ARMOR ID



Protect every login with MFA, without replacing the equipment you own.

Multi-factor authentication for your whole network. Any vendor. On your servers.

HARPER

www.har-per.com

WHAT ARMOR ID IS

A second factor at every point of entry.

A stolen password opens the VPN, the firewall or the remote desktop of any company. Armor ID adds to every login a factor the attacker does not have, without replacing your equipment.

20+

firewall, VPN and network vendors compatible through standard RADIUS

4

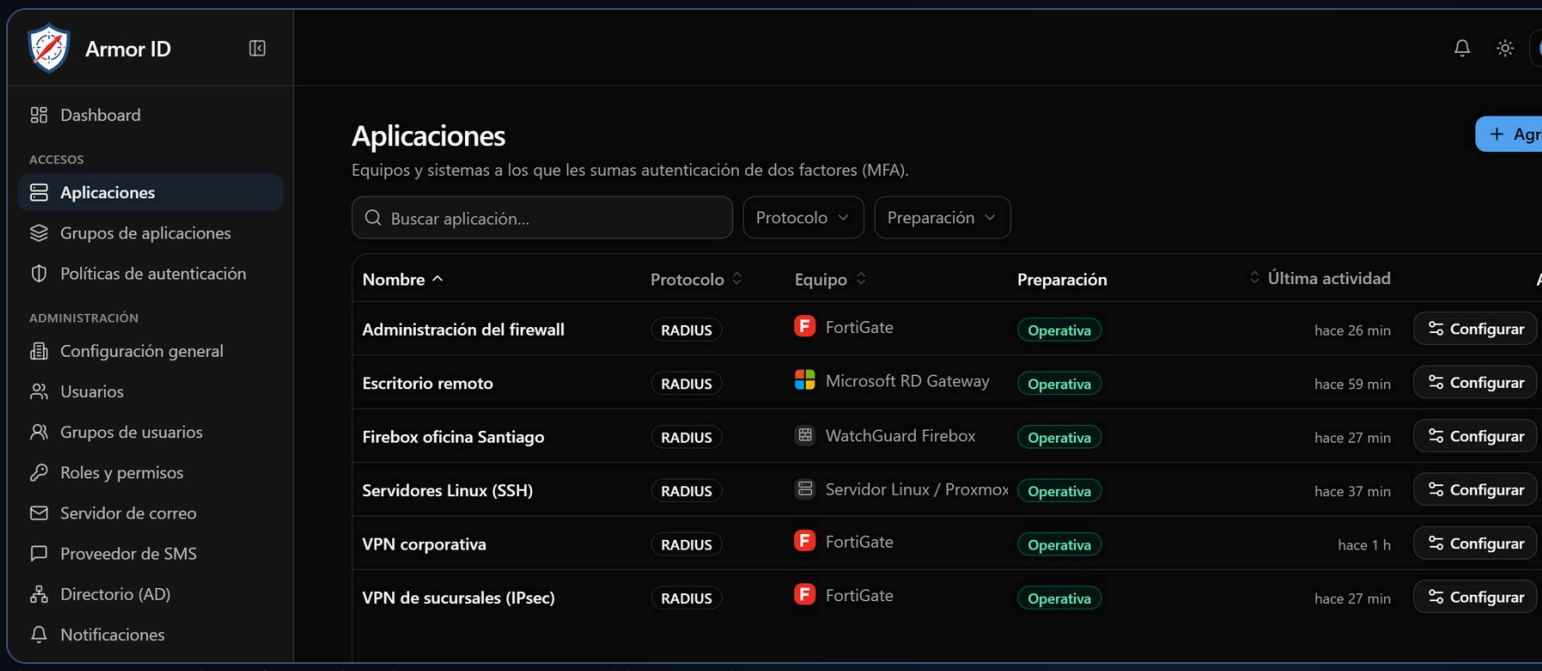
second-factor methods: app code, email, Windows Hello and FIDO2 key

0

user data leaving your network: it runs on your servers

1

console for policies, users, devices and auditing



The Armor ID console: equipment from four vendors protected from one place.

Multi-vendor

One MFA server for firewalls, VPNs and remote desktops from different vendors. No lock-in to a single brand.

On your servers

Installed in your infrastructure, even with no internet access. Your users' data never leaves your premises.

Traceable

Every login, accepted or denied, is written to a chained log that exposes any tampering.

HOW IT WORKS

Sign in as usual.
Get in only once confirmed.

The device hands the password to Armor ID, which validates it against your directory and asks the user for the second factor. Only when it is confirmed does the device let the user in.

WHAT THE USER SEES · A VPN LOGIN WITH AN APP CODE



Types the password
the same one used in Windows

The device asks for the code
Armor ID already validated the password

Reads it on the phone
no data or signal needed

Gets in, and it is logged
a wrong code does not get in

HOW IT CONNECTS TO YOUR NETWORK



If the user does not confirm, access is denied and logged.

CAPABILITIES

Powerful features, clear benefits.

What it asks for to confirm, what it protects and how it stays under control.

Factors

Four ways to confirm that whoever signs in is who they claim to be.

App code

Google or Microsoft Authenticator. Works even when the phone has no data.

Email approval

The user approves or rejects the attempt with one click, on devices with nowhere to type a code.

Windows Hello

Approval on the device itself with face, fingerprint or PIN, through the Armor ID agent.

FIDO2 keys

For the console and the portal, with a physical key and no codes that can be stolen.

Access

The equipment, systems and directories it connects to.

Multi-vendor

Firewalls, VPNs and remote desktops from different vendors, protected from one place.

Windows sign-in

MFA when signing in to the computer and over remote desktop (RDP).

Single sign-on

Web applications over SAML 2.0, with Armor ID as the identity provider.

Active Directory

Syncs users over LDAP or LDAPS, and adds local users for external staff.

Control

What gets logged, who administers and where your data lives.

Tamper-evident log

Chained and signed records: any change to the history is detected.

Roles and permissions

Each administrator sees and does only their part, and every change leaves a trail.

Offline installation

Deployed in containers on your servers, including isolated networks.

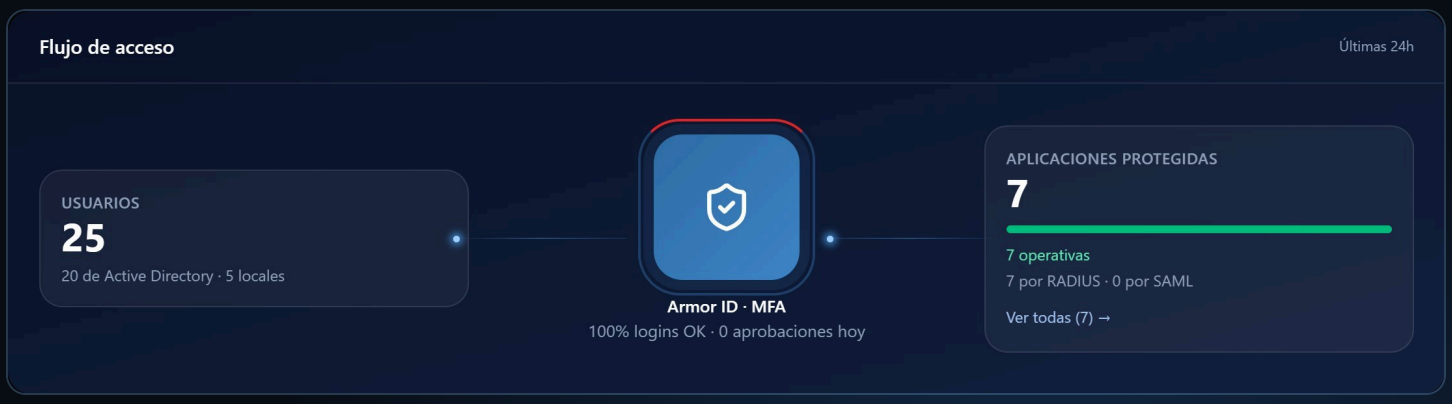
AES-256 encryption

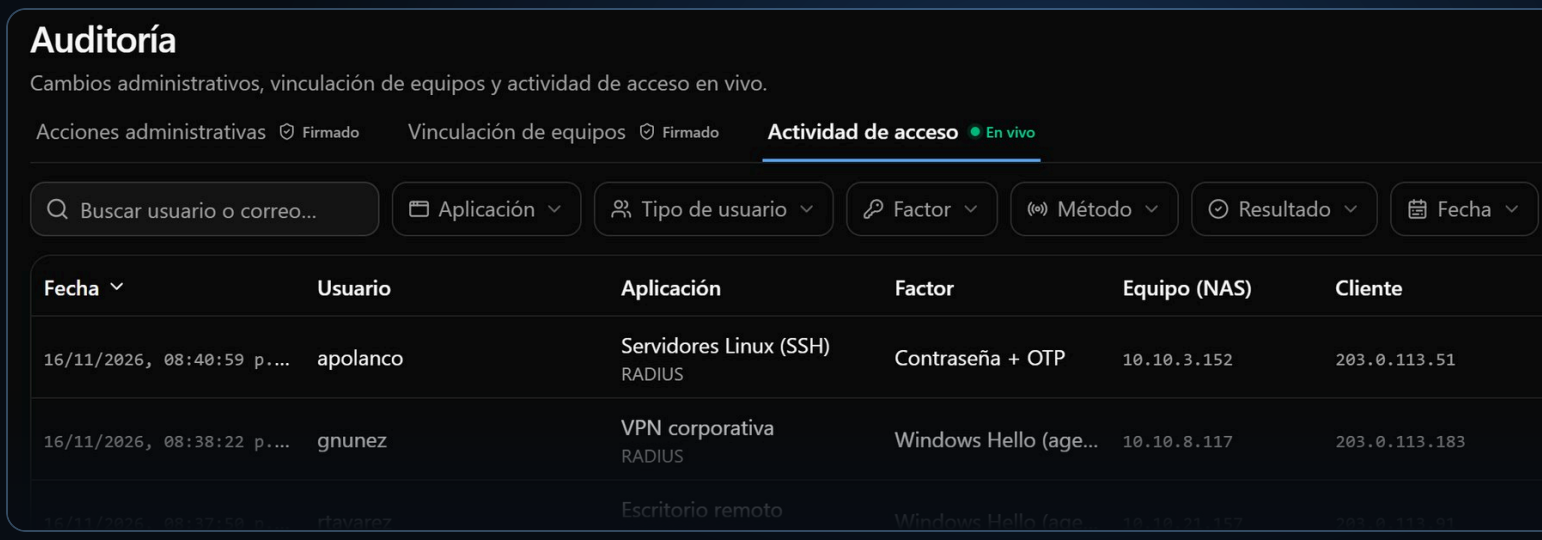
Secrets are stored encrypted, with a dedicated key for each organization.

THE CONSOLE

Everything in view, in real time.

Every login attempt is recorded with who, from where, on which device and with which factor.







The dashboard, the live audit trail and access metrics by application and by user source.

Policies per device

Which factor is required on each VPN, firewall or remote desktop.

Guided enrollment

Users activate their factor on their own, from a link.

Who can get in

Each application open to everyone or only to certain people and groups.

INTEGRATIONS

Works with more than 20 vendors.

If your equipment authenticates over RADIUS, it can use Armor ID. It does not depend on the vendor: it depends on the standard.

By access type

- SSL VPN
- IPsec VPN password and code in one step
- Administrative access to network equipment
- Remote desktop RD Gateway · RD Web
- Windows sign-in local and RDP
- Linux servers over SSH
- Web applications over SAML
- Captive portals

By protocol

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

By vendor

and other vendors compatible with the RADIUS standard

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

SERVER REQUIREMENTS

4 vCPU	8 GB	100 GB	24.04 LTS
processor	RAM · 16 GB recommended	SSD storage	Ubuntu Server

DEPLOYMENT	On-premises, in containers · offline installation available
DIRECTORY	Active Directory or LDAP · local users
SECURITY	Message-Authenticator required · secrets encrypted with AES-256 · chained log

ARMOR ID

Why Armor ID?

Because it protects with MFA what only a password guards today, with the equipment you already own, without taking your data out of your network and with a record of every login that any auditor can review.

Multi-vendor

one MFA server for all your vendors

On-premises

installed on your servers, even offline

Traceable

every login recorded in a chained log



Request a demo

www.har-per.com