Nasstar

Ebook

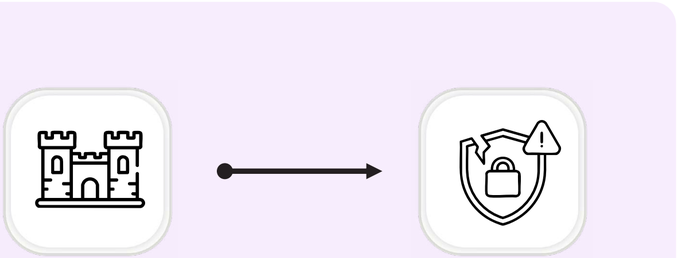
Zero Trust Network Access

From implicit trust to assumed breach

2025

ZTNA keeps your data safer by making sure only the right people on trusted devices can access it. Even if something goes wrong, it limits the damage by containing the threat. Right now, IT teams are under pressure. ZTNA helps by cutting down complexity, easing compliance, and keeping things secure - without getting in anyone's way.

Leigh Walgate
Managing Director | Secure Networks



From employee apps to customer data, your business doesn't live inside four walls anymore. But your virtual private network (VPN) still gives users too much access and provides you too little visibility. Employees, contractors, and even compromised accounts often have access to systems they don't need. That's a huge risk, and it's not worth taking anymore.

Zero Trust Network Access (ZTNA) fixes this. It authenticates every user and device in real time. It shrinks the attack surface, stops lateral movement, and gives you control over who accesses what. That means fewer breaches, fewer sleepless nights, and fewer painful incidents.

Whether you're running cloud-native apps, handling patient records, or juggling global logistics, ZTNA solutions ensure every endpoint earns its place, every time. Remove the uncertainty and help your team shift from reactive firefighting to proactive protection.

The threat

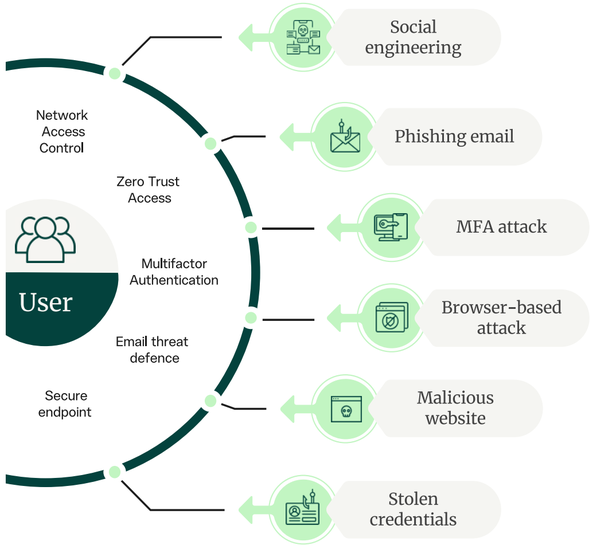
Businesses today are increasingly vulnerable to cyber threats, as threat actors employ a range of tools and techniques to steal sensitive information and access systems and data.

Businesses are responding. Many are patching holes in their defences by adding more security tools - one for identity, one for email, one for endpoint protection, and so on.

But here's the problem...

This patchwork of point solutions can feel like a maze for employees. They're juggling multiple logins, switching between tools, and trying to stay compliant while just trying to get their actual work done.

The result is slower workflows, frustrated users, and a security posture that still has cracks.



80% of all breaches targeted users

*Third Party Threat Intelligence Incident Response Data

Organisations aim to comprehensively protect their users

94%	93%	97%	78%
Own an endpoint security product	Own an email security product	Own an access management product	Own a secure internet access product

But a solution cobbled together through multiple vendors creates an **expensive and disjointed experience**

Nasstar

Impact to your actual day

Let’s walk through a real-world scenario many employees will recognise.

It’s Monday morning. A user starts their day by logging in. Multifactor authentication (MFA) kicks in, as per company policy. So far, so good.

Next comes the hurdle: connecting to the VPN. That means remembering another password - one they don’t use often. After three failed attempts, they’re locked out. Productivity is paused as they call the helpdesk for a reset.

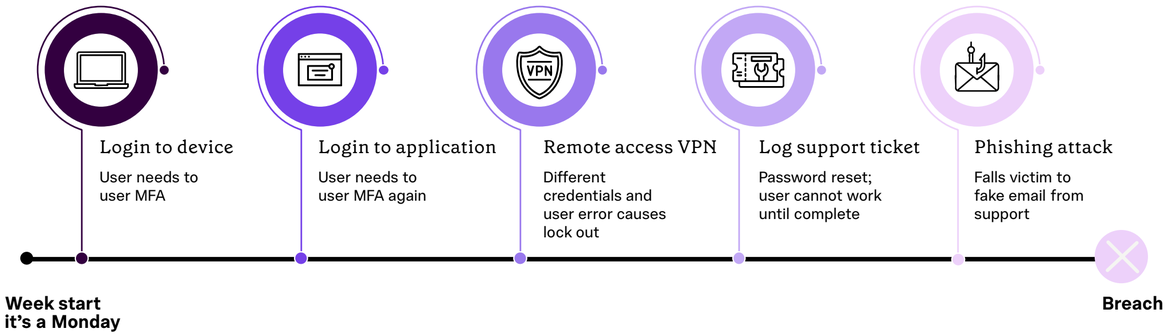
Eventually, they’re back in. But juggling multiple credentials just to access work apps and the company’s private cloud has already cost time and focus

Later that day, a password reset email lands in their inbox. It looks legitimate, and in the frustration of the morning, they click. It’s a phishing attack. Their credentials have been stolen. A breach follows.

What went wrong?

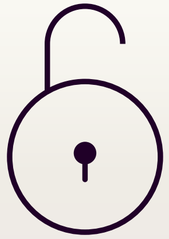
Despite the user’s best intentions, the complexity of managing traditional VPN security gets in the way. It slows people down, causes frustration, and, in the worst cases, creates the very vulnerabilities security measures are meant to prevent.

VPN Timeline



“I should be able to log into my work machine once and then not have to sign into eight different applications.”

Customer Interview



Old VPN

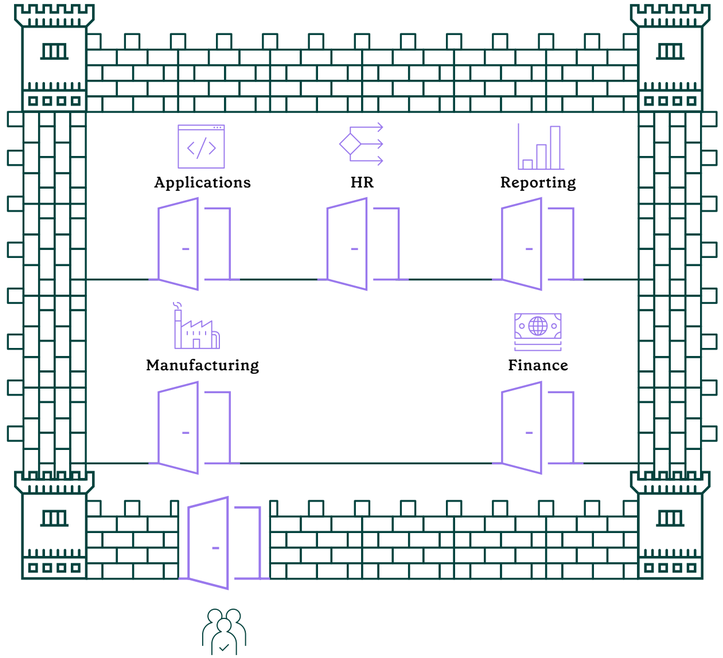
How it works

A VPN creates a secure, encrypted tunnel between your device and a remote server run by the VPN provider.

It works on the idea that once you're connected, you're trusted. So instead of checking your identity over and over, it just focuses on keeping that connection safe.

Think of it like this: once you cross the moat, you're inside the castle. No checks afterwards.

- Once you're connected, you usually get broad access to everything.
- In some cases, network resources become visible too.
- Trust is often static once the connection is established, without ongoing verification.
- If your device is compromised, it could be used to move around the network and find valuable data.
- As the number of remote users increases, managing everything becomes more challenging.
- Old VPNs are making it difficult to scale securely.



ZTNA

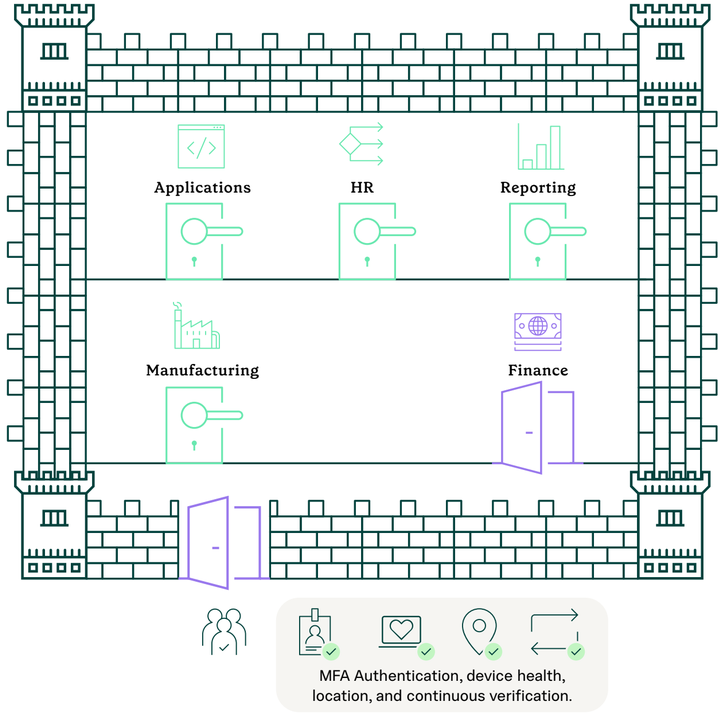
How it works

ZTNA is a security framework that operates on the principle of “never trust, always verify.”

It doesn’t assume you’re safe just because you’re inside the network. Instead, it treats every user and device like a potential risk, whether they’re inside or outside the system.

Before you can access anything, every user and device must be authenticated and authorised. And even then, you only get access to the specific resources you actually need.

- With ZTNA, users only get access to the specific apps they’re allowed to use.
- No network access means malware can’t roam free.
- Trust isn’t permanent. It’s constantly re-checked based on behaviour, device health, and more.
- If you’re not allowed in, you can’t even see what’s there.
- Since it’s built for the cloud, ZTNA scales easily and works well for remote teams.



How it works

ZTNA double-checks every user and device every time before letting them in.

It follows core zero trust rules like: “Assume breach,” “Verify everything,” and “Only give access to what’s truly needed.” That adds up to a much stronger security posture.

1

Verification

ZTNA doesn’t just verify you once. Every access request is authenticated and authorised based on identity and context policies.

2

Role-based access

Users only get what they need, based on their role. Nothing more. That means less risk, fewer mistakes.

3

Conditional access

ZTNA uses multi-factor authentication (MFA) and device checks to verify you and your device.

4

Segmentation

The network is segmented to control traffic flow. That way, if something goes wrong, threats can’t move freely.

5

Hidden by default

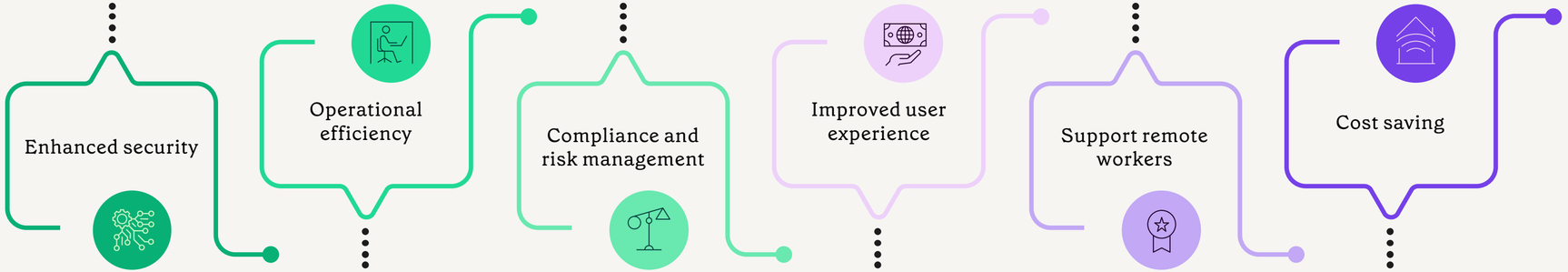
Apps and services stay invisible to outsiders, making it harder for unauthorised users to find and exploit them.

Business outcomes

Continuous verification: ZTNA continuously verifies user identities and device health, reducing the risk of unauthorised access.

Granular access control: Users are granted access only to specific apps and data based on their roles, minimising the attack surface.

Reduced blast radius: If there's a breach, it's contained. Threats can't spread beyond their segment.



Simplified management: Centralised policies make security easier to enforce and maintain.

Scalability: Designed to scale effortlessly as your team and tech stack expand.

Regulatory compliance: Helps you meet compliance requirements by securing access to sensitive data.

Risk mitigation: Proactively addresses security risks, reducing the likelihood of data breaches and associated costs.

Seamless access: Users get secure access to apps without juggling multiple passwords.

Reduced friction: Simple, low-friction sign-ins mean fewer roadblocks and more productivity.

Any-device access: Teams can connect securely from laptops, phones, or tablets. That's perfect for hybrid work.

Smart access control: Access is based on who you are and how secure your device is. Safer connections, every time.

Reduced overhead: Cuts down on overlapping tools, making security simpler and cheaper to manage.

Optimised resources: Smarter use of resources means more value from your security spend.

Impact to your actual day

Let’s run through the same day, but this time **with ZTNA.**

It’s Monday morning again. Our user logs into their device with single sign-on and MFA.

They open up their usual work apps. Whether they’re in the cloud or on-prem, no VPN is required, no confusing bundle of passwords to remember.

Behind the scenes, ZTNA is quietly doing its job: checking the user’s identity, the device health, and where the request is coming from. Everything looks good, so access is granted to the requested resources.

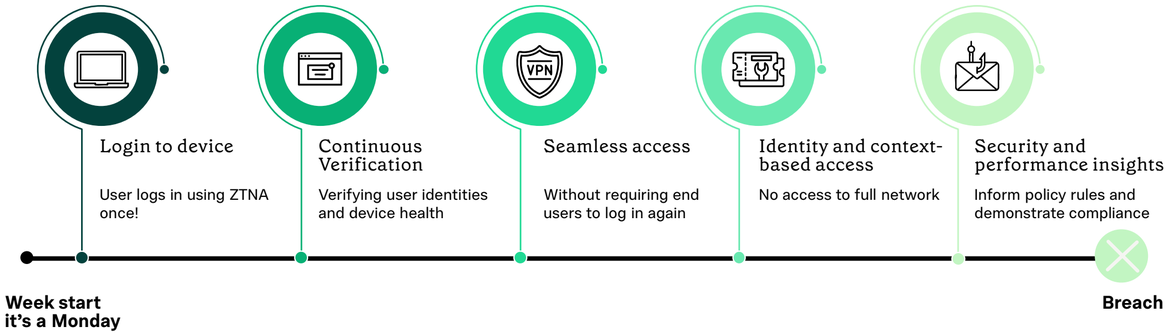
Later in the day, something seems off. Maybe it’s an unusual login time or a strange location. Instead of shutting the user out completely, ZTNA restricts access and triggers an alert. The user isn’t left in the dark, and the threat doesn’t get any further.

How is this different?

ZTNA works in the background. It’s continuously adapting to real-time context and risk. The new set-up means fewer hurdles for users and a much lower risk of falling for phishing or credential theft.

Users stay productive while ZTNA quietly handles the heavy lifting.

VPN Timeline



“I should be able to log into my work machine once and then not have to sign into eight different applications.”

Customer Interview

Why Nasstar?

Expertise you can trust

When you work with Nasstar, you get more than just a service. Tap into deep cyber security expertise that’s backed by proven partnerships and real-world experience.

We’ll deliver consistent protection for your workforce, anywhere in the world, through a single, cloud-native service

- Fully managed, end-to-end Secure Access Service Edge (SASE) solutions
- 24/7 global support
- Strong alliances with top-tier vendors
- Expert deployment, optimisation, and continuous improvement

It's time to move to Zero Trust Network Access (ZTNA) for enhanced protection and efficiency.

Traditional VPNs are no longer sufficient to protect your network from sophisticated cyber threats.

ZTNA offers superior security by continuously verifying user identities and device health, ensuring that only authorised users can access specific applications and data.

Leigh Walgate

Managing Director | Secure Networks

Let’s secure your future together.

Get in touch

nasstar.com