Zero Trust Explained: The Ultimate Guide to Zero Trust Security

NEVER TRUST, ALWAYS VERIFY

strongdm

Table of Contents

TL;DR

This article offers an in-depth review of **Zero Trust** security, including its benefits, best practices, and common barriers to implementation. You'll gain a deeper understanding of Zero Trust models like ZTAA and ZTNA and learn the tools and techniques you need to apply frictionless Zero Trust access control to your infrastructure. Let's dive in.

01

What is Zero Trust?

Zero Trust is a modern security model founded on the design principle “Never trust, always verify.” It requires all devices and users, regardless of whether they are inside or outside an organization's network, to be authenticated, authorized, and regularly validated before being granted access.

In short, Zero Trust says “Don’t trust anyone until they’ve been verified.”

Zero Trust helps prevent security breaches by eliminating the implicit trust from your system’s architecture. Instead of automatically trusting users inside the network, Zero Trust requires validation at every access point. It protects modern network environments using a multi-layered approach, including:

- Network segmentation
- Layer 7 threat prevention
- Simplified granular user-access control
- Comprehensive security monitoring
- Security system automation

With the rise of remote work, bring your own device (BYOD), and cloud-based assets that aren’t located within an enterprise-owned network boundary, traditional perimeter security falls short. That’s where Zero Trust comes in. A Zero Trust architecture (ZTA) is designed as if there is no traditional network edge, retiring the old castle-and-moat model of perimeter security.

In essence, Zero Trust security not only acknowledges that threats exist inside and outside of the network, but it assumes that a breach is inevitable (or has likely already occurred). As a result, it constantly monitors for malicious activity and limits user access to only what is required to do the job. This effectively prevents users (including potential bad actors) from moving laterally through the network and accessing any data that hasn’t been limited.

Zero Trust security can be applied in multiple ways depending on your architecture design and approach.

Type	Detail
Zero Trust Network Access (ZTNA)	Zero Trust Network Access (ZTNA), sometimes referred to as a "software-defined perimeter," is the most common implementation of the Zero Trust model. Based on micro-segmentation and network isolation, ZTNA replaces the need for a VPN and grants access to the network after verification and authentication. As Gartner defines it, under a ZTNA model, "access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network." This minimizes the attack surface, significantly reducing security risk.
Zero Trust Application Access (ZTAA)	Zero Trust Application Access (ZTAA) also operates on Zero Trust principles, but unlike ZTNA, it goes a step further to protect not just the network but applications, too. ZTAA assumes all networks are compromised and limits access to applications until after users and devices have been verified. This approach effectively blocks attackers that enter the network and protects the connected applications.
Zero Trust Access	Zero Trust Access is the umbrella model that encompasses both ZTAA and ZTNA, providing end-to-end Zero Trust across your entire architecture—including all networks and applications. It provides identity-based security that considers not just who is on the network, but what is on the network—extending zero trust to the provider itself. This gives organizations unparalleled data privacy in a true Zero Trust environment.

02
History of Zero Trust Security

John Kindervag developed the original Zero Trust model in 2010. As a principal analyst at Forrester Research, Kindervag realized that traditional access models operated on the outdated assumption that organizations should trust everything within their networks. The thinking was that perimeter-based security (i.e., firewalls) would be enough to validate user access and secure the network entirely. But as more workers started remotely accessing systems through all types of devices and all kinds of connections, this trust structure proved insufficient to effectively manage a distributed workforce. Kindervag recognized this vulnerability and developed Zero Trust in response.

Around the same time, Google began developing its own Zero Trust systems. Google created BeyondCorp for migrating traditional virtual private network (VPN) access policies to a new infrastructure in which no systems are trusted and all endpoints gate and monitor access. Google later developed BeyondProd, which provides a Zero Trust method to securely manage code deployment in a cloud-first microservices environment.

Kindervag's Zero Trust model and Google's BeyondCorp center around a few major tenets:

Type	Detail
Segmentation	Traditional networks exposed direct access to all data assets, servers, and applications. The Zero Trust model segments various subsets of these resources and removes the ability for users to directly access them without first going through a tightly controlled gateway. This is sometimes referred to as "network isolation." Microsegmentation takes this concept further by isolating workloads from one another so that administrators can monitor and control the flow of information between different servers and applications rather than just between client and server.
Access control	Regardless of whether users are physically located in an office or working remotely, they should only be able to access the information and resources that are appropriate for their respective roles. Each segment of the network should authenticate and validate authorization to ensure that traffic is being sent from trusted users regardless of the location or source of the request.
Visibility	Gateways should inspect and log all traffic, and admins should regularly monitor logs to ensure that users are only attempting to access systems that they're permitted to access. Commonly, administrators will use cloud access security broker software to monitor traffic between users and cloud applications and warn when they see suspicious behavior.

With the Zero Trust model, organizations can eliminate direct access to networks and resources, establish granular access controls, and gain visibility into user actions and traffic. However, they need models to guide them through implementation.

Google provides extensive documentation for those wanting to emulate BeyondCorp, which sets an industry standard for Zero Trust. However, most companies find Google's approach to be interesting in theory, but impossible in practice. (Its implementation essentially required a rip-and-replace of Google's existing network components and global architecture.) Instead, companies must rely on a combination of third-party services to implement Zero Trust architecture across their infrastructure.

03

Foundations of the Zero Trust Model

THREE CORE PRINCIPLES

Zero Trust is an integrated, end-to-end security strategy based on three core principles.

- **Never trust, always verify**—Always authenticate and authorize based on all available data points—including user identity, location, device, data sources, service, or workload. Continuous verification means there are no trusted zones, devices, or users. Instead, Zero Trust treats everyone and everything as a potential threat.

- **Assume breach**—By assuming your defenses have already been infiltrated, you can take a stronger security posture against potential threats, minimizing the impact if a breach does occur. Limit the "blast radius"—the extent and reach of potential damage incurred by a breach—by segmenting access and reducing your attack surface, verifying end-to-end encryption, and monitoring your network in real time.

- **Apply least-privileged access**—Zero Trust follows the Principle of Least Privilege (PoLP), which is the practice of limiting access rights for any entity and only permitting the minimum privileges necessary to perform its function. In other words, PoLP prevents users, accounts, computing processes, etc., from having unnecessarily broad access across the network, which leaves your network vulnerable and creates a higher attack surface in case of a breach.

EIGHT PILLARS

These principles create the foundation upon which a Zero Trust Architecture (ZTA) is built. Additionally, the eight pillars of Zero Trust security form a defensive architecture designed to meet the needs of today's complex networks. These pillars each represent a key focus area for categorizing and implementing a Zero Trust environment.

- **Identity security**—An identity is an attribute or set of attributes that uniquely describe a user or entity. Often referred to as workforce or user security, this pillar centers on the use of authentication and access control policies to identify and validate users attempting to connect to the network. Identity security relies on dynamic and contextual data analysis to ensure the right users are permitted access at the right time. Role-based access control (RBAC) and attribute-based access control (ABAC) will apply to policies within this pillar to authorize users.

- **Endpoint security**—Similar to identity security, endpoint (or device) security performs "systems of record" validation of devices (both user-controlled and autonomous devices, such as internet of things devices) that are trying to connect to the enterprise network. This pillar focuses on monitoring and maintaining device health at every step. Organizations should inventory and secure all agency devices (including mobile phones, laptops, servers, and IoT devices) to prevent unauthorized devices from accessing the network.

- **Application security**—Application and workload security include both on-premise and cloud-based services and systems. Securing and managing the application layer is key to successfully adopting a Zero Trust posture. Security wraps each workload and compute container to prevent data collection and unauthorized access across the network.

- **Data security**—The data pillar focuses on securing and enforcing access to data. To do this, data is categorized and then isolated from everyone except users that need access. This process includes categorizing data based on mission criticality, determining where data should be stored, and developing a data management strategy accordingly as part of a robust Zero Trust approach.

- **Visibility and analytics**—Visibility into all the security processes and communication related to access control, segmentation, encryption, and other Zero Trust components provides crucial insights into user and system behaviors. Monitoring your network at this level improves threat detection and analysis while empowering you to make informed security decisions and adapt to ever-changing security landscapes.

- **Automation**—Improve scalability, reduce human error, and increase efficiency and performance by automating manual security processes that apply policies consistently across the enterprise.

- **Infrastructure security**—This pillar ensures systems and services in a workload are secured against unauthorized access and potential vulnerabilities.

- **Network security**—The network pillar focuses on isolating sensitive resources from being accessed without authorization. This involves implementing micro-segmenting techniques, defining network access, and encrypting end-to-end traffic to control network flows.

04
Benefits of Zero Trust

An effectively implemented Zero Trust model should go beyond security. It should enable businesses to operate more effectively, enabling secure, granular access for everyone, including:

- Decreasing infrastructure complexity
- Working in hybrid physical and cloud environments
- Working with a variety of different devices and in different physical locations
- Complying with internal and regulatory standard
-

Virtual private networks (VPNs) often struggle to keep up with the complexity of modern tech environments. And although Zero Trust and VPN are not mutually exclusive, many organizations find that VPN is unnecessary after the adoption of a Zero Trust model.

VPNs offer perimeter-based security that provides network-wide access; in contrast, ZTNAs grant access only to specific resources after verification and authentication. Compared with VPNs, ZTNA strengthens security around internal and external networks by reducing the attack surface and implementing more granular control. Additionally, ZTNA offers increased flexibility and scalability, improving resource utilization and reducing the strain on IT.

This makes ZTNA a great option for CISOs and IT leaders looking for a security solution that addresses the needs of an increasingly remote and distributed workforce.

05

Executive Order: "Improving the Nation's Cybersecurity"

In May 2021 the Biden administration announced a new Executive Order on Improving the Nation's Cybersecurity—and emphasized the need for adopting Zero Trust across public and private enterprises:

"To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. **The Federal Government must adopt security best practices [and] advance toward Zero Trust Architecture..."**

This may leave some IT leaders wondering how to bridge the gap from where they are now to this modern, Zero Trust future. Significant technology and architecture changes can quickly disrupt business-as-usual and complicate daily operations. But standing still isn't an option either. With increasingly broad attack surfaces, legacy perimeter-based security architectures are no longer going to cut it.

06

Barriers to Implementing Zero Trust Network Access

Despite the obvious security gains from a Zero Trust approach, there can be significant obstacles when moving your organization to a new cybersecurity model.

Even with third-party services, many businesses still struggle to successfully implement Zero Trust Network Access. According to a report by Cybersecurity Insiders, only 15% of companies already have a Zero Trust strategy in place, while another 63% of companies intend to develop a strategy in the near future. Similarly, in a survey conducted in 2019, only 16% of physical data centers have implemented a Zero Trust architecture.

If you're planning to adopt a Zero Trust approach, you'll need to anticipate and plan for these potential challenges.

Type	Detail
Accommodating Complex and Hybrid Environments	Modern companies have highly complex and distributed infrastructures. IT leaders face the challenge of creating a Zero Trust strategy that accounts for an environment that may have hundreds of different databases, servers, proxies, internal applications, and third-party SaaS applications. To further complicate matters, each of these may run in multiple different physical and cloud data centers, each with its own network and access policies. For many organizations, bringing a network to a level that conforms with Zero Trust protocols requires a large number of custom configurations and time-intensive development projects. This burden may drive organizations to take shortcuts that are not scalable or secure.
Using a Hodgepodge of Tools	To build infrastructure to support a Zero Trust model in such an organization, you'd have to implement a number of different micro-segmentation tools, software-defined perimeter tools, and identity-aware proxies. This set of tools may include VPNs, multi-factor authentication (MFA), device approval, intrusion prevention systems (IPS), single sign-on (SSO) solutions, and more. However, many of these systems are specific to cloud providers, operating systems, and devices. Many organizations do not support one homogeneous set of devices, but instead run in multiple clouds and physical data centers, have users on both Mac and Windows, have servers running multiple Linux distributions or Windows Server versions, and support all sorts of different network-connected devices. Vendors for these tools often require organizations to buy redundant technologies to support all of these environments. These vendors may also add unnecessary complexity by focusing on the network layer rather than placing controls near users and applications.
Transitioning from Legacy Systems	Additional challenges arise with legacy systems and third-party applications that are designed around implicit trust. Organizations often cannot configure legacy or third-party applications in a way that conforms with a Zero Trust model without rebuilding them. Administrators often have to create their own frameworks and infrastructure to support them, this adds complexity, time, and expense—and requires buy-in at every level.

Type	Detail
Addressing Gaps in Security	Transitioning to Zero Trust can introduce gaps in security that can increase risk. Most organizations adopt Zero Trust over time, taking a piecemeal approach. While this helps manage costs and resources, it can introduce gaps in security, especially if you're migrating from a legacy architecture.
Managing Cost Constraints	Migrating to ZTA can be costly, especially if you are transitioning from a legacy system. A comprehensive Zero Trust framework may require you to build infrastructure from scratch. This means a long-term, multi-phase process that requires significant resources and time. Although these costs can be managed somewhat through incremental adoption, the speed and scale of adoption can be a challenge. Not to mention the costs of training talent and investing resources into maintaining a Zero Trust architecture post-implementation. Even after project development, organizations need to put aside resources for ongoing maintenance. For instance, micro-segmentation requires regularly updating IP data and configuring and verifying changes to minimize access for users. Further, as administrators introduce new systems and applications into the network, they must add them in such a way that conforms to the Zero Trust protocols, often requiring additional framework development.
Balancing Security vs. Performance	Zero Trust prioritizes security by locking down access until a user is verified. The challenge is making sure Zero Trust access management doesn't impact workflows and performance. For instance, if an employee changes roles, they will need updated access to required data. If that role change isn't recognized quickly, users could be locked out of key files they need to do their job—hurting productivity and causing roadblocks in workflows.
Adjusting Mindsets	Building a Zero Trust model in a large organization requires buy-in from key stakeholders to ensure proper planning, training, and implementation. The project touches nearly everyone in the organization, so managers and leaders all must agree on the plan. With many organizations slow to implement such change, the politics of this alone can add a lot of strain on the successful performance of the project.

07

How to Achieve Zero Trust

Zero Trust implementation won't happen overnight. Often, existing infrastructure can be integrated into a Zero Trust approach, but to reach maturity, most networks will need to adopt and incorporate additional capabilities and processes.

Fortunately, transitioning to a mature Zero Trust architecture can occur one step at a time. And in fact, incrementally adopting a Zero Trust security posture can reduce risk as improved visibility enables the organization to adapt to meet threats as they emerge. Follow a strategic plan to adopt Zero Trust as part of a continually maturing roadmap.

From the initial planning to basic, intermediate, and advanced stages, your Zero Trust maturity model should help you improve cybersecurity protection, response, and operation over time.

Migrating to ZTA requires a thorough understanding of your network architecture's current state, including all its assets (both physical and virtual), subjects, and business processes. If this information is incomplete, you will have blind spots in your network security—particularly if there are unknown "shadow IT" components operating within your ecosystem.

By conducting a comprehensive audit and analysis of your network's current state, you can then map out what steps need to be taken to optimize the network for ideal ZTA.

The Cybersecurity and Infrastructure Security Agency (CISA) describes a Zero Trust Maturity Model enterprises can follow based on the key defensive pillars listed earlier. Additionally, it citesgovernance, how you control and direct your security strategy, as another key part of a mature ZTA foundation.

CISA's model represents a gradient of implementation across those key pillars "where minor advancements can be made over time toward optimization." Organizations can take isolated steps focusing on one pillar at a time, with each category progressing at its own pace until cross-coordination is required. This model supports gradual evolution toward Zero Trust, distributing costs and resources over time, and easing the burden of implementation.

The National Institute of Standards and Technology (NIST) has outlined six steps for migrating to a Zero Trust architecture.

1. Identify Actors on the Enterprise.

Who are your subjects and users? In order for Zero Trust to work, your policy engine needs to know who your enterprise subjects are and their access permissions. Pay attention to users with special privileges, such as developers or systems administrators who are often given blanket access on legacy systems. Zero Trust should allow these users enough flexibility to perform their work while applying logs and audit actions to verify and validate access.

2. Identify Assets Owned by the Enterprise.

Zero Trust Architecture also needs to be able to identify and manage assets and devices. These assets include hardware components like laptops, phones, and IoT devices, as well as digital artifacts, such as user accounts and applications.

Managing enterprise assets involves not only cataloging but also configuration management and monitoring. Your architecture should be designed to observe the current state of an asset in order to effectively evaluate access requests.

3. Identify Key Processes and Evaluate Risks Associated with Execution.

The next step is to inventory and rank your business processes and data. Business processes should inform how resource access requests are granted and denied.

Your assessment will help you identify which processes to target first for ZTA migration. You may want to start with low-risk business processes as disruptions are less likely to negatively impact the rest of the organization. Then, you can migrate more complex and business-critical processes.

4. Formulate Policies for the ZTA Candidate.

Which services or processes you target for initial ZTA migration will depend on a number of factors, including:

- The importance of the process to the organization
- The group of subjects affected
- The current state of resources used for the workflow

Assess the value of assets and workflows based on risk. Consider all upstream resources, downstream resources, and entities that are used or affected by the workflow. These can all influence which assets are chosen as candidates for migration.

5. Identify Candidate Solutions.

Once you've identified a list of potential candidates, create and consider a list of solutions to implement Zero Trust strategies. Keep in mind the various Zero Trust principles and requirements as you determine which candidates are best suited for migration.

6. Initial Deployment and Monitoring.

When you've chosen a candidate workflow and identified which ZTA solutions you'll be applying, you can start deployment. This will be an iterative process as you observe and monitor the new solution and update the workflow as needed.

As you build up your Zero Trust architecture and gain confidence in the process, you'll enter a steady operational phase. While you will continue to monitor and make adjustments to the network and assets, you can start planning the next phase of Zero Trust deployment.

07

Zero Trust Best Practices

1. Rigorously enforce authentication and authorization

All resources must be verified and authenticated. This often includes using technologies like multi-factor authentication (MFA) to grant access rather than operating on implicit trust.

2. Maintain data integrity

Measure and monitor the security of all owned assets to ensure data integrity and reduce cyber threats.

3. Gather data for improved security

Regularly collect data from multiple sources, like your network infrastructure and communication to continuously adapt and improve your security posture.

4. Consider every data source and computing device as a resource

Any device that has access to a network should be treated as a resource.

5. Keep all communication secured regardless of network location

Location no longer carries implied trust. Users and devices connecting via external or internal networks must undergo the same security requirements to gain access.

6. Grant resource access on a per-session basis

Enforce least privilege, requiring users to request access for each session.

7. Moderate access with a dynamic policy

Protect resources with a transparent and dynamic security policy that adapts to the evolving needs of the network and its users.

08

How Better.com Used strongDM to Adopt Zero Trust Access

Better.com is an online lender that provides a 100 percent digital home buying process that is faster, easier, and more transparent. As a financial tech company handling sensitive customer data, Better.com needs a robust network security approach. But prior to strongDM, they didn’t have an efficient management system for database access.

Despite their highly digitized public-facing services, their backend management processes and governance operations were highly manual—creating burdensome overhead costs and increased risk of error. As a result, it often took up to a week to get access provisioned. This not only took team members away from higher priority activities but also had a downstream impact on productivity in favor of security. And with 41 databases and five database management systems, this approach was unsustainable—they needed a solution that could help them implement Zero Trust across their systems while scaling and strengthening their data security posture.

That's where strongDM came in. strongDM [makes it easy to grant access and audit access control](). Better.com was able to implement strongDM within a day and started seeing results immediately. In fact, within a week, Better.com saw an increase in user requests once users saw how easy it was to access databases.

And users can access the database from anywhere. "For Zero Trust, strongDM is an amazing tool—BYOD, within the company, outside [the company], wherever you need to go, you can access the data in a secure way," says Ali Khan, CISO at Better.com.

Key benefits included:

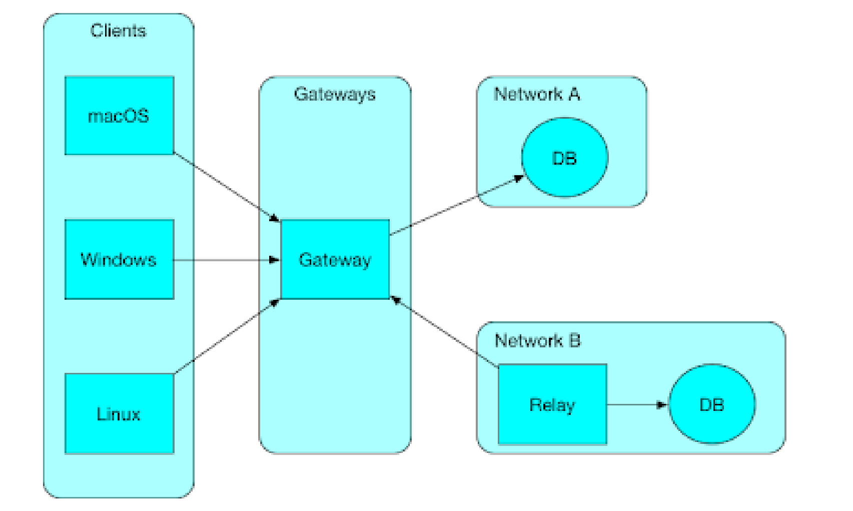
Type	Detail
Proactive data loss prevention	With strongDM, Better shifted from a reactive security posture to a proactive approach to data loss prevention. By monitoring and detecting suspicious activity in real time, Better.com was able to suspend users before they could cause damage.
Faster incident response	strongDM's audit capabilities ensure all activities are logged and tracked, from permission changes to employee queries. This provides peace of mind while ensuring compliance and the ability to respond quickly to potential incidents.
Reduced overhead costs	strongDM relieves the burden on security teams to monitor and manage database connections so they can focus on other priorities. Before strongDM, it took Better.com's team a week to get someone provisioned. Now it takes just minutes.
Improved compliance and regulatory adherence	strongDM enables stronger and simpler compliance without unnecessarily locking down data and preventing business users from accessing the information they need to do their jobs.

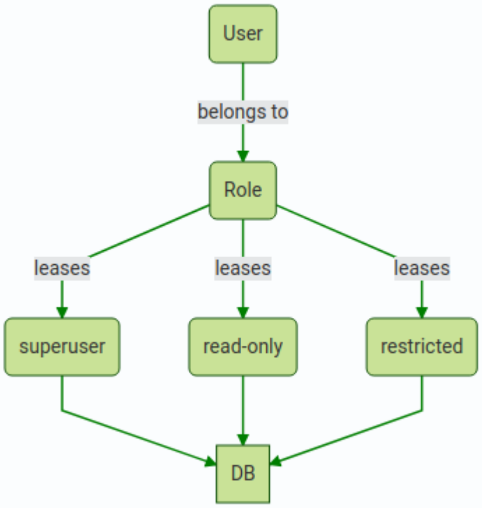
09

Transition to Zero Trust today with strongDM

Access management is a key part of building a successful and robust Zero Trust security posture. But disparate systems and manual processes mean creating unique roles for every individual is a time-consuming and costly endeavor—and one that can leave your network vulnerable. strongDM makes it easy to transition to a Zero Trust security model by managing and auditing access to databases, servers, clusters, and web apps for you.

strongDM simplifies the implementation of Zero Trust to your infrastructure by providing:

Type	Detail
A single Zero Trust tool for all of your infrastructure	strongDM integrates out of the box with any identity provider via OpenID Connect (OIDC) protocols to secure access to any server, database, or other firewalled resource regardless of where it's hosted. You don't have to worry about complex configuration of access controls or using a range of micro-segmentation tools to authenticate users. From a central control plane, admins can view all connected resources, all active users, and all user permissions.
Segmentation	strongDM architecture creates a software-defined network (SDN) that proxies client traffic through a centralized gateway to monitor and manage access to your resources. By doing so, the backend network topology and configurations can be greatly simplified by only processing traffic from the gateway, allowing access logic to be implemented and managed in a single location.  Clients macOS Windows Linux Gateways Gateway Network A DB Network B Relay DB

Type	Detail
Access control	strongDM allows admins to create and assign roles, or a collection of permissions, to groups of users. By doing so, admins can manage access control at a higher level of abstraction and can easily assign permissions across different subsets of users. The implementation of the configuration and network changes is handled automatically and the changes are deployed across the network. In addition to ensuring proper Zero Trust infrastructure, this makes it very easy to onboard and offboard employees, contractors, and vendors. The administrators simply have to link their identity account and assign the appropriate roles, with the backend registrations and access controls automatically set.  User belongs to Role leases leases leases superuser read-only restricted DB
Visibility	By centralizing logic into a control plane, strongDM allows administrators to easily audit usage. This greatly simplifies the process and reduces the possibility of human error.

Imagining an ideal, fully Zero Trust architecture can make the path to achieving it seem daunting (not to mention cost-prohibitive). But it doesn't have to be. Ultimately, Zero Trust isn't a technology but a security framework and philosophy, which means you can build it into your existing architecture without completely ripping out existing infrastructure.

Want to learn more? Get a free no BS demo of strongDM.

10

More Zero Trust Resources

What is Attack Surface and How to Reduce It

7 Network Segmentation Best Practices to Level-up Your Security

Better.com Customer Story

You Can't Have Zero Trust Without Identity and Access Management

Understanding Lateral Movement and How to Prevent It strongdm

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.