Zscaler Announces Industry-First Zero Trust Innovations to Secure Workloads and Cloud VDI

November 8, 2023

Native AWS Workload Tagging integration to provide segmentation granularity by policy, Multi-Session VDI Security and Expanded Cloud Coverage Further Simplify and Expand Zero Trust Security for Cloud Workloads

SAN JOSE, Calif., Nov. 08, 2023 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced advancements to the Zero Trust Exchange™ platform to radically simplify and improve cloud workload security by eliminating lateral movement, reducing operational cost and complexity, and ensuring consistent threat and data protection. Zscaler now uniquely offers native integration with AWS user-defined tags to allow granular Zero Trust VPC segmentation, all ports and protocols inspection for cloud-based VDI and expansion to GovCloud and China regional public clouds.

Public cloud adoption enables digital transformation at scale, driving a massive influx in cloud-based workloads hosting sensitive communications and data with SaaS applications or workloads in multiple public clouds or data centers. As a result, securing these mission-critical workloads is vital for enterprises to ensure their continued success and protect sensitive data. An IDG report states that 35%[1] of customers struggle with increased costs in cloud management and cloud security. Securing cloud workloads without sacrificing protections, expanding the attack surface, increasing operational overhead or degrading performance is a major challenge for organizations embarking on their digital transformation initiatives.

“As a leader in the global energy industry, NOV is leveraging the public cloud to enable our customers to safely produce abundant energy while minimizing environmental impact. Securing our applications and workloads deployed in the public cloud is a paramount priority for us,” said Patricia Gonzalez-Clark, VP of IT Services at NOV. “Using Zscaler technologies, we have transformed and modernized our network and security stack and have benefited immensely from reduced complexity in our environment. Now, we continue our journey with Zscaler by selecting their technologies to secure our workloads across our multi-cloud environments to transform security in the cloud.”

New advancements in Zscaler Workload Communications remove operational complexity, increase security and expand cloud coverage:

- **Workload Segmentation using User-Defined Tags:** On AWS, Zscaler uniquely enables creating custom security groups based on user-defined tags and native attributes. Supporting the AWS maximum tag limit, organizations can leverage their existing workload identities for VPC or network segmentation within the public cloud and eliminate the operational complexity involved in managing security policies based on IP Addresses, FQDNs, and CIDR blocks.
- **Real Time Resource Discovery:** Enabling custom-groups, Zscaler's native integration with AWS automatically discovers VPCs, subnets, and EC2 resources, including their associated tags and attributes in real-time. Enterprises can now effortlessly integrate security definitions based on cloud attributes, eliminating the need for manual configurations.
- **Multi-Session VDI Security:** An industry first, Zscaler inspects all ports and protocols for multi-session, non-persistent VDI deployments in the public cloud. Enterprises can now apply granular threat and data protection policies per individual user session, enabling enterprises to maintain common security policies across all environments.
- **Expanded Cloud Coverage:** Workload Communications now supports Google Cloud Platform (GCP), plus Azure China Regions and AWS GovCloud with FedRAMP certification. With AWS, Azure, and now expanded cloud support, enterprises can secure their cloud workloads consistently and effectively while maintaining the flexibility of public cloud choice.

“As customers accelerate the adoption of public cloud infrastructure they require a simple and effective cloud security platform to protect their cloud workloads and applications. Legacy architectures built with virtual network and security appliances, or backhauling traffic to data centers, fail to deliver consistent cyber defense and add operational complexity and cost,” said Dhawal Sharma, Senior Vice President and General Manager, Zscaler. “These new innovations radically simplify cloud workload connectivity and deliver cyber security including TLS inspection, data protection, and segmentation at cloud scale and cloud speed. Customers can use the Zscaler Zero Trust Exchange platform to connect and protect workloads across Multi-cloud, Hybrid and private cloud, Government Cloud, and Specialist Availability Regions such as China.”

For a deeper dive into the new innovations please read this blog, New Zero Trust Innovations Radically Simplify Cloud Workload Security.

Forward-Looking Statements
This press release contains forward-looking statements that are based on our management's beliefs and assumptions and on information currently available to our management. These forward-looking statements include the potential impact of platform developments, ability to scale and potential cost savings. These forward-looking statements are subject to the safe harbor provisions created by the Private Securities Litigation Reform Act of 1995. A significant number of factors could cause actual results to differ materially from statements made in this press release.

Additional risks and uncertainties are set forth in our most recent Annual Report on Form 10-Q filed with the Securities and Exchange Commission (“SEC”) on March 8, 2023, which is available on our website at ir.zscaler.com and on the SEC's website at www.sec.gov. Any forward-looking statements in this release are based on the limited information currently available to Zscaler as of the date hereof, which is subject to change, and Zscaler will not necessarily update the information, even if new information becomes available in the future.

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 SSE-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.

Source 1 : 2023 Cloud Computing Study report by IDG

Media Contact:
Natalia Wodecki
press@zscaler.com

Investor Relations Contact:
Bill Choi, CFA
ir@zscaler.com