Zero Trust

The changing IT landscape benefits from new dynamic security practices such as Zero Trust. As a strategic initiative that helps prevent successful data breaches, Zero Trust protects modern digital environments through the principle of maintaining strict access controls and not trusting anyone by default.

Most data breaches are caused by excess trust in your network. Lateral movement, data leaks, and insider threat are key problems all industries face. How protected is your organization? Take for instance the largest vertically integrated healthcare provider in the US. They depend on Trace3 for three foundational components of the Zero Trust Framework: micro-segmentation, data protection, and identity management.

**Micro-Segmentation**

We specialize in deploying and operationalizing software defined networks, complete with micro-segmentation to prevent lateral movement.

**Data Protection**

Data is what attackers are after. Zero Trust Networks are based on understanding data flows, data protection, and data classification which diminishes the impact of a data leak.

**Identity Management**

Our identity and access management experts provide your organization with the insights to architect policy-based on identity to combat a potential insider.

**WHY CLIENTS CHOOSE THE TRACE3 SECURITY TEAM**

Trace3 is uniquely positioned to bring together network, cloud, and security to any Zero Trust Networking conversation. Our experts have on average 15 years of experience architecting and deploying next-generation adaptive security solutions. We have perfected the art of CARTA by guiding customers through the various stages of Predict, Prevent, Respond, and Protect.

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