

Secure Hardware-Based VPN

CommLock Connect utilizes a hardware-based Root of Trust incorporating software security features, cryptographic isolation, high through-put, and most importantly, ease of use. It supports both wired and wireless secure network connectivity and its flexible architecture allows for it be at the core of many network security solutions. It is designed as a bump-in-the-line IP network subsystem receiving unencrypted IP traffic as input and transmitting encrypted IP network traffic as output to a single server.



How Does It Work

CommLock Connect provides a private, secure, and trusted network channel for data exchange between an endpoint and the CommLock Server that shields your private cloud / network. The endpoint can be any device supporting standard wired (Ethernet or USB) network connectivity, such as a desktop, laptop, IP phone, or Wi-Fi enabled devices.

Once connected through the CommLock Server, the endpoint has access to any services within your private cloud / network that are set up (e.g., email, VoIP telephony, document sharing, remote desktop, data storage, industrial remote device control). CommLock Connect is cryptographically bound to the CommLock Server providing the secure and trusted VPN to the private cloud / network architecture.

Who Needs CommLock:

- Remote Office Networking - Frequent business travelers, Federal employees, travelers to high-risk locations, and remote employees all demand secure communications.
- Industrial Device Networking - As CommLock Connect doesn't require any software to be loaded on the end device, it is perfect for protecting everything from HVAC units to the nations most critical electrical distribution grids.
- Secure Intranet Office Networking / Enclaves - Protecting data passing through the enterprise LAN segments can be achieved by simply adding CommLock Connect between two LAN end points.

At-A-Glance

Hardware-based VPN protection for:

- Computers
- SCADA equipment
- Healthcare devices
- Mobile platforms

Benefits:

- Security
- Plug-n-Protect
- Sustained 6-10Mbps with some models achieving almost 20Mbps
- Efficiency
- Hardware vs. Software Security - no software vulnerabilities to worry about

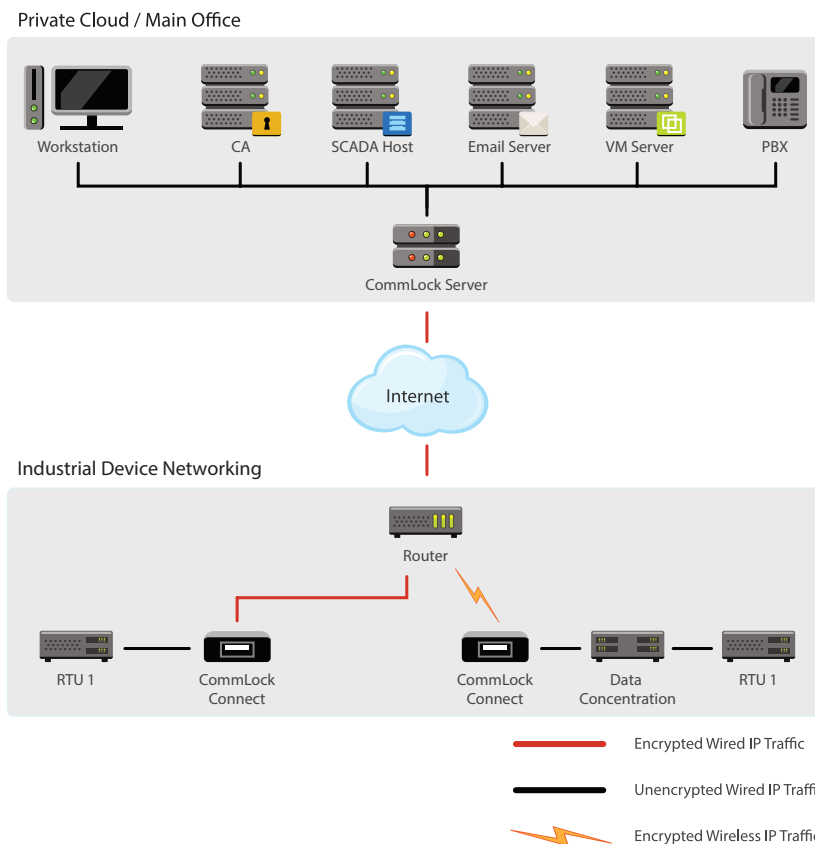
World-class technology to defeat threats

- Replaces your current network connectivity with secure network connectivity
- Secure key/certificate management
- Isolates and protects the endpoint from malicious network activity
- Can be deployed as a Bump-In-The-Line or embedded into an endpoint
- Simple and flexible interfaces (i.e. USB, Ethernet, Serial)
- Plug and Play (no cryptographic knowledge required through setup UI)
- Reduces Time-to-Market for OEMs requiring network security functionality
- Secures any IP-based network
- Wireless security requires WPA2 or better to be implemented
- Small form factor with the WiFi version being 3.4"x2.7"x .45" and the Ethernet version being 3.3"x2.2"x1"
- Custom hardware enclosures and software configurations can be provided

VPN

- VPN system is isolated from the endpoint
- Multiple VPN configurations can be loaded on a single CommLock device

CommLock Connect Industrial Device Networking



VPN Security

- Standards-based or Proprietary
- SSL/TLS Secure Protocol Key Exchange
- Encryption scheme used is configurable for mission (e.g., strongSwan, AES, IPsec, and ECC)

Server Specifications

- VM capable
- 1U dual core

Network Interfaces

- Ethernet IEEE 802.3 Base TX
- USB
- Serial via USB Interface
- WiFi (802.11 b/g/n)

Power Supply

- Via USB interface (5V at 500mA) with WiFi only
- AC adapter (5A at 100-240V)



For more information or to
schedule a demo, contact us at:

info@charontech.com

(703) 662-6061