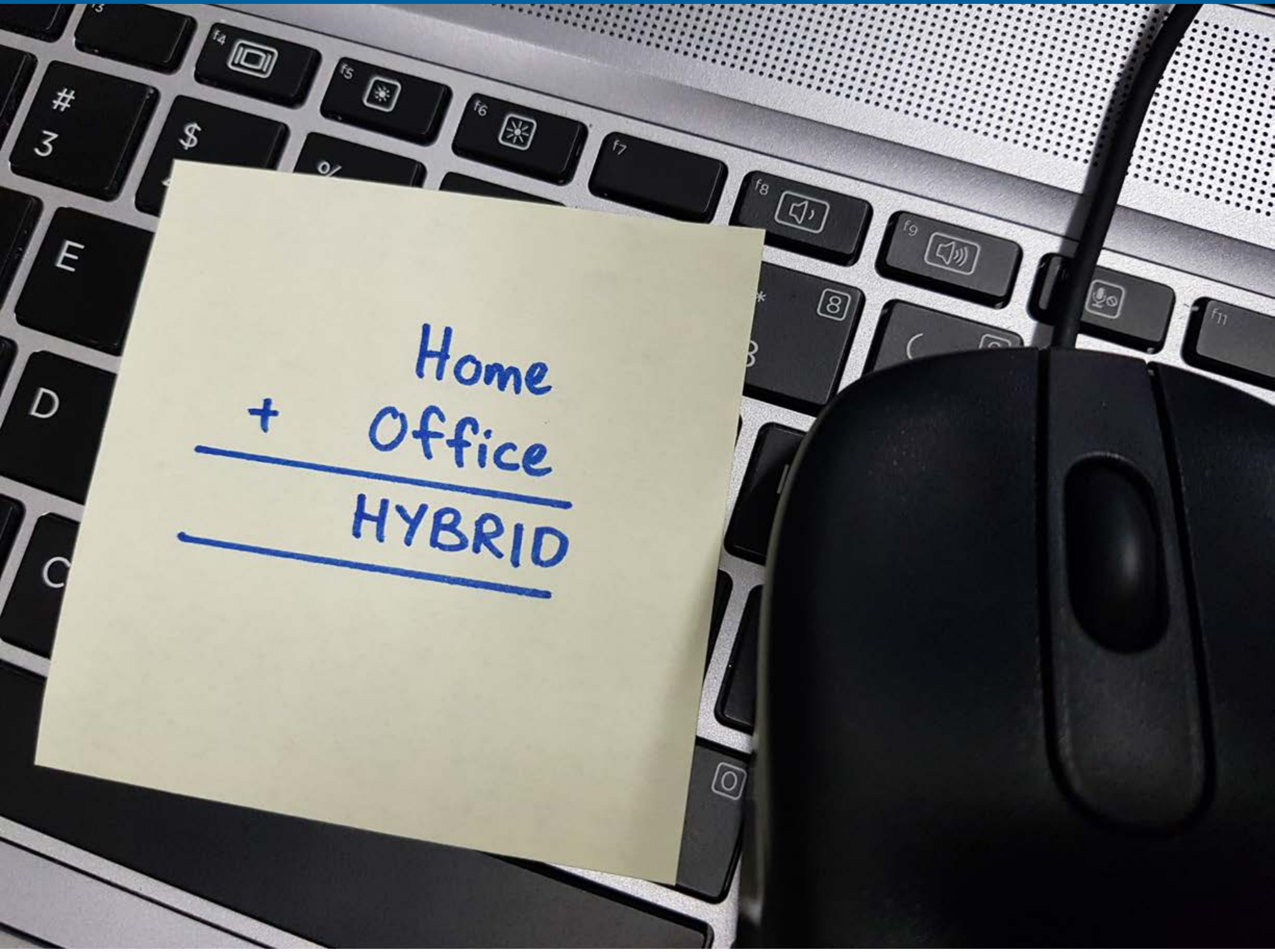
Safeguarding the Hybrid Workforce with a Zero Trust Approach

Discover how a zero trust methodology can more effectively protect the hybrid workplace



AN HMG STRATEGY RESEARCH REPORT POWERED BY ZSCALER

EXECUTIVE SUMMARY

When the world changed in March 2020, CISOs and information security teams found themselves facing a slew of new challenges. As millions of employees suddenly began working from home, any remaining notion of organizations having a defined perimeter to defend was put to rest.

As the global pandemic wore on and most enterprise teams continued to work remotely, it also became evident that existing network architectures were no longer sufficient for safeguarding employees and organizations across a highly distributed workplace. Meanwhile, application migration, shifting out of the data center and into the cloud and SaaS platforms, accelerated at an unprecedented rate - and continues to rise. A study conducted by O'Reilly Media reveals that 48% of organizations plan to migrate 50% or more of their applications to the cloud in 2022 [1].

Another layer to hybrid workforce challenges is the increased security concerns associated with unmanaged personal devices in a work-from-home setting. The continued reliance upon virtual private networks (VPNs) has left many organizations exposed.

These are just some of the reasons why the majority of CISOs and enterprise security leaders are adopting modern zero trust architectures to shore up their defenses and safeguard the organization from end to end.

"One of the primary strengths of a zero trust methodology is the ability to tailor your security controls to specific levels of risk and prioritization of each use case," said **Lisa Lorenzin**, Field CTO, Americas at Zscaler. *"With a modern zero trust solution, you can do that at the right layer of abstraction. You can put these controls inline for a user connecting to an application, rather than between an endpoint connecting to a network."*

As companies continue to expand their digital footprints and build upon their digital product and services portfolios, a zero trust architecture is needed to safeguard all layers of an organization's digital business model. **This helps explain why 61% of CISOs and enterprise security executives believe that a zero trust security model is an effective approach for securing an organization's digital ecosystem**, according to a recent survey of 118 security leaders conducted by HMG Strategy and Zscaler.

HMG Strategy has partnered with Zscaler to gain a deeper understanding of how the threat landscape has changed since companies shifted to hybrid workplaces, where these critical vulnerabilities exist, along with the benefits and opportunities of applying a zero trust architecture. In this in-depth research report, you'll discover:

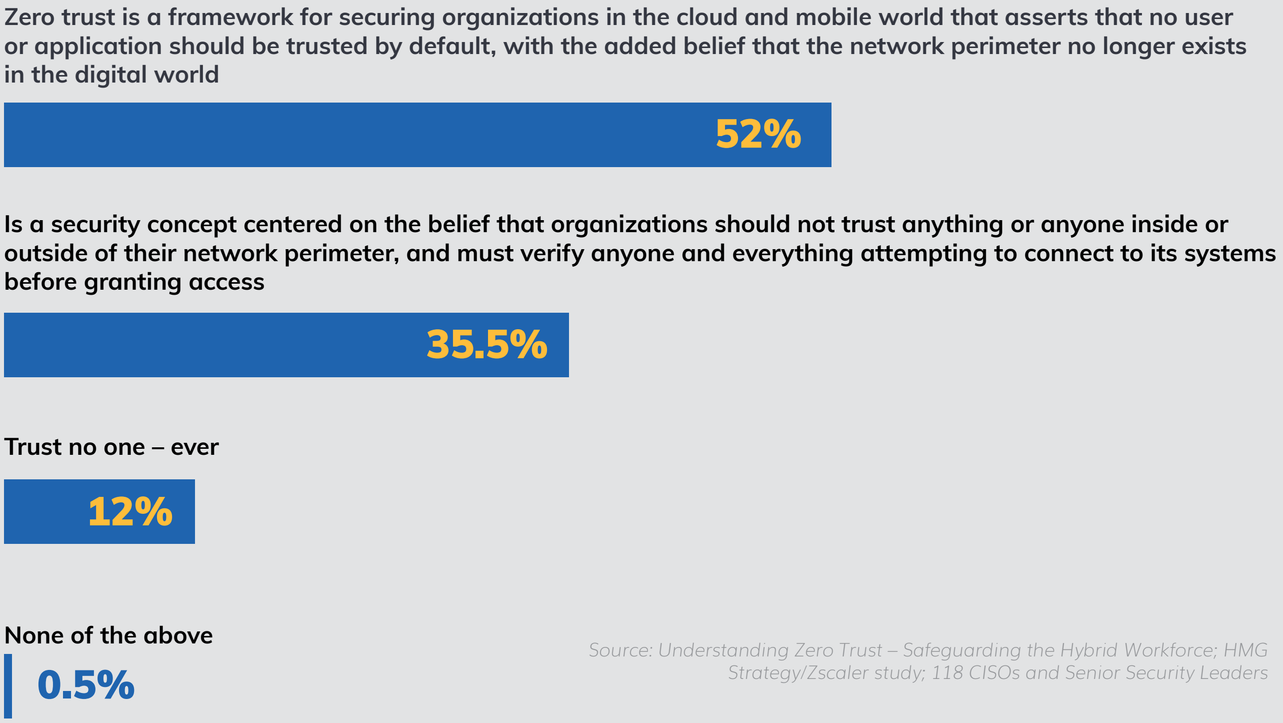
- The primary security risks and challenges associated with the hybrid work environment
- Why current architectures are inadequate for safeguarding the business, as well as the economic losses they generate
- Recent examples of ransomware attacks and network security breaches
- The urgency behind adopting a zero trust architecture
- Real-world examples of companies that are benefiting from the adoption of a zero trust security model
- Recommendations for implementing a zero trust architecture for a hybrid workforce

[1] *2021 Cloud Adoption Report, O'Reilly Media.*

Assessing What Zero Trust Really Is

Which of the following is an accurate definition of zero trust security models?

CHART 1:



Source: Understanding Zero Trust – Safeguarding the Hybrid Workforce; HMG Strategy/Zscaler study; 118 CISOs and Senior Security Leaders

Zero trust is a cybersecurity strategy wherein security policy is applied based on context established through least-privileged access controls and strict user authentication—not assumed trust. A well-tuned zero trust architecture leads to simpler network infrastructure, a better user experience, and improved cyberthreat defense.

> ***"One primary strength of a zero trust methodology is the ability to tailor your security controls to specific levels of risk and prioritizaton of each use case."***
>
> **LISA LORENZIN**
> *Field CTO, Americas*
> **Zscaler**

Tackling the Primary Security Challenges with the Hybrid Work Environment

Although remote work, along with the security challenges associated with unsecured home networks and unmanaged personal devices, has been prevalent for years, the dramatic shift undertaken by companies to a remote work environment beginning in March 2020 exponentially expanded each organization's digital footprint – along with associated vulnerabilities, including the attack surface.

Most employees don't know much about network security or the steps they need to safeguard themselves, as well as sensitive customer and proprietary data. Users simply connect to services through their corporate network firewalls and VPNs, thinking they are secure. But perimeter-based network security leaves them exposed.

On top of this, while some security teams conduct simulated phishing tests to help employees to better understand and recognize a phishing campaign, there's still a level of susceptibility which has left many organizations exposed. This helps explain why 72% of executives are concerned that VPNs may jeopardize IT's ability to keep their environments secure, according to Zscaler's 2021 VPN Risk Report.

VPN Vulnerabilities

The continued reliance on the use of VPNs to safeguard both employees and sensitive corporate data is leaving companies exposed on a number of fronts.

Lorenzin points to three fundamental shortcomings with VPNs:

1. Each VPN gateway has an inbound listener that makes it an exposed attack surface itself.
2. The VPN gateway then becomes a jumping off point for more sophisticated attacks by hackers.
3. The nature of a VPN is inherently open, which forces security teams to explicitly lock employees out of applications and systems they don't or shouldn't have access rights to.

The catastrophic 2021 Colonial Pipeline cyberattack was initiated via a legacy VPN that lacked multi-factor authentication for users. The attack was a classic example of lateral movement by a cybercriminal in an organization's network. Once the attacker stole a user's VPN credentials, they obtained access to Colonial Pipeline's network, moved laterally to access critical financial applications, stole sensitive data and demanded a ransom.

The attack temporarily shut down fuel delivery for most of the East Coast and southern U.S. and prompted the company to pay a $4.4 million ransom in Bitcoin.

Other companies hit by ransomware and other cyberattacks in the hybrid workplace include Brenntag, a German chemical distributor which also paid $4.4 million in Bitcoin ransomware – in this case, to the Darkside ransomware gang after it encrypted devices on Brenntag's North American network and stole unencrypted files.

While cybercriminals attack companies across all industries and sizes, Accenture estimates in 'The Cost of Cybercrime' report that 57% of all cyberattacks are wielded against businesses. According to another Accenture report - 'How Aligning Security and the Business Creates Cyber Resilience' - the average number of attacks per company jumped a whopping 31% in 2021 versus 2020. Meanwhile, the average cost per company of a data breach amounted to $3.86 million, including business downtime, ransomware payments, remediation, legal, and other costs.

Applying a Better, More Cost-Effective Approach

Fortunately, the adoption of a zero trust architecture can not only guard against costly breaches, it can also provide companies with reduced complexity, a better user experience, and data protection, all while eliminating the attack surface.

Sanmina, a leading integrated manufacturing solutions provider that serves the fast-growing segments of the global electronics manufacturing services market, is a prime example. Although the company had adopted zero trust principles and had begun to re-architect its systems during its ongoing cloud transformation to support advanced Industry 4.0 manufacturing practices, the company's security team quickly realized that it couldn't achieve zero trust using traditional VPN technology.

"We needed an access solution appropriate for a modern, perimeter-less world," said **Matt Ramberg**, Vice President of Information Security at Sanmina.

Like many enterprises, Sanmina's workforce of more than 35,000 was increasingly mobile and remote, particularly in the wake of COVID-19, making zero trust a priority.

"On any given day, we have several thousand people working remotely and they need to access tens of thousands of assets," Ramberg said. *"Using VPNs was an outdated practice that actually increased cybersecurity risks by creating attack surfaces."*

After evaluating multiple options, Sanmina decided to expand its Zscaler Zero Trust Exchange™ platform capabilities by adopting Zscaler Private Access™ (ZPA).

A fundamental building block of the Zero Trust Exchange, ZPA connects users and devices with applications, rather than connecting them to the network. Unlike firewalls and VPNs,[2] which create back doors allowing threats to enter, the Zero Trust Exchange makes users and applications invisible to external threats, while preventing lateral threat movement by enabling enterprises to limit user access, connecting them only to the applications they need and not putting them on the corporate network.

"We needed an access solution appropriate for a modern perimeter-less world."

MATT RAMBERG
Vice President of Information Security
Sanmina

[2] *The Top Five Risks of Perimeter Firewalls and the One Way to Overcome Them All - Zscaler*

Sanmina's decision to adopt Zero Trust Exchange has paid multiple dividends. Using Zero Trust Exchange, the company's cybersecurity team can granularly control and protect all traffic between users and applications – unlike VPNs – while protecting internal applications against security vulnerabilities.

Moreover, the returns on Sanmina's Zero Trust Exchange investments have quickly added up. Business users now receive faster, seamless access to both public and private applications compared to their use of firewalls and VPNs.

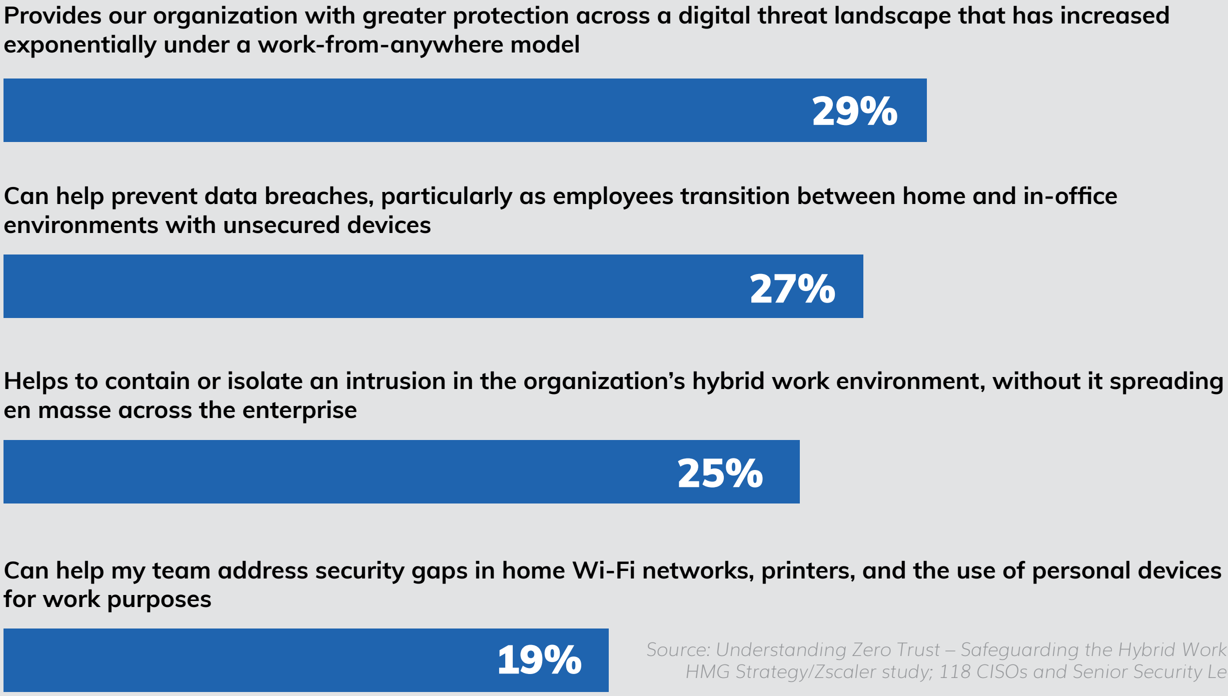
In addition, IT administration expenses are reduced compared with acquiring, configuring, managing, and updating traditional firewalls, VPNs, and web gateways. "*We had multiple physical appliances spread across the globe, each of them requiring their own configurations, rules, patches, updates, and maintenance contracts,*" Ramberg said.

Sanmina's adoption of a zero trust architecture has helped the manufacturer to safely expand its use of Industry 4.0 technologies, lower its IT administration costs, and expedite its M&A processes for greater agility – all while improving the user experience. In the next section of the report, we'll uncover the factors that are driving the urgency behind adopting this proven security methodology, along with examples of other top-tier companies that are benefiting from this transition.

Strengthening Security Via Zero Trust

What are the primary security benefits to applying a zero trust security model to a hybrid work environment?

CHART 2:



Source: Understanding Zero Trust – Safeguarding the Hybrid Workforce; HMG Strategy/Zscaler study; 118 CISOs and Senior Security Leaders

The greatest security benefit of applying a zero trust security model to a hybrid work environment as cited by CISOs and security leaders is the increased protection it provides across a digital threat landscape that has increased exponentially under a work-from-anywhere model.

The Urgency Behind Adopting a Zero Trust Model

As a growing volume of employees return to the office or divide their time between in-office and remote work environments, this has expanded the attack surface and is creating additional vulnerabilities across each company's digital footprint – and additional challenges for CISOs and security teams to address them.

With employees constantly transitioning between in-office and remote work environments with unsecured devices, this opens the door to a greater likelihood of data breaches and other types of cyberattacks being unleashed by cybercriminals and Nation-State actors. This is one of the primary reasons why security leaders who were surveyed in the HMG Strategy-Zscaler study say they are embracing a zero trust architecture.

"Regardless of whether I am in my home office, in a coffee shop, in a corporate office, on my laptop, or connecting in through cloud-based Desktop-as-a-Service, I still need the same access to resources – and I still definitely need the same protection for my outbound traffic," said Lorenzin. *"Zero trust is the best-suited approach because it allows you to have consistent centralized policy and visibility, rather than having to rely upon multiple disparate solutions that may be uncoordinated and lack visibility and control,"* she added.

Careem Safeguards its Global Remote-First Workforce Expansion

A zero trust security model became the obvious choice for **Careem**, the pre-eminent ride-hailing service provider in the Middle East.

When Careem was founded in 2012, it used a traditional castle-and-moat approach for IT security. But as the Dubai-based company has grown exponentially across the Middle East and North Africa with its remote-first workforce in recent years, executives there recognized that its legacy security model was impeding its high-velocity growth.

"With our business expected to quadruple, we realized our legacy security infrastructure was a considerable drain on our resources, preventing us from effectively recruiting workers and inhibiting us from achieving our business goals," explained **Peeyush Patel**, CIO and CISO at Careem. *"We needed to modernize our entire security approach."*

To support its cloud-driven app development model, remote-centric workforce, and explosive business growth trajectory, Careem decided to replace its traditional security infrastructure - including more than fifty firewalls and dozens of virtual private network (VPN) appliances - with a zero trust approach powered by the Zscaler Zero Trust Exchange platform.

"The Zero Trust Exchange platform was the clear choice for creating a zero trust Security Service Edge (SSE) model to protect our data, our employees, and our customers," said Patel.

To streamline and simplify its security infrastructure, Careem adopted multiple services within the Zero Trust Exchange. At the foundation, Careem deployed Zscaler Internet Access^{TM} (ZIA) for securing access to SaaS applications and the internet; Zscaler Private Access (ZPA) for securing access to Careem's private applications running on public cloud infrastructure and within its data center; and Zscaler Digital Experience (ZDX) for proactively detecting and resolving access issues before they affect users.

Within the platform, Careem also uses Cloud Access Security Broker (CASB) for safeguarding data-at-rest by looking inside SaaS applications and IaaS environments, and cloud Data Loss Prevention (DLP) for assisting with regulatory compliance when handling sensitive personal data in the cloud.

Once it deployed the Zero Trust Exchange, Careem immediately enjoyed agility, productivity, and resource benefits across its enterprise, starting with the elimination of network security-related frustrations and costs.

"*Our colleagues were very vocal in their dissatisfaction with VPN access,*" Patel said. "*Adopting the platform, including ZPA, not only eliminated those complaints, but the overall user experience vastly improved – with a corresponding 70% increase in our Net Promoter Score (NPS) among our colleagues and CSRs.*"

In addition, Careem realized considerable resource savings, which it has since reinvested into its development efforts. "*By simplifying access to engineering applications, we've regained approximately 20,000 development hours annually,*" Patel said. "*We've refocused those resources on creating business value.*"

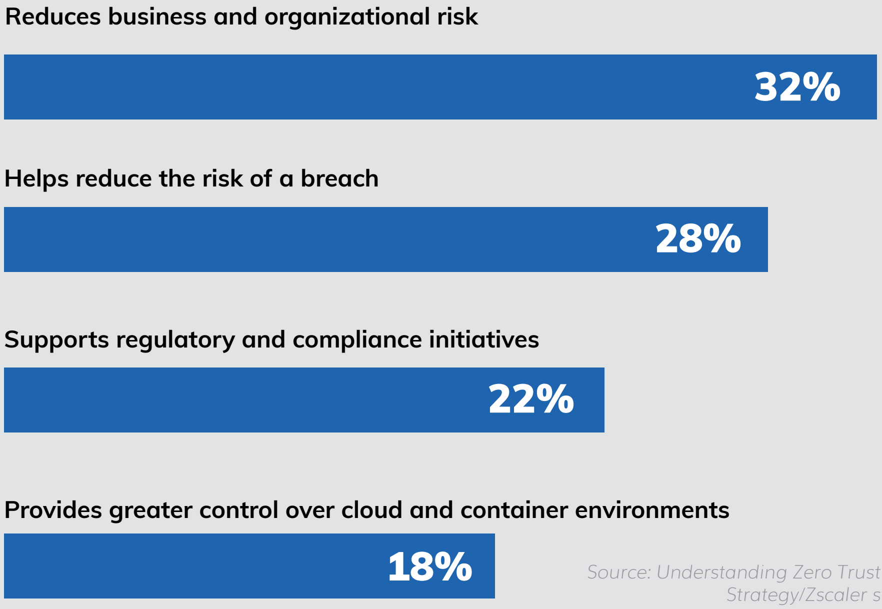
As Careem has experienced, a zero trust approach not only provides stronger controls and safeguards in its hybrid work environment, it also has provided greater agility, productivity, and cost savings. In the final section of the report, we'll share recommendations for deploying a zero trust architecture to better safeguard an enterprise hybrid workforce.

> ***"The Zero Trust Exchange platform was the clear choice for creating a zero trust Security Service Edge (SSE) model to protect our data, our employees, and our customers."***
>
> **PEEYUSH PATEL**
> *CIO and CISO*
> **Careem**

Zero Trust Benefits: Reduced Risk, Greater Control

What are the primary business and operational benefits of adopting a zero trust security model?

CHART 3:



Source: Understanding Zero Trust – Safeguarding the Hybrid Workforce; HMG Strategy/Zscaler study; 118 CISOs and Senior Security Leaders

THE BUSINESS AND OPERATIONAL BENEFITS OF A ZERO TRUST MODEL

The business and operational benefits that Sanmina, Careem and other companies have achieved through the adoption of a zero trust approach maps with the experiences Lorenzin has seen with other Zscaler clients.

“There are four primary benefits to utilizing a zero trust model,” said Lorenzin. “**Number one is flexibility and resilience.** This includes rapid deployment and the ability to quickly adjust to changes as your organization evolves.”

“Benefit number two is increased security,” said Lorenzin. “This includes the ability to remove the external attack surface; the means to reduce and potentially eliminate unauthorized lateral movement.”

Benefit number three is an improved user experience. This includes faster, easier, and more consistent access to applications.

The fourth primary benefit is cost reduction.

“You can eliminate the CapEx (capital expenditures) for not only the multiple VPN gateways deployed around the world but also the stacks of appliances and functions - load balancing, DMZ firewalls, DDoS protection - wrapped around those VPN gateways,” said Lorenzin.

The Four Benefits of a Zero Trust Architecture

1 Flexibility and Resilience

2 Increased Security

3 Improved User Experience

4 Reduced Costs

Starting Your Zero Trust Journey

For CISOs and security leaders who are just embarking on a zero trust journey, a good starting point is identifying a straightforward and simple use case where you can apply zero trust principles, determine the controls your organization already has in place, and then execute on that use case to demonstrate its merit.

"Find a use case that looks like good, low-hanging fruit. Give yourself permission to try something new. Don't tackle the hardest problem first," advised Lorenzin.

From there, security leaders can meet with the CEO and the Board to communicate what a zero trust architecture is and how it is designed to reduce risk, enable the business, and provide the company with greater flexibility and agility than traditional network-centric security approaches. This can include the use of analogies that help paint a picture of a zero trust approach to make the concept easier for non-technical board members to understand.

Security leaders can also share the successes achieved from the pilot project to demonstrate the value of a zero trust approach and to help obtain investment backing for a broader zero trust strategy.

It's also useful to gather feedback and insights from fellow practitioners regarding their own experiences with zero trust deployments. Popular forums for these types of connections include the CXO REvolutionaries Forum. These interactions can also provide recommendations for working with a trusted zero trust partner whose platform is best suited for addressing each prioritized use case while providing the organization with the ability to reach its strategic zero trust goals.

"Take advantage of the tribal knowledge that's out there among people who are further down this path," said Lorenzin.

As we've shared, adoption of a zero trust architecture is not only timely, it's vital for safeguarding the hybrid workforce and digital business. But without question, the rewards are well worth the undertaking.

About HMG Strategy

HMG Strategy is the world's leading digital platform for connecting technology executives to reimagine the enterprise and reshape the business world. Our regional and virtual CIO and CISO Executive Leadership Series, authored books and Digital Resource Center deliver unique, peer-driven research from CIOs, CISOs, CTOs and technology executives on leadership, innovation, transformation and career ascent.

The HMG Strategy global network consists of over 400,000 senior IT executives, industry experts and world-class thought leaders.

To learn more about the 7 Pillars of Trust for HMG Strategy's unique business model, click here.

HMG Strategy: Your #1 Trusted Digital Platform Connecting Technology Executives to Reimagine the Enterprise and Reshape the Business World.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.