PRESIDIO FEDERAL

SOLUTIONS BRIEF

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 Federal 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 Federal 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 Federal ZTN to identify unusual behavior and begins to set up the identification of threats.

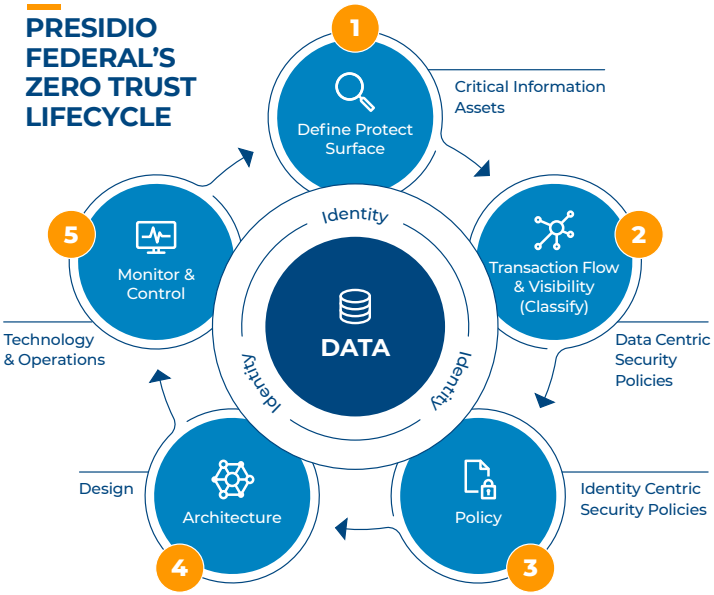
Establishing a set of policy controls incorporating Authentication, Authorization and Access Control supports the goal of only allowing authorized users to access specific data. A detailed review of the architecture identifies cybersecurity gaps to increase the security posture. Continuous monitoring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

AT THE CORE OF A ZERO TRUST STRATEGY

DATA
Your most valuable asset

IDENTITY
Who has access to this information

PRESIDIO FEDERAL'S ZERO TRUST LIFECYCLE



The Presidio Federal 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 Federal 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

Zero Trust Networking Solution

KEY BENEFITS

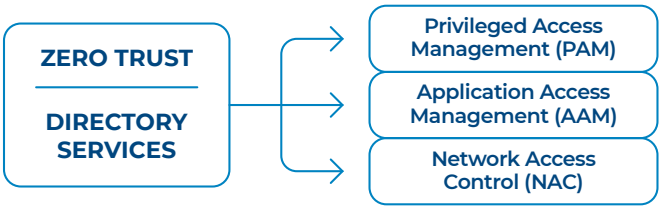
In May 2021, the US Government National Security Agency (NSA) issued an executive order supporting the Nation's cybersecurity goals. "The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity."

Hardening your enterprise with Presidio Federal ZTN will help deter cyber criminals.

Presidio Federal's Zero Trust Networking Solution enables our clients to protect their core data assets with an end-to-end solution. The Presidio Federal ZTN gives clients the confidence that they will be able to safely operate their business.

- Secure and protect sensitive data
- Authorize and validate access
- Identify unauthorized access attempts
- Demonstrate compliance with policies and regulatory requirements

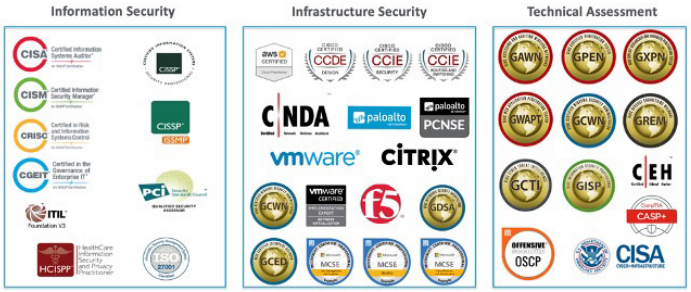
With a large suite of potential vendor solutions, Presidio Federal can recommend the right blend of technologies to meet the specific industry and individual needs of each client.



WHAT MAKES US DIFFERENT

Presidio Federal is a trusted partner to our clients, securing their infrastructure, employees, customers and assets from ever-growing cyber threats. Our clients trust Presidio Federal:

- **Protect Critical Assets** – Presidio Federal's ZTN identifies and protects critical data from unauthorized access
- **Cyber Intelligence** – Our cyber intelligence data is comprised of knowledge from thousands of data sources, dozens of cyber products, transactions, and events, and combined with anomaly detection, can rapidly identify potential risks to thwart cyber-attacks
- **Speed** – Our deep knowledge of every layer of the IT and cyber architecture, combined with proven methodologies supports responding in record time to potential threats



Experience, Education, and Expertise

WHY PRESIDIO FEDERAL

Presidio Federal is a purpose-built and mission-driven IT services and solutions provider dedicated to serving the federal government. We leverages our wealth of experience and deep relationships across our partner ecosystem, creating an environment of active collaboration and real-time responsiveness. Our clients benefit from:

- Services methodology built on recognized industry standards including NIST, CIS, and ISO
- Compliance depth & breadth including PCI, HIPAA, NERC CIP, GDPR, CCPA, SOC 2, ISO 27001, DFARS 800-171, CMMC
- Multi-discipline experts provide for a broad view of client's potential vulnerabilities
- Deep cybersecurity services bench and broad security services solutions provide domain expertise and consistent deliverables

Presidio Federal's Cybersecurity Practice covers a broad security services portfolio. Our highly skilled and tenured cybersecurity practitioners maintain leading industry certifications, provide thought leadership and practical industry experience. We have conducted thousands of engagements across all major industry segments. Let's explore how we can secure your business.

Contact Presidio Federal today: www.presidiofederal.com