



Zscaler Launches Posture Control Solution to Remediate Hidden Security Risks Across Cloud-Native Application Environments

June 22, 2022

New, Purpose-Built Solution Advances Cloud-Native Application Security and Enables DevOps Teams to Contextualize and Remediate High Priority Risks Across the Cloud Application Lifecycle

SAN JOSE, Calif. and LAS VEGAS, June 22, 2022 (GLOBE NEWSWIRE) -- **ZENITH LIVE** -- [Zscaler, Inc.](#) (NASDAQ: ZS), the leader in cloud security, today announced its new Posture Control™ solution, designed to give organizations unified Cloud-Native Application Protection Platform (CNAPP) functionality tailor-made to secure cloud workloads. Integrated into the [Zscaler Zero Trust Exchange™](#), the Posture Control solution enables DevOps and security teams to efficiently prioritize and remediate risks in cloud-native applications earlier in the development lifecycle. The completely agentless solution correlates and prioritizes risks, such as unpatched vulnerabilities in containers and VMs, excessive entitlements and permissions, and cloud service misconfigurations.

“The cybersecurity landscape continues to evolve as more applications reside across multi-cloud footprints, making it more difficult than ever for security, IT, and DevOps teams to keep up with new types of attacks and efficiently prioritize and then remediate cloud risks,” said Amit Sinha, President, Zscaler. “Unlike point cloud security tools, which lack context and overburden operators with alerts while missing the full picture, Zscaler’s new Posture Control solution correlates signals across several cloud security disciplines to identify and prioritize real risk drivers and high priority security incidents. Also, by extending security directly into developer workflows, infosec teams can collaborate more effectively with DevOps teams to proactively secure applications earlier in the development lifecycle.”

Today, most enterprises are forced to implement and manage dozens of point security tools to achieve complete security coverage. These tools operate in silos and are not integrated, leading to visibility challenges, security gaps, and friction among cross-functional teams. However, due to the dynamic nature of the cloud, security risks are made up of a combination of several complex issues that are interconnected across multiple layers. To address them, security teams need a consolidated platform that prioritizes risk across all their cloud environments.

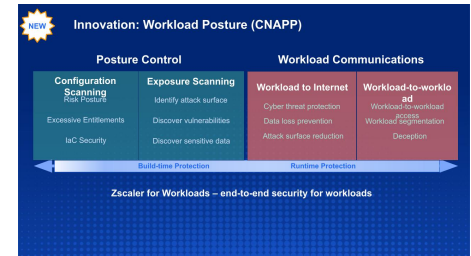
To meet the scale and speed required for cloud-native application development, organizations need a unified approach that envelops the entire Continuous Integration and Continuous Delivery (CI/CD) lifecycle, integrating seamlessly with developer and DevOps workflows. They also need a simplified architecture that correlates issues across multi-cloud environments to better identify high priority security risks and deliver remediation via each stakeholder’s preferred workflows earlier in the development process.

“As organizations increasingly move their applications to the cloud, security teams struggle to keep up with cloud-native development because multiple siloed tools create too many alerts that are difficult to manage and prioritize,” said Melinda Marks, Senior Analyst, Enterprise Strategy Group (ESG). “With its integrated approach, Zscaler’s Posture Control solution can help security and DevOps teams better identify, prioritize, and remediate risks. With solutions like this, organizations can focus on the top issues to greatly reduce their overall risk.”

Zscaler’s new Posture Control solution builds on the security capabilities of Zscaler’s proven Workload Communications solution, which is designed to secure cloud applications at runtime. Integrated with the Zscaler for Workloads service, the Posture Control solution and Workload Communications are combined to unify development and runtime security of cloud-native and VM-based applications running on any service in any cloud. The Posture Control solution delivers comprehensive coverage of all cloud environments in a singular view and a unified data model to enable security, IT, and DevOps teams to secure cloud apps without disrupting the development processes. Following are key features of the Posture Control solution:

- **Advanced Threat and Risk Correlation:** Identify and assess the combination of multiple security issues that may appear to be low-risk individually, but have the potential to create larger, more malicious risks across cloud environments when combined. These correlated risks are unified in a singular view, giving security teams the context they need to properly explore and prioritize risks in the cloud.
- **Agentless Workload Scanning:** Avoid developer friction and eliminate blind spots due to incomplete coverage of security tools with a 100% agentless, API-based approach. VMs and containers are scanned in both registries and in production environments, correlating vulnerabilities with other cloud weaknesses to prioritize actions based on risk rather than on CVSS score alone.
- **Full Lifecycle Cloud Security:** Detect and resolve security issues early in the development phase before they become production incidents with “shift left” security. Zscaler monitors automated deployment processes and sends alerts when critical security issues are found.
- **Risk and Compliance Visualizations Across the Entire Cloud:** Gain 360-degree visibility into risks across the entire multi-cloud footprint, including VMs, containers, and serverless workloads. Zscaler integrates with development platforms like VS Code, DevOps tools such as GitHub and Jenkins, and all major cloud providers to enable visibility and control “from build to run.”
- **Simplified, Fast Deployment and Operations** - Zscaler and HashiCorp, a leader in multi-cloud infrastructure automation,

Cloud-Native Application Protection Platform



Workload Posture CNAPP

have extended their integrations to secure cloud-native workloads in multi-cloud environments. The Posture Control solution can now easily scan infrastructure-as-a-code templates written in Terraform in the development environment. This shift-left approach provides the ability to build security in the CI/CD process, thereby reducing friction between development and security teams, and providing rapid application deployment and better security posture of cloud workloads.

For more details about Zscaler's Posture Control solution, please see [here](#).

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 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.

Media Contacts

Natalia Wodecki
Global PR Director
press@zscaler.com