Make Critical Infrastructure UNHACKABLE

Steve Ridgeway
Executive Vice President
IMPRES Technology Solutions, Inc.

"You can't hit what you can't see!" - Walter Johnson, Washington Senator's Pitcher

TCP/IP is inherently insecure. Instead of digging a bigger moat (IDS, IPS, Firewalls, etc) we hide the connections and network infrastructure from untrusted parties, so you can focus on OPERATIONS and better utilize your people, time, and money.

OVERVIEW

The IMPRES Cyberspace Operations Infrastructure (CSOI) is a solution framework that enables Zero Trust Architectures (ZTA) by harnessing the power of Software Defined Perimeter principles with enhanced Identity governance approaches. CSOI employs micro, macro, and cross-boundary segmentation, including end-to-end encryption, and automatically authenticates, authorizes, and connects (on-demand) secure tunnels using unique device-based cryptographic identities including support for platform IT (ICS/SCADA). CSOI features an intuitive orchestration engine that simplifies the deployment and management of enterprise ZTA relationships, workflow plans, and access policies.

A zero-trust security model takes on more significance with NIST guidance (NIST SP 800-207, 800-52, 800-171B) and the new CMMC requirements for all DIB (Defense Industrial Base) suppliers. By implementing a CSOI zero-trust infrastructure solution across your network, you can simplify the management of network assets, deploy a Software Defined Perimeter to your endpoints and fully cloak the network – MAKE YOUR CRITICAL INFRASTRUCTURE UN-HACKABLE

TECHNOLOGY CONCEPT

CSOI is a zero-trust infrastructure which is a Layer 3 overlay component that provides the foundation to build a robust software-defined perimeter (SDP) solution. It balances accessibility, information security, operational resiliency (mobile, manned, and unmanned systems), and full insider threat protection. CSOI is a strategic resource for those working to build responsive, resilient networks, reducing the network attack surface from insider threats, increasing security protection in coalition environments, and preventing internal/external threats from compromising critical assets. CSOI allows the DOD to rapidly and dynamically configure the control plane to protect critical infrastructure via a software interface with visual and automated functions.

The CSOI Conductor (Zero Trust Orchestration), enforces visibility and access policy for all your 'things' with point-and-click simplicity. Make your 'things' invisible by creating a software-defined network (SDN) that's micro-segmented, encrypted end-to-end, and multi-factor authenticated (MFA). CSOI defines the overlay network segments and systems that protected machines are allowed to access, as well as how they connect on the LAN, WAN, and public Internet. Policy creation and management is simple and requires no advanced training.

Available in cloud, virtual, and hardware form factors, the CSOI Conductor enables fast network provisioning, micro-segmentation, and secure connectivity. All of this is based on unchanging cryptographic machine identities, not network addresses that change and can be spoofed.

For more information on CSOI: https://www.imprestechnology.com/impres-csoi/