Zero Trust – Micro-Segmentation

To assume a Zero Trust security posture, you must first verify that someone or something is trustworthy before granting access. Lateral movement, data leaks, and insider threats are key problems all industries face.

Provide more secure access, protect against gaps in visibilities, and reduce your attack surface with Trace3’s Zero Trust framework. We specialize in deploying and operationalizing software defined networks, complete with micro-segmentation to prevent lateral movement across your network by security threats.

Secure Your Workload
Secure all connections within your apps, across multicloud.

Protect your hybrid multicloud workloads and contain lateral movement with application segmentation. Leverage complete network visibility and determine dependencies within databases and applications.

VISIBILITY INTO WORKLOADS
Gain visibility into what is running and what is critical by identifying workloads and enforcing policies.

APPLICATION SEGMENTATION
Contain breaches and minimize lateral movement with application micro-segmentation.

SECURITY ALERTS
Alert or block communication if a policy is violated by continuously monitoring and responding to indicators of compromise.

Contact us today to learn more about how Trace3 can start you on your Zero Trust journey.