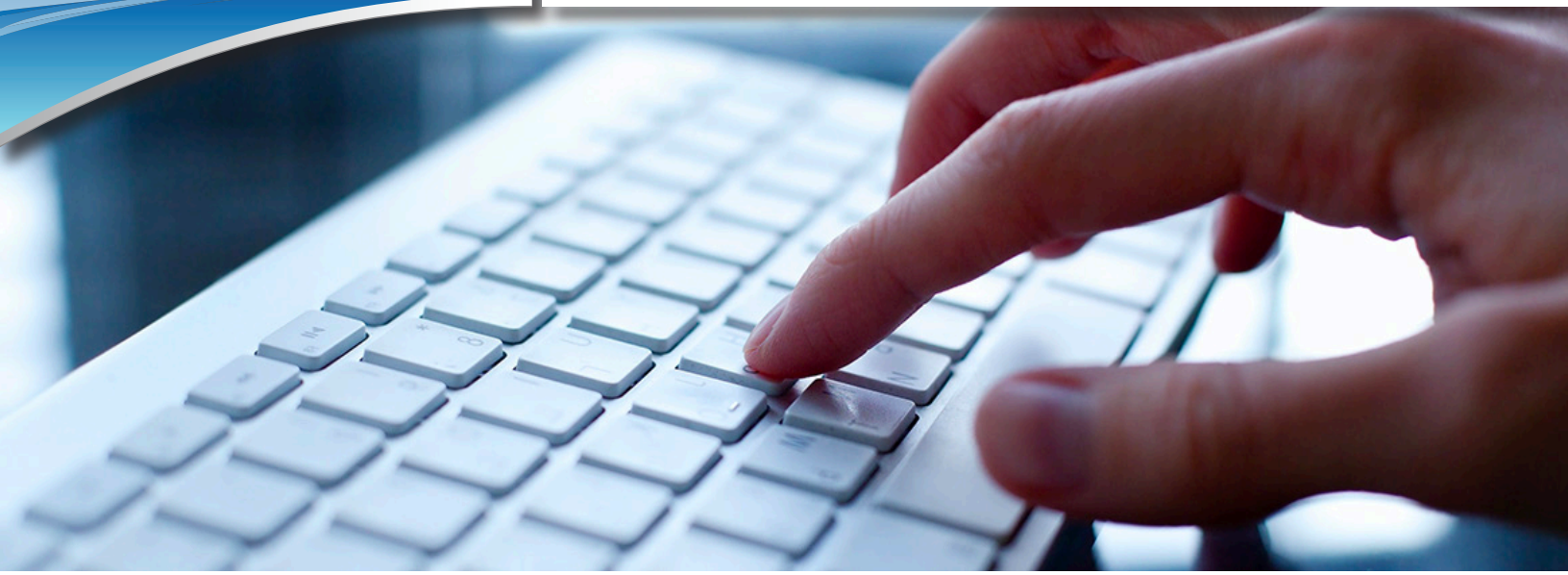
take control of the EDGE

IS A SECUREPCN ZERO TRUST (ZT) COMPLIANT?



Zero Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to users, assets, and resources.

A Zero Trust Architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows.

Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership.

Zero Trust is a strategic initiative that aims to prevent data breaches by eliminating the concept of TRUST from an organization's network architecture. Zero Trust architecture treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized. A Zero Trust architecture leans heavily on components and capabilities for identity management, asset management, application authentication, network segmentation, and threat intelligence.

Call us at **(877) 876-4PCN** to discuss solution options and determine if we are the best choice for your business.

Learn more by visiting online at **securepcn.com**, on our **Linked In** page or by emailing us at **info@securepcn.com**.

SecurePCN™ complies with Zero Trust Architecture.

NIST 800-207 Guidelines

SecurePCN™, like Zero Trust Architecture, is an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure.

Encryption

Your sensitive data is secure. Point to Point (P2PE) with AES 256 is virtually impenetrable using brute-force methods.

Segmentation

Your data NEVER traverses the public internet.
Your endpoint devices (access control panels, alarm panels, cameras/NVRs, POS equipment, workstations, exterior or mobile equipment) will have **no routable IP addresses**. They are essentially invisible to hackers.

Monitoring

Communication is monitored Out of Band (OOB), meaning that we monitor to assure only authorized communication occurs, without touching or monitoring your encrypted data.

- We set **Deny by Default Rules**. No one can add, remove or relocate a device without your authorization.
- No unauthorized phone home capabilities.
- We alert you to **detected anomalies.**

SECUREPCN™
PRIVATE CELLULAR NETWORKS