ARMOR ID



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

Autenticación multifactor para toda su red. Cualquier marca. En sus servidores.

HARPER

www.har-per.com

QUÉ ES ARMOR ID

Un segundo factor en cada puerta de entrada.

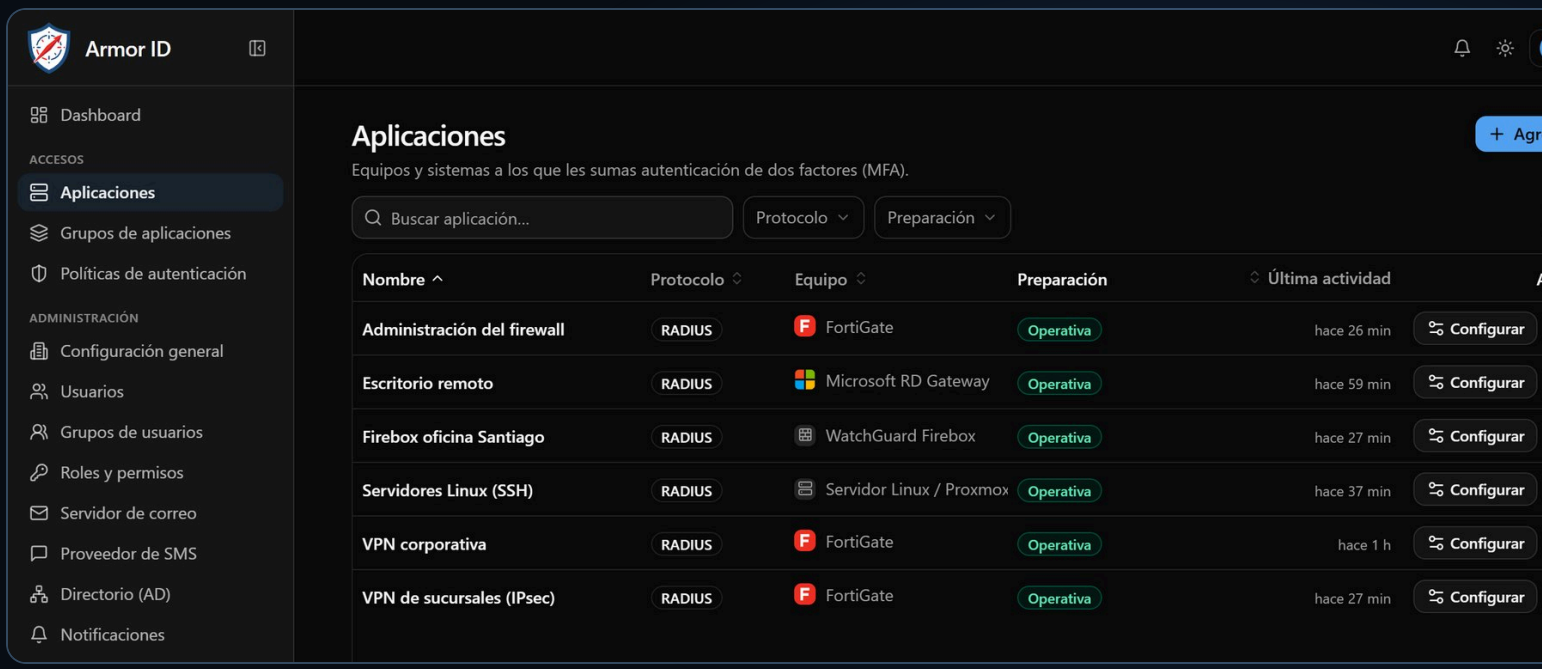
Una contraseña robada abre la VPN, el firewall o el escritorio remoto de cualquier empresa. Armor ID le suma a cada acceso un factor que el atacante no tiene, sin reemplazar sus equipos.

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

4
formas de segundo factor: código de app, correo, Windows Hello y llave FIDO2

0
datos de sus usuarios fuera de su red: corre en sus servidores

1
consola para políticas, usuarios, equipos y auditoría



La consola de Armor ID: equipos de cuatro fabricantes protegidos desde un mismo lugar.

Multimarca

Un solo servidor de MFA para firewalls, VPN y escritorios remotos de distintos fabricantes. No lo ata a una marca.

En sus servidores

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

Trazable

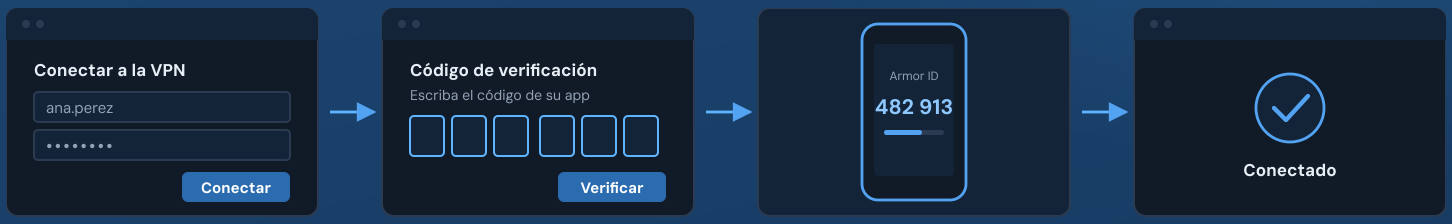
Cada acceso, aceptado o negado, queda en una bitácora encadenada que delata cualquier alteración.

CÓMO FUNCIONA

Se conecta como siempre. Entra solo si confirma.

El equipo le pasa la contraseña a Armor ID, que la valida contra su directorio y le pide el segundo factor al usuario. Solo si lo confirma, el equipo lo deja pasar.

ASÍ LO VIVE EL USUARIO · UN ACCESO A LA VPN CON CÓDIGO DE APP



Escribe su contraseña
la misma de Windows

El equipo pide el código
Armor ID ya validó la contraseña

Lo lee en su teléfono
sin necesitar datos ni señal

Entra, y queda registrado
si el código falla, no pasa

ASÍ SE CONECTA A SU RED



Si el usuario no confirma, el acceso se niega y queda registrado.

CAPACIDADES

Funciones poderosas, beneficios claros.

Lo que pide para confirmar, lo que protege y cómo se mantiene bajo control.

Factores

Cuatro formas de confirmar que quien entra es quien dice ser.

Código de app

Google o Microsoft Authenticator. Funciona aunque el teléfono no tenga datos.

Aprobación por correo

El usuario aprueba o rechaza el intento con un clic, en equipos que no tienen dónde escribir un código.

Windows Hello

Aprobación en el propio equipo con rostro, huella o PIN, mediante el agente de Armor ID.

Llaves FIDO2

Para la consola y el portal, con una llave física y sin códigos que se puedan robar.

Accesos

Los equipos, sistemas y directorios a los que se conecta.

Multimarca

Firewalls, VPN y escritorios remotos de distintos fabricantes, protegidos desde un mismo lugar.

Inicio de sesión de Windows

MFA al entrar al equipo y por escritorio remoto (RDP).

Inicio de sesión único

Aplicaciones web por SAML 2.0, con Armor ID como proveedor de identidad.

Active Directory

Sincroniza usuarios por LDAP o LDAPS, y suma usuarios locales para personal externo.

Control

Lo que queda registrado, quién administra y dónde viven sus datos.

Bitácora a prueba de alteraciones

Registros encadenados y firmados: cualquier cambio en el historial se detecta.

Roles y permisos

Cada administrador ve y hace solo lo suyo, y cada cambio deja rastro.

Instalación sin internet

Se despliega en contenedores en sus servidores, también en redes aisladas.

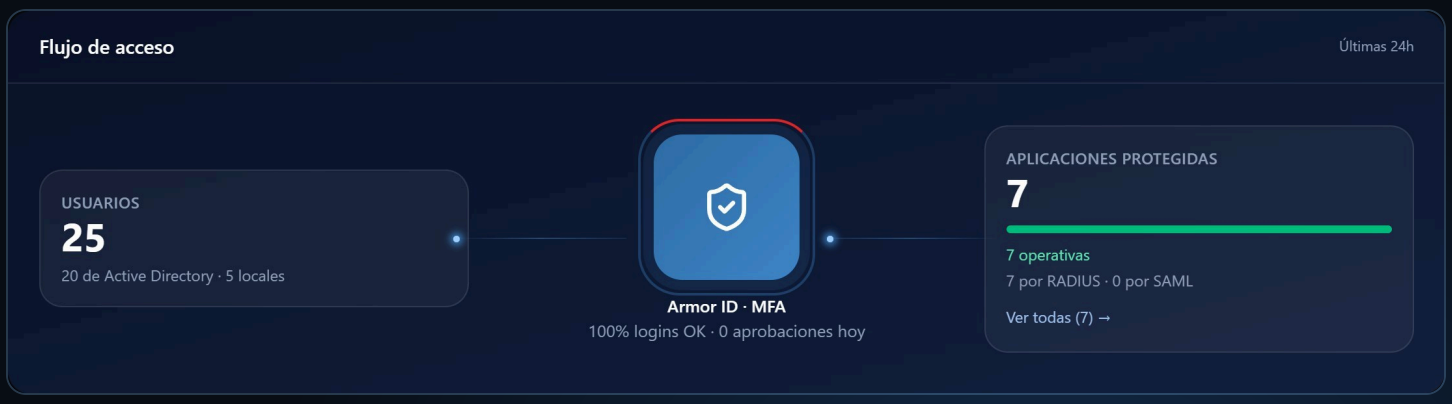
Cifrado AES-256

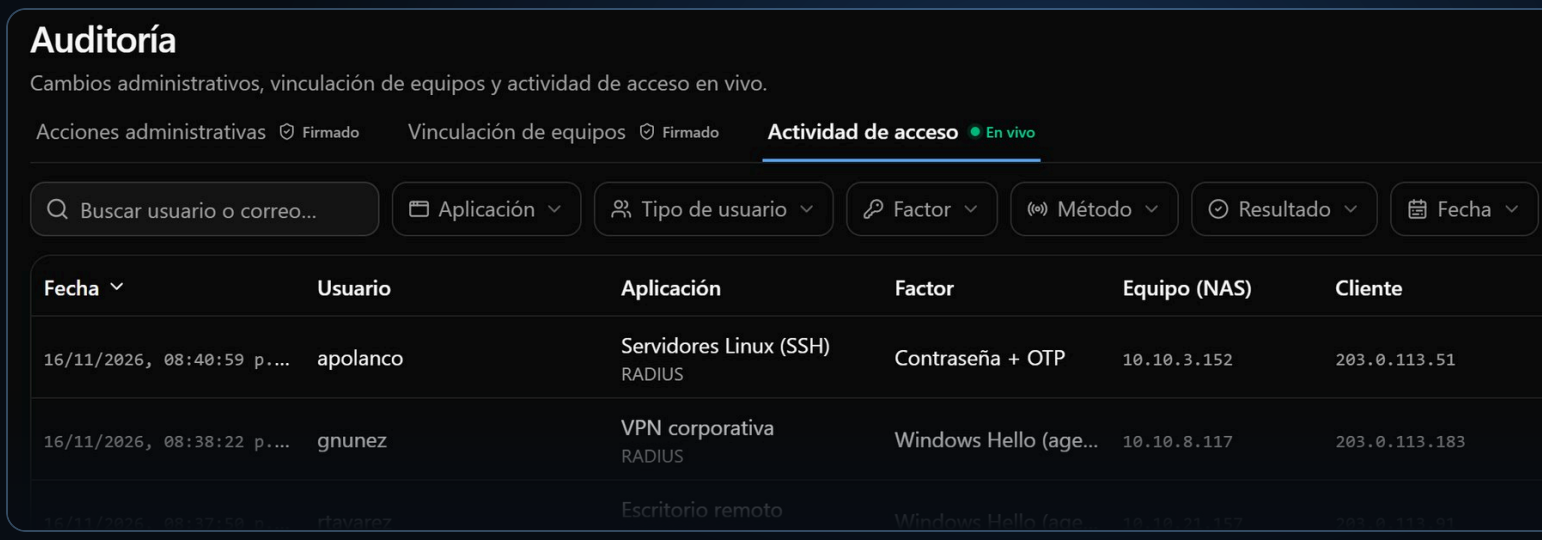
Los secretos se guardan cifrados, con una llave propia para cada organización.

LA CONSOLA

Todo a la vista, en tiempo real.

Cada intento de acceso queda registrado con quién, desde dónde, en qué equipo y con qué factor.







El tablero, la auditoría en vivo y las métricas de acceso por aplicación y por origen de los usuarios.

Políticas por equipo

Qué factor se pide en cada VPN, firewall o escritorio remoto.

Enrolamiento guiado

El usuario activa su factor solo, desde un enlace.

Quién puede entrar

Cada aplicación abierta a todos o solo a ciertas personas y grupos.

INTEGRACIONES

Compatible con más de 20 marcas.

Si su equipo autentica por RADIUS, puede usar Armor ID. No depende del fabricante: depende del estándar.

Por tipo de acceso

- VPN SSL
- VPN IPsec contraseña y código en un paso
- Acceso administrativo a equipos de red
- Escritorio remoto RD Gateway · RD Web
- Inicio de sesión de Windows local y RDP
- Servidores Linux por SSH
- Aplicaciones web por SAML
- Portales cautivos

Por protocolo

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

Por fabricante

y otros fabricantes compatibles con el estándar RADIUS

Fortinet	Cisco	Palo Alto Networks	Check Point	Juniper Networks
WatchGuard	SonicWall	Sophos	Ivanti	F5
Citrix	Barracuda	Forcepoint	Huawei	Hillstone Networks
Stormshield	Zyxel	MikroTik	Ubiquiti	HPE Aruba
Extreme Networks	Ruckus	pfSense	OpenVPN	Microsoft

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
DIRECTORIO	Active Directory o LDAP · usuarios locales
SEGURIDAD	Message-Authenticator obligatorio · secretos cifrados con AES-256 · bitácora encadenada

ARMOR ID

¿Por qué Armor ID?

Porque protege con MFA lo que hoy solo cuida una contraseña, con los equipos que ya tiene, sin sacar sus datos de su red y con un registro de cada acceso que cualquier auditor puede revisar.

Multimarca

un solo servidor de MFA para todos sus fabricantes

Local

instalado en sus servidores, incluso sin internet

Trazable

cada acceso registrado en una bitácora encadenada



Solicite una demostración

www.har-per.com