ARMOR ID

Proteja sus accesos con MFA, sin cambiar los equipos que ya tiene.

Armor ID agrega un segundo factor a sus VPN, firewalls, escritorios remotos y al inicio de sesión de Windows. Funciona con equipos de múltiples marcas y corre en sus propios servidores.

20+
marcas de firewall, VPN y equipos de red compatibles por RADIUS estándar

4
formas de segundo factor para sus usuarios

0
datos de sus usuarios fuera de su red

1
consola para políticas, usuarios y auditoría

CÓMO SE CONECTA A SU RED



Multimarca

Un solo servidor de MFA para equipos de distintos fabricantes. No lo ata a una marca.

En sus servidores

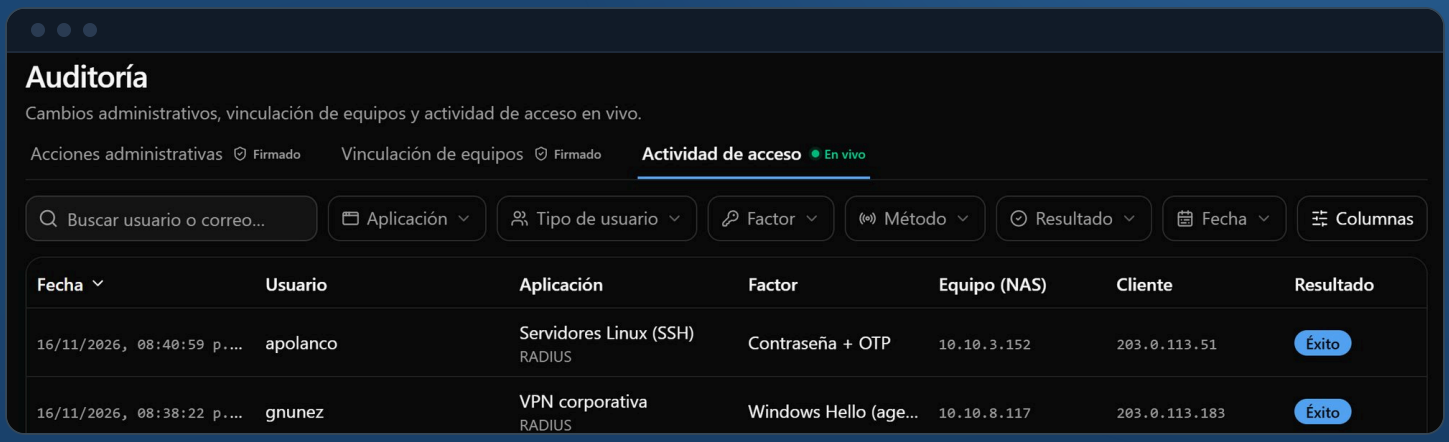
Se instala en su infraestructura, incluso sin salida a internet. Sus datos no salen de su casa.

Trazable

Cada acceso, aceptado o negado, queda en una bitácora encadenada que delata cualquier alteración.

LA CONSOLA

Cada acceso, a la vista.



Auditoría: quién entró, desde dónde, a qué equipo y con qué factor. Captura con datos de ejemplo.

Qué protege

- VPN SSL e IPsec
- Acceso administrativo firewalls y equipos de red
- Escritorio remoto RD Gateway · RD Web
- Inicio de sesión de Windows local y RDP
- Servidores Linux SSH
- Aplicaciones web SAML 2.0

Cómo confirma

- Código de app TOTP
- Aprobación por correo
- Windows Hello con el agente de Armor ID
- Llave FIDO2 consola y portal
- Usuarios de Active Directory o LDAP
- Usuarios locales personal externo

Estándares

- RADIUS RFC 2865
- RadSec RFC 6614
- TOTP RFC 6238
- SAML 2.0
- FIDO2 / WebAuthn
- LDAP y LDAPS

REQUISITOS DEL SERVIDOR

4 vCPU	8 GB	100 GB	24.04 LTS
procesador	de RAM · 16 GB recomendado	de disco en SSD	Ubuntu Server

DESPLIEGUE	En sus instalaciones, en contenedores · instalación sin internet disponible
SEGURIDAD	Message-Authenticator obligatorio · secretos cifrados con AES-256 · bitácora encadenada

¿Quiere verlo funcionando con sus equipos?

www.har-per.com