Gigamon®

SURVEY

The IT & Security Landscape for 2020 and Beyond and the Role of Zero Trust

Introduction

Today's IT landscape is increasingly complex, especially in light of the pandemic, which has dramatically altered working practices around the globe and brought flexible working to the fore. Of course, this evolving landscape does not come without problems. IT practitioners and decision makers are routinely faced with challenges and threats, which could inflict significant consequences if not managed properly. From issues such as shadow IT, legacy systems affecting performance and low employee awareness/apathy, through to bad actors and hostile nation states looking to cause disruption, IT and security teams face a plethora of internal and external challenges on a daily basis affecting both infrastructure and operations.

Many are therefore looking to implement security strategies and solutions which can help alleviate some of the burden caused by such issues. One such approach is Zero Trust. Whilst not an entirely new concept, Zero Trust has been attracting increasing interest since Google's adoption of the framework, and now, given the current climate, is seen by many as one of the most secure ways enterprises can operate.

This survey report looks into how Zero Trust is perceived, understood and has worked in three key European markets – the UK, France and Germany – to provide a more holistic view of Zero Trust architecture in this region. The report also addresses how IT decision makers have been affected by the pandemic, what is challenging them, and how Zero Trust and its applications are viewed within the wider business – especially at the board level.

Methodology

The data used in this report was conducted by Vitreous World, which adopted an online methodology and recruited a mix of senior decision makers. Interviews were conducted in the UK, France and Germany, with all respondents guaranteed anonymity as part of the study.

Fieldwork was carried out between July 15th and July 24th 2020. The sample comprised of the following professionals:

- **500** respondents split across Germany (200), France (150) and the UK (150)
- All working for companies with more than 1,000 employees
- Job titles included: Chief Information Officer **(18 percent)**, Chief Information Security Officer **(18 percent)**, Chief Technology Officer **(16 percent)**, Network Manager **(15 percent)**, Director of Network Operations **(9 percent)**, and Network Architect **(8 percent)**
- When asked about their involvement in the decision-making process within their organisation **66 percent** help reach the final decision as part of a group or committee, **23 percent** make the final decision with input from staff or management, and **11 percent** stated that they are the sole decision maker (significantly more likely in the UK – **26 percent**)

The data was split into two strands, those respondents classed as having high awareness of Zero Trust – such as those already using the architecture or looking to implement it, and low awareness – those who were unaware of the concept or how to implement it.

Some questions covered both strands of respondents, and this report will address common concerns and challenges, alongside specific attitudes from high and low awareness respondents.

This report not only explores attitudes towards Zero Trust and its implementation, but also addresses how it actually benefits the organisation and the end user. At a time when everyone across the globe is trying to grab onto a semblance of normality, IT plays an important role in facilitating fluid working practices while ensuring the organisation's data, networks and infrastructure remain secure.

We believe that Zero Trust can help achieve just that, and we hope this report provides the clarity you seek to help inform your current or future IT and security strategy.

The most pressing challenges and threats facing IT and security decision makers in the wake of the pandemic

More attacks and vulnerabilities exacerbated by work from home and employee disengagement

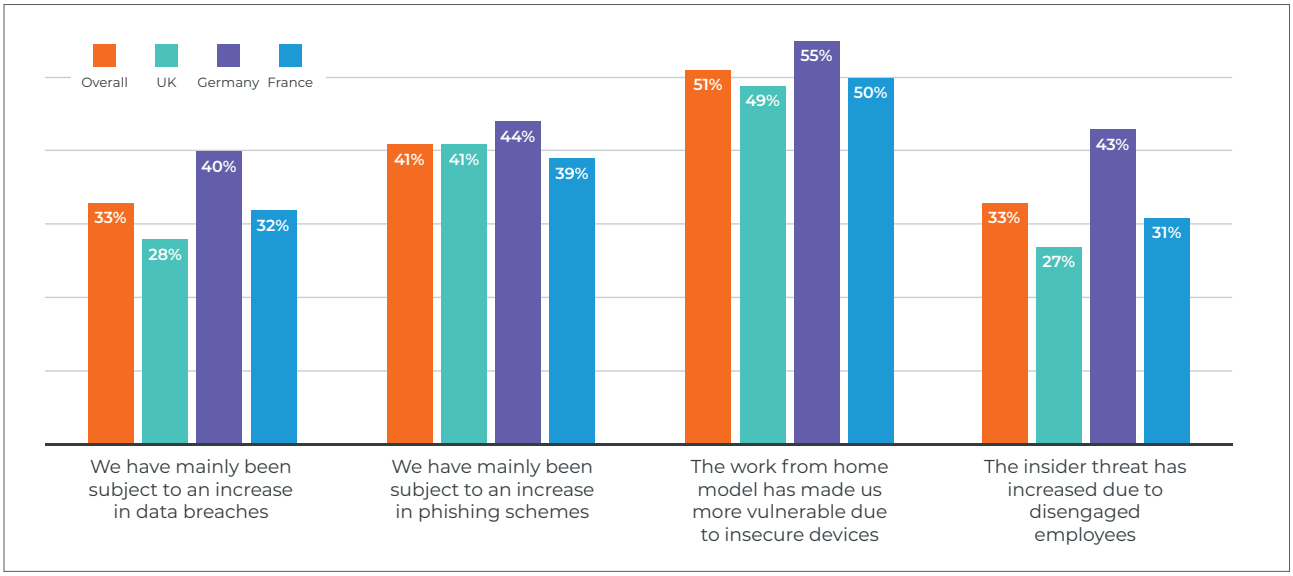
In light of the shift towards home working and the rise in the reporting of incidents regarding data breaches, we wanted to understand the current threatscape.

Most organisations said they had seen an increase in the number of threats since the beginning of the year. Although threat detection systems are considered to be flexible, or somewhat flexible, by the majority – the current work from home model appears to have made organisations more vulnerable.

Overall, **84 percent** of respondents said that their organisation had seen a rise in the number of threats since the start of this year. Respondents reported that:

- The work from home model has made us more vulnerable due to insecure devices – **51 percent**
- We have mainly been subject to an increase in phishing schemes – **41 percent**
- We have mainly been subject to an increase in data breaches – **33 percent**
- The insider threat has increased due to disengaged employees – **33 percent** (particularly in Germany **(43 percent)** when compared to the UK **(27 percent)** and France **(31 percent)**)

When asked how flexible, or not flexible, their network and threat detection system is with regards to accommodating the challenges of remote working for employees, the largest proportion **(46 percent)** said that their system is flexible and mainly designed to support remote working, both long- and short-term. **31 percent** stated that their system is somewhat flexible, meaning while it is not designed for employees to access the server remotely, they do have a temporary fix in case of emergency and **20 percent** said that their system was hybrid – a system designed to support employees working on and off-site equally.



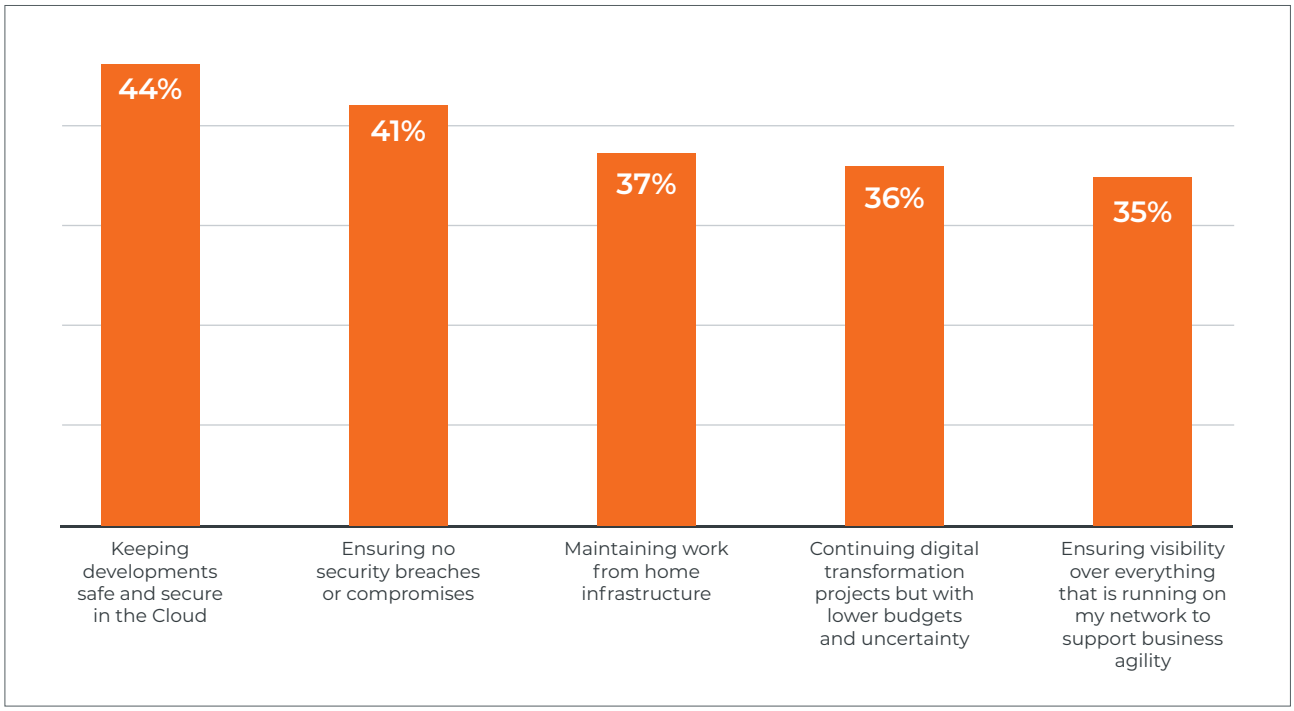
Digital transformation, shadow IT and employee security awareness cause headaches for decision makers

Overall, respondents said that their biggest IT challenges over the next few years will be digital transformation **(50 percent)**, shadow IT **(45 percent)**, and employee security education **(37 percent)**. An increase in data and applications to monitor and protect **(36 percent)** and managing a complex working landscape **(35 percent)** also scored highly.

The range of answers again emphasises that IT departments are under pressure to support new business requirements and ensure that systems are protected from threats coming from inside and outside the organisation. There is no one-size-fits-all solution to address all their requirements, based on the fact many aspects – such as how employees use and abuse the network – are often out of their control.

In terms of responding to these challenges, alongside the aftermath of the pandemic, IT decision makers' priorities for the rest of the year focused on maintaining and evolving business processes. Keeping developments safe and secure in the Cloud **(44 percent)** was ranked as respondents' top priority, followed by ensuring no security breaches or compromise **(41 percent)**, and maintaining work from home infrastructure **(37 percent)**. Continuing digital transformation projects but with lower budgets and uncertainty **(36 percent)** and ensuring visibility over everything that is running on the network to support business agility **(35 percent)** also ranked highly, implying that IT leaders are keen to consolidate operations to promote agility and efficiency whilst uncertainty remains.

With security threats on the rise and infrastructure under added strain, IT leaders are having to deal with issues unthinkable just a few months ago. What is clear from this report is that employees present a significant security challenge for businesses – shadow IT, employee education and the insider threat were all picked out as problems faced. To be successful in the coming months and years, IT leaders will need to minimise these preventable threats, enabling them to devote time and effort to more strategic initiatives, such as progressing digital transformation efforts and securing their organisation against the rise in bad actors.



Why organisations are adopting or planning to adopt Zero Trust

Zero Trust architecture has typically had negative connotations within the industry due to its 'trust no-one' approach and the effect this could have on employee productivity. With this research, we wanted to explore the weight of this view and draw out the benefits of starting a Zero Trust journey. To do this, we first had to understand how much IT leaders know about Zero Trust, and how many have already adopted the architecture. Overall, **89 percent** of respondents were found to have a 'high awareness' of Zero Trust architecture. The way we ascertained this level of awareness is presented below, as well as the subsets of respondents we derived depending on their feedback.

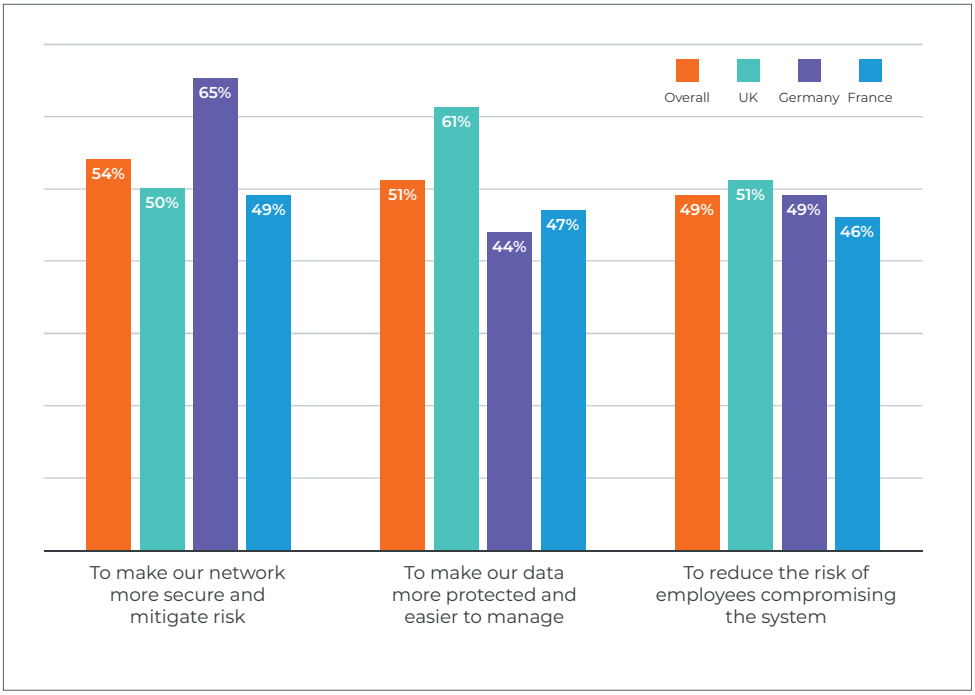
When asked "how familiar, or unfamiliar, are you with the term 'Zero Trust' architecture", **75 percent** of high awareness respondents stated they are already adopting or plan to adopt Zero Trust architecture (adopters and potential adopters). Whereas only **24 percent** stated they looked into Zero Trust but decided it was not the right strategy for them (non-adopters).

It was interesting to understand the key challenges of a Zero Trust journey, both from the perspective of those who have gone through it, and those that are deliberating the prospect. Of course, before any project begins, certain groundwork needs to be completed. Respondents advised that, before starting the journey towards Zero Trust, employee support **(28 percent)**, necessary funds **(27 percent)**, network visibility **(26 percent)** and board buy-in **(19 percent)** are the most important things to have in place.

We also wanted to understand the motive behind adopting the approach. Potential adopters and adopters chose to initiate the Zero Trust journey for a number of reasons, but the top three were:

- To make our network more secure and mitigate risk – **54 percent** (particularly true in Germany – **65 percent**)
- To make our data more protected and easier to manage – **51 percent** (especially in the UK where this is the top answer at **61 percent**)
- To reduce the risk of employees compromising the system – **49 percent**

Interestingly, these benefits are correlated to the challenges IT leaders expect to face in the new normal, implying that Zero Trust is seen as a viable solution for keeping enterprises safe from both internal and external threats. By embracing the 'trust no-one' approach, IT leaders are able to gain control over increasingly complex networks, reducing the chance for employees to adopt bad digital habits and enabling better protection for critical assets such as personal or sensitive data.



Zero Trust enhances IT strategy but is it attainable?

The majority of respondents were united in their belief that Zero Trust enhances, or would enhance, their IT strategy **(61 percent)**; in the UK this figure rose to **70 percent** (compared to **61 percent** in Germany and **54 percent** in France). **30 percent** of respondents reported that Zero Trust had/would underpin their IT strategy. In France, this figure was as high as **35 percent** – versus **24 percent** in the UK and **28 percent** in Germany.

However, adopting a Zero Trust framework is not for everyone: non-adopters stated that Zero Trust wasn't the right approach for them because they believed they had the wrong company culture **(65 percent)**, they felt it was too time consuming **(65 percent)** or they couldn't see the ROI **(60 percent)**. However, with shifting working practices, these sentiments may change with time.

We then asked participants if they thought Zero Trust was actually attainable, as the non-adopters had outlined some interesting hesitancies which we wanted to address. Overall, **77 percent** of respondents disagreed with the statement "Zero Trust is completely unattainable", especially in Germany **(88 percent)** versus France **(72 percent)** and the UK **(73 percent)** – suggesting that the majority believe it to be attainable. We saw strong agreement scores for the statement "Zero Trust is a journey, not a tick box exercise" **(77 percent)**, highlighting that many realise it is not a quick transformation. Respondents recognise that Zero Trust continues over a long period of time and drives a culture of constant improvement and evolution of security practices, as it is not simply a product businesses can buy.

The two biggest challenges respondents expected to encounter on their Zero Trust journey were the need for a culture shift **(40 percent)** – "employees don't like being questioned, investigated and cross-checked, negative connotation in the 'never trust, always verify' message" – and the presence of legacy and fragmented systems **(39 percent)** – "trying to integrate with and reorganise existing systems is a challenge. Most successful deployments have been 'baked in' from day one."

The benefits of Zero Trust architecture

One of the biggest benefits of Zero Trust identified by respondents was productivity, with **87 percent** saying that productivity had/would have improved since beginning their Zero Trust journey. Almost a quarter **(24 percent)** said productivity had/would have improved a lot, **63 percent** said that it had/would have improved a bit/marginally, **11 percent** said it had/would stay the same. For those whose productivity had improved, or those who predicted it would, since the start of their Zero Trust journey, **43 percent** said this was because the system had/would run faster, **35 percent** said there were/would be fewer security breaches, and **23 percent** said that downtime had/would have been reduced. From this we can surmise that the architecture is solving common challenges within the industry, improving operations.

This was confirmed, as **76 percent** agreed that 'given the increase in attacks, it would be unwise not to consider a Zero Trust approach'. Almost two in three **(60 percent)** agreed that 'Zero Trust will be a key trend in IT over the next 18 months due to the current global situation and the benefits it provides', and **97 percent** said that Zero Trust had helped/could have helped their business as it deals with the impacts of the current global situation. This help encompassed agility **(67 percent)**, enhancing security in light of an increase in remote working **(66 percent)**, and helping to combat the rise in bad actors **(53 percent)**.

But what about its perceptions internally? Considering the time and investment required for successful implementation, we wanted to understand how Zero Trust is considered by employees, and most notably, the board.

When asked about board involvement with Zero Trust we saw differing results. One third of respondents **(33 percent)** said Zero Trust should 'absolutely be discussed at board level' and **27 percent** said it should be a priority at any boardroom table given the current climate. However, just over half **(53 percent)** agreed with the statement that 'Zero Trust is openly talked about at board level'.

Almost a third of respondents **(30 percent)** agreed that 'Zero Trust isn't talked about at board level, but feeds into our digital strategy, so it's handled by the CIO'. Furthermore, **49 percent** agreed with the statement 'IT/security teams understand the value behind Zero Trust, but it hasn't yet escalated up to the board'. These results imply that there is a distinct split between how it is perceived within different businesses and that major IT overhauls are not reaching the attention of the wider C-suite.

IT decision makers are learning from their experience

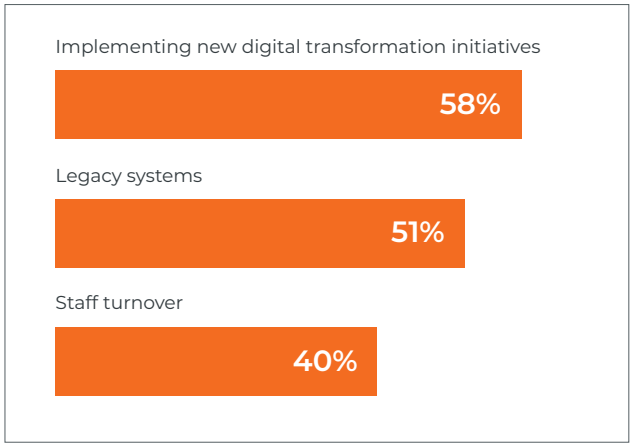
More than nine in ten, **91 percent**, said that they had learnt lessons regarding IT since the start of this year, with the key take-outs being:

- We should have been more prepared for remote working – **33 percent**
- We should have better optimised existing tools/applications running on our network to do more without additional investment – **18 percent**
- We should have been more agile in our approach and processes – **16 percent**

If they had to go through the same experience again, respondents would do one of the following three things: a full audit on the state of their IT infrastructure to make better informed decisions, better educate and train their employees on security policies and threat, or prioritise investing in new IT architecture (all three selected by **36 percent**), and **32 percent** of respondents would either remove all applications and tools that were taking up unnecessary storage and traffic on the network, or streamline their IT approach and processes.

Where enterprises are spending their pennies

Currently the three biggest cost centres within IT are implementing new digital transformation initiatives **(58 percent)**, legacy systems **(51 percent)**, and staff turnover **(40 percent)**.



Whilst not uncommon within the industry, these issues can cause productivity headaches, with team changes often disruptive and extensive training required to get the replacement up to speed. When we asked IT decision makers about their biggest productivity challenges, they cited:

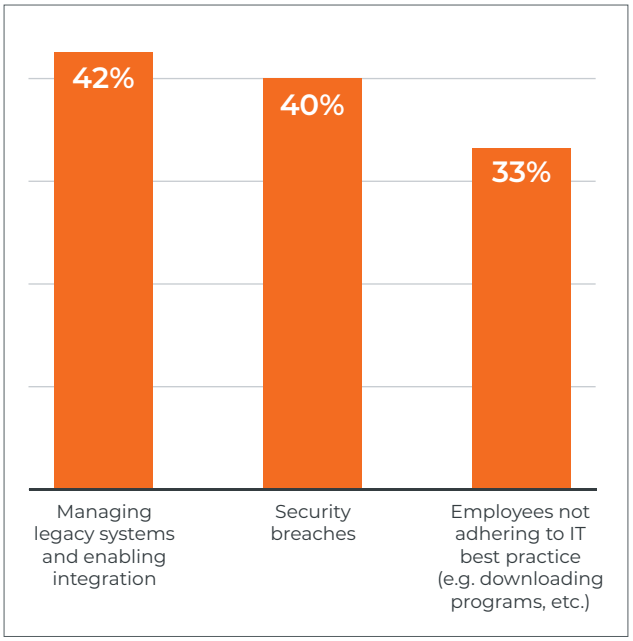
- Managing legacy systems and enabling integration – **42 percent**
- Security breaches – **40 percent**
- Employees not adhering to IT best practice (e.g. downloading programmes, etc.) – **33 percent**

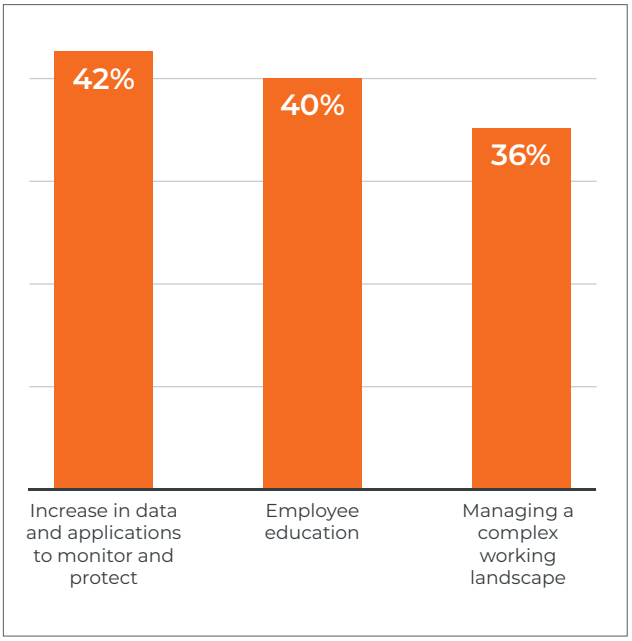
However, they expected these issues to shift, and when looking forward over the next 12 months to three years, respondents believe the biggest challenges will be:

- Increase in data and applications to monitor and protect – **42 percent**
- Employee education – ensuring users understand how their actions could compromise the network and organisation – **40 percent**
- Managing a complex working landscape – ensuring platforms that have been set up to enable remote working are maintained long-term – **36 percent**

What is clear is that enterprises will need to put in place watertight strategies to protect increasing volumes of data, as firms become ever more data-driven. A policy of protection and prevention will be vital, and will rely on employees playing their part and not letting bad actors in the back door unintentionally. No wonder employee education is ranked so highly, as employees have the potential to undo any work done via a relatively simple mistake.

For those looking to implement a protect and prevent policy Zero Trust seems like the obvious answer. As businesses adapt to the new normal, it has never been more important that they stay secure and adapt to evolving network requirements, without forgoing network performance. Zero Trust can achieve this.





Key learnings

1. The perception of Zero Trust is changing

The pandemic has left enterprises vulnerable, by their own admission. Zero Trust architecture is now seen as a strong contender to help corporations address their security issues, and not seen negatively by the majority.

2. Culture remains a barrier

An intangible issue which plagues enterprises, this is seen in answers from those who chose not to implement Zero Trust specifically due to it not fitting company culture, but board support and uncertainty about where the responsibility for this initiative sits are also cited as barriers.

3. Network complexity is a growing headache

As the IT function becomes more sophisticated, so does its complexity. The working from home model has exacerbated this, leading to enterprise IT and NetOps teams feeling more vulnerable. Add to this the increase in threats since the start of the year and it is easy to see why enterprises crave full network visibility and the removal of problems like shadow IT which disrupt a holistic approach.

4. Digital transformation is key – but budget will dictate the extent

Half of respondents still see this as a priority, but a third believe it will be on reduced budgets. With those who chose not to implement Zero Trust citing budget and lack of ROI as a key motivator of that choice, decision makers will need to prioritise their transformation projects to ensure they are able to meet digital requirements in light of reduced funds.

5. The Cloud is growing in importance

Respondents specifically cited the Cloud as a priority for the rest of the year in terms of keeping developments safe. With many looking to continue and expand work from home operations, it is likely its importance will only augment, thanks to its ability to maintain a fluid and mobile workforce without compromising on security.

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

09.20_04