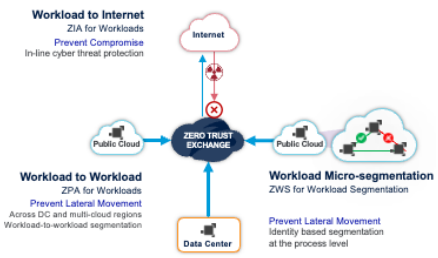
# Zscaler Extends its Proven Zero Trust Exchange Platform to Deliver Zero Trust for Workloads

December 8, 2021

**Advancements to the Zscaler Zero Trust Exchange Help Organizations Protect Workloads in Multi-Cloud Environments While Simplifying Connectivity and Boosting Application Performance**

SAN JOSE, Calif., Dec. 08, 2021 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), a leader in cloud security, announced the general availability of its new Workload Communications solution, part of the Zscaler Zero Trust Exchange™, which extends Zero Trust security to workloads and applications hosted in public clouds. Zscaler's cloud-native platform eliminates attack surfaces, prevents lateral threat movement, inhibits compromise of workloads, and stops data loss. It also helps IT teams simplify multi-cloud workload connectivity by moving away from traditional IP-based routing and VPNs between cloud environments to expedite enterprises' cloud transformation initiatives.

**Zero Trust Workload Communication**




Zscaler's new Workload Communications solution, part of the Zscaler Zero Trust Exchange, extends Zero Trust security to workloads and applications hosted in public clouds. Zscaler's cloud-native platform eliminates attack surfaces, prevents lateral threat movement, inhibits compromise of workloads, and stops data loss. It also helps IT teams simplify multi-cloud workload connectivity by moving away from traditional IP-based routing and VPNs between cloud environments to expedite enterprises' cloud transform

With the deployment of enterprise workloads in multiple regions and cloud providers, legacy mesh networks are becoming costly, hard to implement, scale, and manage. Attempts by legacy vendors to adapt antiquated, castle-and-moat VPN and firewall architectures to the public cloud have allowed an unprecedented number of cybersecurity attacks, in addition to networking and application performance challenges for enterprises. As a result, organizations must rethink their approach to securing and connecting cloud-based applications and consider adopting new architecture able to simplify multi-cloud connectivity, elevate application performance, and provide comprehensive protection. Recent findings from the Zscaler ThreatLabZ research team underscore these challenges and outline the growing threat from unsecured workloads in the cloud and the need for inspection of all content including encrypted traffic.

To meet these needs, Zscaler has extended its Zero Trust Exchange to deliver the industry's first Zero Trust for cloud workloads solution that secures cloud-to-internet, cloud-to-cloud, cloud-to-data center, and intra-cloud communications. Acting as an intelligent switchboard, traffic is routed to the Zscaler platform where connections are brokered using business policies based on identity and context to connect workloads directly to other workloads, without accessing the corporate network. Zscaler's approach eliminates the attack surface by making workloads invisible to the internet, simplifies application connectivity by removing networking bottlenecks, and delivers superior application performance by reducing app-to-app latency. Collaborating with major cloud providers, such as Amazon Web Service (AWS), Zscaler delivers a network-agnostic Zero Trust fabric to secure cloud workloads and accelerate migration to the cloud.

Today's general availability of Workload Communications extends the proven capabilities of the Zscaler Internet Access™ (ZIA™) and Zscaler Private Access™ (ZPA™) services to cloud workloads, allowing enterprises to secure all workload communications over any network, including internet, direct connect, express route and others. With these innovations, Zscaler enables customers to implement the following use cases:

- **Application-to-Internet Communications** – Cloud Applications require access to the internet for a variety of reasons, from communicating with third-party Application Programming Interface (API) services to receiving software updates. Using the Zero Trust Exchange, internet access is secured with ZIA policies that now include DLP and threat prevention while making workloads completely invisible to potential cyberthreats.

- **Multi-Cloud Application-to-Application Communications** - Multi-cloud networking allows organizations to secure connectivity across heterogeneous cloud environments. ZPA policies secure workload communications across cloud providers, regions, and virtual private clouds (VPCs) in the same public cloud for seamless and secure application communication without the complexities and performance bottlenecks that legacy technologies create.

- **Intra-Cloud Application-to-Application Communications** – To enable secure workload-to-workload communications inside a cloud, VPC/VNet, or data center, Zscaler uses a combination of macro and micro-segmentation to verify software identity. This includes microsegmentation of business-critical environments to prevent unauthorized communication between applications.

"To properly secure cloud workloads, three critical areas – security, connectivity, and performance – need to be addressed, which legacy approaches have not been able to solve," said Amit Sinha, President, CTO, Zscaler. "Zscaler has solved all three challenges with a new architecture that extends our Zero Trust Exchange, already trusted by thousands of enterprises to secure millions of users, to cloud workloads for stronger security, simpler connectivity, and better performance. Zscaler's new architecture eliminates the need for organizations to extend their corporate network to the cloud, which results in a bigger attack surface, operational complexity and performance bottlenecks."

**Customer and Partner Quotes:**

"As we move more applications to the public cloud, we must ensure a high level of compliance with internal and external requirements, avoid security

risks from inconsistently applied controls, and reduce legacy infrastructure costs," said Rui Cabeço, IT Service Group Manager & Global Outbound Connectivity Lead at Siemens. "With Zscaler's Workload Communications, we can easily standardize security policies for both users and applications regardless of where they are located. We gain visibility into the public cloud, achieve compliance, and lower costs by not backhauling traffic, and simultaneously reduce data center resource consumption."

"While we share the responsibility of cloud security with our enterprise customers, we are customer obsessed in helping our customers accelerate secure workload migration to AWS to achieve scalability and agility," said Mona Chadha, Director of Category Management, AWS. "Zscaler provides customers with a Zero Trust security model that simplifies cloud networking and security while eliminating the need for virtual firewalls and mesh or site-to-site networks. Having Zscaler solutions available in AWS Marketplace allows customers to easily subscribe, accelerate time to market while meeting compliance and security requirements."

**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 SASE-based Zero Trust Exchange is one of the world's largest in-line cloud security platforms.



**Media Relations Contact:**
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/5abb33a2-92f0-4f2f-a512-e5fc04445084