Zscaler Introduces Innovations in Intelligent Segmentation to Extend Zero Trust to Branches, Factories and Clouds

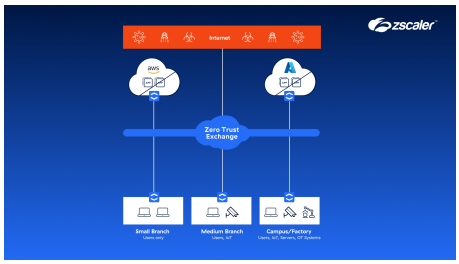
November 12, 2024

New Solution Prevents Lateral Movement from Ransomware Attacks, Cutting Firewall and Infrastructure Spend in Half

SAN JOSE, Calif., Nov. 12, 2024 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced the industry's first Zero Trust Segmentation solution to provide a more secure, agile and cost-effective means to connect users, devices, and workloads across and within globally distributed branches, factories, campuses, data centers, and public clouds.

While traditional networks, including SD-WAN and site-to-site VPN, have extended enterprise connectivity to branches and clouds, they have also inadvertently accelerated the spread of ransomware. Although firewalls are used to do segmentation on networks, they add complexity, increase costs, and fail to provide adequate security. Zero Trust Segmentation for branch and cloud is an innovative solution that prevents ransomware attacks, turns branches into simplified café-like environments and in the process eliminates the need for firewalls, network access control (NAC), SD-WAN and site-to-site VPNs.

Zscaler Zero Trust Segmentation Zolution



Zero Trust Segmentation Solution

With a Zero Trust architecture, organizations are no longer required to extend the corporate network from the data center to distributed locations and public clouds. Each branch, factory and public cloud becomes a virtual island that communicates directly with the Zscaler cloud security platform over any broadband connection. The Zscaler Zero Trust Exchange™ platform then applies business policies to securely connect users, workloads and devices. As a result, Zscaler minimizes the attack surface associated with public IPs, prevents ransomware from spreading between locations, and eliminates firewalls, SD-WAN and the reliance on Direct Connect and ExpressRoute.

"Traditional network and security architectures enable the spread of ransomware," said Dhawal Sharma, EVP of Product Management at Zscaler. "Using firewalls to segment business networks is extremely complex, turning into a never-ending initiative for many organizations. Integrating advanced technology from the recent AirGap acquisition, Zscaler Zero Trust Segmentation now offers the most advanced, robust protection against ransomware attacks, which can be implemented in days. Additionally, it delivers up to 50% cost savings by eliminating the need for legacy firewalls and complex infrastructures."

Zero Trust Segmentation for Branches and Factories

With the increasing prevalence of IoT devices and operational technology (OT) systems in today's branch offices and factories, security leaders are urgently working to protect their environments from sophisticated attacks. A recent Zscaler ThreatLabz report revealed that over 50% of OT devices rely on legacy, end-of-life operating systems with known vulnerabilities, leaving them highly susceptible to attacks. Zscaler's solution securely segments every device—including legacy OT— within hours, without north-south firewalls.

"As OT devices are becoming increasingly common in our environment, ensuring their security is a top priority," said Brian Morris, Vice President, Chief Information Security Officer, Gray Television. "Zscaler Zero Trust Branch has been nothing short of transformative. It has not only helped us reduce network costs, but has significantly reduced cyber risk and helped accelerate M&A integration."

Zero Trust Segmentation for Data Center and Public Clouds

Relying on firewalls to secure workload communications in hybrid and multi-cloud environments increases business risk and complexity. Each internet-facing firewall presents a discoverable attack surface and can lead to inconsistent cyber threat and data protection, as each public cloud service provider operates differently. Zscaler Zero Trust Segmentation standardizes multi-cloud workload security for internet-bound traffic, communication between clouds and data centers, between Virtual Private Clouds (VPCs), and between workloads and processes. This scalable approach eliminates the need for firewalls, site-to-site VPNs, Direct Connect, or ExpressRoute, simplifying and strengthening security across diverse cloud environments.

"Cloud is a critical component of our infrastructure, and we depend on Zscaler's Zero Trust architecture to secure our cloud workloads," said Shanker Ramrakhiani, CISO at IIFL. "Zscaler's Zero Trust Cloud has empowered us to enforce consistent security across our data centers and multiple clouds, simplifying operations and significantly reducing the risk of lateral threat movement."

Zero Trust Segmentation currently supports AWS and Azure, with GCP support slated for February 2025.

To learn more about Zero Trust Segmentation, please visit http://zscaler.com/ztsegmentation.

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.

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 expected benefits of the new Zero Trust Segmentation solution to Zscaler's customers. 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, including those factors related to our ability to successfully implement and deploy our Zero Trust Segmentation solution across platforms and we believe this will result in improved efficiency and cost savings for our customers. Additional risks and uncertainties are set forth in our most recent Annual Report on Form 10-K filed with the Securities and Exchange Commission ("SEC") on September 12, 2024, 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.

Media Contact:

Zscaler PR
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/5923424e-3292-4b01-b160-0a3945e51bc5