

Minimize Business Risks with  
**Timus SASE**

# **VPNs** vs. **Zero Trust** **Network Access**

What's the difference?



ZERO TRUST NETWORK PROTECTION

# Why **VPNs** are outdated and unsafe



- They're not always-on making it difficult to enforce compliance.
- They're credential-based, and dark web is full of stolen VPN credentials
- Once a hacker gets in, they can move laterally across the whole network

## Why **Zero Trust Network Access (ZTNA)** is the better approach

ZTNA is the best way to ensure secure remote access. Unlike VPNs, it thoroughly verifies the identity of the user before granting access.

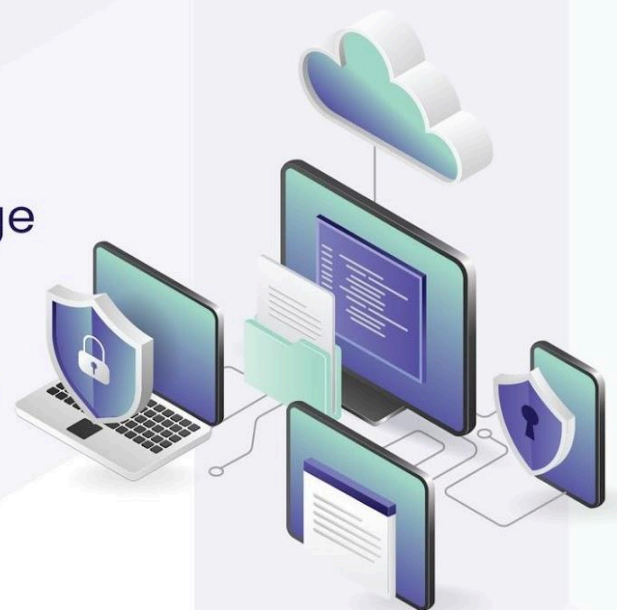
### **Timus ensures secure connections with:**

- Always-on Encrypted Tunnels
- Identity-Based Verification
- Adaptive Multi-Factor Authentication (MFA)
- Device Posture Check

### **Protect your company with:**

- SW-defined Security Perimeter
- Granular Access Control
- No Blind-Spots in Network Usage
- Least-Privilege Principles

ZTNA empowers an organization to minimize its business risks due to sporadic use of VPNs, or unencrypted network access. With **Timus**, MSPs can achieve zero trust and enforce compliance to policies and regulations.





# The evolution of work

## The office era

- Work from an office
- People work 9–5 Mon–Fri
- Desktops and laptops

VS

## The cloud era

- Work from anywhere
- Always on
- Desktop, laptops, mobile, tablets

## The old way of working

- Desktop apps
- Office wifi and networks
- Mostly internal collaborators
- Data lives on a server in the office

VS

## The new way of working

- SaaS apps
- Public and private wifi networks
- Internal and external collaborators
- Data lives everywhere

## The cyberthreat then

- Individual hackers
- Hacking for fun
- One-off hacking attempts at specific targets
- Exploiting technical vulnerabilities

VS

## The cyberthreat now

- Organized hacking cartels
- Professional, profit-driven hacking
- Large scale, AI-powered cyberattacks at scale across multiple levels and devices
- Exploiting both technical and human vulnerabilities

## Technology then

- Hardware-based firewalls
- VPNs
- Credential-based permissions
- Endpoint security

VS

## Technology now

- Cloud firewall
- Zero Trust Network Access
- Identity-based permissions
- Cloud (application) security

# ★ Hear real success stories from our partners with Timus

Brightworks Group, a leading Managed IT Services company, sought the perfect remote access solution to support their clients in the hybrid workforce era. After facing numerous challenges and failed trials, they discovered **Timus Networks**.

Following a successful short trial, Brightworks Group adopted **Timus** for both their company and clients, achieving outstanding results and satisfaction.

**brightworks**  
human focused IT

“ We were pleasantly surprised how MSP-friendly Timus is as a company in terms of the solution, support and simple pricing – and it actually works.

So it kind of ticks all the boxes for me. ”

**Ian Miller**

Director of Engineering, Brightworks Group



**20%**

reduction in  
annual IT  
budgets due to  
security tool  
consolidation

**30%**

drop in  
support tickets

**<1**

avg number of  
days to deploy  
and setup  
Timus