Zero Trust – Data Protection

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 is a comprehensive approach to securing all access across your networks, applications, and environment. 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.

Secure Your Workplace

Secure all user and device connections across your network, including IoT.

Software-Defined Access (SD-Access) helps you gain insight into users and devices. Identify threats and maintain control over all connections across your network, including Internet of Things (IoT) devices like cameras, manufacturing equipment, heart pumps, and more.

NETWORK ACCESS
Grant the right level of network access to users and devices with network authentication and authorization.

NETWORK SEGMENTATION
Classify and segment users, devices, and applications on your network with network segmentation.

CONTAIN THREATS
Contain infected endpoints and revoke network access by continuously monitoring and responding to threats.

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