



- *Hidden Networks*
- *Hardened Security*
- *Trust You Can Verify*

Mission

Safeguard digital environments with cutting-edge technology and unparalleled expertise.

Who We Are

Cyber Intel Solution (CIS) is a leading innovator in cybersecurity solutions. With over two decades of expert level cyber and intelligence experience from national to tactical, with emergent technologies, and across advanced cyber operations, CIS is dedicated to providing state-of-the-art products and consulting services. CIS stands as a leader in safeguarding critical assets with the highest levels of security.

Our Unique Offerings

CIS delivers a proprietary, state-of-the-art Cyber Security suite, featuring dynamic, portable, and commercially available off-the-shelf (COTS) solutions. These solutions offer randomized, anonymous protection for Data-in-Transit, Data-at-Rest, and secure communication, ensuring the highest level of security in every scenario.

Differentiators

Transparency

Our encrypted Software Defined Network (SDN) keeps server locations and public IPs hidden for uncompromised privacy.

Anonymity

Our secure managed attribution platform ensures your information remains private and protected.

Security

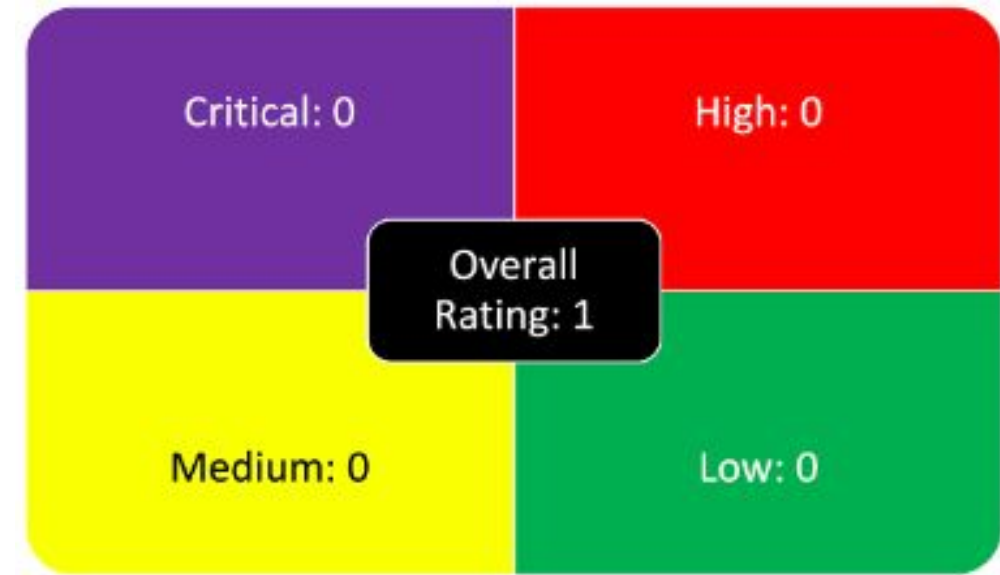
Our CISEN infrastructure follows the highest security standards with multiple layers of protection and IDS.

Tailored Solutions

We provide fully customized cybersecurity solutions for industries, individuals, and departments.



CIS Alignment with DISA Next Strategy



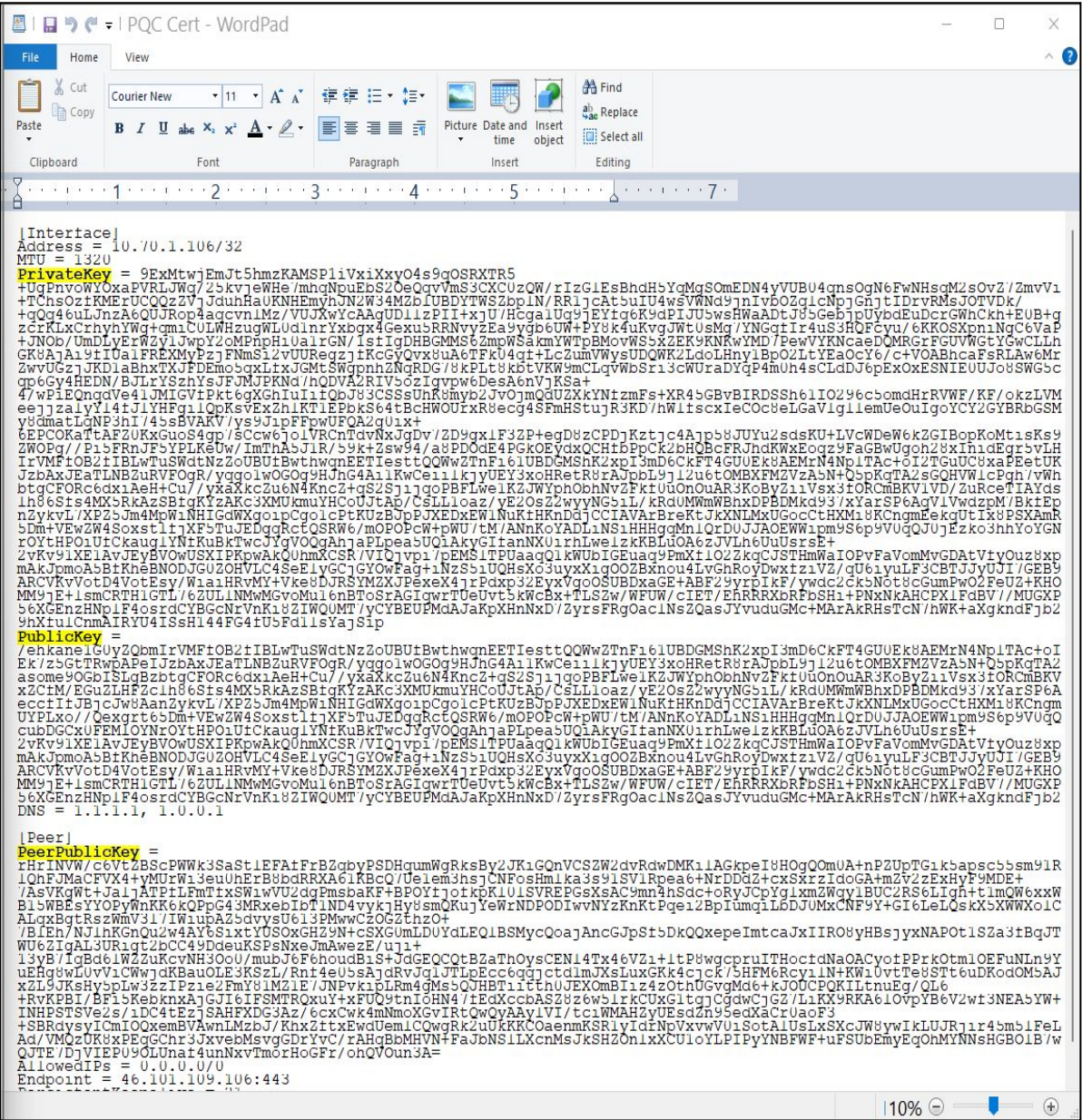
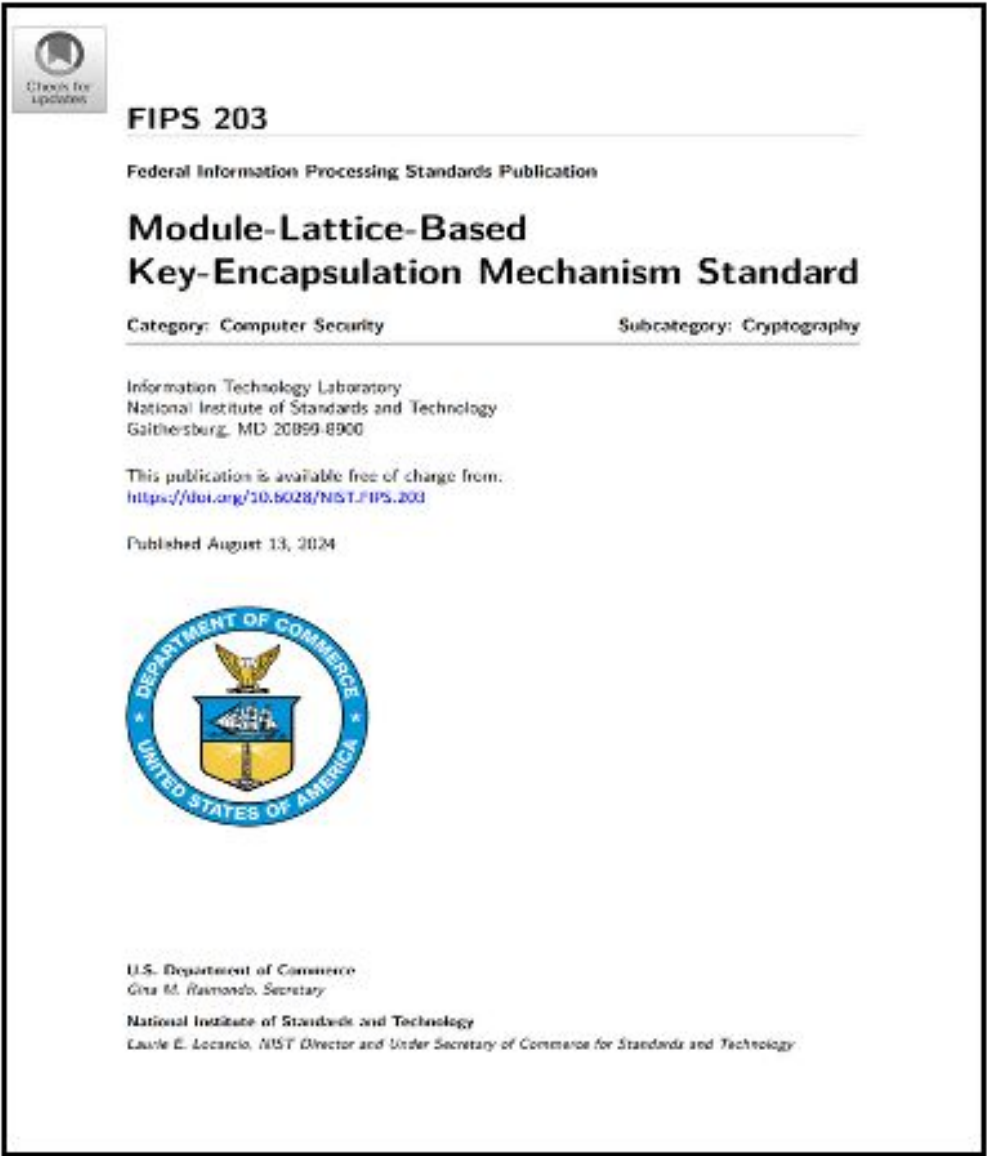
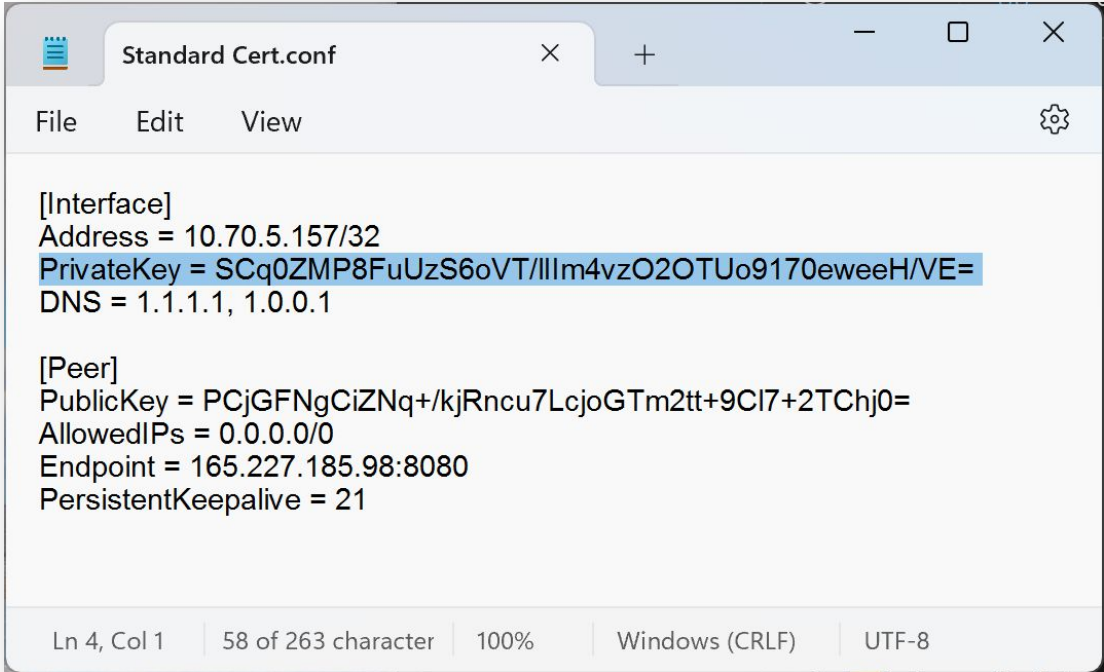
Independently Tested, Existing ATO

- **Goal 1 – DISN, & Goal 2 - ZT – CIS Plug & Play Interoperability**
 - Infrastructure & end point agnostic – from mobile to multi-cloud, data centers, & critical infrastructure; **diverse scaling solutions**
 - ZT Compliant Technology
- **Goal 1 – DISN, Goal 2 – Hybrid Cloud, & Goal 5 Consolidated Network – CIS Unparalleled Protection**
 - **SLASH CYBER RISK BY 99.999%** with **99.9%** uptime
 - ALL threat vectors – **attack** (e.g. man-in-the-middle), **denial**, & **data**
 - **Privacy first**, remove **third-party vulnerabilities** & selectors
 - Infrastructure & end point agnostic
 - Ultra-low latency <5ms, up to 400Gbps instantaneous, resiliently up 99.99%
- **Goal 3 – NLCC – CIS Highest Cryptography Standard**
 - Federal Information Processing Standards (FIPS) 203 compliant
- **Goal 3 – NLCC, & Goal 6 – Zero Trust Tools – CIS Pi Epsilon PQC Comms Platform - Support to Secure Mobile Devices**
 - Post-quantum secure & optional cyber anonymous hardening, no logs; decentralized chat, voice calls, group video, & file share



What does a PQC certificate look like?

Current Standard

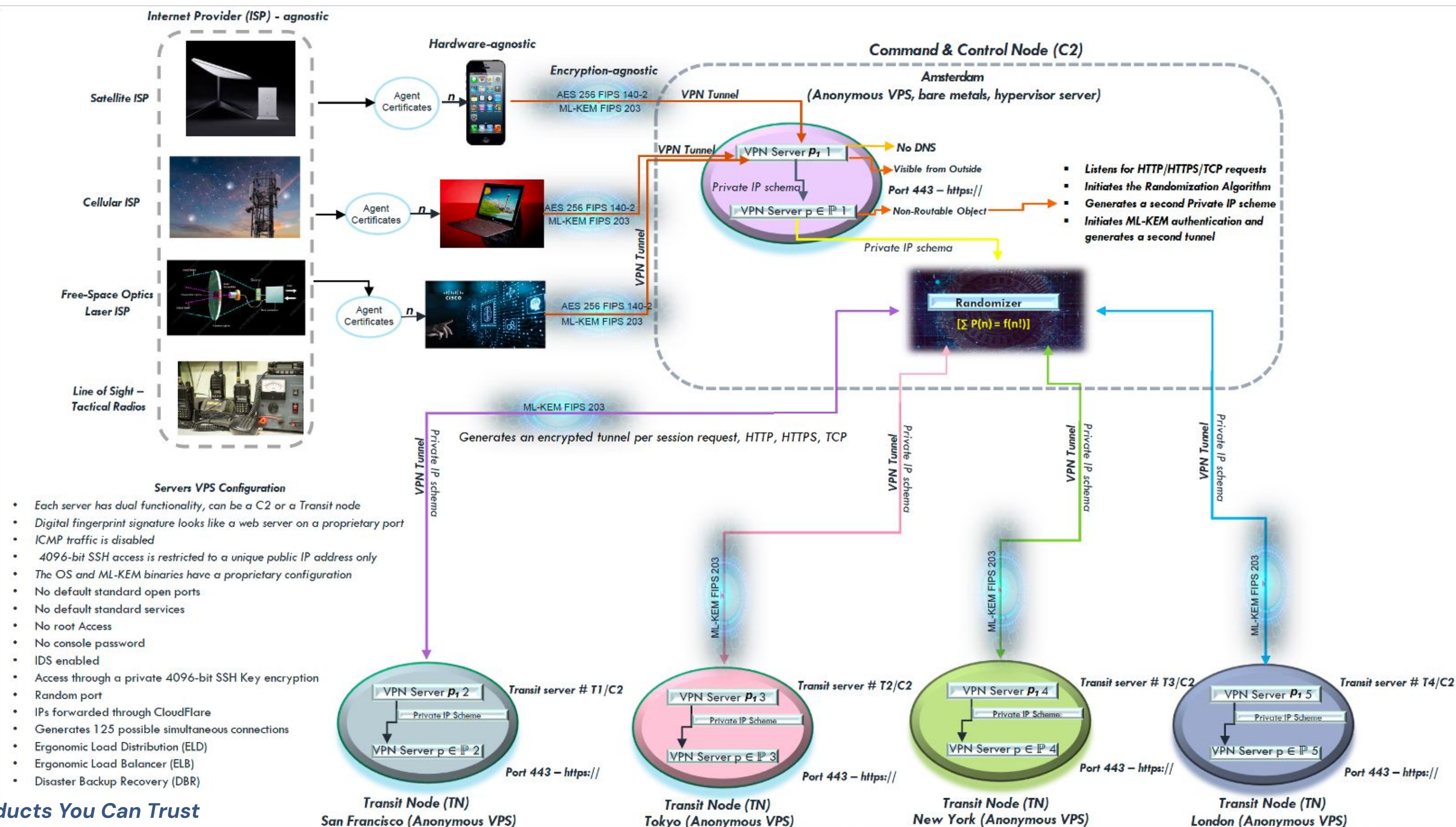


Post-Quantum Standard





CIS Encrypted Network (CISEN)





CYBER INTELL SOLUTION

CIS SOLUTIONS – Live Demo



Pi Epsilon Communication Platform

A future secure, untraceable, & distributed communication platform you own

**Untraceably Private + Post-Quantum
Cryptography +
99.999% Cyber Hardened**

The *Pi Epsilon (Pi Ep) communication platform* is a cutting-edge **decentralized, anonymous, post-quantum encrypted** solution where **you own your information** and infrastructure choices.

- Armored **voice, text/chat**, and **video conferencing**
- **Leverage Apps with No third-party** touching your data
- **Hides in plain sight** & installs on **any computer**
- 99.999% **cyber hardened** by *Virtual Dissimulated Encrypted Server (VDES)*
- Pairs well with our non-attribution *Mobile 5G Travel Router with WiFi and Cipher Phone*



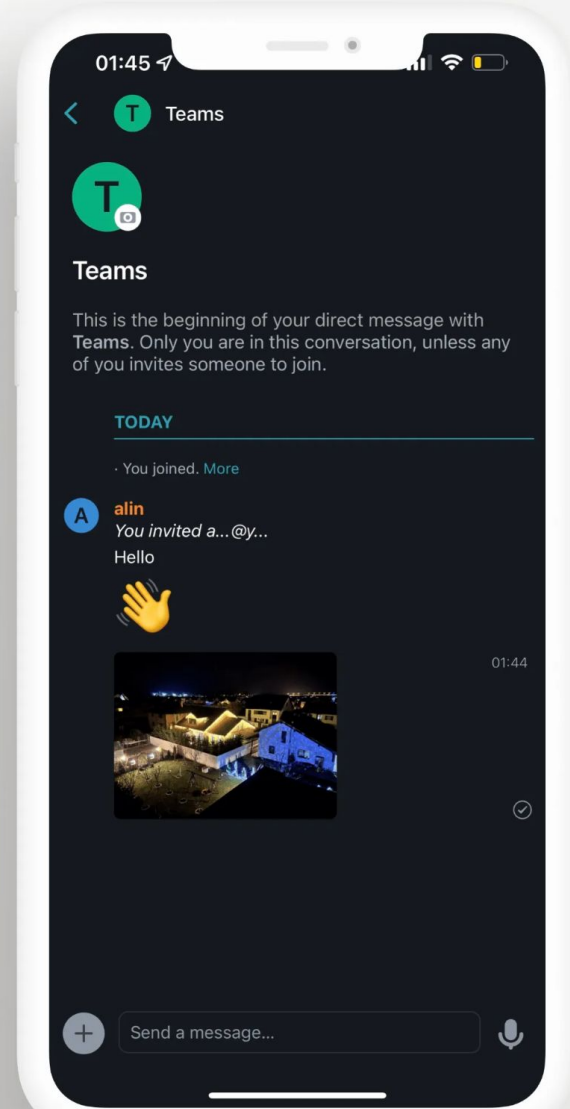
Your Brand

CIS App or White Label for 3rd Party Apps



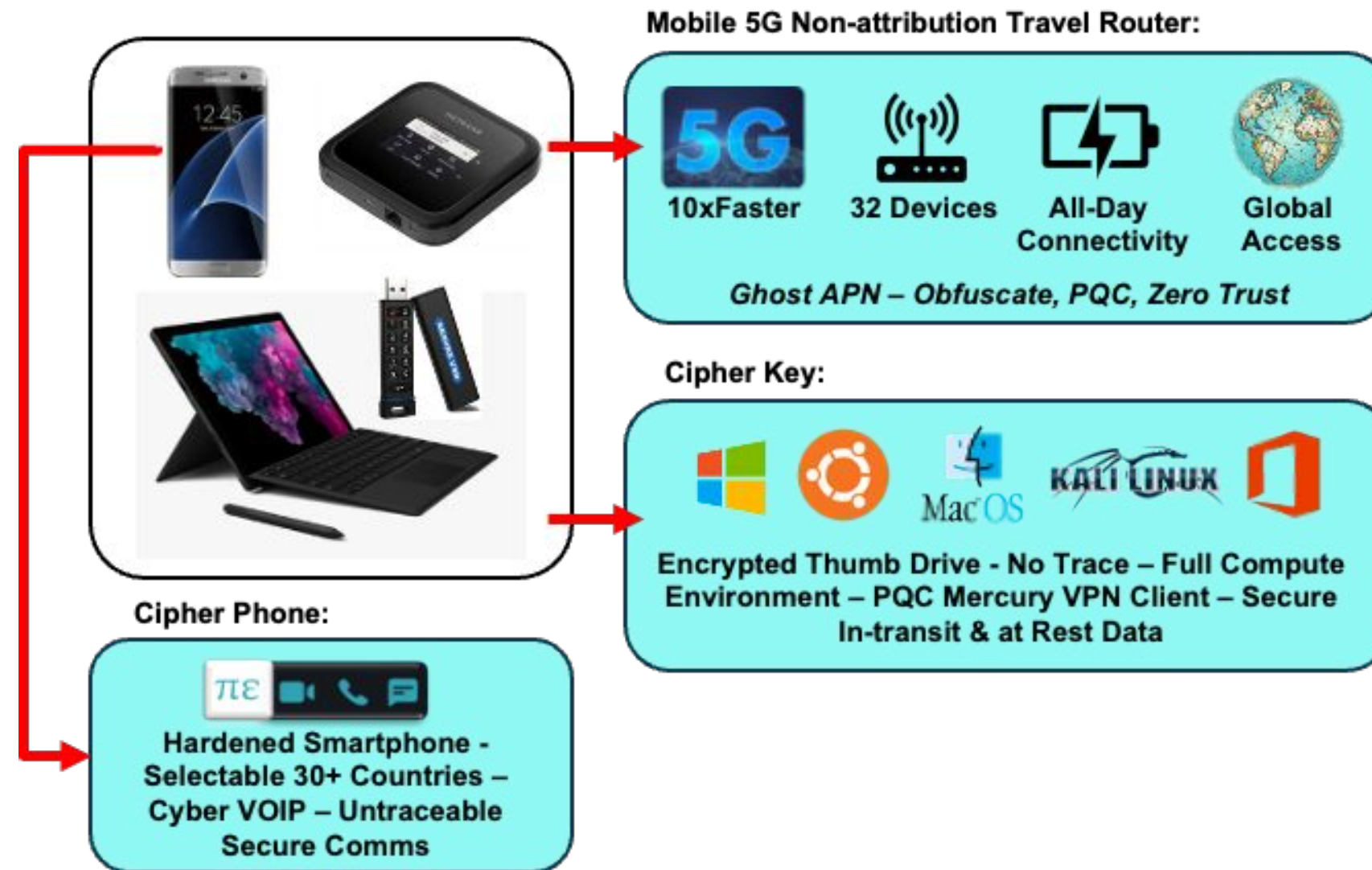
Backstops & Secures Existing Communications

**Complete
experience**





Mobile Cyber Tool Kit (CTK) Solutions



Portable Communications Solution – Mobile Cyber Kit

For the ultimate protection and mobile experience CIS offers the *Mobile Cyber Kit*, composed as a single mobile solution kit with a Cipher Phone, Cipher Key, a specially configured tablet or laptop computer, and a *Mobile 5G WiFi* Travel Router; best deployed with the *Pi Epsilon Π E (Pi Ep) Communications Platform*.

All solutions are available separately.

Mobile 5G Non-attribution Travel Router:

Anonymous Global 5G internet solution

- Speeds up to 10x faster than 4G
- Wi-Fi 6E enabled, up to 32 devices
- All day battery-powered connectivity
- Global internet access
- Carrier provided Access Point Network (APN) or optional private *Ghost APN* to obfuscate, dual-layer PQC encrypt, and privately route cellular data

Cipher Key:

Cutting-edge encrypted bootable thumb drive for a no trace full compute environment on the fly

- Supports Windows, Ubuntu, MacOS, & Kali Linux; Microsoft Office suite, secure chat & encrypted email
- PQC Mercury VPN Client; secure data in-transit & at rest
- Seamless with other CIS solutions

Cipher Phone:

Cyber hardened smartphone

- *Selectable numbers in 30+ countries with Cyber VOIP*
- *Untraceable secure comms offered through Pi Epsilon*



Secure Distributed Infrastructure

End Point & Enclave Protection - Anywhere

Protecting edge servers, critical infrastructure, Internet of Things connected devices, distributed private networks, and edge to cloud access, the *Iron Edge Gateway (IEG) Router and Server* provides protected transport and scales with the number of connections you need. IEG is also available as an anonymous and post-quantum protected *Virtual Private Server (VPS)* you control, with intrusion detection. Options scale from a single connection, to 10 connections with Professional, and 100 with Enterprise.

Distributed Storage Synchronization – Digital Dead Drop (3D)

The *Digital Dead Drop (3D) Data Server* is a state-of-the-art and scalable zero detect or intercept secure data management, synchronization, and backup solution for distributed applications.

Post-Quantum Encrypted Data Storage – DATA VAULT

DATA VAULT is a private encrypted data storage server with post-quantum cryptography protecting both your data-at-rest and data put into motion in write or distributed access. Storage sizing options are 16 TB, 24 TB, 32 TB, 64 TB, 100 TB, and up to Petabyte scale.

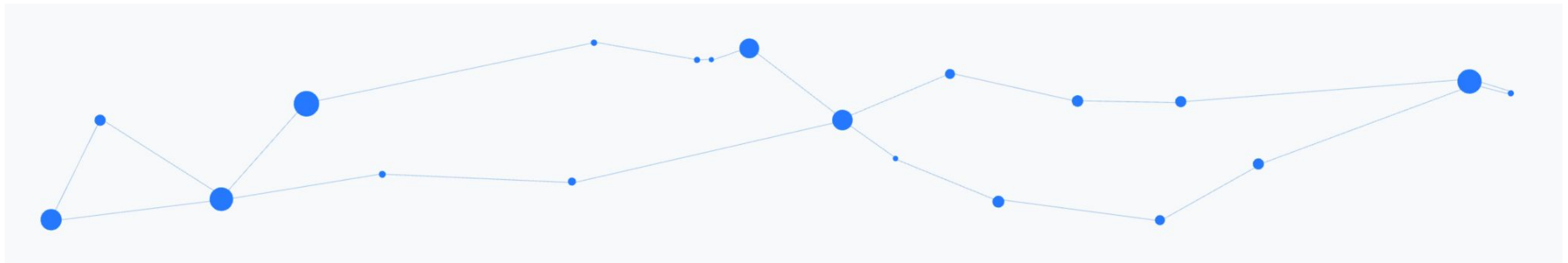




Invisibly Quantum Servers & Services

Protect Public Internet Facing Servers, Websites & Services

CIS employs advanced deception-based techniques to camouflage and protect critical server and services infrastructure, no matter where they reside. A *Virtual Dissimulated Encrypted Server (VDES)* deploys in front of a public internet facing server, routing all traffic through the *CIS Encrypted Network (CISEN)* hiding your server's real address and access point(s). Additional options include high-fidelity decoys and misdirection design features. For your own private network or system isolation needs CIS offers a *Standalone Virtual Private Network (VPN) Server* with advanced cryptography, robust security, and absolute anonymity.



Protect Sensitive Internal Data, Servers & Services – PQC Labyrinth Network

For uniquely private services or servers – such as a closed distributed ledger validation network, private blockchain, or closed network communications and data services – CIS offers the *Inner Trusted Labyrinth – Non-Routable Object (InTL-NRO)* Network with post-quantum protection. This solution set deploys and protects your capabilities within the *CIS Encrypted Network (CISEN)* as your own private enclave.



Post-Quantum CIS Exchange Email Server

PQC Private Email Hosting

CIS's *Exchange Mail Server* enhances security with **cyber hardening**, **anonymization**, and **post-quantum encryption**. You take ownership of your email infrastructure, eliminating third-party vulnerabilities.

- **End-to-End Encryption:** When deployed inside of your EEN, SecureXchange access to your emails is fully PQC, protecting the content from unauthorized detection and access. Email encryption for delivery to outside users is compatible with standard encryption tools.
- **Flexible Server Placement:** The service can be hosted on a dedicated Virtual Private Server (VPS) or any preferred location, providing flexibility and control to the administrator and users. This option includes Gray Zone and adversary environments.
- **Virtual Dissimulated Encrypted Server (VDES):** This technology hides the real server location, obfuscating its identity, services, and ports preventing attack surface scanning, access discovery, and unauthenticated users access.
- **Independence from External Providers:** The system operates independently in infrastructure you control. Removes all third-party dependencies.
- **Complete Control:** Admins have complete control over the server, allowing for customization according to needs.





CYBER INTELL SOLUTION

Points of Contact

CIS:

Alex Purta
CEO, Cyber Intell Solution LLC
ceoaro@cyberintellsolution.com
+1.443.618.6326

Capture Lead:

Jon Hoffman
Global Grove Technology
jon.hoffman@globalgrovetech.com
+1.703.282.4266