

The State Of Zero Trust Transformation 2023

FROM PREVENTION TO ENABLEMENT:

*Leveraging the Full Potential of Zero Trust for
the Highly Mobile and Cloud-Centric Enterprise*



Contents

- 03. [Executive summary](#)
 - 05. [State of zero trust: Fast facts](#)
 - 06. [Section I: The cloud context behind zero trust](#)
 - 13. [Section II: Securing the case for zero trust](#)
Regional POV: The voice of the Americas
 - 22. [Section III: Turning to zero trust to deliver hybrid ways of working](#)
Regional POV: The voice of APAC
 - 30. [Section IV: Taking a zero trust approach to integrating emerging technologies](#)
Regional POV: The voice of EMEA
 - 35. [Section V: The road to unlocking the full potential of zero trust](#)
 - 38. [About Zscaler and Zscaler Zero Trust Exchange](#)
 - 40. [Methodology](#)
-



Executive summary

Nathan Howe | VP, Emerging Technology & 5G, Zscaler

Against a backdrop of rapid digital transformation, zero trust has emerged as the ideal framework for securing enterprise users, workloads and devices in their highly distributed cloud and mobile-centric world.



And IT leaders globally are waking up to this, as zero trust moves into the mainstream — disrupting decades of legacy security and networking principles.

More than 90% of those IT leaders that have started their migration to the cloud have implemented, or are in the process of implementing, a zero trust security strategy

in the next year. That's according to the findings of our latest global survey, which sought insights from over 1,900 CIOs, CISOs, CDO, CTOs and Heads of Infrastructure, from organizations that have already begun migrating applications and services to the cloud.

This is good progress, and the reasons behind it show continued optimism for the implementation of a zero trust architecture beyond the next 12 months.

22%

With only 22% fully confident their organization is leveraging the complete potential of their cloud infrastructure, the results indicate a need to think beyond just security going forward

Indeed, as their cloud journeys continue, the security case for zero trust certainly appears clear. More than two-thirds (68%) of IT leaders either agree that secure cloud transformation is impossible with legacy network security infrastructure or that zero trust network access has clear advantages over traditional firewalls and VPNs when it comes to securing remote access to applications.

But with only 22% fully confident their organization is leveraging the complete potential of their cloud infrastructure, the results indicate a need to think

beyond just security going forward. When approached from a holistic IT perspective, zero trust has the potential to unlock a wealth of opportunities in an overall digitization process — yes, it can prevent large-scale cybersecurity attacks, but it can also do so much more, from driving greater innovation, to supporting better employee engagement or delivering tangible cost efficiencies.

As organizations grapple with providing a new class of modern workplace — hybrid in approach and reliant on a whole host of emerging

technologies such as IoT/OT, 5G and even the metaverse — they must broaden the lens through which they see both zero trust and digital transformation. A zero trust platform has the power to redesign business and organizational infrastructure requirements: to become a true business driver that not only enables companies to offer the hybrid working model that employees are demanding, but to become fully digitized organizations with all the benefits this entails, from agility and efficiency to future-proofed infrastructure.

We commissioned this research to uncover the state of zero trust transformation within organizations today. What we found is promising — implementation rates are strong. But the rationale behind implementation could be more ambitious. There is an incredible opportunity for IT leaders to educate business decision makers on zero trust and bring it to the table as a high-value business driver — it's the missing link helping businesses to empower and ready themselves for future technologies, today.

STATE OF ZERO TRUST

90% More than 90% of organizations that have started their migration to the cloud have implemented or are in the process of implementing a zero trust security strategy in the next 12 months

88% Globally, 88% of IT leaders have some level of confidence that their organization is leveraging the potential of cloud infrastructure, but only 22% are fully confident

REGIONALLY, FULL CONFIDENCE IN LEVERAGING CLOUD INFRASTRUCTURE'S POTENTIAL STAND AT:



#1 ZTNA is the #1 priority for zero trust technology investment over the next 12 months — indicating the importance of remote access for the hybrid workplace

68% More than two-thirds (68%) of IT leaders either agree that secure cloud transformation is impossible with legacy network security infrastructure or that zero trust network access (ZTNA) has clear advantages over traditional firewalls and VPNs when it comes to securing remote access to applications

54% of IT leaders indicated that they believed VPNs or perimeter firewalls are both ineffective at protecting against cyberattacks or providing visibility into application traffic and attacks

THE MAIN BARRIERS TO LEVERAGING THE FULL POTENTIAL OF THE CLOUD:

45% Challenges of securing data in the cloud and data privacy concerns

42% Network complexity and security hardware hard to scale

40% Third-party and remote access to IoT & OT

33% Inconsistent connectivity and poor remote access experience for users

SECURITY, ACCESS AND COMPLEXITY ASIDE, THE TOP REASONS FOR IMPLEMENTING A ZERO TRUST ARCHITECTURE DO NOT FEATURE STRATEGIC BUSINESS DRIVERS:

65% Improving the detection of advanced threats or web application attacks and broadening security for sensitive data

44% Securing remote access for vendors, partners and operational technology

27% Improving secure connectivity for a hybrid workforce

24% Reducing the cost and complexity of legacy network security

Section I

The cloud context behind zero trust adoption

When we refer to the “cloud” in this survey, we are talking about applications, data and workloads that are delivered as hosted services over the internet, instead of a local data center within a corporate network. Examples include Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or private applications built in or hosted in the cloud.

Before we dive into the specifics of zero trust, we wanted to set the context for its adoption — to examine what is happening in the broader IT landscape around it, and specifically where organizations are in their cloud journeys.

There is no doubt that the events of the past few years have accelerated the shift into the cloud.

In many organizations, the process is already well underway — if not already finished.

We interviewed over 1,900 CIOs, CISOs, CDO, CTOs and Heads of Infrastructure around the world from organizations that have already begun migrating applications and services to the cloud. Of those, almost half (46%) said the migration

process was 100% complete.

But while 88% of IT leaders have some level of confidence that they are making best use of their journey to the cloud, only 22% are completely confident their organization is leveraging the full potential of cloud infrastructure today.

RESPONDENTS VERY CONFIDENT THEIR ORGANIZATION IS LEVERAGING THE FULL POTENTIAL OF CLOUD INFRASTRUCTURE TODAY


22% Total

14% Europe

42% The Americas

24% APAC

% OF RESPONDENTS VERY CONFIDENT THEIR ORGANIZATION IS LEVERAGING THE FULL POTENTIAL OF CLOUD INFRASTRUCTURE TODAY

 Roll over the countries to see more detail.

Europe:

The Americas:

APAC:



Examining regional differences, European IT leaders show the most doubt in their cloud infrastructure use, with only 14% expressing total confidence. In the Americas, however, this number jumps to 42%.

While there is no clear single cause for this disparity, one potential reason may be the intercultural differences in the adoption speed of innovative technologies, where Europe traditionally takes a more careful approach and additionally puts more focus on data privacy. Additionally, with Europe's well established connectivity infrastructure and strong manufacturing focus, there is less drive towards immediately embracing innovations like 5G and it takes longer lead times to change established business processes. As we will explore further in a later section, organizations in the Americas have a higher focus on emerging technologies, such as Artificial Intelligence, Machine Learning and Augmented Reality, suggesting that there are already plans in place for cloud infrastructure to support more sophisticated use cases.


But more broadly, why were organizations struggling to unlock the full potential of the cloud?

On the surface, security appears as the top barrier, with IT leaders selecting two security-related reasons to lead their response to this question:

TOP BARRIERS TO EMBRACING THE FULL POTENTIAL OF THE CLOUD

- 45%** Data privacy concerns and challenges securing data in the cloud
- 42%** Network is highly complex to adapt and network security is hard to scale
- 40%** Challenges in enabling third-party access and remote access to IoT and OT systems
- 33%** Inconsistent connectivity and poor remote access experience for users

THE MAIN BARRIERS TO EMBRACING THE FULL POTENTIAL OF THE CLOUD, BY COUNTRY

 Roll over the countries to see more detail.

Across Europe and APAC, data privacy concerns dominate:

In the Americas, organizations are grappling with challenges around securing data in the cloud:

Meanwhile, Singapore and Japan, in particular, are struggling with scaling network security hardware:



In a cloud-based environment, the attack surface is increased exponentially, with every internet-facing service, user and device becoming a potential entry point, a vulnerable front door that needs to be secured against threats.


And organizations have good reason to be concerned. In a cloud-based environment, the attack surface is increased exponentially, with every internet-facing service, user and device becoming a potential entry point, a vulnerable front door that needs to be secured against threats. More on that to follow in our next section.

But a glance at the overall motivations behind cloud migrations points to a much more fundamental barrier in how IT leaders are viewing cloud — and one that is no doubt impacting its effective use. When asked about the main factors driving digital transformation projects in their organizations, three factors came out on top: reducing costs, facilitating tech innovation, and managing cyber risk.

TOP FACTORS DRIVING DIGITAL TRANSFORMATION PROJECTS ACCORDING TO GLOBAL IT LEADERS ARE:

-  Reducing **IT infrastructure** costs
-  Facilitating innovations like **5G and Edge Computing**
-  Mitigating **cyber security** risk
-  Managing **multi-cloud environments**
-  Improving ability to attract and retain **top talent**

THE TOP FACTORS DRIVING DIGITAL TRANSFORMATION PROJECTS BY COUNTRY

 Roll over the countries to see more detail.



All very practical — and all driven by IT. In fact, the high importance of reducing costs, while understandable in the current climate, indicates that there may still be a distinct lack of understanding

around the main benefits of the cloud. And this, in turn, could be impacting on the approach to and use of those technologies that are being brought in to support it. **Enter zero trust.**

There is no doubt that the events of the past few years have accelerated the shift into the cloud

Section II

Securing the case for zero trust

Zero trust is a holistic approach to securing modern organizations, based on least-privileged access and the principle that no user or application should be inherently trusted. It begins with the assumption that everything is hostile, and only establishes trust based upon the user identity and context, with policy serving as the gatekeeper every step of the way. In the United States, the National Institute of Standards and Technology (NIST) defines the underlying principle of a zero trust architecture as “no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).” It’s an overhaul of the old proverb, “Never trust. Always verify.”


With security, access and complexity bubbling to the top of IT leaders’ cloud concerns, it is unsurprising that more organizations are taking an interest in zero trust as a means to overcome these hurdles. The responses showed that organizations

are building a good base level understanding of the security advantages of zero trust against more traditional approaches in this new operating environment.

When asked about traditional network and security infrastructure,

54% of IT leaders indicated that they believed VPNs or perimeter firewalls are both ineffective at protecting against cyberattacks or providing visibility into application traffic and attacks. Another 68% either acknowledged that when it comes to

secure remote access to applications, zero trust network access (ZTNA) has clear advantages over traditional firewalls and VPNs, or that secure cloud transformation cannot be achieved with legacy network security infrastructure.

 Roll over the countries to see more detail.

Respondents who agree that secure cloud transformation is impossible with legacy network security infrastructure, and that zero trust network access has clear advantages over traditional firewalls and VPNs when it comes to securing remote access to applications

Respondents who agree that VPNs / perimeter firewalls are either ineffective at protecting against cyberattacks or provide poor visibility into application traffic and attacks:

Respondents who agree that in addition to security, IT teams need integrated tools to effectively analyze, troubleshoot, and resolve user experience issues:



90%

More than 90% of respondents that have started their migration to the cloud have implemented or are in the process of implementing a zero trust security strategy in the next 12 months.



Beyond this awareness, what proves to be most promising is that they are acting accordingly. More than 90% of respondents that have started their migration to the cloud have implemented or are in the process of implementing a zero trust security strategy in the next 12 months.

Italy and India lead the way when it comes to implementing a zero trust security strategy, with 97% of Italian organizations and 96% of Indian organizations confirming they either have one in place or are in the process of doing so.



Roll over the countries to see more detail.

Percentage of organizations that have zero trust security already in place, are currently rolling it out, or are in the strategic planning process to roll it out:



Zero trust is still seen predominantly as a siloed IT-centric (security) solution ... but zero trust could offer organizations so much more than this.


But unfortunately, having a zero trust security system in place, or having plans to roll one out, certainly does not indicate that it is being leveraged to its full potential as a business enabler.

In fact, the findings indicate that zero trust is still seen predominantly as a siloed IT-centric (security) solution, which means immediate security challenges are being addressed and tactical benefits are being achieved — but zero trust could offer organizations so much more than this.

TOP REASONS FOR IMPLEMENTING ZERO TRUST ARCHITECTURE

- 65%** Improving the detection of advanced threats or web application attacks and broadening security for sensitive data
- 44%** Securing remote access for vendors, partners and operational technology
- 27%** Improving secure connectivity for a hybrid workforce
- 24%** Reducing the cost and complexity of legacy network security

TOP REASON FOR IMPLEMENTING A ZERO TRUST INFRASTRUCTURE ACROSS THE WORLD:

 Roll over the countries to see more detail.

To improve detection of advanced threats:

To improve detection of web application attacks:

To broaden security to protect sensitive data:

To provide secure remote access for vendors, partners, contractors:



This approach to zero trust — using it for security purposes only at the beginning of a transformation journey — significantly limits its potential, at a time when so much is riding upon an organization's ability to digitize and innovate, at speed and at scale.

When properly understood and not seen as merely a technology or product, it allows companies to simplify their infrastructure, rethink how they are doing business and enables an organization's transformation into a fully digitized business. For instance, companies that have achieved zero trust would have a full and accurate

inventory of all their applications and everything they have within their organization. Based on this inventory, they are then able to make strategic decisions around how they can optimize processes, reduce costs, eliminate legacy hardware and improve efficiency.

But to achieve these strategic benefits, the message around zero trust must be able to breach the boardroom and become a part of the broader business strategy. Today, it's clear that there is still uncertainty and probably a skills gap around what zero trust means and its impact on the business. The urgent task at hand is to help business leaders, including

CIOs, to understand that the goal of zero trust is to introduce simplicity into the overall infrastructure by removing administration-intensive hardware so that it can more easily deliver the exact business outcomes an organization needs — all while maintaining top-level security.

Looking at the zero trust technologies that organizations are prioritizing for investment in the next twelve months, there is some evidence this understanding of the business benefits is evolving — but at a notably different pace across the regions globally and with plenty of scope for improvement.

TOP ZERO TRUST TECHNOLOGIES THAT ORGANIZATIONS ARE INVESTING IN

30%

Zero trust network access (ZTNA)

29%

Cloud firewall

27%

Data loss prevention (DLP)

REGIONAL POV: THE VOICE OF THE AMERICAS

Amit Chaudhry, Senior Director, Product Marketing



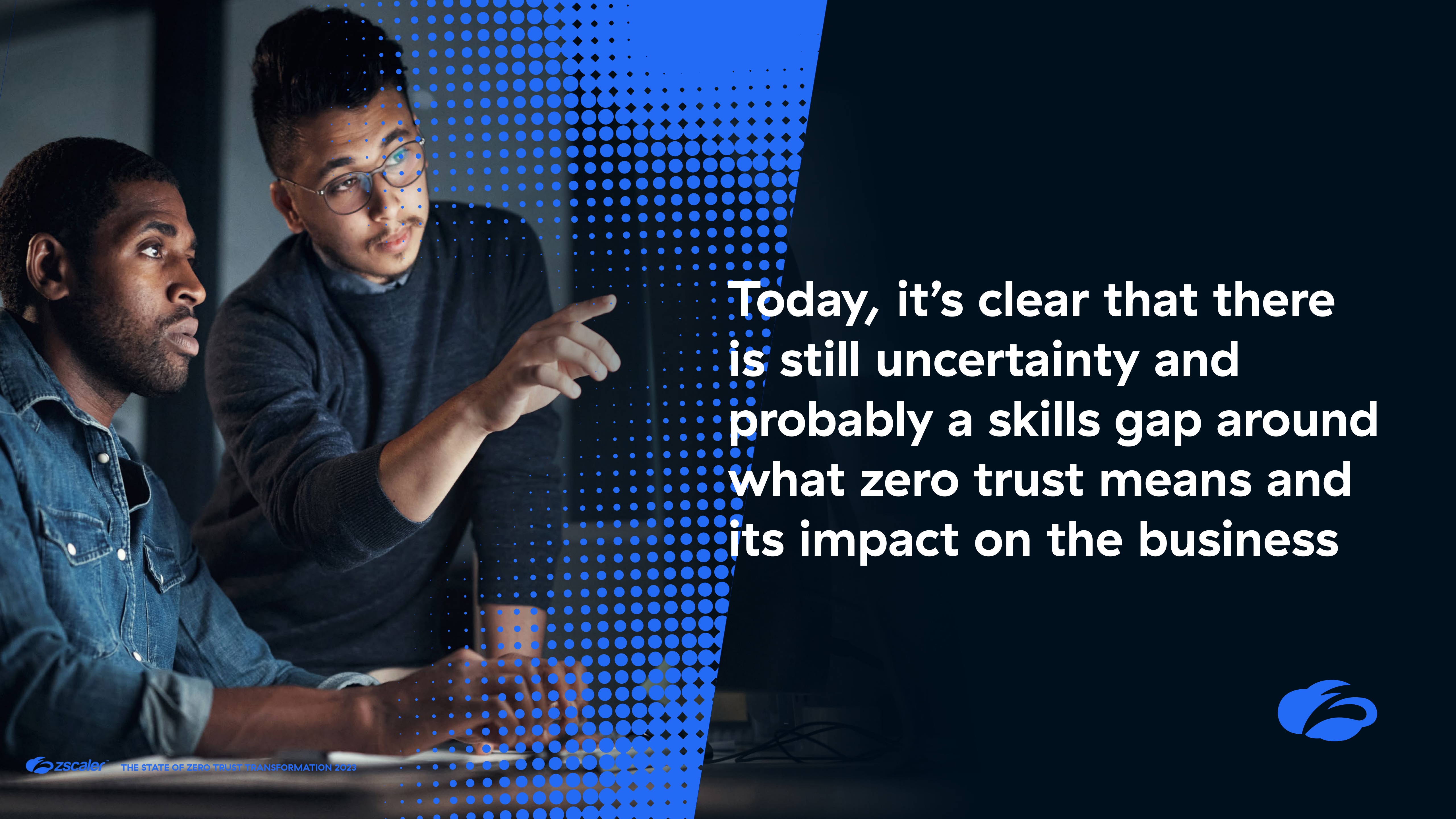
Organizations today are embracing cloud, mobility, AI, IOT, and OT technologies to make business more agile and competitive. Users are everywhere, and so is their data. But naturally, for fast and productive collaboration, they want direct access to apps from anywhere at any time.

This explosive pace of digital transformation has provided bad

actors with a window of opportunity to exploit decades-old network and security architectures. Attack numbers have become unparalleled, particularly ransomware and supply-chain attacks. And as these become more sophisticated, perimeter-based security using VPNs and firewalls is failing to secure the network and deliver a good user experience.

To realize the vision of a secure

hybrid workplace, organizations are rapidly moving away from firewalls and VPNs to zero trust architecture which secures fast and direct access to applications from anywhere at any time. Built on the principle of least privilege access where connection is made based on identity and context, zero trust is perhaps the simplest yet the most important idea relating to the way data is protected.

A photograph of two men in a meeting. The man on the left is a Black man with a beard, wearing a blue denim shirt, looking towards the right. The man on the right is an Asian man with glasses and a mustache, wearing a grey sweater, pointing his right hand towards a screen. The background is a dark blue wall with a pattern of small white dots. A large blue graphic element with a white dot pattern is on the right side of the image.

Today, it's clear that there is still uncertainty and probably a skills gap around what zero trust means and its impact on the business



Section III

Turning to zero trust to deliver hybrid ways of working

Hybrid work infrastructure refers to an infrastructure which enables employees to switch work environments seamlessly between physical and remote locations, without any limitations and administrative complexity.

When the first lockdowns sent organizations scrambling to set employees up from home, little did we know that this “temporary measure” would unlock the door to a whole new way of working and that, in fact, work itself would never be the same.

Instead, today’s workforce has options: work from home, the office or any

other location — and they (should) have the technology to make it happen.

Respondents predicted that in the next 12 months, their workforce will still be fully embracing the different options available to them, split between full-time office workers (38%), fully remote (35%) and hybrid (27%). These numbers are relatively consistent across the globe.

While nearly two-thirds (62%) of IT leaders say their organizations embrace the hybrid world or offer their staff the full flexibility to work remotely, the fact that over a third (38%) predict that they are going to be back in the office full-time is both surprising and worrying. While this may be understandable for certain

industries that rely on face-to-face interactions (such as healthcare and hospitality), in favourable market conditions, it could also lead many organizations to struggle to attract and retain talent if they are unable to offer the flexible working environment that employees have come to expect over the past few years.

19%

Globally, only 19% of the surveyed IT decision makers indicated that a hybrid work specific zero trust-based infrastructure is in place already.

PERCENTAGE OF WORKFORCE EXPECTED TO BE FULL-TIME REMOTE, FULL-TIME IN-OFFICE, OR HYBRID, OVER THE NEXT 12 MONTHS

38% Full time office workers

35% Fully Remote


27% Hybrid

Intent aside, whether their IT and security infrastructure is fully equipped to handle this evolving mix is another matter entirely. Globally, only 19% of the surveyed IT decision makers indicated that a hybrid work specific zero trust-based infrastructure is in place already, highlighting that organizations are not fully ready to handle this highly distributed

working environment on a broad scale. Next to those who have already updated their infrastructure, a further 50% are in the process of implementing or are planning a zero trust based hybrid strategy.

And amongst those implementing or planning to implement zero trust to provide secure remote access for vendors, partners,

contractors or factory and equipment operators — i.e., those by their nature working in a hybrid environment — there's a clear indication that zero trust network access is a priority investment area for the next 12 months. This suggests a high demand for meeting the immediate challenges of the ongoing shift to a hybrid working landscape.

 Roll over the countries to see more detail.

Implementing a zero trust based hybrid strategy is a priority in:

Meanwhile, the following countries are predominantly still in the planning stage:

Overall, the UK seems to be the most reluctant to adopt zero trust-based hybrid strategies, with 21% of organizations saying that they have currently no plans to implement a hybrid infrastructure, and further 20% preferring to stick with their traditional remote access technologies.



Naturally, security is a top concern for increasingly hybrid organizations.

TOP SECURITY CONCERNS FOR ORGANIZATIONS SHIFTING TO HYBRID WORK:


- 54%** both operational technology (OT) systems and internet access
- 53%** Private apps on premises or private apps and workloads in the cloud (on IaaS, PaaS)
- 32%** Internet of Things as well as Remote Access Internet access

But it's important to note that these results show that security in a hybrid working environment is not just about keeping threats out — it's also about how you can securely provide access to infrastructure to a wide range of users, from employees to third-party suppliers and business partners.

Building on this, despite the understandable focus on security, the reasons given by those implementing or planning a zero trust-based hybrid work infrastructure also begin to allude to the broader business impact of zero trust solutions, with implications for employee experience and productivity.

REASONS FOR IMPLEMENTING OR PLANNING TO IMPLEMENT A ZERO TRUST-BASED HYBRID WORK INFRASTRUCTURE

- 52%** Employees face inconsistent access experiences for on-premises and cloud-based applications and data
- 46%** Employees face productivity loss due to network access issues
- 39%** Employees are not able to access applications and data from personal devices

 Roll over the countries to see more detail.

Countries reporting a higher amount of inconsistent access experience were

In Europe, only around half of the responding organizations reported suffering from the same inconsistency, with

Productivity losses due to network access issues were cited as the dominant reason for changing to a new infrastructure in



Those respondents whose organizations are using traditional, VPN-based hybrid work infrastructure reported that they were still grappling with some more fundamental remote working issues.

User experience is vital for productivity in hybrid-work environments — that is one of the key learnings from the last year. And our results indicate that the regions have reacted with different speed when it comes to modernizing their infrastructure to address experience issues to date. To deliver optimum user experiences in today's increasingly dispersed enterprise environment, user traffic should be steered to the application via the shortest possible route to avoid latency

and congestion. Organizations must factor in the mobility of the modern hybrid employee, who must be dynamically routed to the required application from any location with optimized bandwidth, whether working from home, in the office or on the road. Experience aside, if an employee is unhappy with the performance of access to his business-critical applications, they might also seek ways to avoid security controls, further compounding the potential for negative impact.

In comparison, those respondents whose organizations are using traditional, VPN-based hybrid work infrastructure reported that they were still grappling with some more fundamental remote working issues. These include complexity in administering different security infrastructures for on premise and remote employees (47%), employees experiencing slow application performance (39%), and difficulty for IT in monitoring and troubleshooting user experience for remote users (37%).

While there remain many security concerns around a shift to hybrid work, responses like these reflect the much wider challenge that hybrid ways of working present organizations — one which incorporates access, experience and performance.

Zero trust — when understood correctly — provides an answer to all of these, delivering a simplicity which allows IT to focus its attention on responding to constantly changing expectations and business requirements.

REGIONAL POV: THE VOICE OF APAC

Heng Mok, CISO, APJ



Asia Pacific (APAC) is a great example of how “one size does not fit all.” A melting pot of cultures and lifestyle, each and every market in this region has a different approach to working. Even before the pandemic, we have observed significant differences, with markets like Japan and Singapore following a more hierarchical structure, while Australia and India had a more relaxed working model.

With the APAC region comprising some of the most locked down cities globally, these nuances are even more pronounced now as we emerge from lockdowns. Amongst the survey respondents, the majority of IT decision makers from Japan and Singapore expected their workforce to come into the office full-time, a stark contrast from those surveyed in Australia and India, who expected their workforce to be fully remote.

However, we do expect to see even more organizations doubling down on hybrid work models in the long run. Many organizations I have spoken with are opting for hybrid work practices to reap the intangible benefits of attracting and retaining talent. With heightened competition for the limited talent pool, it is unsurprising that many are incorporating similar policies and looking at technology stacks to support this transition much more seamlessly.



User experience is vital for productivity in hybrid-work environments — that is one of the key learnings from the last year.

Section IV

Taking a zero trust approach to integrating emerging technologies

Emerging technologies refer to new or rapidly developing technologies, whose practical applications are still largely unrealized, but are expected to have a significant impact on businesses and to drive competitive advantage.

Of course, digital solutions to enable remote working aren't the only technologies that organizations are trying to get their hands on. In today's digital age, operational technology plays an increasing role. This segment of an organization's business model, which historically has relied heavily on legacy systems and processes, will see a fundamental transformational shift towards new, emerging technologies,

each with its own set of exciting possibilities for further simplification and automation of business processes.

But organizations must think even further ahead, also taking into consideration additional upcoming technological advancements to future-proof infrastructure decisions. IT decision makers have to take ownership of the various directions in which the business can be heading, based on


innovations, and be open-minded about how emerging technologies can support their business functions in an effective way. Zero trust can be the missing link, helping businesses to empower and ready themselves for future technologies today.

In line with the motivations behind cloud migration and digital transformation in general, our results showed that a focus on wider strategic outcomes is

something that seems to be missing from how organizations are planning emerging technology projects.

When asked about the single most challenging aspect of implementing emerging technology projects, 30% said adequate security, followed by budget requirements for further digitization (23%). However, only 19% cited dependency on strategic business decisions as a challenge.

THE MOST CHALLENGING ASPECT OF IMPLEMENTING EMERGING TECHNOLOGY PROJECTS, BY REGION

 Roll over the countries to see more detail.

Security concerns posed the greatest challenge to the following countries

Meanwhile, the following countries are struggling predominantly with budget requirements:

A lack of vision seems to be the main thing standing in between organizations and emerging technologies

The only country where most companies identified a dependency on strategic business decisions as the biggest roadblock



While the budget concerns are predictable, the focus on securing the network while ignoring strategic business alignment is interesting. Organizations are focused on security without a full understanding of security's business benefit — further proof that zero trust is not yet understood as a business enabler. As they plan for emerging technology use cases like augmented reality, digital twins and virtual construction, low latency and high-performance application access also becomes a concern. This is especially true in the Americas, where interest in emerging technologies over the next three years is also particularly high.


RELEVANCY OF LOW LATENCY & HIGH-PERFORMANCE APPLICATION ACCESS IN THE NEXT THREE YEARS

55% Europe

79% The Americas

62% APAC

TOP PRIORITY TECHNOLOGIES BY 2025	GLOBAL	EUROPE	AMERICAS	APAC
Cloud-based access to operational technology and industrial control systems	34%	29%	40%	38%
Implementation of 5G technology for enhanced connectivity	32%	29%	39%	32%
Reducing carbon footprint of the business	29%	28%	28%	30%
Implementing Artificial Intelligence/Machine Learning projects	27%	22%	39%	28%

 Roll over the countries to see more detail.

Organizations focusing on cloud-based access to OT and industrial control:

Organizations prioritizing the implementation of 5G technologies:

Organizations who state that the reduction of carbon footprint is the #1 priority:

Only organizations in the Netherlands see the expansion of edge computing as most important (29%), while the US is focusing hard on implementing AI and ML projects (43%).



We can already start to see how these prioritized emerging technologies could ladder up to broader business outcomes. However, our results still suggest that there is a lack of wider vision within organizations. There needs to be a much more conscious alignment within the business on the competitive advantages to be gained through emerging technologies and their strategic deployment — which of course includes how they are secured.



REGIONAL POV: THE VOICE OF EMEA

Nathan Howe, VP of Emerging Technology

European organizations are less likely to be first movers with regards to the adaption of new or emerging technologies. Even if Europe has been the cradle of the industrial revolution with mechanical inventions, the region has been surpassed long ago with regards to digital technology adoption. APJ has become the center of gravity for technology around chip making and the knowledge to innovate brings people from across the globe together to develop transformational technologies in Silicon Valley.

Against this background, it is not surprising that Asia has recognized the power of 5G already to move beyond wireless into a next way of connectivity as foundation for digitization. While the Americas are somewhere in-between, Europe is still uncertain how to uplevel to 5G for their digitization efforts. However, Europe is ready to grow dramatically in digital cloud and emerging technologies as the shift of geo—political trends, like chip shortages and supply chain issues, requires countries to establish onshore centers of excellence in the region.

Section V

The road to unlocking the full potential of zero trust

Based on these findings, how should organizations approach their zero trust journeys?

The challenges caused by legacy network and security architectures are pervasive, long-standing and require a rethinking of how connectivity is granted in the modern world. This is where zero trust architecture must be leveraged — an architecture where no user or application is trusted by default. Zero trust is based on least-privileged access, which ensures that trust is only granted once identity and context are verified, and policy checks are enforced.

This approach treats all network communications as hostile, where communications between users and workloads, or among workloads themselves, are blocked until validated by identity-based policies. This ensures that inappropriate access and lateral movement are prevented. This validation carries across any network environment, where the network location of an entity is no longer a factor and not reliant on rigid network segmentation.

Zero trust began as a new way to protect networks. Eventually, it expanded beyond on-premises networks, but was still focused primarily on securing private application traffic. For too long traffic was considered based on its relationship to a network, rather than doing away with the network altogether. Today, organizations have to become aware of the full potential of zero trust to protect SaaS applications, traffic to and from public clouds, and even users as they access the public internet. And the originators of that traffic can be workloads, as well as users. Access can be made transport-agnostic, with traffic flowing via any router and coming over any network, wired or wireless, 4G or 5G, and future extensions.

It's past time to apply zero trust principles to all traffic, regardless of origin and regardless of destination. Now, it's time to stop thinking about what entity is connecting to what network, and instead use zero trust to connect all entities directly using business policies. In the age of the cloud, the internet is the new corporate network, and all traffic is fair game to connect the right entity to the right entity directly using business policies.

What steps can organizations begin taking today to ensure that they can transform into the secure, agile, flexible and efficient businesses they need to be to cope not only with today's macroeconomic environments, but with emerging technology requirements?

There are three key recommendations:

1

Organizations need to reconsider their understanding of zero trust looking at it as an enabler of secure digital transformation and a driver of business outcomes

With its increased levels of visibility and control, a zero trust-based architecture removes the complexity of modern IT and allows organizations to focus on getting the outcomes they need from their technology, from high performance and an enhanced user experience to reduced costs.

2

There is a need for further education to dispel fear, uncertainty and doubt around what zero trust means and its full impact on business

The CIO and CISO have a vital role to play here to bring the expanded message of zero trust to the boardroom, focusing on how it aligns with business strategy.

3

Emerging tech needs to be looked at as a competitive business advantage and zero trust-enabled infrastructures lay the foundation for the future today

The decision for what emerging technologies to pursue should be driven by the overall business vision and the organization's current and future needs, not trends or 'cool' factor. Zero trust is here to support the secure and performant connectivity requirements of emerging trends.

So, once the mindset has changed to acknowledge that zero trust is a true business enabler, how should organizations go about ensuring a zero trust architecture that successfully achieves these business outcomes?

Zscaler has implemented zero trust as a core architectural component of the Zero Trust Exchange, and it permeates through every element of the SSE framework. This includes a zero trust approach for users accessing any application (internal or external), IoT/OT connectivity, and workloads accessing resources in a multi-cloud environment or on the internet itself. The principles of Zero Trust allow secure hybrid work-from-anywhere as a business strategy, enabling employees, business partners, and customers to work from the location best suited for their productivity — a key requirement for business continuity, remote talent acquisition, and the delivery of increasingly popular hybrid working environments.

The Zscaler Zero Trust Exchange is a cloud-native service that provides employees, partners, and customers with fast, direct, and secure access to external and internal applications — regardless of location, device, or network.

It also incorporates the seven essential elements of zero trust architecture, which are grouped into the following three categories:



Verify

Zero trust architecture first terminates the connection and establishes

1. Who is connecting?
2. What is the access context?
3. Where is the connection going?



Control

Zero trust architecture then aims to:

4. Assess risk
5. Prevent compromise
6. Prevent data loss



Enforce

Before finally establishing a connection, zero trust architecture will:

7. Enforce policy

Keeping these elements in mind will be the foundation for cloud-first organizations to accelerate digital transformation, and to evolve into organizations which are ready for whatever the future brings.

About Zscaler and the Zscaler Zero Trust Exchange

Zscaler is universally recognized as the leader in zero trust, with the largest, easiest-to-use, and most mature zero trust platform.

The Zscaler Zero Trust Exchange, our cloud native platform, can be relied upon for your zero trust journey. Unlike legacy networking and security products, the Zero Trust Exchange is a purpose-built cloud platform. Its security starts with terminating each connecting, which allows for deep inspection of content and verification of access rights based on identity and context.

The Zero Trust Exchange operates across 150 data centers worldwide, ensuring that the service is close to your users, co-located with the cloud providers and applications they are accessing, such as Microsoft 365 and AWS. It guarantees the shortest path between your users and their destinations, providing comprehensive security and an amazing user experience.

You can learn more about our easy-to-use platform [here](#).

A man with a beard, wearing a high-visibility yellow jacket over a green shirt and climbing gear, is looking at a tablet. He is standing in a field of tall grass with wind turbines in the background. The image has a blue dotted pattern overlay on the right side.

The Zero Trust Exchange operates across 150 data centers worldwide

Methodology

ATOMIK Research surveyed 1,908 senior decision makers (CIOs / CISOs / CDOs / Head of Network Architecture) in EMEA (UK, Germany, France, The Netherlands, Sweden, Italy, Spain), AMS (USA, Mexico, Brazil) and APAC (Japan, India, Australia, Singapore). The research was conducted between 31 May and 28 June 2022. The sample comprised 43% of organizations of up to 4,999 employees, 32% of 5,000 up to 9,999 employees and 25% of 10,000 or more employees.