ZTNA
Zero Trust Network Access

Never trust. Always verify!

timus

Introduction

In recent years, especially after the pandemic, Zero Trust Network Access (ZTNA) has been one of the most influencing concepts in the network and cybersecurity world.

IT teams have traditionally relied on virtual private networks (VPNs) to provide secure remote access to distributed workforces. But VPNs and traditional network architectures simply cannot keep up with the increasing demand for scalability of secure access. ZTNA, far from being an over-hyped buzzword, will soon become the standard means by which organizations configure their security and access control systems. Remote working and migration to the cloud, which the pandemic has greatly accelerated, are pushing the concept of “zero-trust” forward. Often referred to as software-defined perimeter (SDP) services, ZTNA provides seamless and secure connectivity to private applications without placing users on the network or exposing applications to the internet.

Gartner, who coined the term ZTNA back in 2019, has made up-to-date forecasts for the rapidly growing ZTNA market. The company predicts that 80% of new digital business applications opening up to ecosystem partners will be accessed through ZTNA by 2022. And by 2023, 60% of all enterprises will phase out most of their remote-access VPNs in favor of ZTNA solutions. The Gartner team also estimates that 40% of all enterprises will adopt ZTNA for uses besides VPN replacement, such as third-party access, multi-cloud access, and activities related to M&As or divestitures.

If you're not familiar with ZTNA, this white paper will help you compare ZTNA and VPNs and show how you can secure your remote workforce within a zero-trust framework.

80%

New business applications using ZTNA

2022

60%

Shift from VPNs to ZTNA

2023

40%

ZTNA adoption (other than VPN replacement)

2023

Contents

What is ZTNA?

The zero-trust framework has been developed to help today's businesses secure their most valuable assets in a distributed cloud-native environment. Within the last decade, companies have begun distributing their data, assets, applications and services across multiple environments and cloud infrastructures. This decentralized approach has rendered the traditional castle-and-moat security strategy ineffective, as network security can no longer be restricted to a single location, group of devices, or group of users.

With many organizations shifting their priorities to a "zero trust" approach, zero-trust network access (ZTNA) represents a strategy for achieving an effective security model.
It is a set of technologies and functions that provide remote users secure access to internal applications. It operates on an adaptive trust model in which trust is never assumed, with access granted on a need-to-know basis defined by granular policies.

The Definition of 'ZTNA'

With many organizations shifting their priorities to a "zero trust" approach, zero-trust network access (ZTNA) represents a strategy for achieving an effective security model. It is a set of technologies and functions that provide remote users secure access to internal applications. It operates on an adaptive trust model in which trust is never assumed, with access granted on a need-to-know basis defined by granular policies.

Castel-and- moat security strategy is no longer effective

ZTNA provides a clear and defined framework for organizations to follow. It is also a component of the SASE (Secure Access Service Edge) model, which includes, in addition to ZTNA, next-generation firewalls, SD-WAN and other services in a cloud-native platform.

Why ZTNA?

Zero-trust is based on the idea that there is no network edge. It requires a system design that assumes all users and services represent a potential threat – even if they are inside your network. Your system requires continuous evaluation of access requests before granting access rights to any of your resources. Logins, connections and API tokens will be short-lived, and users and devices will be continually verified for their identities and privileges.

This “never trust, always verify” approach allows you to monitor access to your applications and services closely. Your organization requires tight access control and maximum observability in a cloud-native world, where users can be physically distributed using multiple devices within secure and unsecured networks.

Why Does Your Application Need ZTNA?

“Don’t trust anyone unless they can prove their trustworthiness.”

This is the main philosophy that ZTNA was developed on. While this may seem a rather paranoid approach, it remains the only smart way to access your network and keep your people, apps and data safe.

"Inside is safe, outside isn’t”, or not?

While this approach may look safe, it no longer meets today's security challenges. Your workforce largely works remotely and utilizes cloud solutions. This, in turn, makes you increasingly vulnerable to attacks. You may think it's safe inside, but if hackers get in, they can easily access everything on your network.

3 Essential Functions of ZTNA

Verification

Continuously verify inside and remote access requests based on identities and context.

Enforcement

Define the access conditions and policies by which certain users can or cannot access specific resources.

Monitoring

Log and analyze all access attempts, ensuring that mandatory policies align with business needs.

How does ZTNA Work?

The connector application installed in the user devices establishes an outbound connection to the ZTNA service through a secure, encrypted tunnel. This serves to verify the security status of user devices and provide access to allowed applications via the secure tunnel. The service is primarily responsible for authenticating users with their credentials and continuously verifying their behaviors.

ZTNA removes app access permission from network access action. The separation of the two components reduces all risks to the network and will only provide application access to authorized users. Users do not enjoy access to the entire network but only to the apps they need for their work.

ZTNA removes app access permission from network access action.

BASIC PRINCIPLES

Never trust. Always verify.

Your system should continually ask users and services to verify their identity, device, location, and other data attributes to ensure that only privileged users and services can gain access. Tokens, sessions and connections should be short-lived, requiring re-authentication from users and services to continue accessing sensitive resources to a data center, like SD-WAN.

Constantly monitor and observe

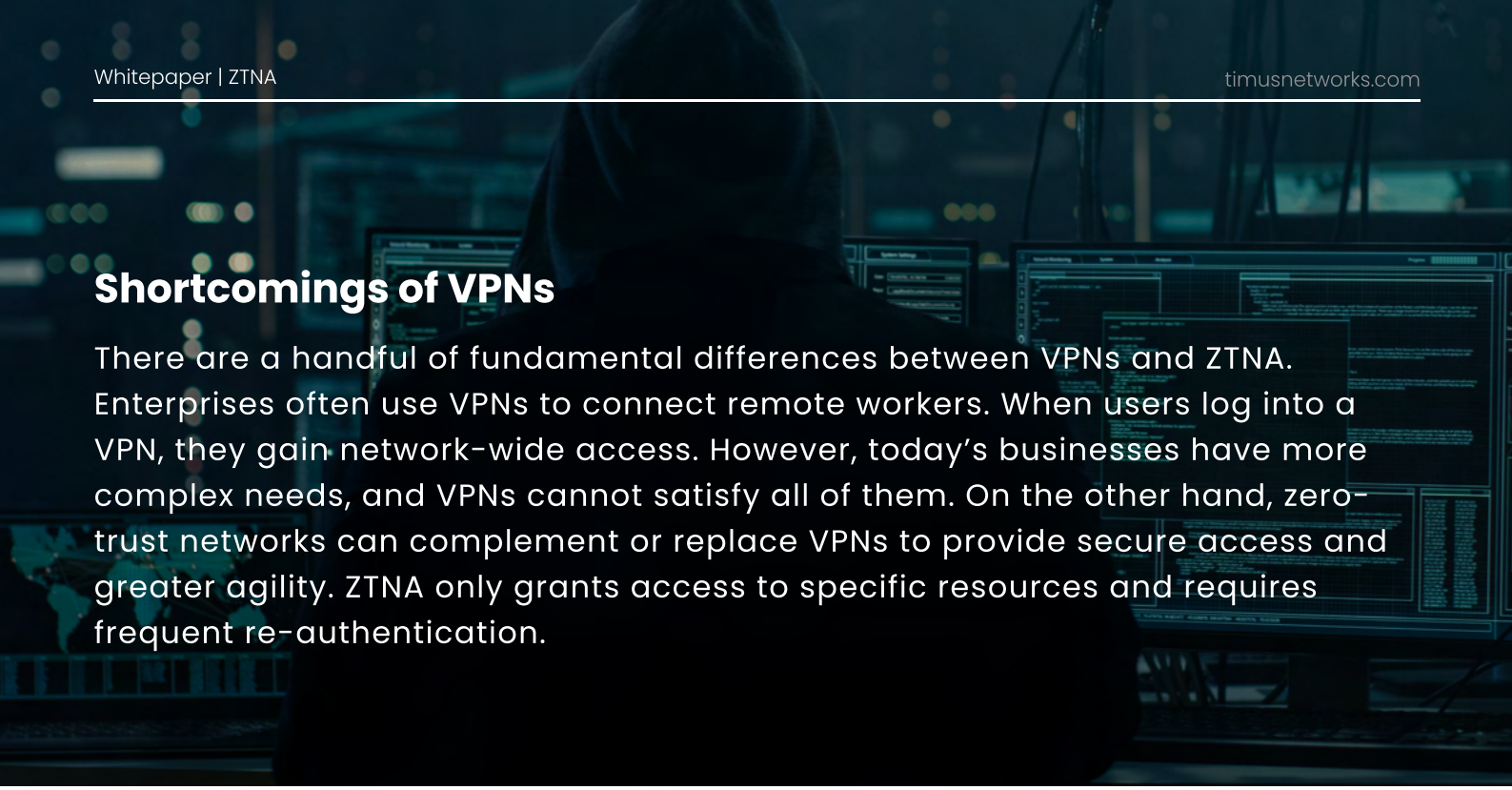
Continuous monitoring and observability allow you to understand and evaluate – in real-time – which users are trying to access which resources. It also provides your network and security teams with real-time information on Key Characteristics of potential threats, anomalous behavior, and active security incidents. This allows them to act quickly and decisively to resolve potential security incidents and limit the blast radius of a possible breach.

Limit privileges to those who need them

Ensuring that users only enjoy access to needed resources is a core tenet of the zero-trust framework. It is important to know which of your users require access to which resources and what they will do with them to limit unauthorized access. This is an important component of the micro-segmentation principle.

Micro-segmentation

By dividing your network into smaller, more focused segments, you can minimize the scope and impact of breaches and potential security incidents. These network segments are independent of one another and are designed to prevent would-be attackers from moving sideways across your network. Each segment has its own users, roles and access policies that are constantly evaluated and monitored.



Shortcomings of VPNs

There are a handful of fundamental differences between VPNs and ZTNA. Enterprises often use VPNs to connect remote workers. When users log into a VPN, they gain network-wide access. However, today's businesses have more complex needs, and VPNs cannot satisfy all of them. On the other hand, zero-trust networks can complement or replace VPNs to provide secure access and greater agility. ZTNA only grants access to specific resources and requires frequent re-authentication.

Shortcomings of VPNs

VPNs cannot satisfy the complex needs of today's businesses

Resource Utilization

As the number of remote users grows, the increasing load on a VPN server can cause unexpectedly high latency, requiring new resources to be added to meet rising demand or peak usage times. This can also put a strain on an organization's available workforce.

Flexibility & Agility

VPNs do not provide the granularity of ZTNA. Installing and configuring VPN software on all end-user devices that need to connect to corporate resources can be difficult. Conversely, it is much easier to add or remove security policies and user authorizations in ZTNA.

Granularity

Once inside a VPN perimeter, the user gains access to the entire network. ZTNA takes the opposite approach and does not grant access to an asset unless it is specifically authorized for that user. VPNs and ZTNA can, however, be used in combination with one another, thus providing an extra layer of security if a VPN is compromised.

VPNs and ZTNA: What's the Difference?

	VPN	ZTNA
Design	Simple barrier	Multiple barriers
Access	Network	Application / Resource
Administration	No application declaration and complex access assignment	Application declaration and fast access assignment
Conformity Check	Simple	Granular
Verification	One time	Continuous
Security	Perimeter-based, low	Identity-based, high

Benefits of ZTNA

There are a handful of fundamental differences between VPNs and ZTNA. Enterprises often use VPNs to connect remote workers. When users log into a VPN, they gain network-wide access. However, today's businesses have more complex needs, and VPNs cannot satisfy all of them. On the other hand, zero-trust networks can complement or replace VPNs to provide secure access and greater agility. That's because ZTNA only grants access to specific resources and requires frequent re-authentication.

ZTNA addresses this need by offering granular, context-aware access to business-critical applications without exposing other services to potential threats.

Dividing networks into micro-segments

ZTNA allows organizations to create software-defined perimeters and divide corporate networks into multiple microsegments, thus preventing the lateral movement of threats and reducing attack surfaces in the event of a breach.

Making applications invisible on the internet

ZTNA creates a virtual darknet and prevents application discovery on the public internet, protecting organizations from internet-based data exposure, malware and DDoS attacks.

Securing access to legacy apps

ZTNA can extend its benefits to legacy applications hosted in private data centers, thus facilitating secure connectivity and offering the same level of security as web applications.

Leveraging the user experience

ZTNA provides secure, fast, seamless, and direct cloud access to private applications, providing a consistent experience for remote users accessing SaaS and private applications.

Benefits at Multiple Layers

Company

- Security risks are limited by a reduced attack surface and micro-segmentation
- The elimination of legacy security systems serves to bolster security and reduce costs
- A simpler user experience increases security compliance

Administrator

- A single console for managing role-based access policies
- Unified access control for all on-premises and cloud resources
- Integration with existing security and identity providers
- User and device-indexed logging for in-depth security and performance monitoring
- Split tunneling routes non-essential traffic over the internet, not your network

User

- A consumer-like app installation experience that requires no device configuration
- Higher performing connections to resources serve to increase productivity
- Frictionless remote access makes working from home easier and more efficient

Do Ransomware Attacks Drive ZTNA Adoption?

A study of 5,400 IT professionals has revealed a direct correlation between ransomware attacks and the adoption of a zero-trust approach.

Q: How did the pandemic impact your plans to adopt a zero-trust approach?	Not hit by ransomware within the last year	Hit by ransomware within the last year	Hit by ransomware within the last year, paid ransom
It created a need for zero-trust that didn't exist before	39%	47%	59%
It allowed us to increase our budget with a view to moving to zero-trust	36%	50%	57%
We diverted resources from other activities in order to move to zero-trust	29%	39%	54%

Conclusion

By 2023, 60% of all organizations are expected to replace VPNs with ZTNA

Zero-trust is more than just a restatement of two common but important security principles: least-privileged access and resource concealment. More importantly, the zero-trust approach reduces risk and increases business agility by eliminating implicit trust and continually assessing user and device trustworthiness based on identity, adaptive access, and comprehensive analytics. With the zero-trust approach, only approved users are given access to approved resources, while unapproved resources are neither seen nor accessed by unapproved users.

As the workforce migrates to remote environments, security risks are coming with them. As remote working becomes more commonplace, it is increasingly important for organizations to address these risks and prepare to meet – and overcome – new security challenges. This is where ZTNA comes in. Adoption of ZTNA has been accelerated by the Covid-19 pandemic and the shift to remote working, both of which have led to scalability and performance issues in traditional virtual private networks (VPNs).

With digital transformation efforts, many organizations will have more systems, applications and data in the cloud than on their on-premises networks. In light of this new reality, ZTNA services move verification, validation and privilege assignment services to the user location – namely, the cloud.

But ZTNA services will not replace perimeter security overnight. The castle and moat security format will continue to be used in many settings. Over time, however, organizations will start implementing security models like ZTNA to provide more secure targeted access to valued resources while eliminating issues associated with trusted access.

Key Findings of Forrester's Research

- The recent explosion of data, applications, remote users, mobile devices, and bring-your-own-device (BYOD) capabilities have increased security risks. It has also increased the potential for blind spots for security teams tasked with identifying and neutralizing online threats.
- Enterprises remain vulnerable since distributed environments can reduce visibility and increase attack areas. More than 75% of respondents report increased levels of vulnerability in their organizations due to larger attack surfaces. What's more, novel security solutions and integration challenges can lead to dangerous gaps in security.
- Technology solutions can make or break your security strategy. Research has found that 70% of enterprises lack a cohesive approach to security. And while IT decision-makers are facing increased pressure from upper management, they are also grappling with cultural issues between their IT and security teams.

About Timus

Timus is a unified platform built to secure the modern workplace.

timus

timusnetworks.com

15April2022-Version:001