HERA
Powered by waterfall

Hardware-Enforced Remote Access for OT Networks

HERA® integrates robust hardware-enforced cybersecurity protections with enterprise-grade remote access capabilities, ensuring safe and secure remote access, made for OT environments and cyber-physical assets.

Hardware-enforced Protections

Hardware-enforced security at the site perimeter
HERA ensures OT systems remain secure by leveraging robust hardware-based measures.

Isolated communication between client and site
Communication channels are non-routable, minimizing opportunity for attack pivoting.

Client application security reinforced
A combination of application security and TPM provide the strongest client security, far surpassing browser-based alternatives.

Enterprise-grade Remote Access Experience

Management
User Management
Session moderation
Zero Trust Controls
Multi-site management
Active directory integration
MFA support

Audit
Session recording
SIEM reporting
Logging

Supported Protocols
SSH
RDP
VNC

Bandwidth
Requires low-bandwidth. Fully functional in unstable networks

Benefits

Security-first Design
Prioritizing cybersecurity in every aspect.

Maintain Physical Segregation
A solid barrier against cyber threats.

Minimal Increase to Attack Surface
Reduces risk and exposure.

Full-featured Remote Access Solution
Comprehensive tools for modern OT requirements.

Proven Security Pedigree
Decades of experience distilled into every Waterfall Security product.

How it works

HERA Client

The HERA client uses simple and filterable protocols to separately:

- Capture and encrypt keystrokes and mouse moves before sending to HERA Gateway.
- Receive screen captures from HERA Gateway, decrypted and displayed.

Communication channels are non-routable, minimizing exposure to external threats.

The HERA client utilizes the hardware Trusted Platform Module (TPM) for:

- Key storage.
- Hardware restricted user access.

Encryption keys remain protected from software-based attacks. Hardware-user coupling eliminates the risk of session hijacking or credential theft.

HERA Gateway

The HERA Gateway is comprised of two unidirectional gateways, each physically able to send information in only one direction.

- Inbound HERA with hardware filters to receive, decrypt, validate, and filter user keystrokes and mouse movements.
- Outbound HERA to encrypt and send screen captures to the user.

HERA ensures that OT networks remain isolated from external TCP/IP traffic.

HERA Gateway includes an internal app for activating user actions on local systems and computers.

Remote Access, Without Network Connectivity

Free Consultation