At Zenith Live 2026, Zero Trust Cloud Takes Workload Security Further

June 5, 2026

Zenith Live 2026 marks an important moment for Zero Trust Cloud, with announcements that focus not just on new capabilities, but on better outcomes for customers securing modern applications. From extending Zero Trust Gateway into Google Cloud through Google Cloud Network Security Integration to bringing host-based microsegmentation to GKE, these innovations are designed to simplify workload protection, minimize operational complexity, reduce overall TCO, and help security teams apply policy more consistently across cloud and Kubernetes environments. Together with customer sessions from organizations including Aflac, NOV, Northern Trust, Henkel, MRH, and IIFL, they show how Zero Trust Cloud is being used to strengthen security posture, support compliance, and scale protection across multicloud infrastructure.

Zero Trust Gateway support for Google Cloud through Network Security Integration

Zero Trust Cloud now supports Zero Trust Gateway in Google Cloud through Google Cloud Network Security Integration (NSI), now available in customer preview. Zscaler now gives organizations a more operationally efficient and scalable way to secure cloud traffic without redesigning application connectivity or relying on firewall-centric architectures. By inserting security natively into Google Cloud traffic flows, customers can apply policy closer to workloads, improve visibility into application communications, and standardize security controls across environments. The result is faster adoption of consistent cloud security controls, lower operational overhead for networking and security teams, and reduced risk from unmanaged east-west and north-south traffic.

NSI gives Google Cloud customers a native way to steer traffic through partner security services without forcing changes to application design. In practice, it allows Zscaler to inspect and control policy on cloud traffic using Google Cloud's service insertion framework. Architecturally, NSI uses a producer-consumer model: Zscaler operates the security service in Google Cloud, while customer workloads connect through Google Cloud constructs that direct selected traffic for inspection.

A key technical element of the integration is NSI's use of GENEVE encapsulation, which preserves packet context as traffic is sent to the security service. That allows security policy to operate with better awareness of the original flow, rather than treating traffic as generic forwarded packets. The result is a more cloud-native a model that avoids the complexity of distributed route manipulation or legacy appliance placement strategies. Instead of forcing security teams to retrofit legacy controls into cloud environments, Zero Trust Gateway can be inserted into Google Cloud traffic paths using native integration points and applied closer to the workload communication layer.

This is especially relevant for organizations standardizing on Google Cloud and looking for a simpler way to extend inspection and policy definitions across north-south traffic, east-west traffic, and cloud egress use cases without increasing architectural complexity.

Additionally, as a fully managed service from Zscaler, customers stand to significantly reduce their overall Total Cost of Ownership (TCO) — eliminating Data Transfer Out (DTO) costs, compute overhead from standing up security appliances, and the manpower required to manage and maintain security infrastructure.

Zscaler Microsegmentation: host-based microsegmentation comes to GKE

The second announcement is that Zscaler Microsegmentation now extends host-based microsegmentation to Google Kubernetes Engine (GKE). For organizations running containerized applications, this brings more precise control to environments where workload identities are dynamic, east-west communication is constant, and lateral movement remains a primary risk. Traditional segmentation approaches often depend on IP ranges, static topology assumptions, or coarse-grained boundaries that are difficult to maintain in Kubernetes. Host-based microsegmentation shifts cybersecurity closer to the workload, making it easier to define legitimate application communication and continuously uphold least-privileged access as environments scale.

Kubernetes environments increase the number of workload identities, service-to-service communication paths, and short-lived compute instances that security teams need to control. Pods scale up, terminate, and move across nodes, which makes static network-based controls harder to maintain over time. In these environments, east-west traffic becomes the primary risk plane, because once an attacker gains access to a node or workload, lateral movement across service paths becomes the immediate concern.

Host-based microsegmentation helps address this by applying segmentation closer to where the workload actually runs. Rather than relying only on cluster-level or network-level controls, security teams can control more granular policy aligned to application behavior and expected communication paths. This is important in GKE environments, where organizations need security controls that match the operating model of managed Kubernetes rather than add more network complexity.

For customers adopting GKE for modern application delivery, host-based microsegmentation provides a security control plane better aligned to how containerized workloads actually run: ephemeral, distributed, and service-oriented. The business outcome is stronger protection for containerized applications, reduced lateral movement risk, and a segmentation model that is easier to operationalize as Kubernetes environments grow.

Customer sessions at Zenith Live 2026: how Zero Trust Cloud is being applied

Alongside the product announcements, Zenith Live will feature customer sessions that show how Zero Trust Cloud is being used to solve real cloud security challenges at scale.

Customer	Topic for breakout session at ZLive 2026*
Aflac	How Zscaler Microsegmentation helps address compliance and regulatory requirements through tighter workload isolation, least-privileged access, and reduced lateral movement.

NOV Inc.	How Zero Trust Cloud supports a more holistic workload security model by combining multicloud egress protection with host-level microsegmentation.
Northern Trust	Best practices and lessons learned from deploying workload protection consistently across multicloud environments while managing policy, segmentation, and phased rollout.
Henkel	Practical guidance for implementing workload protection across cloud environments with a focus on policy consistency, segmentation design, and staged deployment.
MRH	How organizations can use Zero Trust Gateway to onboard workload security in the public cloud with a managed service model designed for faster implementation and lower deployment risk.
IIFL	How Zscaler Microsegmentation can support regulatory compliance while helping organizations deliver segmentation projects more efficiently and cost-effectively.

These sessions add an important layer to the announcements. They show that the value of Zero Trust Cloud is not theoretical. Organizations are applying these capabilities to meet regulatory requirements, unify security controls across cloud platforms, reduce the operational burden of multicloud security, and move toward a more consistent model for workload protection. For details of these breakout session please visit Zenith Live events page here.

Why these announcements matter

At Zenith Live 2026, the message is clear: workload security has to evolve with the architecture it is protecting. As organizations expand across cloud and Kubernetes environments, they need security controls that are more native, more granular, and easier to operationalize at scale. With Zero Trust Gateway support for Google Cloud through NSI, host-based microsegmentation for GKE, and customer stories that show these approaches working in practice, Zero Trust Cloud is helping customers move toward a more consistent, scalable, and effective model for protecting modern workloads.