

Cybersecurity

Zero Trust Networking Solution



THE CHALLENGE

The cyber landscape has become increasingly challenging for organizations of all sizes. Data is a new currency for criminals, and organizations are seeking ways to protect their assets, and support their cybersecurity regulatory compliance standards. They realize that it is not “IF they will get hacked, it’s WHEN”.

THE SOLUTION

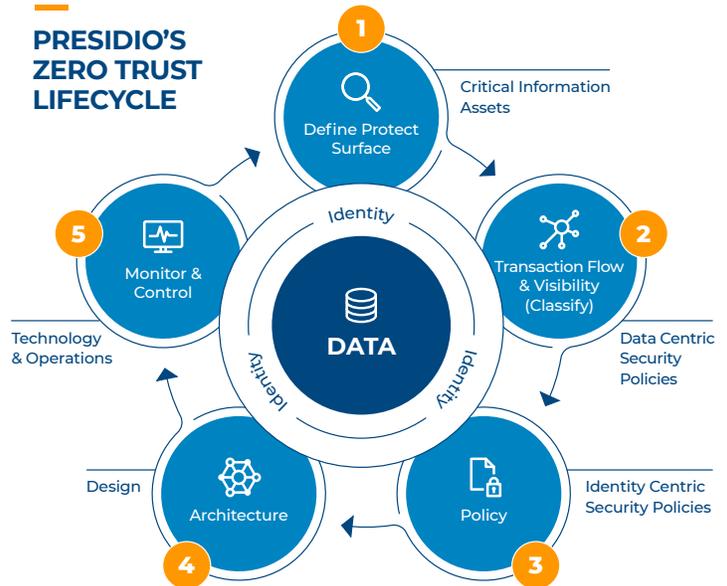
The Presidio Zero Trust Networking (ZTN) Solution introduces a structured approach to protecting data. The fundamental purpose of Zero Trust is to move from “Trust but Verify” to “Never Trust, Always Verify”.

Data and identity are at the core of Zero Trust. The Presidio approach recognizes that data is no longer stored in one central location, nor is it accessed in one location or on one device. Usage patterns of the data help to establish a baseline and allows the Presidio ZTN to identify unusual behavior and begins to set up the identification of threats.

Establishing a set of policy controls incorporating Authentication, Authorization and Access Control supports the goal of only allowing authorized users to access specific data. A detailed review of the architecture identifies cybersecurity gaps to increase the security posture. Continuous monitoring recognizes that the threat landscape is continuously evolving, and organizations are constantly changing.



PRESIDIO'S ZERO TRUST LIFECYCLE



The Presidio Zero Trust Networking Solution approaches the evolution for each client leveraging a 5-step process.

- 1. Define & Protect the Surface** – Identify where your data is, define what data is important and worth protecting.
- 2. Map & Classify** – Begin mapping access behavior and data dependencies using Identity and Access Management (IAM) techniques
- 3. Establish Policy** – Review written and unwritten policies and practices to revise or develop access and monitoring rules – incorporate AAA (Authentication, Authorization, and Access Control)
- 4. Architectural Assessment** – Implement the architecture to protect against security vulnerabilities
- 5. Monitor & Maintain** – Once the Presidio ZTN Solution has been implemented, it needs to be constantly monitored, recognizing that threats are becoming more advanced, more users and endpoints are vulnerable to these threats; and in support of normal business operating changes such as mergers and acquisitions

