Zscaler Study Finds 90% of Global Enterprises are Adopting Zero Trust, Yet Have Not Unlocked the Full Business Potential

December 6, 2022

- *More than 90% of organizations migrating to the cloud have implemented, are implementing, or are in the process to implement a zero trust architecture*
- *Only 22% of global IT decision-makers claim to be 'fully confident' their organization is leveraging the potential of their cloud infrastructure, presenting an opportunity for zero trust*
- *68% agree that secure cloud transformation is not possible with legacy network security infrastructures or that Zero Trust Network Access (ZTNA) has clear advantages over legacy firewalls and VPNs*
- *ZTNA is the top priority for zero trust investments over the next 12 months – indicating the importance of remote access for the hybrid workplace*

SAN JOSE, Calif, Dec. 06, 2022 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, found that more than 90% of IT leaders who have started their migration to the cloud have implemented, are implementing, or are planning to implement a zero trust security architecture. Supporting the mass migration to zero trust to secure users and the cloud, more than two thirds (68%) believe that secure cloud transformation is impossible with legacy network security infrastructures or that ZTNA has clear advantages over traditional firewalls and VPNs for remote access to applications. This is according to The State of Zero Trust Transformation 2023 report, which draws on a global study of over 1,900 senior IT decision makers at organizations globally, which have already started migrating applications and services to the cloud.

Zscaler's research shows that against a backdrop of rapid digital transformation, IT leaders believe zero trust – built on the principle that no user, device or application should be inherently trusted – is the ideal framework for securing enterprise users, workloads and IoT/OT environments in a highly distributed cloud and mobile-centric world. Approached from a holistic IT perspective, zero trust has the potential to unlock business opportunities across the overall digitization process, from driving increased innovation to supporting better employee engagement, or delivering tangible cost efficiencies.

The Leading Cloud Concerns

IT leaders identified security, access and complexity as top cloud concerns, creating a clear case for zero trust to overcome these hurdles. When asked about legacy network and security infrastructures, 54% indicated they believed VPNs or perimeter-based firewalls are both ineffective at protecting against cyberattacks or providing poor visibility into application traffic and attacks. This further validates the findings that 68% agree that secure cloud transformation is impossible with a legacy network security infrastructure or that ZTNA has clear advantages over traditional firewalls and VPNs for secure remote access to critical applications.

The Cloud Context – A Lack of Confidence

While progress on zero trust is strong, Zscaler found that globally only 22% of organizations are fully confident they are leveraging the full potential of their cloud infrastructure, so while organizations have made solid initial steps on their cloud journey, there is a massive opportunity to capitalize on the benefits of the cloud. Regionally, the results vary with 42% of organizations in the Americas feeling fully confident in the use of their cloud infrastructure, compared with 14% of organizations across EMEA and 24% in APAC. While India (55%) and Brazil (51%) are leading on a country level followed by the US (41%) and Mexico (36%), European and Asian countries are less confident: in Europe, Sweden (21%) and the UK (19%) are leading followed by Australia (17%), Japan (17%) and Singapore (16%). The remaining European countries are lagging behind: The Netherlands with 14%, Italy (12%), both France and Spain at 11% and Germany with 9%. This chasm between the most progressive country being more than six times the most laggering country shows varying confidence levels of the cloud by region and further presents an opportunity for education and closing the skills gap.

While at first glance security appears to stand in the way of fully realizing the full potential of the cloud, the motivations behind cloud migration suggest a more fundamental barrier in how IT leaders view the cloud. IT leaders cited data privacy concerns, challenges to securing data in the cloud, and the challenges of scaling network security as among the top barriers to embracing the cloud's full potential. However, when asked about the main factors driving digital transformation initiatives in their organizations, the top three factors were cost reduction, managing cyber risk, and facilitating emerging technologies like 5G and Edge computing, suggesting there may still be a distinct lack of understanding around how to fully capitalize on its broader business benefits.

Meeting the Hybrid Mix with Zero Trust

IT leaders surveyed in Zscaler's research predicted that in the next 12 months, their organizations' employee base will continue to be fully embracing the different work style options available to them, split between full-time office workers (38%), fully remote (35%) and hybrid (27%). However, it also found that organizations may still be unequipped to handle the ever-evolving mix of hybrid working requirements.

Globally, only 19% indicated that a hybrid work specific zero trust-based infrastructure is already in place, suggesting that organizations are not fully ready to handle the security of 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.

Employee user experience was mentioned as the top reasons for implementing a zero trust-based hybrid work infrastructure. More than half (52%)

agreed that implementation would help tackle inconsistent access experiences for on-premise and cloud-based applications and data, 46% that it would tackle productivity loss due to network access issues, and 39% that using zero trust would allow employees to access applications and data from personal devices. These views reflect the wider challenge beyond security that hybrid working presents around access, experience and performance, and the role zero trust plays in response.

The Potential of Zero Trust as a Business Enabler

In line with the motivations behind cloud migration, Zscaler found that a focus on wider strategic outcomes is missing from how organizations are planning emerging technology initiatives. Asked about the single most challenging aspect of implementing emerging technology projects, 30% cited adequate security, followed by budget requirements for further digitization (23%). However, only 19% cited dependency on strategic business decisions as a challenge.

While budget concerns are natural, the focus on securing the network while ignoring strategic business alignment suggests organizations are focused on security without a full understanding of its business benefit, and that zero trust itself is not yet understood as a business enabler.

"The state of zero trust transformation within organizations today is promising – implementation rates are strong," said Nathan Howe, VP of Emerging Tech, 5G at Zscaler. "But organizations could be more ambitious. There's an incredible opportunity for IT leaders to educate business decision-makers on zero trust as a high-value business driver, especially as they grapple with providing a new class of hybrid workplace or production environment and reliant on a range of emerging technologies, such as IoT and OT, 5G and even the metaverse. A zero trust platform has the power to redesign business and organizational infrastructure requirements: to become a true business driver that doesn't just enable the hybrid working model employees are demanding, but enables organizations to become fully digitized, benefiting from agility, efficiency and future-proofed infrastructure."

Zscaler makes four key recommendations for organizations to capitalize on zero trust:

1. **Not all zero trust offerings are created equal:** It's important to implement a true zero trust architecture built on the principle that no user or application is inherently trusted. It starts with validating user identity combined with business policy enforcement based on contextual data to provide users, devices and workloads direct access to applications and resources – never the corporate network. This eliminates the attack surface so threats can't gain access to the corporate network and move laterally thus improving the security posture.

2. **Zero trust as enabler of transformation and business outcomes:** With its increased levels of security, visibility and control, leverage holistic a zero trust-based architecture to remove the complexity from IT operations to allow organizations to focus on gaining improved business outcomes as part of their digital transformation initiatives and remain competitive.

3. **Zero trust for the boardroom:** To align with business strategies, CIOs and CISOs should leverage the findings to help dispel fear, uncertainty and doubt around what zero trust means and to promote its full business impact with key decision makers.

4. **Zero trust-enabled infrastructures as foundation for the future:** Emerging technologies need to be looked at as a competitive business advantage and zero trust will support the secure and performant connectivity requirements of emerging trends.

Additional Resources

To access the full The State of Zero Trust Transformation 2023 report, visit The State of Zero Trust Transformation 2023 report.

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.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so 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 SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Media Contact:
Natalia Wodecki
Global PR Director
press@zscaler.com