Gigamon®

Zero Trust is gaining momentum.

Start your journey now.

The concept of Zero Trust is gaining traction as interest in adoption is growing.

Traditionally, Zero Trust has held negative connotations due to its 'never trust, always verify' message that led businesses to believe employee productivity would be hindered by the extra hoops they would have to jump through to access the network. However, the Gigamon EMEA Zero Trust survey uprooted this theory by finding that **87%** of those who had started on their Zero Trust journey reported that adopting the framework has improved their productivity.

Of course, it's impossible to consider IT and cybersecurity without the context of the 'New Tomorrow' that the world was catapulted in 2020. The monumental and almost overnight shift to remote working – which is slowly morphing into flexible working – has expanded and evolved the cyberthreat landscape and created new challenges for IT and security pros, something **84%** decision makers reported. As such, Zero Trust is now being viewed as a strategic investment to help alleviate this additional burden. In fact, **97%** of respondents who had started their Zero Trust journey stated that the framework has or could help their business as it deals with the current global situation.

Increasing threatscape

84% of IT decision makers have reported an **increase in cyberthreats**, with **51%** believing that the shift to WFH has increased vulnerability

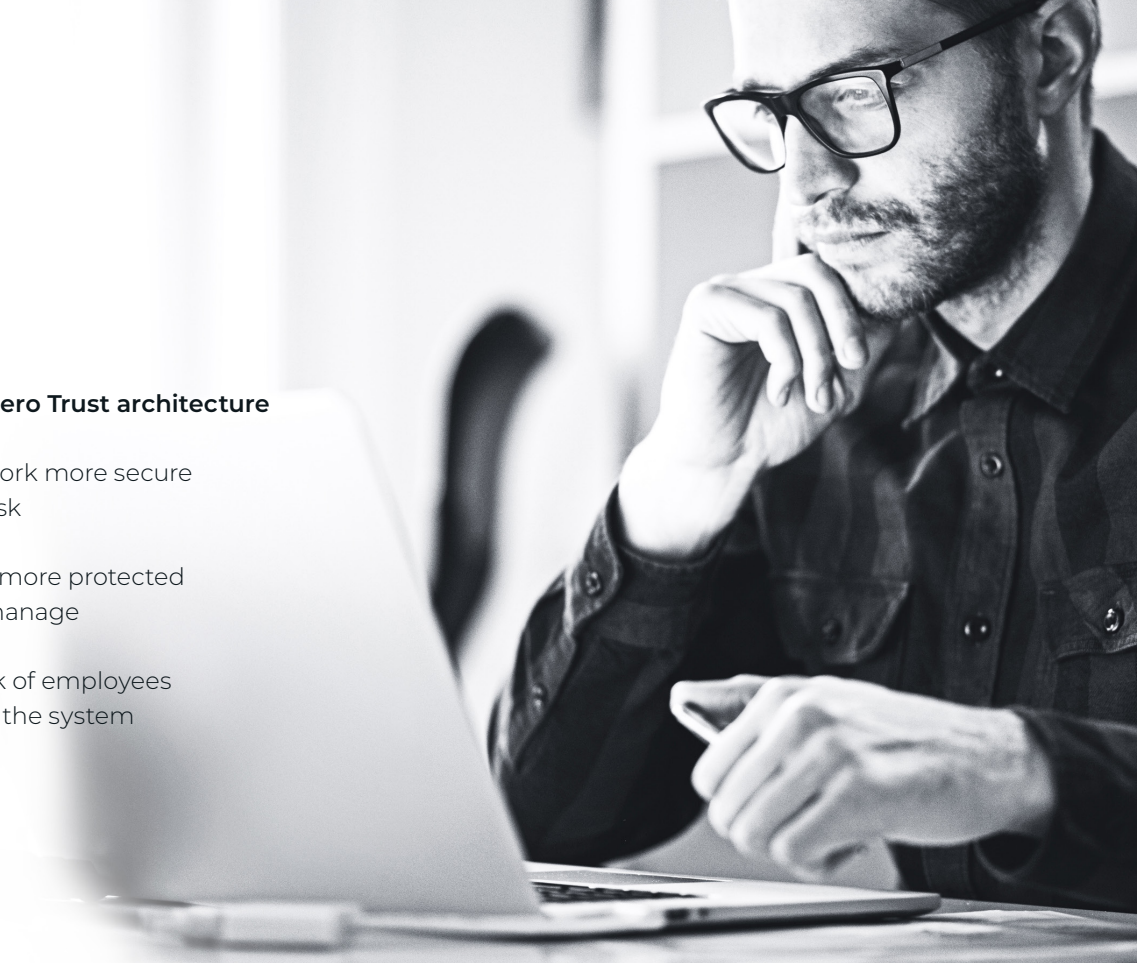
41% have been subject to an increase in **phishing** schemes

33% have been subject to an increase in **data breaches**

33% have faced an increased **insider threat** due to disengaged employees

Changing perceptions

The survey collated the responses of 500 IT and security decision makers across the UK, France and Germany, and supported our hypothesis that Zero Trust is a force for good. More and more companies are delving into the concept of Zero Trust and starting on their own journeys towards adopting this architecture. As such, comprehensive awareness of the framework is growing. The survey found that **89%** of respondents had a high awareness of Zero Trust, **76%** of which were adopters or potential adopters. The high proportion of respondents that were adopting or looking to adopt the framework prove that Zero Trust is a competitive advantage for businesses, rather than a necessary evil.



Main reasons to adopt Zero Trust architecture

54% Make our network more secure and mitigate risk

51% Make our data more protected and easier to manage

49% Reduce the risk of employees compromising the system

Staying secure

Zero Trust doesn't assume that any user or device is safe based on pre-existing credentials, but instead scrutinises asset behaviour and only grants access to the network and its resources based on this information.

In fact, the main reason for adopting Zero Trust architecture is increased security – with **54%** stating that the reason they started or are looking to start a journey towards Zero Trust is to secure the network and mitigate risk.

Visibility also plays a key part, as it's impossible to monitor what you can't see. With complexity growing and the network itself evolving, having an uncompromised view of everything on the network is paramount. This is why protecting data and making it easier to manage was the second most cited reason for adopting Zero Trust architecture at **51%**.

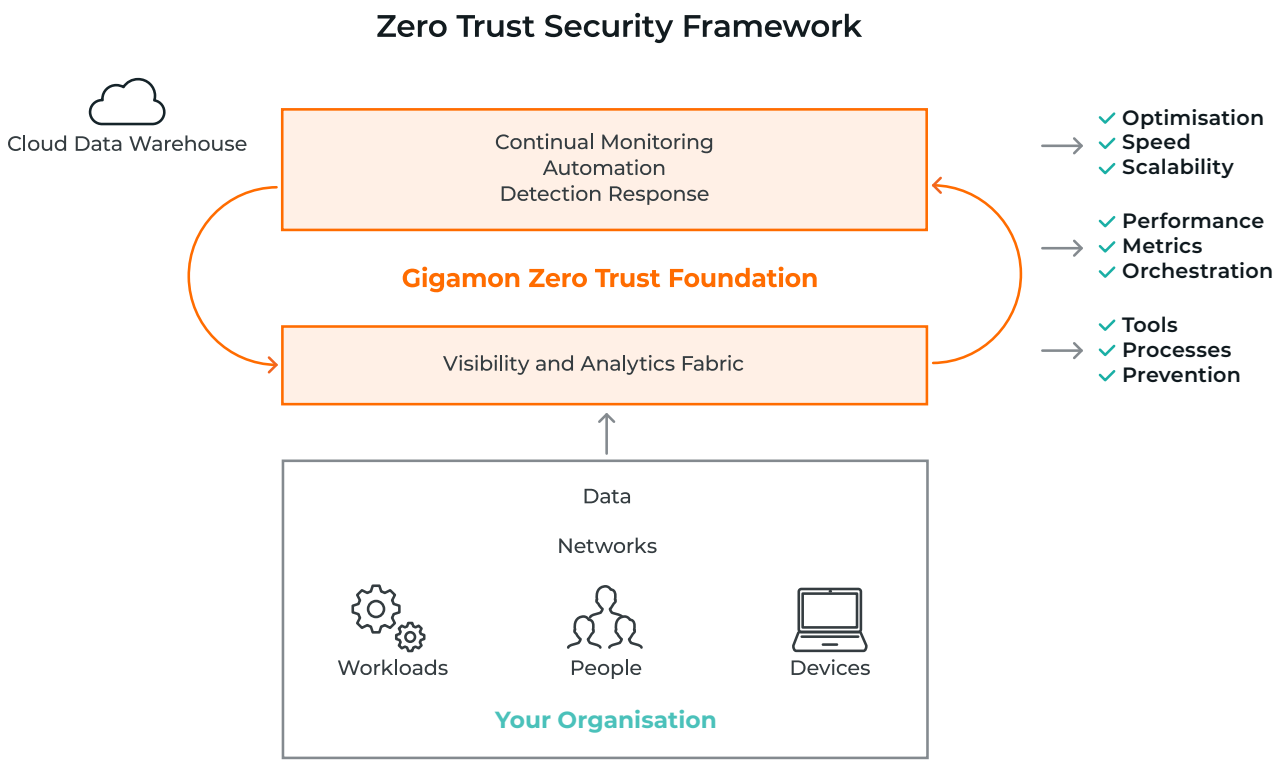
Culture clash

The fluid working model that has become the 'new normal' has allowed Zero Trust the opportunity to prove its value, as businesses adjust their practices and processes to cope with the changing landscape. This model gives employees far greater responsibility for keeping the network secure, something cybercriminals are only too happy to take advantage of. The Gigamon survey found that culture was both a barrier and a motivator behind organisations' Zero Trust journeys. Shadow IT and employee education were cited as top challenges facing respondents, signalling that businesses may be looking to adopt Zero Trust to minimise the insider threat. Conversely, **65%** of respondents who decided not to adopt the framework cited wrong company culture as the top reason behind this decision and getting employees on board was named the most important thing to have in place before starting the journey towards Zero Trust.

The role of Zero Trust in the New Tomorrow

There is no doubt that Zero Trust has a significant part to play in the 'New Tomorrow' of enterprise working practices and cybersecurity. Zero Trust is a vital investment for businesses as the cyberthreat landscape expands over the next year and beyond. With this framework, IT and security decision-makers can ensure organisations stay secure without compromising productivity or user experience.

Zero Trust visibility – we've got you covered

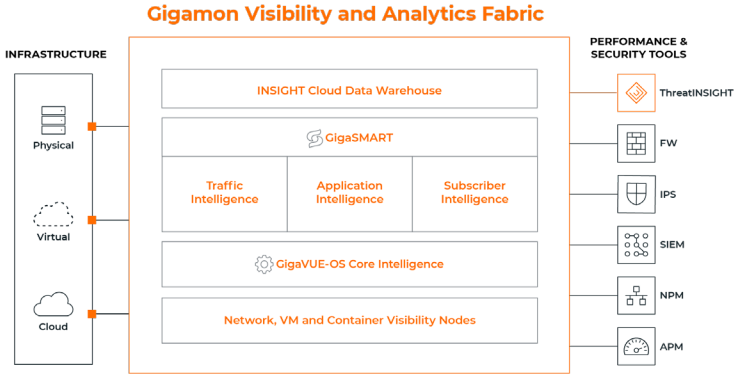


The bedrock tenet of Zero Trust is to move the defensive perimeter from the edge of the network to every asset within the network, which is an impossible task if you don't have comprehensive visibility.

Visibility into all information in motion is the cornerstone of an effective Zero Trust approach. This includes: identifying and classifying data; mapping flows of sensitive data; decrypting traffic for complete visibility (of North-South and East-West traffic); performing basic network segmentation; understanding the network topology; and inventory devices and applications. This is where the Gigamon Visibility and Analytics Fabric comes in.

Gigamon Visibility and Analytics Fabric

The Gigamon Visibility and Analytics Fabric sits between a business' infrastructure and its performance and security tools. It collects all information in motion across physical, virtual and cloud infrastructures, transforming it before distributing it to an organisation's tools. It goes beyond any network packet broker to deliver a smarter, more proactive approach to network management, monitoring and security. It delivers optimised, full-fidelity data to security and performance monitoring tools, dramatically improving tool effectiveness and efficiency. High-velocity threat detection and response provides peace of mind, while advanced orchestration and automation enables your NetOps and InfoSec teams to do more, faster.



Once all information in motion has been discovered, it must be given context within the environment. As part of Gigamon Visibility and Analytics Fabric, Application Intelligence continuously monitors traffic by filtering apps and providing the right metadata to each tool for effective inspection. This empowers IT teams and analytics tools with unrivalled application visibility and control by gathering clear, actionable and reliable data

Start your journey today.

for efficient monitoring and security analytics. In practice, this could be leveraged to identify self-assignment or expired SSL certificates, the volume and type of DNS requests including non-standard ports, or suspicious remote SHH sessions. With App Visualization, App Filtering and App Metadata, Application Intelligence provides unprecedented visibility into applications on the network, their behaviour and user experience.

Finally, InfoSec teams must be able to monitor the traffic, detect threats and respond quickly. This includes monitoring for insider threats, credential theft and data exfiltration; leveraging network detection tools; analysing decrypted traffic; implementing policies for automated response; and facilitating triggered response actions. Gigamon ThreatINSIGHT allows teams to detect, investigate and respond to threats in real time.

SSL/TLS Decryption

It's crucial to consider encrypted traffic when assessing visibility. Industry standards like SSL/TLS are used to encrypt data as it is exchanged over IP networks, creating a secure channel between the server and the end user's computer or other devices as they exchange information over the internet. While protecting data, encryption also blinds network security and application monitoring tools as it can be leveraged by cybercriminals to conceal malware, hide command-and-control traffic and cloak the exfiltration of stolen data.

The decryption of SSL/TLS traffic is crucial for the effectiveness of security and monitoring tools, as well as to eliminate blind spots and give teams full insight into all network assets. However, it is extremely computationally intensive and can introduce network latency. Given the amount of encrypted traffic on the network and the importance of traffic inspected for a Zero Trust approach, businesses must leverage centralised SSL/TLS decryption to effectively decrypt traffic, share it with the relevant tools and then re-encrypt it.

GigaSMART SSL/TLS Decryption enables NetOps and applications teams to obtain complete visibility into SSL/TLS traffic regardless of protocol or application – including TLS 1.3 – so they can monitor application performance, analyse usage patterns and secure their networks against data breaches and threats using encrypted communications. Sitting within the Gigamon Visibility and Analytics Fabric enables GigaSMART decryption to decrypt traffic once and share it with every tool that needs to inspect it before re-encryption. This removes the need for traffic to be continually decrypted and re-encrypted as it is inspected by each tool, which is where latency becomes a factor, as well as simplifying troubleshooting.

With the **Gigamon Zero Trust Foundation**, enterprises can seamlessly undertake their journey towards achieving Zero Trust architecture by gaining full visibility into all information in motion, including encrypted traffic, analysing it and implementing policies around that data, and maintaining real-time threat detection and response.

Contact Gigamon today to learn how we can help you along your journey towards Zero Trust.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 www.gigamon.com

EMEA Headquarters
100 Brook Drive, Green Park, Reading, RG2 6UJ United Kingdom
+44 (0)118 304 0300 emea-info@gigamon.com

01.21_01