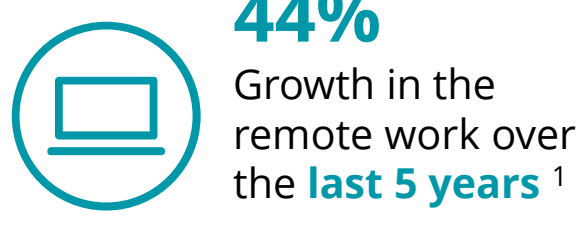


## Zero Trust Network Access

The importance of Zero Trust Network Access (ZTNA) solutions for Corporate Networks

The corporate network is described as trusted on a traditional approach. However, due to the **rise of remote work** and the **increased use of cloud-based applications**, the network perimeter has become more difficult to define. Users are not only accessing the applications through the corporate network but also from **any location outside** the company. It is crucial to understand how to increase network access security in this new paradigm.

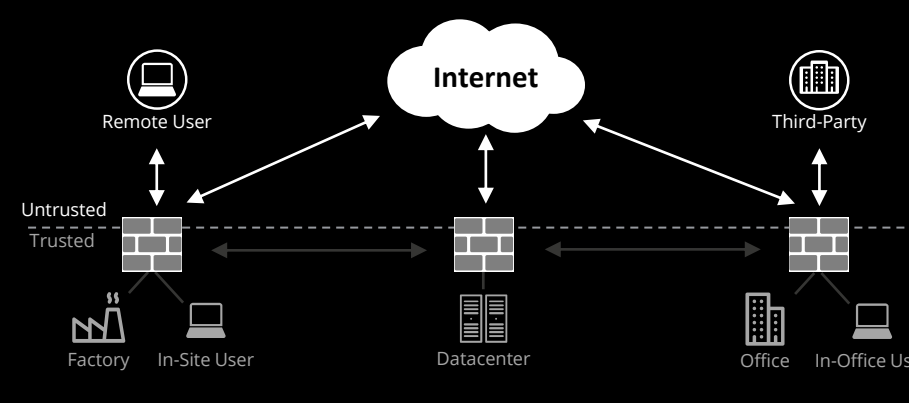


Sources: <sup>1</sup> NorthOne, <sup>2</sup> CloudAwards

## What is the difference between the Traditional perimeter security and Zero trust security approach?

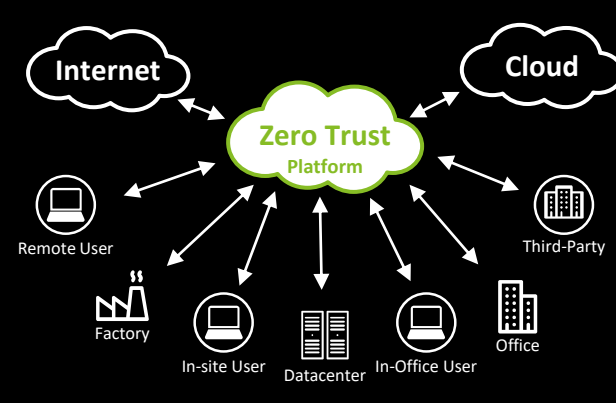
### Traditional perimeter security

This type of architecture was designed considering that users are **in the office or site** and all applications are at the **datacenter**. The corporate network is considered a **trusted** network and external connections are **untrusted**.



### Zero trust security

Zero Trust Security applies the principle of **never trust**, always verify, by eliminating implicit trust and continuously validating the **Identity of the user**, whether inside or outside the security perimeters.



The traditional perimeter is no longer the best practice recommended to fulfil network security requirements of the organizations. As cloud becomes the new datacenter and users continue to work from different locations, **identity needs to become the new perimeter**, by refusing access to any device or process that fails to offer an identity with the correct permissions

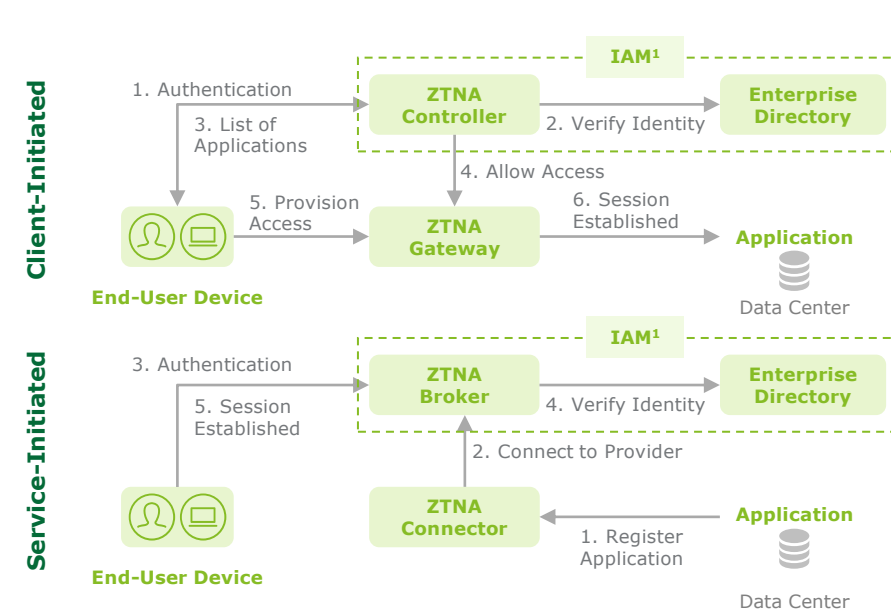
## What is ZTNA?

ZTNA is one of the SASE (Secure Access Service Edge) architecture components, and aims to replace the traditional network access model with user/application **identity-centric** software-defined perimeters

### How does it work?

- Whenever a user, device, or app tries to access a corporate resource, ZTNA verifies that they are a trusted entity, following the Zero Trust principle **never trust, always verify**
- It does this **based on user identity**, not their IP address. It can examine context (such as device type, geolocation, security posture, specific resources being accessed) to automatically apply the right policy
- ZTNA ends up creating an identity context-based, logical-access boundaries around business applications, **restricting and securing on-premises and cloud access**

### Simplified architecture

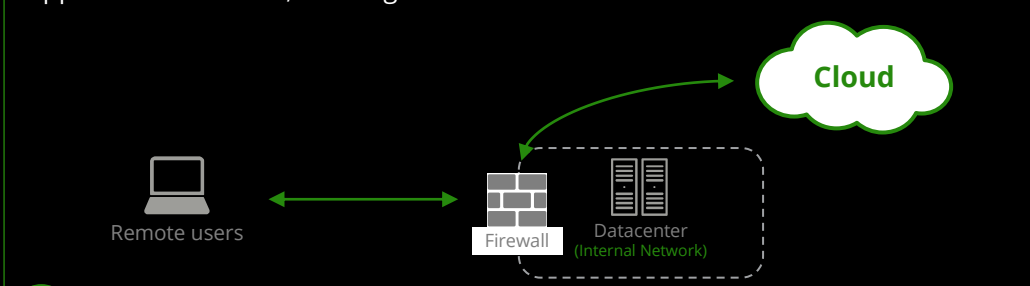


As organizations continue their Zero Trust Security journey, it is expected that more companies will change from their traditional VPN to ZTNA solutions. Gartner predicts that **"By 2023, 60% of enterprises will phase out most of their remote access VPNs in favor of ZTNA."**

## What are the main differences between VPN and ZTNA?

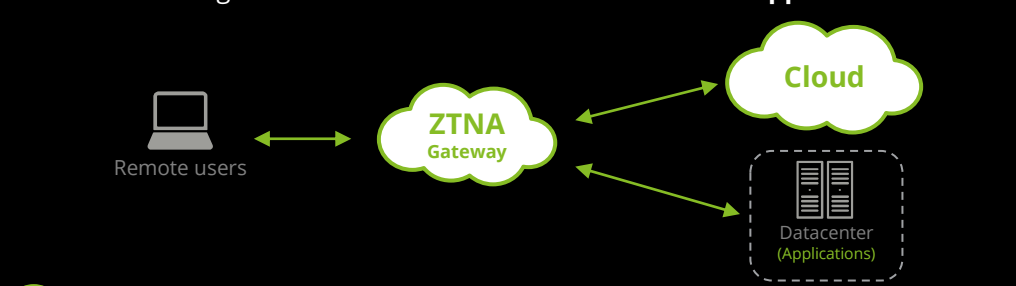
### Virtual Private Network (VPN)

VPN allows remote users to **connect to the company network** to access internal applications/ services, creating a secure tunnel between the **user** and the **network**



### Zero Trust Network Access (ZTNA)

ZTNA allows remote users to **connect to specific internal applications/ services**, creating a secure tunnel between the **user** and the **application**



- #### VPN FEATURES
- The user connects to the corporate network using internet or MPLS connections
  - The user has **visibility** over unnecessary corporate services and applications
  - The company has **partial visibility** of the user activity (e.g., only the up/ downtime)
  - The VPN concentrator is **visible from the Internet** (more exposed to cyberattacks)
  - User experience can be degraded by low **latency** or **inefficiency** of communication

- #### ZTNA FEATURES
- The user connects to an **application/ service** through the internet
  - Ensures user **least privileged access** and **visibility** to corporate applications
  - The company can have **full visibility** of the user activity (e.g., which application is used)
  - Applications/ services are **protected** and **invisible** from the Internet
  - Better user experience when using ZTNA due to the **proximity of cloud processing**

To ensure that organizations take the full potential of ZTNA, there are a set of **best practices that should be considered** when implementing the solution

- Identify ZTNA use cases & prioritize critical assets** - Before the implementation, organizations should **identify their ZTNA use cases** to ensure that the **most valuable business assets are protected first**, and policies are applied to restrict access to sensitive applications
- Ensure full visibility over existing architecture** - Ensure that there is a **clear visibility** over the existing **network topology, applications** and **users**. It is important to understand who are the users, existing devices and applications, and their location in the network
- Apply the principle of least-privileged** - Determine **who** in the organization requires access to **what** resources, **how** and **when** this access is required, to ensure that access is **only granted to resources that need the access** to perform daily functions
- Enable user Multifactor Authentication (MFA)** - Verify the user identity with **Multi-factor Authentication**, enabling an **additional verification layer** to authenticate users attempting to access the most sensitive data or to elevate their privileges
- Update/ review policies regularly** - Ensure that there are processes in place to **maintain** and **continually review/ update existing policies**, to ensure that they regularly **improve** and **refine access policies over time**, considering applications and business changes

## How can Deloitte help?

Our team combines technology and engineering expertise with business strategic skills that allow us to be a unique partner for the whole IT and OT transformation journey

- Trust-worthy advisor for **every step of Zero Trust Network Access solution**, with a proven methodology from vendor assessment to design until implementation
- Unique technology and engineering offerings**, with a proven track record in network and security transformations programs
- Multidisciplinary specialized teams, which combine the **high technical expertise** with **business and strategic consulting teams**

## Contacts

### Sponsors

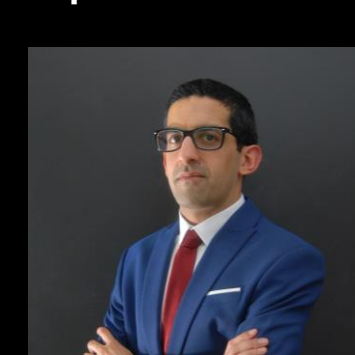


**Pedro Tavares**  
Partner  
petavares@deloitte.pt



**Luís Abreu**  
Partner  
labreu@deloitte.pt

### Experts



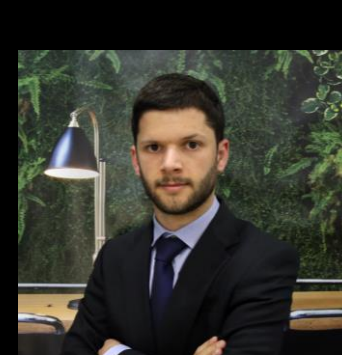
**Vikash Laxmidas**  
Telecom Engineering Excellence  
Manager  
vlaxmidas@deloitte.pt



**André Santiago**  
Telecom Engineering Excellence  
Manager  
ansantiago@deloitte.pt



**José Mesquita**  
Telecom Engineering Excellence  
Manager  
jmesquita@deloitte.pt



**David Andrade**  
Telecom Engineering Excellence  
Senior Consultant  
davandrade@deloitte.pt

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's more than 345,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.