BYTES | Smarter together

AN ESSENTIAL GUIDE

ZERO TRUST | IN 2023

FIND OUT MORE

WWW.BYTES.CO.UK

CONTENTS

BYTES
INTRODUCTION

By acting as an independent, trusted advisor, **our customers benefit from a wealth of knowledge that aids in the delivery of an end-to-end and integrated methodology to cyber security.** Our consultancy led approach enables our team to fully understand our customers challenges and business goals, ensuring we deliver innovative and relevant security solutions.

Bytes uniquely brings together cyber consultancy, solution specialists, pro-services, support and managed services under one roof.

> Our ultimate goal is to support our customers in reducing their cyber risk, protecting their brand and safeguarding their data.”

Luke Kiernan, *Head of Cyber Security*, Bytes

MEET OUR *HEAD OF CYBER SECURITY*, LUKE KIERNAN

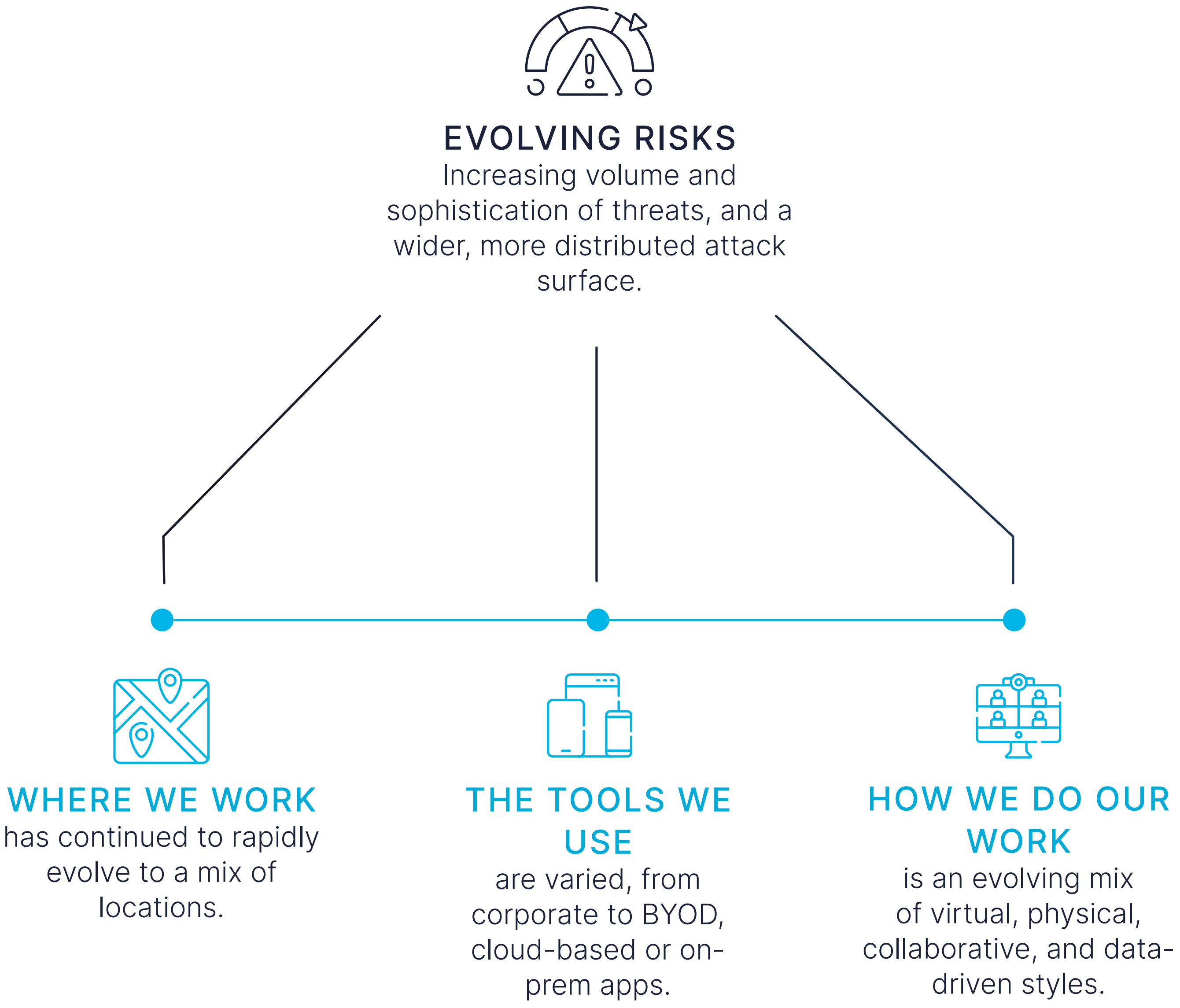
> Bytes brought in experts with different specialities that have really contributed to our overall security strategy and helped us get to where we want to be.”

Jonathan Freedman, *Head of Tech & Security*, Howard Kennedy

LEARN MORE ABOUT OUR WORK WITH HOWARD KENNEDY

COMPANY CREDENTIALS / BYTES

TODAY'S WORKING WORLD



EVOLVING RISKS

Increasing volume and sophistication of threats, and a wider, more distributed attack surface.

WHERE WE WORK

has continued to rapidly evolve to a mix of locations.

THE TOOLS WE USE

are varied, from corporate to BYOD, cloud-based or on-prem apps.

HOW WE DO OUR WORK

is an evolving mix of virtual, physical, collaborative, and data-driven styles.

WHY ZERO TRUST?

Today's organisations require a security model that effectively adapts to the complexity of the modern environment, embraces the hybrid workplace, and protects people, devices, apps, and data wherever they're located.

The never trust, always verify **Zero Trust** approach to security protects organisations by managing and granting access based on the continual verification of identities, devices and services.

This guide aims to provide a collection of useful, expert-led insights and best practices on the **Zero Trust** framework – unpacking the model's guiding principles and leading pillars, and uncovers how best to accelerate your deployment journey.

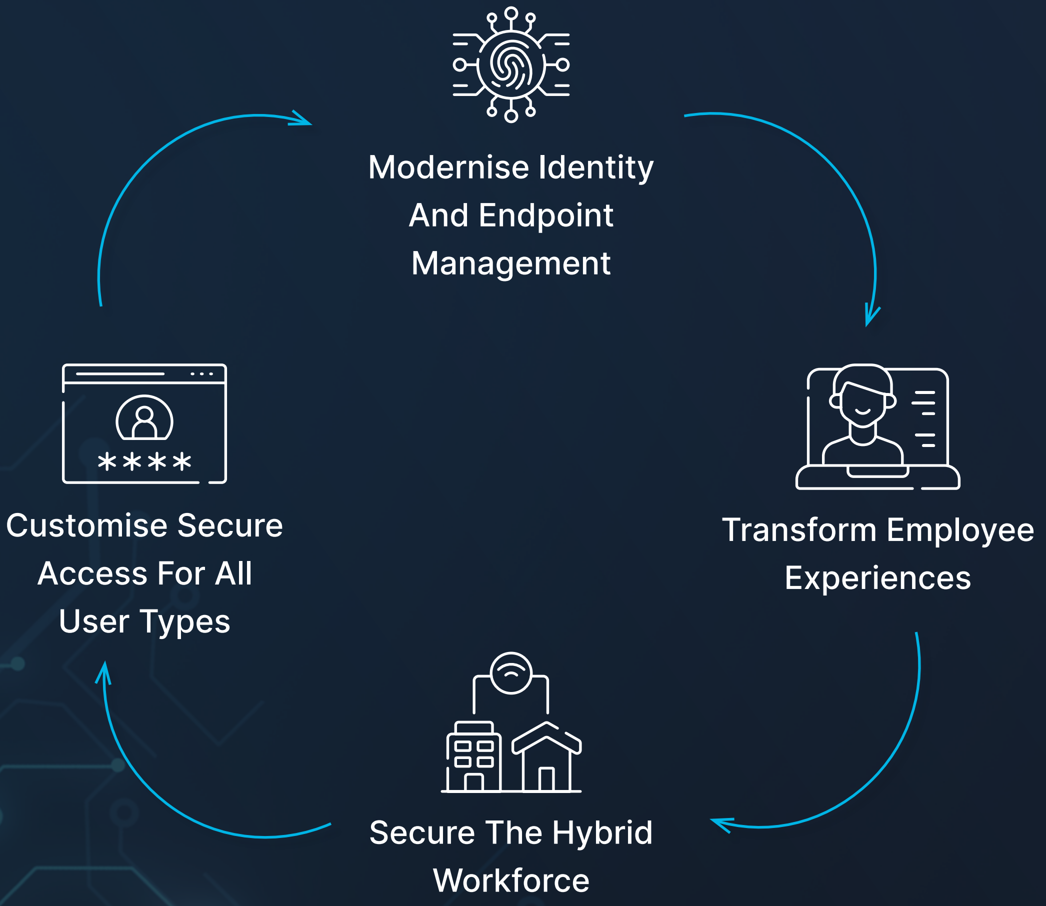
Demystifying Zero Trust, ISF

With the growing ferocity of threats, shifting tides of business demands, increasing diversity and distribution of the workforce and the evolving work environment, the case for adopting a **zero trust** strategy has become more compelling.

"**Zero Trust** demands that organisations adhere to a high degree of information security good practice. In doing so, it helps to recognise the importance of better understanding the workforce, the roles they undertake, and the resources needed to effectively execute their jobs while also protecting the organisation."

SECURE DIGITAL TRANSFORMATION

Building **Zero Trust** Foundations enables organisations to...



Modernise Identity And Endpoint Management

Transform Employee Experiences

Secure The Hybrid Workforce

Customise Secure Access For All User Types

ZERO TRUST IS A KEY SURVIVAL SKILL FOR DIGITAL TRANSFORMATION

You don't have to rip and replace technology to get started. Start by aligning your **Zero Trust** investments to your current business needs and focus on getting quick wins. Each win adds incremental value to reduce risk and improves the security posture of your digital estate. It's never too late to get started and no scope is too small.

The Zero Trust Model, Forrester Research, 2023

> "By adopting the concepts and architectural components of **Zero Trust**, organisations can become more secure while easing compliance burdens and ultimately reducing costs."

FORRESTER

WHAT IS ZERO TRUST:
THE LEADING PRINCIPLES

Never Trust, Always Verify

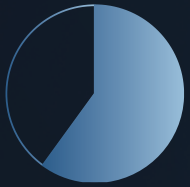
Trust nothing by default - by requiring all users, regardless of location to be authenticated, authorised and continuously validated.

Apply Least-Privileged Access

Give your users only as much access as they need, across all services, minimising each user's exposure to sensitive resources.

Assume Breach

Assume attackers are inside and outside your network, therefore no user or machine should automatically be trusted.



60%

World-renowned Research company, Gartner, predicts that by the end of 2023, 60% of organisations will be adopting a **Zero Trust** security model instead of virtual private networks.

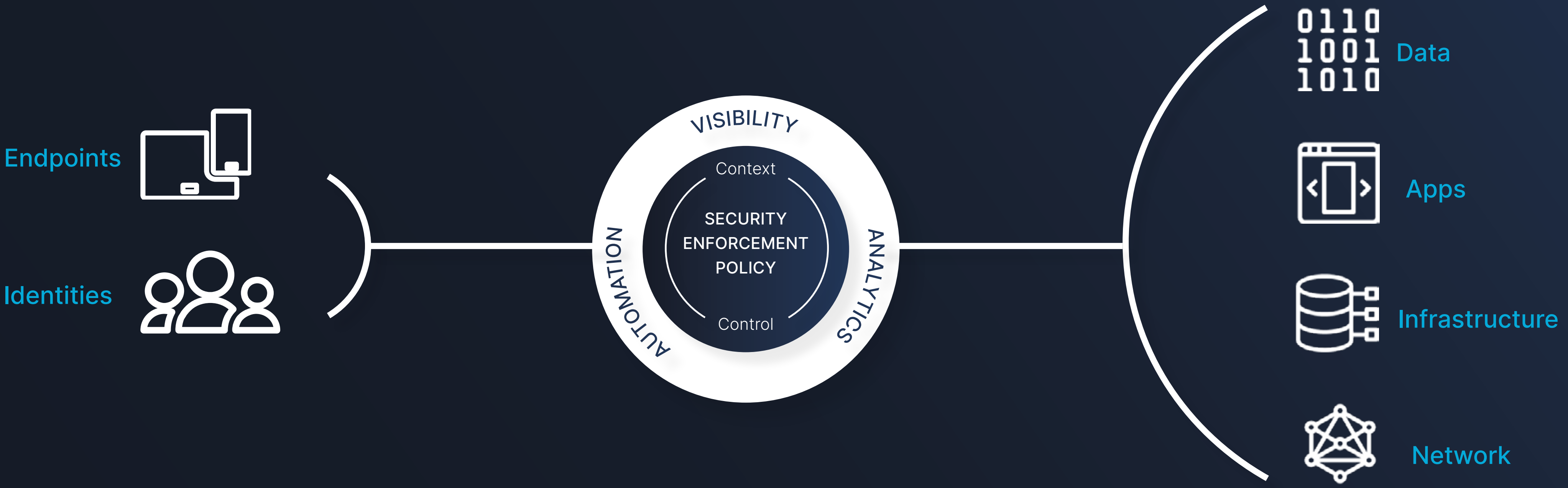
> “The **Zero Trust** approach to Cyber Security is designed to protect businesses from today's threats.”
>
> Gartner

UNDERSTANDING ZERO TRUST: THE ARCHITECTURE

Key learnings from the past few years has allowed for the **Zero Trust** architecture to become more refined. This has encouraged emphasis on the critical importance of integrating policy enforcement and automation, threat intelligence, and threat protection across security pillars.

Microsoft

Microsoft states that these integrated elements "**act upon telemetry across every pillar to inform decisions with real-time signals**".



Each of these elements serves as a source of the signal, a control plane for enforcement, and a critical resource to defend.
You should appropriately spread your investments across each of these elements for maximum protection.

UNPACKING ZERO TRUST:
NETWORK

Flat networks are a serious threat to the modern network. With a single compromised user or server being able to access any part of the network, segmentation is a must.

Micro-segmentation technologies have modernised the approach, transforming the way that businesses architect their network, removing the need to physically segment the technologies.

These technologies ensure that sensitive or high-priority areas of a network can be separated from potentially higher risk areas. Assuming breach within a network is a must, but segmentations allow for containment of the breach.

> **Zero Trust** is a philosophy that can be applied to any Technology… every organisations journey will take a different route. Finding the right mix of technologies to implement its core principles is what will ultimately unlock the full benefits of **Zero Trust** security for a more resilient business.”

Wolfgang Goerlich, *Advisory CISO*, Cisco

> Rebuilding security infrastructure around a **Zero Trust** approach using point solutions may lead to complex deployment and inherent security gaps. To avoid that, Check Point offers a more practical and holistic approach to implement **Zero Trust**, based on single consolidated cyber-security architecture, Check Point Infinity. “

Ian Porteous, *Regional Director*, Check Point

UNPACKING ZERO TRUST: INFRASTRUCTURE

With the adoption of cloud, SAAS and hybrid working, traditional network security technologies are not enough to achieve zero trust and often require multiple disconnected security tools.

ZTNA (Zero Trust Network Access) technologies enable users to securely connect directly to an organisation's data, application & services, regardless of where it presides.

The by-product of this, is that it enables business transformation and safe adoption of new technologies. ZTNA technologies provide a singular platform for all of a user's connections and applies least privilege whilst doing so.

Netskope on ZTNA

"ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. ZTNA not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources."

netskope

UNPACKING ZERO TRUST:

IDENTITY

Identity impacts two of the three core principles of **Zero Trust.** Implementing the right identity technology is pivotal in executing a **Zero Trust** strategy.

In this area of technology, we can streamline authentication and authorisation processes, automate onboarding and offboarding, as well as apply just-in-time privilege and access to applications and systems. When integrated with the wider security stack (ie. Network, Email, Endpoint), Identity technology can enrich the understanding of the user and behaviour to enhance the efficacy of your overall security posture.

Okta on Identity

> By starting with an identity-centric approach to security organisations are able to ensure the right people have the right level of access, to the right resources, in the right context, and that access is assessed continuously—all without adding friction for the user. Ideally this begins with an identity and access management (IAM) solution".

okta

UNPACKING ZERO TRUST:
APPLICATIONS

Application access in the context of Zero Trust is based on the security model used to manage access to an organisations applications at the application level.

When a user, regardless of if they are inside or outside the network perimeter wants to access an application, the access request is valuated based on access controls.

Additionally, with application access requests being justified on a case by case basis, it provides enhanced visibility into how those applications are being used, as well as reducing the attack surface area by only providing the minimum amount of access needed.

Application access links closely with the Identity, Network and Visibility & Analytics pillars of **Zero Trust.**

Mimecast on Application Security

> "To prevent lost productivity and downtime, security, IT, and governance professionals must better secure and manage messaging and collaboration tools. Mimecast delivers a set of solutions that help organisations better manage risk through fast and accurate threat detection and remediation, as well as enhanced visibility into conversation topics and sentiments. Mimecast solutions also diminish the risk of shadow IT by providing visibility beyond email to modern messaging and collaboration channels".

mimecast

UNPACKING ZERO TRUST: DATA

Businesses run on data, however most businesses struggle to get a full grip of the data within their organisations. This often leads to increased security risk and a lack of understanding where their data lies.

DLP (Data Loss Prevention) technologies not only prevent sensitive data from leaving the business, maliciously or not, but also help businesses understand where their sensitive data lies.

Understanding the data within the organisation is the first step to adopting a **Zero Trust** approach, followed by ensuring the right users have the access to the right data - never trust, always verify. Once the right users have access to the right data, DLP technologies can prevent any unwanted data leakages.

“

Forcepoint on Data-First Approach to **Zero Trust**

By taking a data-first approach to **Zero Trust** architecture, organisations can continuously vet and monitor users and data, keeping users safe wherever and however they log in. This enables organisations to deploy dynamic data policies, as opposed to relying on the outdated traditional perimeter and its all-or-nothing approach”.

Forcepoint

UNPACKING ZERO TRUST:
DEVICES

The second principle of Zero Trust asks us to assume a breach; not just that we will be breached in the future but also that we may already have been.

We need technology on our side to understand the risks potentially residing within our environments, as well as to provide robust protection for all future activity. In complementing the other technology areas of a **Zero Trust** strategy, devices can be best looked after at the Endpoint security level.

From a user workflow perspective, these tools look beyond the initial authorisation and access stage and examine user behaviour for any signs of malicious intent.

Understanding the Value: CrowdStrike (Zero Trust Ecosytem Partners) on Zero Trust

“

Enhance user experience with intelligent conditional access. Extend multifactor authentication (MFA) to improve security posture. Assess and share endpoint security posture with CrowdStrike **Zero Trust** ecosystem partners. Leverage APIs to connect your favourite tools. Provide visibility and control of USB devices connected to the enterprise.”

CROWDSTRIKE

VISIBILITY & ANALYTICS

VENDOR: RAPID7

The final area of technology in a **Zero Trust** strategy encompasses all that's been achieved up to this point - providing a holistic view of all ongoing events and traffic passing through networks, whether on-premise, or in the cloud.

By utilising a tool that provides visibility & analytics, organisations are able to focus their time on the more critical tasks and projects.

Enriched by data from all other technology areas, visibility and analytics tools allow for a single pane of glass to quickly distribute tasks and gain insights into what our security investments are doing and where attention may be needed.

Rapid7 on Visibility & Analytics

“

Zero trust is a security concept that assumes that all user and network activity is untrusted until proven otherwise. To implement this concept effectively, visibility and analytics are critical components. Visibility provides a comprehensive understanding of activity, allowing organisations to identify and mitigate security threats in real-time. Analytics helps organisations to analyse the data collected from their business, detect patterns, and make informed decisions.

Together, visibility and analytics enable organisations to validate the identity of users and devices, monitor risk and threats and enforce security policies, providing a robust and effective defense against cyberattacks, threats and data to support a effective Cyber Operating Model by providing real-time insights into security activity, visibility and analytics help organisations to ensure that their **zero-trust** security posture remains effective and up-to-date”.

RAPID7

ZERO TRUST ADOPTION:

BEST PRACTICE FOR SUCCESSFUL DEPLOYMENT OF THE MODEL

Plan:

Create a structured plan that focuses on the overall objective and outcomes.

Build a business case that is aligned with your organisation, taking your business goals and risks into account will support with the planning and implementation of a **Zero Trust** strategy.

Key points to highlight when looking to build a successful business case:

- Modern work to support “work from anywhere at time”
- Enable secure and rapid cloud migration
- Cost savings through simplification of the security stack

Key benefits include:

- Pro-active risk avoidance
- Risk management
- Security and compliance agility

Implement:

Having a robust plan that incorporates multiple stakeholders that understand and are brought into the overall objective.

Assign goals to relevant departments and create accountability. Ensure there is a blend of short term and long term goals.

Take into consideration the different technologies that will need to be utilised and understand integration points between solutions.

Microsoft has found that technical strategies and architectures naturally group into these security initiatives:

- Productivity security
- Modern security operations
- Operational Technology (OT) and Internet of Things (IoT), if applicable to the organisation
- Datacenter, services, and API

ZERO TRUST ADOPTION:

BEST PRACTICE FOR SUCCESSFUL DEPLOYMENT OF THE MODEL

Continuous Review:

Ensure that technology, people and process are continuously reviewed and improved.

Defining success criteria against **Zero Trust** metrics are key, as well as putting in place steps that allow for continuous improvement.

Measure effectiveness and progress by using quantitative analytics from Security tooling.

American Council for Technology Industry Advisory Council

> **Zero Trust** can provide a mature solution today that does not need to add operational complexity or require major architecture changes. In fact, it can simplify operations while increasing security and protecting critical, high value assets.”

act-iac Accelerating Government

‘Zero Trust Cybersecurity Current Trends,’ American Council for Technology Industry Advisory Council

ZERO TRUST ADOPTION: TIPS AND TRICKS FOR CREATING A ZERO TRUST PLAN

Questions to Ask

Can you currently continuously monitor user activity & behaviour?

How flat is your network?

Do you know the number of cloud applications & services in use?

Is remote access given at a network or application level?

How do you currently verify identity?

How granular are your user permissions?

Is all traffic regardless of encryption, inspected?

Are data and files reinspected at any point?

Considerations

Focus should be given in the following areas:

Well managed identity

Informed and aware employees

Well managed devices

Robust, secure connectivity

Consistent policies

Governed data

Data location (current & future)

Classifications of user activities/user profiles

What You Will Need

Maturity Assessment - Assess your maturity against the following areas: identity, devices, connectivity, data & SecOps.

Solution Inventory - Inventory of Security Solutions detailing functionality.

Risk Assessment – Understanding current and perceived risk will focus and prioritise the plan.

Success Plan/Criteria – Detailed and defined success metrics.

WHAT'S NEXT?

Embracing **Zero Trust** as part of your Cyber Security strategy can be daunting. Establishing where and how to begin can be tough.

To support our clients in their journey to a modern security architecture with **Zero Trust**, Bytes have created the **Zero Trust** Overview. Delivered by our agnostic in-house specialists, you'll receive tailored guidance & support - shaped around your organisation's environment – to ensure your **Zero Trust** Journey is the best it can be.

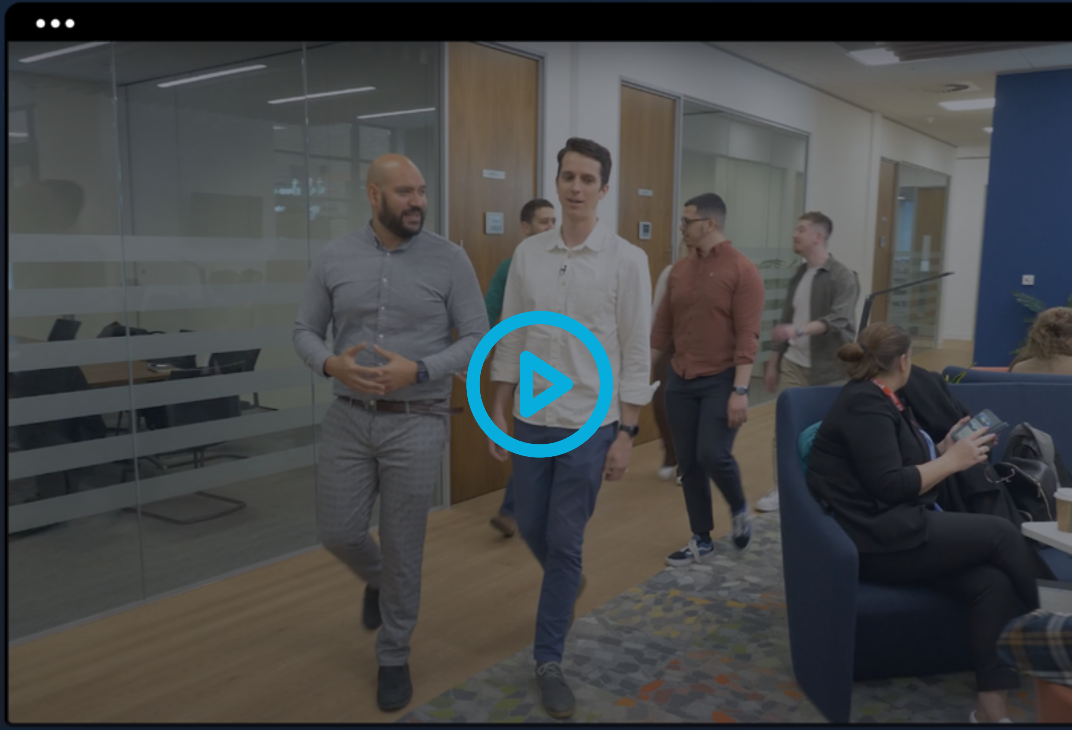
What to Expect:

The engagement is a 1:1 interactive session with one of our specialists. The engagement looks to cover the following agenda:

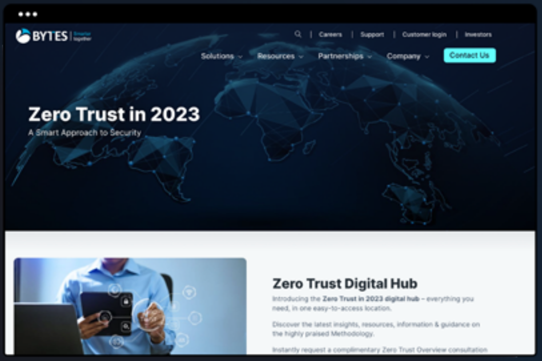
- What is **Zero Trust**?
- Core Principles and Technologies
- Analyse and Discover Gaps
- Vendor Considerations & Integrations

Visit bytes.co.uk or email tellmemore@bytes.co.uk to find out more.

Meet our **Zero Trust** Team



USEFUL RESOURCES



Zero Trust in 2023

A Smart Approach to Security

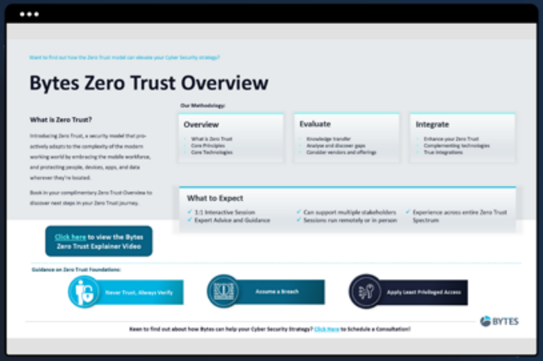
Zero Trust Digital Hub

Introducing the **Zero Trust in 2023 digital hub** – everything you need, in one easy-to-access location.

Discover the latest insights, resources, information & guidance on the highly praised Methodology.

Instantly request a complimentary Zero Trust Overview consultation

Zero Trust Hub


Want to find out how the Zero Trust model can elevate your Cyber Security strategy?

Bytes Zero Trust Overview

What is Zero Trust?

Introducing Zero Trust, a security model that pro-actively adapts to the complexity of the modern working world by embracing the mobile workforce, and protecting people, devices, apps, and data wherever they're located.

Book in your complimentary Zero Trust Overview to discover next steps in your Zero Trust journey.

Our Methodology:

Overview
- What is Zero Trust
- Core Principles
- Core Technologies

Evaluate
- Knowledge transfer
- Analyse and discover gaps
- Consider vendors and offerings

Integrate
- Enhance your Zero Trust
- Complementing technologies
- True integrations

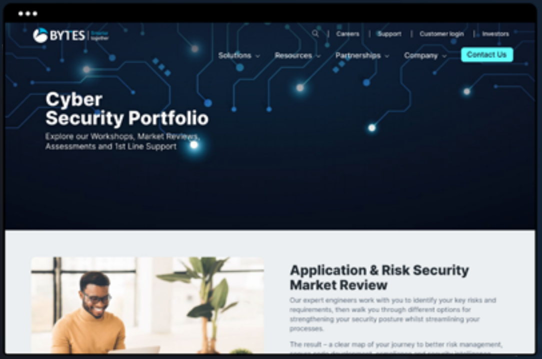
What to Expect
- ✓ 1:1 Interactive Session
- ✓ Expert Advice and Guidance
- ✓ Can support multiple stakeholders
- ✓ Sessions run remotely or in person
- ✓ Experience across entire Zero Trust Spectrum

Click here to view the Bytes Zero Trust Explainer Video

Guidance on Zero Trust Foundations:

Keen to find out about how Bytes can help your Cyber Security Strategy? Click here to Schedule a Consultation!

Zero Trust Flyer



Cyber Security Portfolio

Explore our Workshops, Market Reviews, Assessments and 1st Line Support

Application & Risk Security Market Review

Our expert engineers work with you to identify your key risks and requirements, then walk you through different options for strengthening your security posture whilst streamlining your processes.

The result – a clear map of your journey to better risk management,

Cyber Security Portfolio of Workshops

Zero Trust Explainer Video