

GUIDE

Zero Trust, Explained

A Practical Guide to Protecting
People, Data and Access



Introduction

2

There was a time when cybersecurity felt easier to explain. Users sat at office desks, applications lived in a data centre, and a firewall kept threats out. For a long time, protecting that physical perimeter made total sense.

Then, the way we work shifted. Cloud platforms, SaaS, mobile devices, and hybrid setups changed where people sit, how apps are delivered, and where data lives—a shift accelerated rapidly by COVID.

Today, suppliers, contractors, and clients expect seamless access from anywhere. The result is simple to describe, but difficult to manage:

- People are everywhere.
- Applications are everywhere.
- Data is everywhere.

If everything is moving, the old question “Is this inside the firewall?” no longer works. The real question is: “Is this person, on this device, doing the right thing right now?”

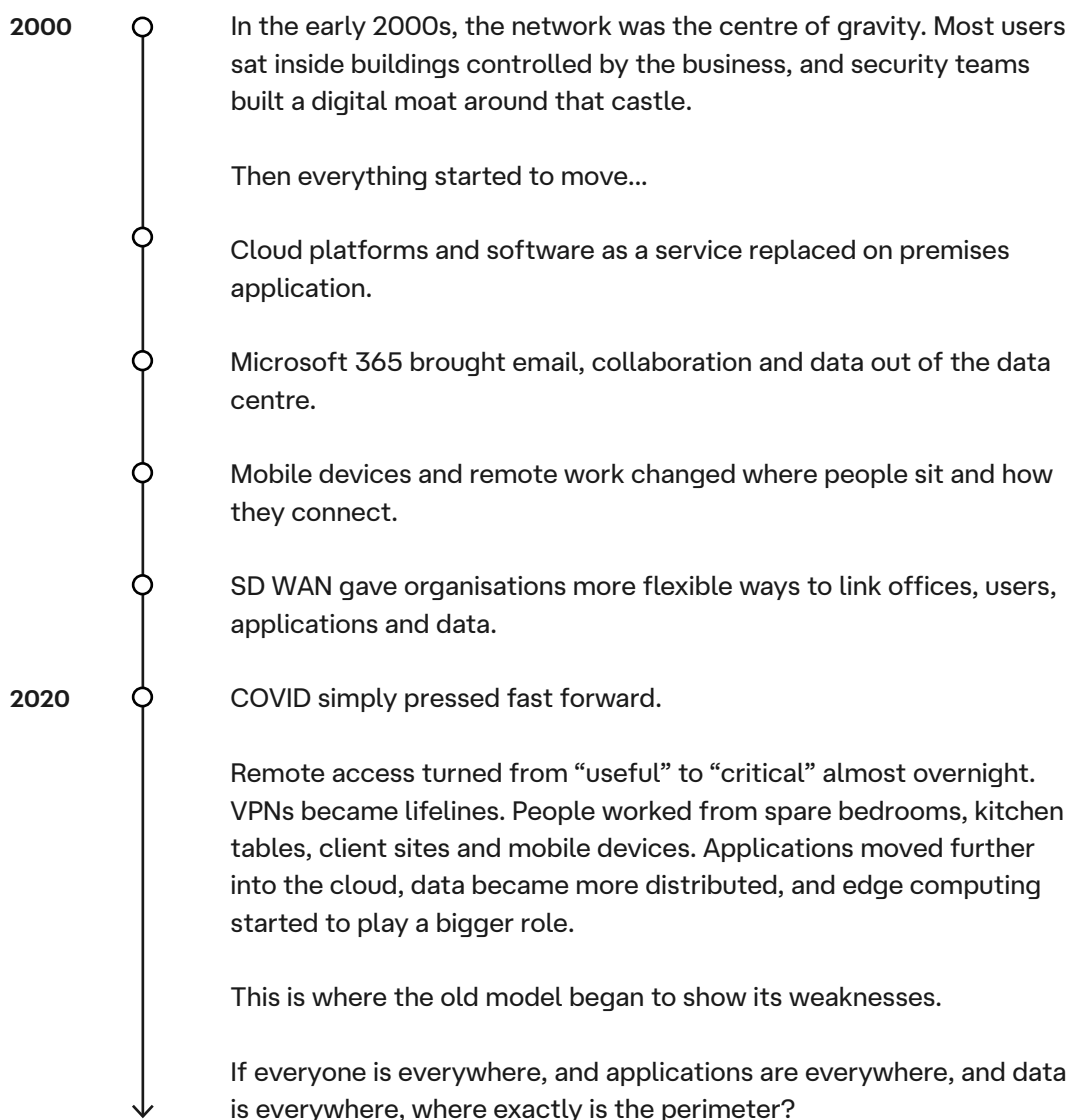
This guide explains Zero Trust in plain language and shows where Zero Trust Network Access (ZTNA) fits into a wider security programme. It is written for the people who make critical decisions – managing directors, CIOs, IT leaders, finance directors and CEOs – as well as the teams who run and maintain the technology day to day.

You will see how your existing controls fit into four clear pillars; visualise how ZTNA changes access in real organisations – from councils and law firms to large care agencies. You will also see where to start with understanding your security posture with Syntura’s Zero Trust Scorecard and Readiness Assessment.



From perimeter security to people inspired security

Over the last 15 to 20 years, the evolution of cybersecurity has been defined by the breakdown of the traditional network perimeter.



At Syntura, our ethos is delivering people inspired solutions. We start from how people work and how organisations operate, then design security to support that reality. That is why we talk to customers about Zero Trust and help them discover our Zero Trust and ZTNA solutions.

What Zero Trust really means

Zero Trust is often quoted and easily misunderstood. Let's start with what it is definitely not:

- It does not mean you stop trusting your people.
- It does not mean making life deliberately difficult for users.
- It does not mean buying one product and declaring the problem solved.

Zero Trust is a security philosophy built around a simple idea: **never assume trust, always verify it.**

The UK National Cyber Security Centre describes Zero Trust as an approach that removes inherent trust from systems, networks and services, focusing instead on validating every interaction and granting only the minimum access needed to perform a task or set of tasks.



Let us understand this with an analogy:

When you walk into an office building, you show an ID badge at reception. The badge proves who you are, but it does not mean you can walk into the finance office, open HR records, access the server room, sit in a board meeting or remove confidential documents.

- Your identity is what allows you to enter.
- Your role determines where you can go.
- Your behaviour may be observed.
- Your access may be limited.
- Your actions may be logged.

Zero Trust brings this common sense into the digital world. A successful login should not automatically mean broad access to the business. A known device should not automatically be trusted forever. A user who passed authentication at 9am should not automatically be trusted at 3pm if their behaviour, location or device health has changed.

That is not paranoia, it is modern risk management in an era of constantly evolving threats.

Zero Trust in practice: the main building blocks

Most Zero Trust frameworks, including NCSC & NIST, talk about similar building blocks: users, devices, networks, applications, data & analytics. In practical terms, this means:

Identity & users	Who is requesting access, and how their identity is verified and managed (IAM, MFA, PAM, roles and groups).
Devices & posture	Whether the device is healthy, compliant and protected (endpoint protection, EDR/XDR, patching, vulnerability management).
Network & connectivity	How users connect, and how traffic is segmented and secured (SD WAN, VPN, ZTNA, secure remote access, WAN encryption).
Applications & data	Which systems and information are exposed, and under what conditions (access policies, DLP, cloud security controls).
Analytics & monitoring	How behaviour is observed and incidents detected (SIEM/ SOAR, threat intelligence, UEBA, security operations).

Zero Trust is not a single product that covers all of this. It is an architectural approach that pulls these building blocks into one coherent programme.

Identity comes first

Zero Trust begins with identity.

If you cannot confidently answer “*Who is this?*”, it is very hard to answer “*Should they have access?*” That is why a modern Zero Trust programme usually starts with:

- A strong identity and access management platform (e.g., Microsoft Entra ID) with clear role and group structures.
- Multi factor authentication for all remote and sensitive access.
- Privileged access management for admin and high risk accounts.
- Clean joiner–mover–leaver processes so access follows the person’s role and is removed promptly when they leave.

From Syntura’s perspective, this is where our Modern Workplace and Managed Identity/Endpoint services support the journey – making sure people, accounts and devices are in good shape before you introduce ZTNA and other Zero Trust controls.

The Four Pillars: Verify, Protect, Detect, Recover

To keep Zero Trust practical and simple, it helps to think of your security strategy in four, distinct pillars:



VERIFY

Who are you, which device are you using, and under what conditions?



PROTECT

What do you genuinely need to reach, and how is that access secured?



RECOVER

If the worst happens, how fast can you recover and keep operating?



DETECT

If something goes wrong, how quickly will you know?

While these four pillars aren't a rigid, formal standard, they provide a simple, human framework to organize your Zero Trust outcomes, fully aligned with mainstream industry guidance.

Where does Zero Trust Network Access (ZTNA) fit?

This is the part that is easy to get wrong. It is not the parts, it is the sum of the parts.

ZTNA is not Zero Trust. MFA is not Zero Trust. PAM is not Zero Trust. SASE is not Zero Trust. A firewall is not Zero Trust. Each is a component only in the Zero Trust landscape.

At its core, Zero Trust Network Access (ZTNA) changes how users connect to your applications. Instead of giving access to the entire network, ZTNA works like a smart security checkpoint, it connects verified users on safe, vetted devices only to the specific applications they are authorised to use.

Within our four-pillar security model, ZTNA sits primarily in Verify and Protect segments:

- **Verify:** ZTNA acts as the ultimate gatekeeper. It constantly checks signals like identity, Multi-Factor Authentication (MFA), and device health to confirm exactly who the user is and whether their device is secure enough to connect.
- **Protect:** ZTNA enforces a strict “least-privilege” approach. Instead of dropping users onto the network where they can look around, it connects them directly, and only, to the specific systems they need to do their jobs.

While its main job is to verify and protect, ZTNA also plays a vital supporting role in Detect and Recover:

- **Detect:** Every connection generates detailed, session-level logs. By recording exactly who accessed which app, when, and under what conditions, ZTNA feeds this rich contextual data directly into your SIEM/SOAR platforms and managed cyber services, making potential threats much easier to spot.
- **Recover:** If an account is compromised, ZTNA acts as a firebreak to contain the “blast radius.” Because attackers can’t roam freely across your broader network, the threat is confined to a small, isolated area. While ZTNA minimizes the damage, full recovery still relies on your dedicated backup, disaster recovery, and business continuity solutions.

That is why Syntura positions ZTNA as one key element within a broader Zero Trust and secure connectivity strategy, alongside identity, endpoint protection, SIEM/SOAR, and disaster recovery and business continuity services.

For a closer look at how ZTNA works in practice, Syntura has written blog articles which sit alongside this guide to help your teams dig into the technical details without losing the bigger picture:

- [VPN Is Dead. You Just Haven’t Buried It Yet](#)
- [How ZTNA Actually Works: A Plain English Guide for IT Teams](#)
- [Five Reasons Your Organisation Needs ZTNA, And Why Now](#)

Zero Trust in everyday situations

Frameworks are useful, but people remember incidents and examples. Here are three situations most organisations can relate to and how Zero Trust changes the picture.



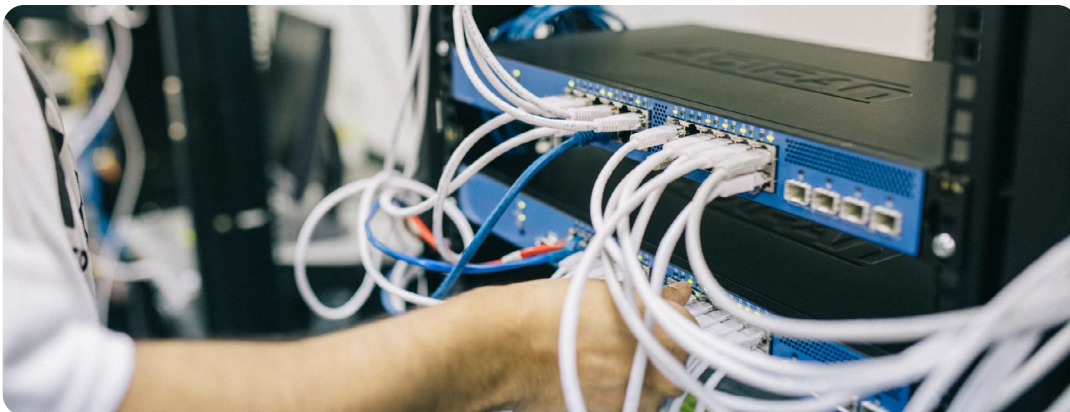
1. Management: the travelling executive

A senior leader is travelling and needs access to Microsoft 365, internal files and board papers. In the traditional model, access might be granted because the username and password are correct, the VPN connects, and the user appears authenticated.

In a Zero Trust model, the organisation asks more intelligent questions:

- Is this a known device?
- Is MFA satisfied?
- Is the location unusual?
- Is the device compliant?
- Is the session behaving normally?
- Does this person need access to all systems, or only specific applications?

The executive still gets work done, but access is granted based on risk and context, not assumptions. That is Verify and Protect in action, without unnecessary friction.



2. IT operations: the engineer with admin access

9

An IT engineer needs administrative access to a production system. In many environments, admin rights are “always on”. They exist all the time, whether they are needed or not. That creates unnecessary risk. In a Zero Trust model, privileged access is treated differently:

- The engineer requests access.
- The request is approved.
- MFA is enforced.
- Access is granted for a defined period.
- Activity is logged.
- Privileges are removed automatically when the task is complete.

This protects the engineer, protects the business and creates a clearer audit trail if something needs to be reviewed later. It combines Verify, Protect and Detect, with Recover as an option if something still goes wrong.



3. Finance and risk: the cyber insurance conversation

A finance director is preparing for cyber insurance renewal; the insurer asks familiar questions.

- Do you enforce MFA?
- Do you manage privileged access?
- Do you have endpoint protection?
- Do you monitor security events?
- Do you secure remote access?
- Do you have tested backups?
- Do you have an incident response process?

Without a streamlined programme, those answers sit in different teams, tools and spreadsheets. With a Zero Trust approach, the organisation has a clearer structure for managing access, reducing privilege, monitoring activity and recovering from incidents.

For finance teams, risk becomes easier to understand. For insurers, it shows maturity. For the board, it creates a clearer link between cyber investment and business resilience.

Zero Trust and ZTNA in different organisations

Zero Trust is a philosophy. ZTNA is one of the ways it shows up in real environments alongside identity, endpoint, monitoring and resilience controls. Here are three examples that reflect the kinds of organisations Syntura works with today.

Use case 1: UK council with hundreds of contractors

Context

A large council is responsible for housing, social care, highways and environmental services. Hundreds of external contractors – social workers from partner organisations, repairs teams, auditors, and temporary staff – need access to council systems from unmanaged devices and varied locations.

Challenge

- Traditional VPN gives contractors broad network access once they log in.
- It is difficult to restrict them to only the applications and data they genuinely need.
- Offboarding is inconsistent; accounts and access paths can linger after contracts end.
- Security and compliance teams struggle to demonstrate least privilege access and clean joiner–mover–leaver processes.

How Zero Trust + ZTNA changes this

- Contractors are assigned role based access profiles that define exactly which applications and data they can reach.
- ZTNA publishes only those applications, never the underlying network, and checks identity, device posture and context every session.
- When a contract ends, disabling the identity automatically removes all access; there is no VPN tunnel or shared password left behind.
- Security teams gain session level audit logs showing who accessed what, when, and under what conditions.

Outcome

The council can safely work with a large, fluid ecosystem of external partners while proving to auditors and regulators that citizen data is accessed on a least privilege, fully logged basis.

Use case 2:

Law firm protecting client confidentiality

Context

A mid-to-large law firm has partners, solicitors, support staff and external counsel working from courts, client offices and home. Case files, practice management systems and document repositories contain highly sensitive information.

Challenge

- Traditional VPN places remote users “on the network”, exposing more systems than they strictly need.
- Remote Desktop and legacy access paths make micro segmentation difficult.
- Client confidentiality demands strong access controls and demonstrable audit trails.
- Cyber insurers and regulators increasingly expect identity centric, least privilege access rather than broad VPN tunnels.

How Zero Trust + ZTNA changes this

Zero Trust Network Access replaces the “connect first, verify later” model of VPN with a “verify first, access never assumed” approach. Every access request is evaluated against identity, device posture and context before granting access to a specific application – not the whole network, just the application.

- A solicitor accesses the practice management system from a personal device at home: ZTNA checks device health, enforces MFA, and grants access to that application only. No other network resource is visible.
- A barrister requires access to a case bundle: they receive scoped, time limited access to a specific matter folder, with no persistent VPN account and no lateral movement into other matters.
- A partner travels internationally: access is evaluated against geo risk policy; anomalous patterns trigger step up authentication or session termination.
- IT investigates a potential compromise: per session, per application logs provide a granular audit trail, and the blast radius is confined to the affected session.

Privileged admin access follows the same principles: rights are elevated just in time for specific tasks, fully recorded, and automatically revoked when the work is complete.

Outcome

The firm can support fully hybrid work while showing clients, regulators and insurers that access to sensitive matters is tightly controlled, continuously verified and fully auditable.

Use case 3:

Large care agency with distributed clinicians

Context

A large care agency employs doctors, nurses, therapists and admin staff across multiple sites, care homes and community locations. They rely on clinical applications, scheduling systems, HR and finance tools, and shared collaboration platforms.

Challenge

- Clinicians and agency staff need fast, reliable access from many locations and devices, often on short notice.
- Legacy VPN or site based access either grants too much reach or forces staff through slow, centralised paths.
- Protecting patient information while enabling mobile, multi site work is increasingly difficult.
- Ensuring consistent security controls across employed staff and agency workers is a constant overhead for IT and compliance.

How Zero Trust + ZTNA changes this

- Each clinical role (doctor, nurse, therapist, and admin) is mapped to the specific systems they genuinely need – clinical records, scheduling, prescribing, and reporting.
- ZTNA provides app level access, verifying identity and device posture before each connection and throughout the session.
- Care critical applications are segmented and published securely; staff never receive wide network access where they could accidentally browse into systems they do not need.
- Agency workers can be onboarded and offboarded rapidly; when their assignment ends, their identity and access profile are revoked centrally.

Outcome

The agency delivers flexible, responsive care across sites without compromising patient confidentiality or operational resilience and can show commissioners and regulators a clear story about how access is governed.

Where do you start?

Every organisation faces different challenges, but whether you are a council managing hundreds of contractors, a law firm protecting sensitive data, or a care agency coordinating mobile clinicians, the first step is always the same: understand where you are today.

To help you get clear, Syntura offers two simple entry points:

1.

SYNTURA ZERO TRUST SCORECARD

A quick, structured check that maps your maturity across identity, access, protection, detection, and resilience; 7 questions and 5 minutes indicate where you stand.

2.

ZERO TRUST READINESS ASSESSMENT

A deeper, no-obligation session with our specialists to understand your infrastructure and security goals and draft a practical roadmap. Where appropriate, we can run a ZTNA proof-of-concept on our UK-sovereign platform so you see the impact in your environment before buying anything.

A typical transformation journey

Clarify where you stand



Complete a scorecard, current-state review, and transformation health check.

Strengthen identity & devices



Clean up IAM, MFA, PAM, and endpoint posture alongside managed cyber services.

Introduce ZTNA



Roll out secure remote access starting with your highest-risk systems and user groups.

Build out detect & recover



Layer in SIEM/SOAR, managed cyber operations, cloud backup, and DRaaS to ensure incidents are both visible and survivable.

The bottom line

Zero Trust isn't about buying another tool. It's about building a safer, more resilient organisation around the people who make it work.