Zscaler Advances Zero Trust Security for the Digital Business Disrupting Decades of Legacy IT Security and Networking Models

April 20, 2021

Security Innovations, Resources for CxOs and IT Practitioners, and Zero Trust Deployment Programs Overcome Security Barriers to Accelerate Digital Transformation

SAN JOSE, Calif., April 20, 2021 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced innovations for the Zscaler Zero Trust Exchange™ platform and new programs designed to secure digital businesses. New security solutions, resources for IT execs and practitioners, and deployment guides to expedite zero trust adoption are redefining the rules of IT security for today's internet-driven, cloud-first businesses. The combination of these offerings provides digital businesses a holistic approach to securing modern organizations and the pragmatic skills and blueprints needed to be competitive.

Digital transformation has fundamentally changed the way modern businesses innovate and operate. This seismic shift has been accelerated by enterprises' move to cloud-based SaaS models and the internet becoming the new corporate network -- shattering 30 years of IT networking and security principles. While direct-to-internet connectivity for access to cloud applications and workloads has democratized information flow and improved business agility, it has also destroyed the castle-and-moat security architecture exposing businesses to new threat vectors resulting in more large-scale security breaches.

Zero trust starts with validating user identity combined with business policy enforcement based on contextual data from user, device, app and content to deliver authorized direct access to applications and resources. This means that no entity (user or application) is inherently trusted. Built on three fundamental tenets, the Zscaler Zero Trust Exchange makes the cloud safe by securely connecting the right users to the right applications.

1. **Connect users and applications to resources**, not the corporate network, preventing lateral movement of threats, thus reducing security and business risk.

2. Make **applications invisible** to the internet. Applications protected behind the Zero Trust Exchange are not visible and cannot be discovered, thus eliminating the attack surface.

3. Use a **proxy architecture**, not a passthrough firewall, for content inspection and security. The only way to ensure effective cyber threat defense and data protection is by requiring content inspection, including encrypted traffic, and policy enforcement, before it reaches its intended destination.

Platform: New Security Solutions to Take Advantage of the Most Advanced Zero Trust Platform
Studies show that 77% of IT security teams believe they will move to a hybrid working model[1] resulting in the need for new and advanced security requirements. The introduction of three innovations for the Zero Trust Exchange platform helps IT security teams bring zero trust security to every digital business, strengthens safe web access, and dramatically simplifies the adoption of zero trust policies.

- **Extending Cloud-Native Zero Trust On-Premises** – The new **Zscaler ZPA ™Private Service Edge** software makes ZPA the only cloud-native solution that spans both cloud and on-premises environments. Hosted by the customer but managed by Zscaler, it securely brokers users to private applications and removes the need for on-premises network segmentation. This makes ZPA Private Service Edge ideal for on-premises environments and locations subject to internet access challenges by providing local brokering between on-premises users and latency-sensitive applications, resulting in greater performance for users, less complexity for network admins, and less risk for business data. ZPA Private Service Edge is generally available today.

- **Mitigating Web-based Attacks and Data Leakage** – A majority of external attacks target users through their web browsers, making browsers a large surface area for threats. Zscaler's new, natively integrated **Cloud Browser Isolation** solution creates an isolated browsing session that enables users to access any webpage on the internet without allowing sensitive data to flow down to the local device or the corporate network. Users do not directly access active web content, preventing the delivery of malicious code. Cloud Browser Isolation allows customers to offer a safer web experience while helping ensure sophisticated attacks, ransomware, or data exfiltration will not impact endpoints or targeted users.

- **Simplifying Security Policies Through Automation –** New APIs automatically create policies for newly discovered services and revokes user access based on time settings. Machine learning (ML) enhancements allow for auto-segmentation of application workloads. These innovations speed up the time it takes to set policies and simplifies micro-segmentation - freeing up time to focus on other vital projects.

People: Elevating the Role of IT Executives and Delivering Advanced Skills for Security Practitioners

- **Elevating the Role of IT Executives** – The newly formed **REvolutionaries** forum is an online CXO community for IT leaders to learn techniques for advancing their zero trust strategy, engage in executive-only events, and evaluate the maturity of their digital transformation journey.

- **Offering Advanced Skills Training for Security Practitioners** – To train IT practitioners on best practices for using zero trust services, Zscaler has formed the **Zero Trust Academy**, a certification training program focused on securing access to private apps, SaaS apps, and the internet with Zscaler solutions.

Process: Validated Designs and Blueprints to Facilitate Zero Trust Deployments

- **Building a Programmatic Path to Zero Trust** - **Zscaler's Zero Trust Ecosystem** of technology partners have made it easier for IT practitioners to modernize their legacy security models. New joint validated designs provide the blueprints with prescriptive guidance for security architects to simplify rapid deployments of zero trust security architectures. Visit the Zscaler Zero Trust Ecosystem to access resources from global partners and market leaders, such as CrowdStrike, IBM Security, Microsoft, Okta, Ping Identity, SailPoint, SentinelOne, Splunk, and VMware CarbonBlack across identity management, endpoint security, and security operations.

"The accelerated adoption of digital transformation compounded with more employees working from anywhere has opened the floodgates to targeted cyber attacks. Security teams face challenges everyday posed by managed and unmanaged endpoints and identities, streams of unfiltered data, and the complexity of managing user access to critical business applications," said Amol Kulkarni, chief product officer at CrowdStrike. "CrowdStrike's Zero Trust Assessment provides continuous, real-time security device posture assessments and Zscaler's frictionless integration with ZTA provides an identity and data-centric approach for dynamic conditional access to applications. The integration delivers customers a holistic zero trust solution that encompasses data, people, devices, workloads and networks."

"As enterprises continue to adopt a cloud-first strategy, a cloud-native zero trust security model has become a necessity," said Sendur Sellakumar, CPO and SVP of Cloud, Splunk. "Splunk and Zscaler have jointly developed design guides and robust product integrations to help IT security teams prevent and detect attacks, dynamically control policy and risk, and accelerate threat response in alignment with zero trust best practices."

A complete list of quotes from our supporting partners can be found at https://www.zscaler.com/partners/technology/zero-trust-quotes.

Industry Analyst Quote
"Thanks to cloud and mobility, our infrastructure, applications and data are everywhere, and as a result of the growing work-from-home (WFH) phenomenon, users are now more scattered than ever," said Eric Hanselman, Principal Research Analyst, 451 Research, part of S&P Global Market Intelligence. "Perimeter-based controls are thus quickly becoming obsolete, making the zero trust approach of using a cloud-native architecture to disperse security controls for performance and scale the more appealing way to protect businesses.[2]"

Additional Information

- ESG Research Report: The State of Zero-trust Security Strategies - https://www.esg-global.com/research/esg-research-report-the-state-of-zero-trust-security-strategies

To learn more about this announcement see https://www.zscaler.com/zero-trust-moment.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange platform 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 in-line cloud security platform.

Zscaler™ and the other trademarks listed at https://www.zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

Media Contact:
Natalia Wodecki
press@zscaler.com

[1] *2021 VPN Risk Report*, Cybersecurity Insiders, https://info.zscaler.com/resources-industry-reports-vpn-risk-report-cybersecurity-insiders
[2] 451 Research, part of S&P Global Market Intelligence, *2021 Trends in Information Security*, December, 2020