Zscaler 2021 “Exposed” Report Reveals Corporate and Cloud Infrastructures More at Risk Than Ever From Expanded Attack Surfaces

June 15, 2021

First of Its Kind Global Report Reveals Hospitality, Telecom Industries are Most Vulnerable to Undiscovered Network Breaches and Offers Ways to Mitigate Risk

Key Findings

- The report analyzed the attack surface of 1,500 companies, uncovering more than 202,000 Common Vulnerabilities and Exposures (CVEs), 49% of those being classified as “Critical” or “High” severity
- The report found nearly 400,000 servers exposed and discoverable over the internet for these 1,500 companies, with 47% of supported protocols being outdated and vulnerable
- Public clouds posed a particular risk of exposure, with over 60,500 exposed instances across Amazon Web Services (AWS), Microsoft Azure Cloud, and Google Cloud Platform (GCP)

SAN FRANCISCO, June 15, 2021 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced the release of “Exposed” , the industry’s first global report on the state of corporate attack surfaces. Based on data sourced between February 2020 and April 2021, the report provides a first-ever look at the impact of attack surface exposure during the COVID-19 pandemic. In the report, Zscaler notes that as businesses began offering more remote work options, their attack surfaces grew concurrently with their dispersed workforce. Coupled with increased reliance on public cloud services and vulnerable enterprise VPNs, large organizations not using zero trust security became more vulnerable to network intrusion attacks. “Exposed” identifies the most common attack surface trends by geography and company size while spotlighting the industry’s most vulnerable to public cloud exposure, malware, ransomware, and data breaches.

“The sheer amount of information that is being shared today is concerning because it is all essentially an attack surface,” said Nathan Howe, Vice President, Emerging Technology at Zscaler. “Anything that can be accessed can be exploited by unauthorized or malicious users, creating new risks for businesses that don’t have complete awareness and control of their network exposure. Our goal with this report is to provide a view of what the internet sees of a company’s information landscape and offer useful tips on how to mitigate risk. By understanding their individual attack surfaces and deploying appropriate security measures, including zero trust architecture, companies can better protect their application infrastructure from recurring vulnerabilities that allow attackers to steal data, sabotage systems, or hold networks hostage for ransom.”

While attack surface vulnerabilities impact organizations of all sizes, major international companies with more than 20,000 employees are more vulnerable due to their distributed workforce, infrastructure, and greater number of applications that need to be managed. To better understand the scale of the problem, Zscaler analyzed organizations in all geographies, partitioning the findings from 53 countries into three regions for ease of understanding – the Americas, EMEA, and APAC.

EMEA at Risk
The report found that while 59 percent of surveyed organizations were based in the Americas, the EMEA region led the world in overall exposure and potential risk, with 164 CVE vulnerabilities. EMEA-based businesses had the most exposed servers, with an average of 283 exposed servers and 52 exposed public cloud instances each. They were also more likely to support outdated SSL/TLS protocols and had greater risk of CVE vulnerabilities on average. The EMEA region was followed by the Americas, with 132 CVE’s (20 percent lower than EMEA), and APAC, with an average of 80 CVE possible vulnerabilities (51 percent lower than EMEA).

While the report demonstrated that EMEA businesses had the most online exposure, all regions showed vulnerabilities, making it critical for IT teams to adopt best practices, including zero trust security, to minimize the attack surface and eliminate exposure no matter where they are based.

Top Exposed Industries
In addition to presenting geographic data, the report tracked corporate attack surfaces by industry, pinpointing the types of organizations most likely to be targeted by cybercriminals. The report analyzed a diverse group of companies, spanning 23 different industries, and found that telecommunications organizations were the most vulnerable and had the highest average number of outdated protocols in their servers. Telecom companies had the third highest average of exposed servers to the internet, increasing the risk of being targeted by cybercriminals for DDoS and double extortion ransomware attacks.

The report also showed that the hospitality industry – including restaurants, bars, and food service vendors – had the highest average of exposed servers and public cloud instances; with AWS instances exposed 2.9 times more often than any other cloud providers. With the COVID-19 pandemic pushing many restaurants to offer online ordering, the rapid adoption of digital payment systems has increased risks for both businesses and customers.

Three Steps to Reduce an Attack Surface
With the number of cyberattacks increasing daily, business IT teams must minimize their attack surface as part of an overall organizational security policy. Without comprehensive security measures, such as a zero-trust model, digital transformation initiatives and cloud migration efforts can also create new vectors of attack and threaten business continuity, professional reputation, and employee safety. Although no approach will be completely effective, Zscaler recommends the following tips for minimizing corporate network risks:

- **Get visibility into your risk of exposure:** Knowing your visible attack surface is key to effective risk mitigation. As more and more applications move to the cloud, it becomes mission-critical to be aware of entry points that are exposed to the

internet. Remember, you can't attack what you can't see.

- **Recognize the failings of VPNs and firewalls:** In the age of cloud and mobility, these perimeter-based technologies significantly increase your attack surface. Stay current with the latest updates to the CVE database. Be sure to remove support for older TLS versions from servers to reduce risk.
- **Make apps invisible to threats with Zero Trust:** Applications protected behind the Zscaler Zero Trust Exchange™ are not visible or discoverable, thus removing an attack surface. The Zero Trust Exchange helps IT security teams ensure that no entity (user or application) is inherently trusted, while helping improve user productivity, mitigate risk, increase business agility and reduce cost and complexity. To discover your attack surface before threat actors do, try the free Zscaler attack surface analysis tool here.

For more information, including access to the full report, please see "Exposed": The world's first report to reveal how exposed corporate networks really are.

Lisa Lorenzin, Senior Director of Transformation Strategy at Zscaler, will be discussing the "Exposed" research results and the tool used to complete the attack surface analysis in an upcoming Zenith Live 2021 session: *Secure Access to Private Apps: The Cornerstone to your Zero Trust Journey*; scheduled for June 15, 2021, at 11:30am PT.

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 the world's largest in-line cloud security platform.

Media Contacts
Natalia Wodecki
Global PR Director
press@zscaler.com

A PDF accompanying this announcement is available at: http://ml.globenewswire.com/Resource/Download/1595ca0e-f54f-4eac-a626-f28e55e13588