HERA
Powered by waterfall

Hardwaregestützter Fernzugriff für OT-Umgebungen

HERA® integriert robuste hardwaregestützte Cybersecurity-Maßnahmen mit Funktionen für den Fernzugriff. Dies gewährleistet einen sicheren Remote Access speziell für OT-Umgebungen und physische Systeme.

Hardwaregestützte Schutzmaßnahmen

Hardwaregestützte Sicherheit am Standort
HERA gewährleistet die Sicherheit von OT-Systemen durch den Einsatz robuster hardwarebasierter Maßnahmen.

Isolierte Kommunikation zwischen Client und Standort
Die Kommunikations-kanäle sind nicht routingfähig. Das minimiert die Möglichkeit eines Angriffs auf den Standort.

Verstärkt Anwendungssicherheit für den Client
Die Kombination aus Anwendungssicherheit und TPM übertrifft browserbasierte Alternativen bei weitem.

Sicherer Fernzugriff für Unternehmen

Management
Benutzerverwaltung
Moderierte Sessions
Zero-Trust-Kontrollen
Multi-Site Management
Active-Directory-Integration
MFA-Unterstützung

Auditing
Aufzeichnung von Sessions
SIEM Reporting
Logging

Unterstützte Protokolle
SSH
RDP
VNC

Bandbreite
Beansprucht geringe Bandbreite
Voll funktionsfähig auch unter instabilen Netzwerkbedingungen

Vorteile

Security-First Design
Cybersicherheit hat bei allen Belangen Vorrang.

Setzt physische Trennung durch
Eine solide Barriere gegen Cyberangriffe.

Minimiert die Angriffsfläche
Senkt das Risiko und minimiert das Gefährdungspotenzial.

Mit allen Funktionen ausgestattete Remote-Access-Lösung
Umfassende Tools gemäß moderner OT-Anforderungen.

Bewährte Sicherheitsphilosophie
In jedem einzelnen Produkt von Waterfall Security steckt jahrzehntelange Erfahrung.

Und so funktioniert es

HERA-Client

Der HERA-Client verwendet einfache und filterbare Protokolle, um separat:

- Tastatureingaben und Mausbewegungen zu erfassen und verschlüsselt an das HERA-Gateway zu senden.
- Bildschirmaufnahmen vom HERA-Gateway zu empfangen, zu entschlüsseln und anzuzeigen.

Die Kommunikationskanäle sind nicht routingfähig, was die Gefährdung durch Bedrohungen von außen minimiert.

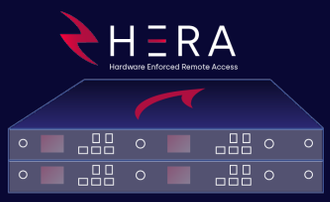
Der HERA-Client nutzt die Hardware des Trusted Platform Module (TPM) zur

- Schlüsselspeicherung
- und für einen auf bestimmte Hardware beschränkten Benutzerzugriff.

Die Verschlüsselungscodes bleiben vor softwarebasierten Angriffen geschützt. Die Hardware-Benutzer-Kopplung beseitigt das Risiko von Session Hijacking und den Diebstahl von Benutzerdaten.

HERA-Gateway

Das HERA-Gateway besteht aus zwei unidirektionalen Gateways, von denen jedes physisch nur dazu in der Lage ist, Informationen in eine Richtung zu senden.



- Das Inbound-Gateway von HERA verfügt über Hardware-Filter zum Empfangen, Entschlüsseln, Validieren und Filtern von Tastatureingaben und Mausbewegungen der Benutzer.
- Das Outbound-Gateway von HERA verschlüsselt den Bildschirmausschnitt und sendet ihn an den Remote User.

HERA sorgt dafür, dass OT-Netze zuverlässig vom externen TCP/IP-Verkehr isoliert bleiben.

Das HERA-Gateway verfügt über eine interne App zur Aktivierung von Benutzeraktionen auf lokalen Systemen und Computern.

Remote Access ohne Netzanbindung

Kostenlose Beratung