Red Helix

ZTNA 101: An Introduction to Zero Trust Security

CONTENTS

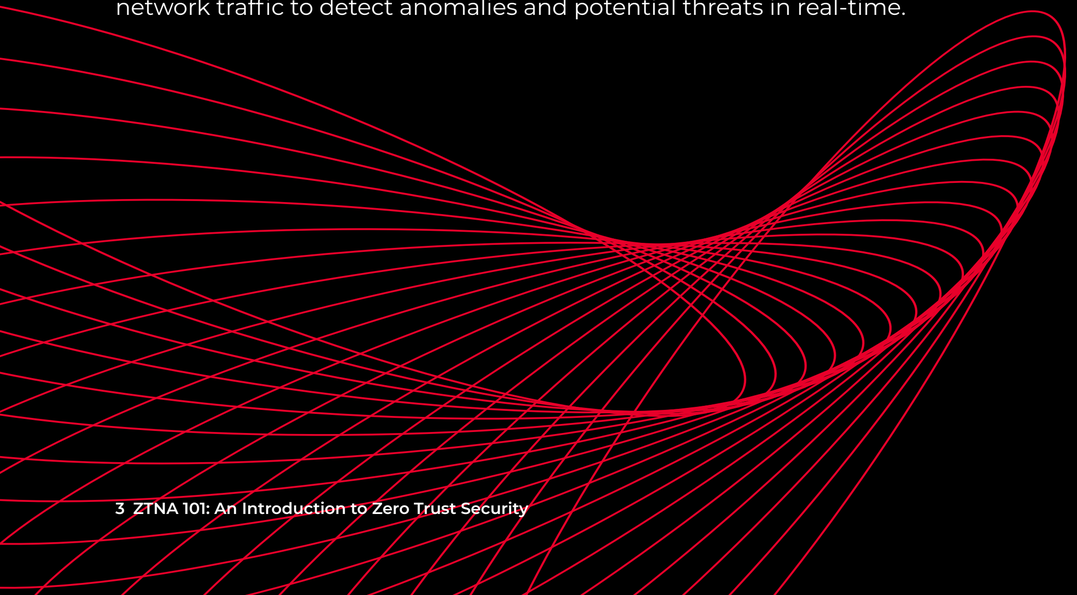
What is ZTNA?

In today's dynamic work environment, securing your network is more critical than ever. Red Helix offers comprehensive Zero Trust Network Access (ZTNA), ensuring that only authenticated users gain access to your resources, regardless of their location.

ZTNA is a modern cyber security approach to securing network access, enforcing strict identity verification, continuous monitoring, and least-privilege access. ZTNA has emerged as a response to the insufficiency of traditional security models which haven't evolved to suit the current remote and cloud-first environments.

Understanding the Zero Trust Principles

The Zero Trust model operates on the principle of "never trust; always verify". This approach requires continuous authentication and granting permission at each level to minimise the risk of unauthorised access. ZTNA limits lateral movement across the network via micro-segmentation. This prevents malicious actors from accessing the entire network and limits potential damage. It also provides more effective against advanced persistent threats (APTs), which have become more common cyber security threats. Least privilege access means that users are granted the necessary visibility to perform their jobs, no more or less. ZTNA continuously monitors user behaviour and network traffic to detect anomalies and potential threats in real-time.



How Does ZTNA Work?

Users must be authenticated based on multiple factors (multi-factor authentication or MFA) before accessing any resource. Each device must also meet specific security checks (e.g., endpoint protection) before they are granted access. Internal resources are not visible on the internet, meaning that those who do not need to access sensitive data cannot see it. ZTNA uses a range of dynamic policies and contextual rules that adapt based on user behaviour, device health, and location. Trust is continuously assessed at each level and user/device access can be adjusted accordingly. This means that user and device preferences can be catered ad hoc, providing support for client or browser-based access. Multi-tunnelling allows users to connect to multiple clous, SaaS, and on-prem resources simultaneously. This can also be done from any location allowing a wide berth of access.

Benefits of ZTNA

- Reduced Attack Surface
- Simplified management
- Enhanced security for remote workforces
- Ensured compliance
- Improved user control and access monitoring
- Scalable alongside growing workforces
- Flexible with variety of infrastructures

ZTNA Versus Legacy Systems (VPN, firewalls, IDS)

ZTNA is becoming essential in today's cyber security landscape as organisations shift away from outdated technologies like VPNs and firewalls in favour of more secure solutions.

Legacy security models open up the entire network to a user or device once they've gained access to one aspect of the network. This has led to **91% of cyber security professionals expressing concerns that compromised VPNs could lead to serious security breaches in their IT infrastructure**. For example, the common assumption that everything behind the firewall is safe, is dangerous. Once attackers gain access, they can move laterally across the network, exploiting vulnerabilities within internal systems. This concept of lateral movement is a common tactic used by attackers to escalate privileges and gain access to sensitive resources. While VPNs offer valuable functionality, they provide broad access to network resources, which can increase the risk of a security breach if compromised. **In 2024, 56% of organisations experienced one or more VPN-related cyber attacks**.

VPNs and firewalls require complex configurations and ongoing maintenance, which can introduce misconfigurations and potential security gaps. The reliance on VPNs also means handling extensive user authentication and access control mechanisms that are often cumbersome and prone to errors. In contrast, ZTNA is more adaptable and targeted, allowing for customisation based on specific network requirements. It grants users only the necessary permissions, minimising the potential attack surface and enhancing overall security.

Security risks associated with VPNs include user access to all network resources, the potential for weak authentication, or even a single point of failure. This can lead to a variety of threats such as phishing attacks or credential stuffing if any of these points of defence are suboptimal. Additionally, if multi-factor authentication (MFA) is not enforced or is improperly implemented, this increases the vulnerability access point of VPN for attackers. A VPN often serves as the single point of failure for network access. If the VPN server is compromised or fails, it could block access to all internal resources, causing operational disruptions. The knock-on effects of this range from downtime to reputational damage and brand distrust.

ZTNA	Traditional VPN
Zero Trust model (continuous verification, least privilege)	Trust-based model (initial authentification grants user access across the network)
Granular access to specific applications	Broad access to the entire network
Fast due to direct connections	Slow due to backhauling traffic
Cloud-based, easier to set up	Requires configuration on user devices and corporate network
Flexible for remote and mobile users	Less flexible so is better suited for fixed locations
Easily scaled to accomodate growth	Can be complex to scale for large numbers of users

ZTNA Best Practices

You need to weigh up the pros and cons to ensure deploying ZTNA is the best decision for your organisation.

When implementing ZTNA, it is important you have considered the security risks and preexisting tools to ensure your solution will integrate with existing infrastructures. Therefore, a preliminary security assessment is recommended to identify sensitive assets and potential threats. The solution should be deployed in phases (starting with critical applications and services) and is expected to integrate seamlessly with your existing security stack such as EDR, SIEM, identity management tools, etc.

For a successful ZTNA deployment, it is important that you begin with a clear understanding of your organisation's specific needs and objectives. This is to guarantee you remain on the correct path and know what you want out of the tool. All the relevant stakeholders (Security, IT, Operations, etc. depending on your organisation) should be involved in the onboarding process. Throughout deployment, you should be repeatedly adapting policies based on potential conditions that may arise and feedback from testing.

As always, there are careful considerations which you must be aware of to prevent any surprises. The transition to a Zero Trust model requires a change in how organisations view and handle security, potentially requiring a shift in corporate culture. Older systems may not be compatible with ZTNA systems and so may require additional customisation and/or tools. This means that initial set up can be complex and potentially expensive. It is also difficult to ensure that the user experience remains optimal during this transition period as unforeseen issues may arise. This is why many organisations opt for an MSSP to set up and manage the solution.

The Future of ZTNA

With cyber threats becoming more sophisticated, ZTNA will continue to evolve to meet new challenges in the threat landscape. A recent report indicated that **ZTNA is the top priority for zero trust investments over the next 12 months**. Modern ZTNA solutions minimise the negative impact on user experience during deployment through seamless access, single sign-on integration, and adaptive authentication. These unique functions ensure an optimal user experience.

The integration of AI and machine learning into ZTNA solutions is enabling even more adaptive, real-time security policies based on user and network behaviour analysis. Machine learning will enhance anomaly detection, policy adaptation, and improve automation. This is increasingly valuable as emerging threats become more sophisticated because ZTNA will evolve to handle them.

As businesses increasingly operate across a wide range of third-party services, supply chains, and ecosystems, ZTNA will help secure access to these extended environments. The supply chain is becoming ever more complex which invites new vulnerabilities into these connected environments. In recent years, **63% of breaches have involved external partners or vendors**, meaning organisations need to be increasingly vigilant to ensure they are not the weak link. Compromising one's supply chain is poor for organisation's reputability and finances, so it is essential to remain vigilant. Third-party/vendor access can be controlled within a Zero Trust framework, which is paramount as **59% of organisations have reportedly experienced a data breach which was caused by a third party**. Capabilities such as contextual and dynamic policy enforcement, and integration with third-party Identity and Access Management (IAM) systems allow for a personalised cyber security solution.

In the face of escalating cyber risks, ZTNA is more than a security tool, it represents a fundamental shift in how organisations safeguard their operations.

A Seamless Transition to ZTNA

The Challenge

So Energy, a renewable energy supplier serving 300,000 customers, faced frequent outages with its existing remote access solution. This instability impacted both employees and customers, requiring a more reliable system that provided secure, seamless connectivity while restricting access to critical resources for authorised personnel only.

By partnering with Red Helix, So Energy aimed to enhance security, improve user experience, and outsource solution management for greater efficiency.

The Solution

Red Helix implemented a Zero Trust Network Access (ZTNA) service, backed by Appgate technology. After a successful one-month proof of value (PoV), So Energy found ZTNA to be the most stable and resilient option.

ZTNA follows a “never trust; always verify” model, ensuring strict authentication checks before granting network access. This modern approach surpasses traditional VPNs, offering better flexibility, precision, and security against cyber threats.

The Result

The implementation of ZTNA provided So Energy with:

- Enhanced security: Identity-based access control and micro-segmentation to reduce risks.
- Improved performance: Localised connections to minimise latency.
- Consistent user experience: Reliable access across different networks (office, mobile, Wi-Fi).
- Accredited encryption: Secure connections regardless of location.
- Resilience: High-availability infrastructure ensuring continuous access.
- Backup support: Managed service for smooth operation.
- Flexibility: Scalable licensing to meet seasonal demand fluctuations.

The Outcome

With ZTNA, So Energy now has a secure, scalable, and efficient remote access solution that integrates easily with existing systems. Employees can connect securely from anywhere, ensuring operational continuity.

The Red Helix team made the transition to ZTNA remarkably seamless. Their expertise, coupled with a user-friendly approach, made implementation quick and completely hassle-free. Their technical teams provided first-class support throughout the entire activation and beyond. Red Helix really put the work in and now feel like an extension of our own team.

- *Karl Ford-Lissenden, Head of IT, So Energy*

How Does Red Helix Provide ZTNA Services?

Red Helix's Partnership with Appgate

To deliver top-tier ZTNA solutions, Red Helix has partnered with Appgate, a leader in secure network access. This collaboration ensures that your organisation benefits from cutting-edge security measures tailored to modern work environments.

Implementing Zero Trust is a strategic process that requires careful planning. Red Helix is committed to guiding you through this journey, ensuring that the transition enhances your security posture and operational effectiveness. Our expertise ensures that your path to Zero Trust is seamless and customised to your organisation's unique needs.

Why Choose Red Helix?

Red Helix will guide you through your transition to ZTNA, covering everything from initial setup to continuous operation. This includes handling the defining of your access policies, aiding deployment across your infrastructure, and helping with configuration on your network. This allows organisations to focus on innovation while we handle the security aspect. With our deep expertise in integrating ZTNA into existing IT and OT systems, we ensure smooth integration with your security tools and infrastructure. We also customize our services to align with the specific requirements of your environment, offering scalable solutions that evolve as your business grows. Our subscription-based pricing model offers predictable costs, giving you financial clarity and control.

We tailor our services to align your specific requirements with customised solutions. Our team provides expert guidance and continuous support throughout your Zero Trust implementation. Our long-standing collaborations with industry leaders like Appgate ensure you receive the best security solutions available.

ZTNA with Red Helix ensures seamless integration, we can easily connect with your existing IT and OT systems. Your solution will be designed to meet the unique needs of your organisation. It will also scale in tandem with your growing and changing needs. Our subscription-based pricing for financial clarity and control. Employing Red Helix's ZTNA Managed Service can mitigate the costs associated with the complexity and cost of an inhouse ZTNA. You can also discuss potential cost savings in the long term, such as reduced breach costs or less time spent managing traditional security models.

ZTNA is symptomatic of a fundamental shift in securing remote work, cloud adoption, and hybrid IT environments, minimising risk, securing sensitive assets, and ensuring long-term resilience.

Embrace the future of network security with Red Helix's ZTNA Managed Service and fortify your organisation against emerging threats.

Contact us today to find out how this can benefit you.

+44 (0)1296 397711

info@redhelix.co.uk

Phoenix House
Smeaton Close
Aylesbury
Buckinghamshire
HP19 8UW

Red Helix

redhelix.com