Zero Trust – Identity Management

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.

Trace3’s Zero Trust framework helps you prevent unauthorized access, contain breaches, and reduce the risk of unauthorized lateral movement through your network. Our identity management experts provide necessary insights to architect a policy-based approach to establishing user trust and identity at the edge.

Secure Your Workforce

Ensure only the right users and secure devices can access applications.

Edge security strategy helps protect your users and their devices against stolen credentials, phishing, and other identity-based attacks. It verifies user identities and establishes device trust before granting access to applications.

USER IDENTITY
Verify the identity of all users with effective, strong multi-factor authentication (MFA) before granting access to corporate applications and resources.

USER DEVICES
Inspect all devices used to access corporate applications and resources in real-time, at the time of access, to determine their security posture and trustworthiness.

APPLICATIONS
Protect every application by defining policies that limit access to the users and devices that exceed the organization’s risk tolerance levels.

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