vendors.

Zero Trust is an essential component of an alternative remote access solution. However, many Zero Trust offerings are costly and hard to implement. They often require more management, rather than less, as employees, clients, vendors, etc. each require specific access policies.

With teams running multi-platform deployments and combining legacy systems with new technologies, **Zero Trust can get complicated**. Active Directory doesn't speak Druid, and Okta certainly doesn't directly speak to Sybase, etc.

"But what about access?"

> "[Nearly] every environment is a burning tire fire of sadness and regret. The only question is how honest people are going to be about that." — **Corey Quinn** | Cloud Economist

And so what do you do? Too often, you find yourself spending a ridiculous amount of money on shelfware. Why does it become shelfware? Because it's so freakin' hard to deploy.

04

Zero Trust, Without the Friction

Before you scrap your entire infrastructure and start from scratch, consider this: Apart from being unrealistic, this choice still leaves you stuck. New challenges will continue to surprise us. New tech will rise up to meet new needs. Companies need a VPN alternative that is **nimble enough to adapt to a shifting technology landscape.**

strongDM is an infrastructure API that enables DevOps teams to manage and audit access to any back-end infrastructure, both in the cloud and on-prem. It essentially takes all that's good of PAM and zero trust, and makes it easy to implement. This includes servers, databases, Kubernetes clusters, web apps—even the cloud drivers themselves. It lets you introspect as to what's happening to provide you with an audit trail. And this is true whether you're in enterprise, corporate, or small to midsize business settings.

05

The Future of Infrastructure Access

Betterment

> "Just like AWS for compute power, and Kubernetes for container orchestration, strongDM is the gold standard for access and auditing."
>
> **Drew Blas** | Director, Internal Engineering at Betterment

Meet The Gold Standard for Access and Auditing

Type	Detail
strongDM Fills Security Gaps Left by Your VPN.	Before using strongDM to enforce least privilege, Greenhouse Software took a VPN-based approach to segmentation. This left their data and systems open to VPN vulnerabilities as users had unrestricted access to the entire private network. With strongDM, Greenhouse's admins grant read-only access to specific databases and servers, so even if an attacker gains access to a computer, they can't use it to break into the entire network.
strongDM Scales with Modern Infrastructure.	The vast majority of companies have old legacy stuff—Oracle, Sybase, Teradata, Db2. But they also have Memcached or Redis, and they're using Kubernetes in production. They've got a hodgepodge of stuff, and they want something that manages access to all of it seamlessly. That's what you need in a VPN alternative. And that's what strongDM offers.
strongDM Provides an Audit Trail and Logs.	strongDM logs every user authentication, ssh, query, administrator action, and RDP command and stores them in an encrypted repository. This helps you ensure compliance with organizational standards, and also detect security violations and performance problems. "Before strongDM, we were dependent on the database or application's logs to provide us with the audit data we needed, which often was not enough … With strongDM we get full auditability into everything a person does—when

Type	Detail
	they connect, what commands they type, what data they retrieve. We're able to see everything." —Dave Anderson, Director of InfoSec, Greenhouse Software
strongDM Manages Access Without Disrupting Workflow.	strongDM actually improves workflow, allowing you to: • Delegate authentication to your SSO or identity provider. • Keep credentials off the end user's workstation. • Onboard and offboard in minutes from a single point of provisioning. • Create an encrypted tunnel between a user and the thing they're accessing. "Developers won't tolerate tools that slow them down or force them to use substandard workflows. strongDM is the only security product that actually makes their lives easier." — Drew Blas, Director, Internal Engineering at Betterment.
strongDM Enforces Least Privilege with Zero Trust.	strongDM uses Zero Trust Network Access (ZTNA) to enforce least privilege. This approach has helped companies like Better Mortgage access databases in a way that is both easier and more secure. strongDM provides Zero Trust as a service, enabling organizations of any size to implement a Zero Trust infrastructure. "For Zero Trust, strongDM is an amazing tool. BYOD, within the company, outside—wherever you need to go you can access the data in a secure way." - Ali Kahn, CISO, Better
strongDM is Easy to Implement.	strongDM provides native support to everything you're already using, so deployment is easy. "When strongDM said deployment would take an hour, I assumed they were full of it and blocked out a full day. We finished in 45 minutes." - Peter Tormey, Manager DataOps, SoFi

Now it's your turn.

How would your day-to-day improve if you replaced the VPN? Let us know. Book some time with us for a free, no-obligation walk-through of strongDM.

To learn more on how strongDM helps companies replace VPN, make sure to check out our VPN Alternative Use Case.

strongDM's infrastructure access platform gives every business secure access controls in a way folks love to use. Trusted by the Fortune 500 to fast-growing businesses like Peloton, 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. strongDM is intentionally distributed. Head to **www.strongdm.com** to learn more.