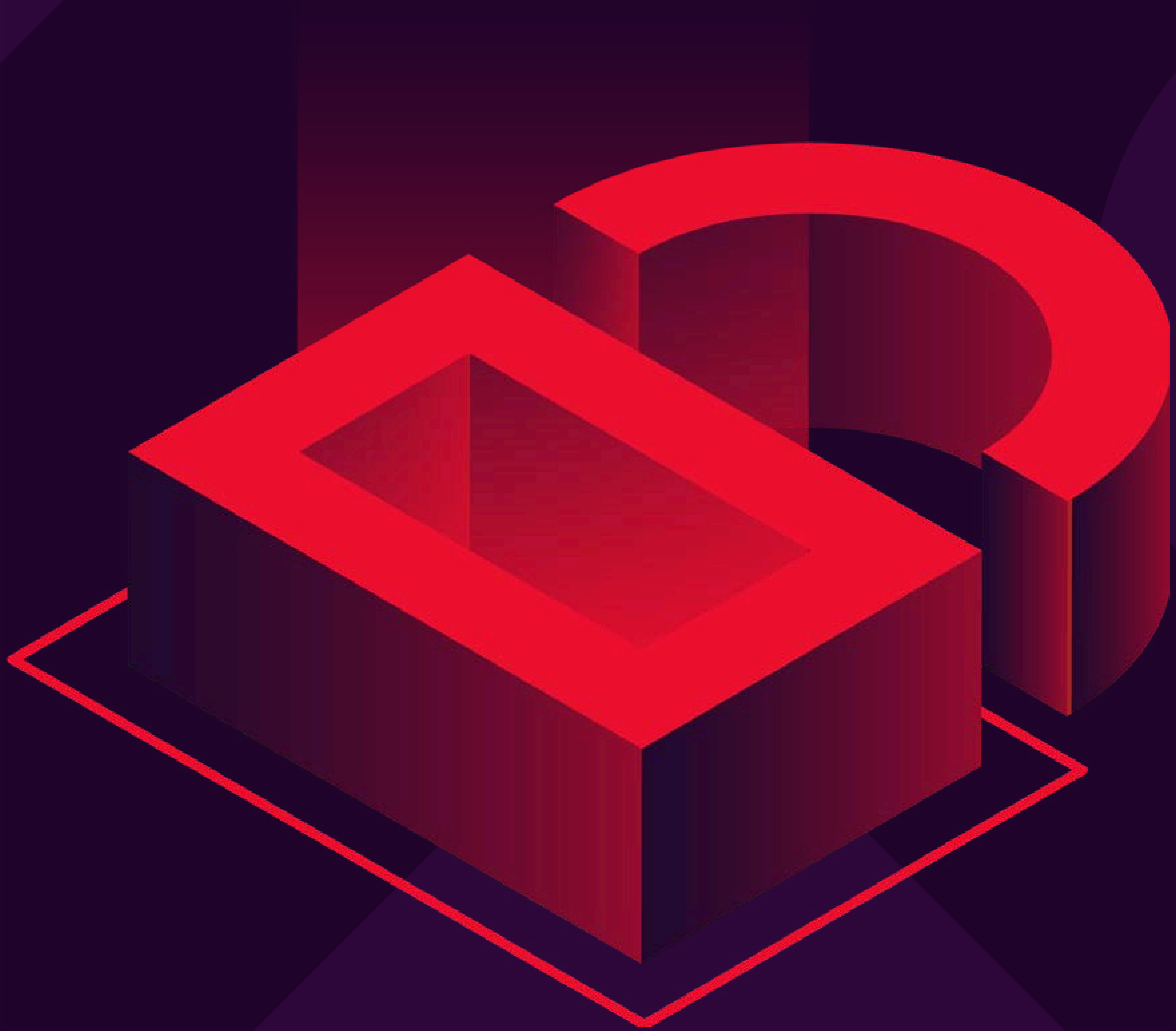
FourNet®

Quick Guide to

Zero Trust Network Access (ZTNA)



Welcome to our Quick Guides to Cyber Security.

These guides have been created to give you an overview of the key pillars and solutions needed to overcome the challenges arising from Cyber threats.

Other guides in our security series:

Secure Infrastructure | Quick Guide on Edge/Perimeter Security

Secure Infrastructure | Quick Guide to Zero trust Network Access

Secure Infrastructure | Quick Guide to Cloud Security

Secure Infrastructure | Quick Guide to Data and Compliance

Secure Infrastructure | Quick Guide to Socially Engineered

Secure Infrastructure | Quick Guide to Endpoint Security

In these guides, we outline all the major risks and threats, security trends, common challenges, and impacts. Finally, we consider the best ways to calculate and mitigate the risks to your organisation, the key measures which should be introduced, and outline how FourNet's best-in-class security solutions can help.

If you take one concept from this series, it is that effective cyber security requires a layered approach to be successful. Also be mindful that compliance does not make an organisation secure and relying solely on technology to provide the solution won't combat the inherent risks humans pose.

Building the right security culture and strategy is like Lego, needing many pieces to intersect and interplay to help mitigate the increasing level of risk our organisations face.

In this guide, we look at the emergence of Zero Trust Network Access and how this can help to bolster defences to protect against external and internal threats in a world where the network and users are increasingly distributed.

Contents

01 Overview of ZTNA
02 Security Challenges that have led to ZTNA
03 How ZTNA works for organisations
04 Consideration when looking to implement ZTNA
05 The Benefits of ZTNA
06 How FourNet can Help

Overview of ZTNA and Background to the Technology

Zero Trust Network Access or (ZTNA) is a security framework that challenges the traditional perimeter-based security model, which assumes that everything inside the network is trusted.

In contrast, ZTNA operates on the principle of "never trust, always verify," ensuring that no entity, user, or device is trusted by default, regardless of whether it is inside or outside the network perimeter. ZTNA continuously validates every user or device attempting to access resources, requiring explicit verification and authorisation before granting access.

67% of the UK Employees are Fully Remote or Hybrid Workers

Forbes

The technology has evolved as an answer to the increasing complexity of modern IT environments, characterised by cloud adoption, remote working, and the growing number of devices now accessing corporate networks. With ever-increasing distributed environments, the concept of a secure perimeter has become obsolete, driving the need for a security model that is dynamic and adaptable to modern threats.

ZTNA leverages various technologies such as multi-factor authentication (MFA), identity and access management (IAM), encryption, and micro-segmentation to provide secure access to applications and services. It aims to reduce the attack surface, minimise unauthorised access, and strengthen the overall security posture of an organisation.

Security Challenges that Have Led to ZTNA

Security threats have increased exponentially, and several key security challenges have catalysed the development and adoption of ZTNA

Perimeter Security is No Longer Sufficient

The traditional castle-and-moat security model, which focuses on securing the network perimeter, is ineffective in today's digital environment, where data and applications are often spread across multiple locations (on-premise, cloud, and hybrid environments). Once an attacker breaches the perimeter, they often have broad access to the internal network.

Insider Threats

Trusted insiders with legitimate access to the network can inadvertently or maliciously cause harm. With ZTNA, access is granted based on the principle of least privilege, reducing the likelihood of insider threats.

Remote/Hybrid Working and BYOD (Bring Your Own Device)

The rise of remote work and employees using personal devices to access corporate networks have expanded the attack surface significantly. Securing these diverse endpoints with traditional tools is challenging and prone to vulnerabilities.

Cloud Adoption and SaaS

Organisations increasingly use cloud services and SaaS applications, making traditional network security solutions inadequate for protecting sensitive data. Cloud environments require more dynamic security that adapts to complex, distributed infrastructures to deliver the right levels of protection.

Advanced Threats and APTs (Advanced Persistent Threats)

Cyber attackers are increasingly using sophisticated methods such as lateral movement and advanced persistent threats to compromise networks. Traditional security solutions often fail to detect these techniques early, leading to significant data breaches.

How ZTNA Works for Organisations

ZTNA enhances an organisation's cybersecurity by focusing on identity, context, and policies to manage access to resources. Here’s how it works

Identity-Centric Access Control

ZTNA starts with strong authentication and authorisation, ensuring that access to resources is granted only after confirming the identity of the user or device. This is often achieved through multi-factor authentication (MFA) combined with single sign-on (SSO) solutions to streamline access while maintaining security.

Micro-Segmentation

ZTNA divides the network into small segments, reducing the attack surface and ensuring that users or devices have access only to specific applications or data they need for their role. This limits lateral movement in case of a breach.

Encryption and Secure Tunnels

Encryption and Secure Tunnels ZTNA encrypts all communications between users, devices, and applications, making it difficult for attackers to intercept or manipulate data. Secure tunnels are created for specific sessions, further protecting data in transit.

Context-Aware Security

ZTNA solutions continuously evaluate the context of access requests, considering factors such as device health, user location, and behaviour. Access decisions are made in real-time based on the current risk profile, not just on static credentials.

Zero Trust Policy Enforcement

Policies are enforced across all access points, ensuring consistent security. This includes monitoring user activities, detecting anomalous behaviour, and immediately revoking access if suspicious activity is detected.

01 Overview of ZTNA

02 Security Challenges that have led to ZTNA

03 How ZTNA works for organisations

04 Consideration when looking to implement ZTNA

05 The Benefits of ZTNA

06 How FourNet can Help

Considerations When Looking to Implement ZTNA

When considering the implementation of ZTNA, organisations should evaluate the following:

Assessment of Current Infrastructure

Conduct a thorough assessment of the existing IT infrastructure to understand where ZTNA can be integrated. Identify key applications, data, and user groups that need protection, and determine how ZTNA will interact with legacy systems.

Cloud and Hybrid Environment Compatibility

Since many organizations operate in cloud or hybrid environments, ensure that the ZTNA solution can seamlessly integrate with cloud services and support applications hosted both on-premises and in the cloud.

User Experience

While security is a priority, user experience should not be sacrificed. Implementing ZTNA should not overly complicate access for legitimate users. Consider solutions that offer a balance between security and ease of use, such as incorporating SSO and MFA to streamline access.

Scalability

As the organisation grows, so should its ZTNA solution. Choose a ZTNA platform that can scale with your business, accommodating more users, devices, and applications without compromising security.

Policy Management

Managing and defining access policies is a core aspect of ZTNA. Ensure that the ZTNA solution offers intuitive policy management tools that allow security teams to create, enforce, and update policies easily as the organization's security needs evolve.

Vendor Evaluation

Selecting the right ZTNA provider is critical. Evaluate vendors based on their track record, technology stack, integration capabilities, and support offerings. Look for solutions that offer flexibility and customisation to meet your specific security needs.

01 Overview of ZTNA

02 Security Challenges that have led to ZTNA

03 How ZTNA works for organisations

04 Consideration when looking to implement ZTNA

05 The Benefits of ZTNA

06 How FourNet can Help

The Benefits of ZTNA

Implementing ZTNA offers numerous benefits for organisations aiming to bolster their cybersecurity

Enhanced Security Posture

By adopting a "zero trust" approach, ZTNA minimizes the risk of unauthorized access, data breaches, and lateral movement within the network. Continuous verification and contextual access decisions help mitigate both internal and external threats.

Reduced Attack Surface

ZTNA narrows the attack surface by limiting access to only the necessary resources and isolating sensitive data and applications from the broader network. Micro-segmentation further reduces the likelihood of widespread compromise.

Improved Visibility and Control

ZTNA provides detailed insights into who is accessing what resources, from where, and under what conditions. This improved visibility helps security teams detect and respond to potential threats faster.

Seamless Remote Work Support

With the rise of remote work, ZTNA allows organizations to securely extend access to corporate resources without the need for traditional VPNs. This ensures that remote employees can work efficiently while maintaining high security standards.

Adaptability to Modern Environments

ZTNA is designed to work in complex, distributed environments, making it ideal for organisations that are transitioning to the cloud or already operate in hybrid models. The ability to enforce security consistently across on-premise, cloud, and remote environments makes ZTNA a future-proof solution.

Compliance and Risk Management

ZTNA helps organisations meet regulatory requirements by ensuring that access to sensitive data is tightly controlled and monitored. By reducing the risk of data breaches and ensuring proper logging and auditing, ZTNA can aid in achieving compliance with various industry standards (e.g., GDPR, HIPAA).

In Conclusion

Zero Trust Network Access (ZTNA) represents a significant shift in how organisations approach cybersecurity. By eliminating the inherent trust associated with traditional perimeter security models and focusing on continuous verification, ZTNA addresses the security challenges posed by modern IT environments, remote work, and cloud adoption.

While implementation requires careful planning and consideration, the long-term benefits in terms of enhanced security, reduced risk, and adaptability make ZTNA a crucial strategy for organisations seeking to future-proof their cybersecurity posture.

How FourNet Can Help

Our clients benefit from our experience working with some of the biggest names in government, healthcare, and finance. We have delivered solutions that have been recognised as Best of Breed by industry bodies such as Government Digital Service (GDS).

At FourNet, our solutions are designed to always protect your organisation from downtime - whether it's network failure or an attack on your infrastructure - so you can concentrate on what matters most: keeping people safe.

Trusted by Mission Critical Organisations

FourNet are trusted by some of the most secure and mission critical organisations in the UK including Whitehall, Downing Street, Cheshire Fire and Rescue, South Coast Ambulance Service, and others. Offering a diverse portfolio of solutions for both public sector and private enterprise with cloud solutions like ANTENNA and Agile Cloud.

We also provide highly available contact centre solutions delivering 999 & 111 services to the public and back-office solutions to support a flexible, agile workforce and have highly accredited and security cleared engineers and consultants.

Helping You to Understand Security Posture

FourNet's security specialists are here to help your organisation detect, defend, and repel threats from whatever threat vector they emerge. Our team of experts will work alongside you to identify and remediate areas of concern or risk. We work with you to build a business case to demonstrate ROI and payback periods based on your current costs and KPIs. Get in touch to schedule an initial discovery call.

Managed Security to Remove the Worries

We offer a range of managed solutions from the world's leading security vendors all underpinned by SC and DV level security cleared engineers and consultants. Our best-in-class security cleared service management from our dedicated secure Service Desk, FourNet provides a fully managed service desk and Security Operations Centre (SOC) with 24/7 phone support and multi-factor authenticated ITSM access.

Whether you are looking to secure and control access to critical systems or wanting to outsource security to a managed SOC we can help. We work with you to create an understand your organisation and provide the help, solutions, and support where it is needed most.

Discover if your Network is Ready for Emerging Threats

Discover whether your security solutions are keeping pace with the threat landscape with a FourNet Cyber Assessment.

Get in touch to arrange your assessment

Check out our Other Guides to Cybersecurity

FourNet

Quick Guide on

Socially Engineered Attacks

FourNet

Quick Guide on

Data Compliance

FourNet

Quick Guide on

Endpoint Security

Click Here >>

Manchester Office (HQ)
3 Scholar Green Road,
Cobra Court,
Manchester. M32 0TR
Tel: 0845 055 6366

hello@fournet.co.uk
fournet.co.uk

FourNet PR & Media Office
Tim Reid
e-mail: treid@fournet.co.uk