ARMOR ID

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

Armor ID adds a second factor to your VPNs, firewalls, remote desktops and Windows sign-in. It works with equipment from multiple vendors and runs on your own servers.



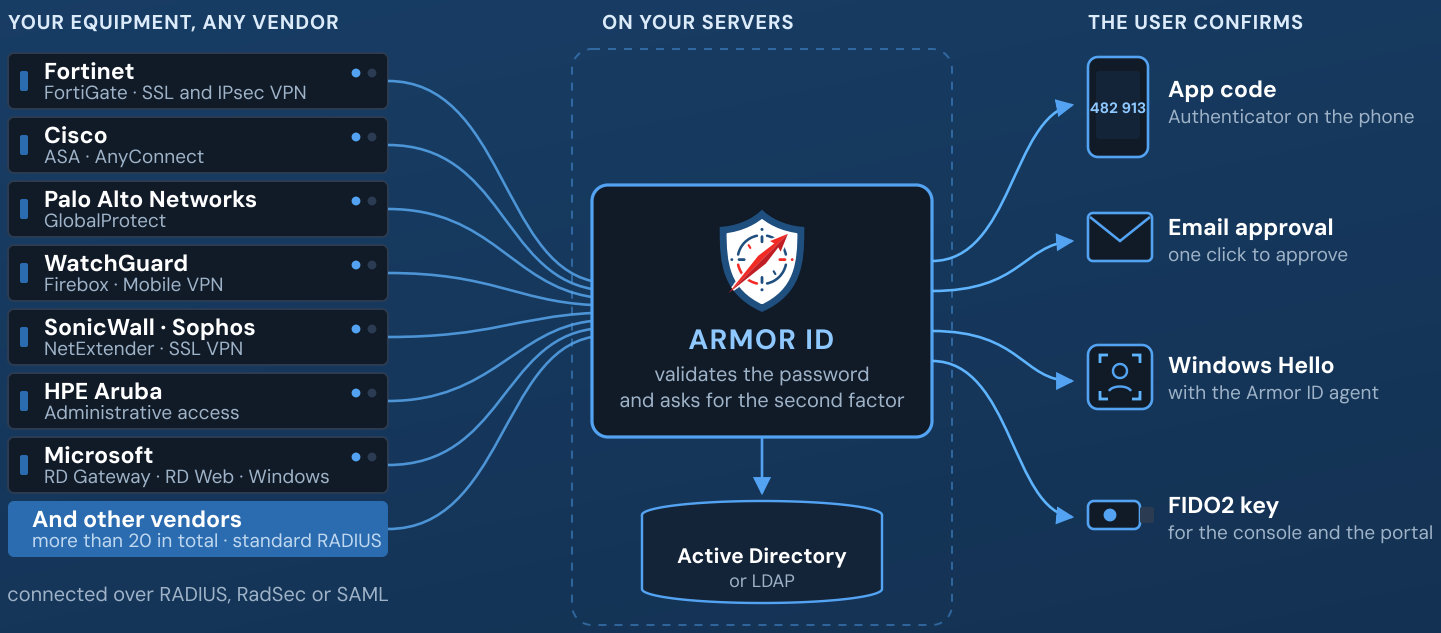
20+
firewall, VPN and network vendors compatible through standard RADIUS

4
second-factor methods for your users

0
user data leaving your network

1
console for policies, users and auditing

HOW IT CONNECTS TO YOUR NETWORK



Multi-vendor

One MFA server for equipment from different vendors. No lock-in to a single brand.

On your servers

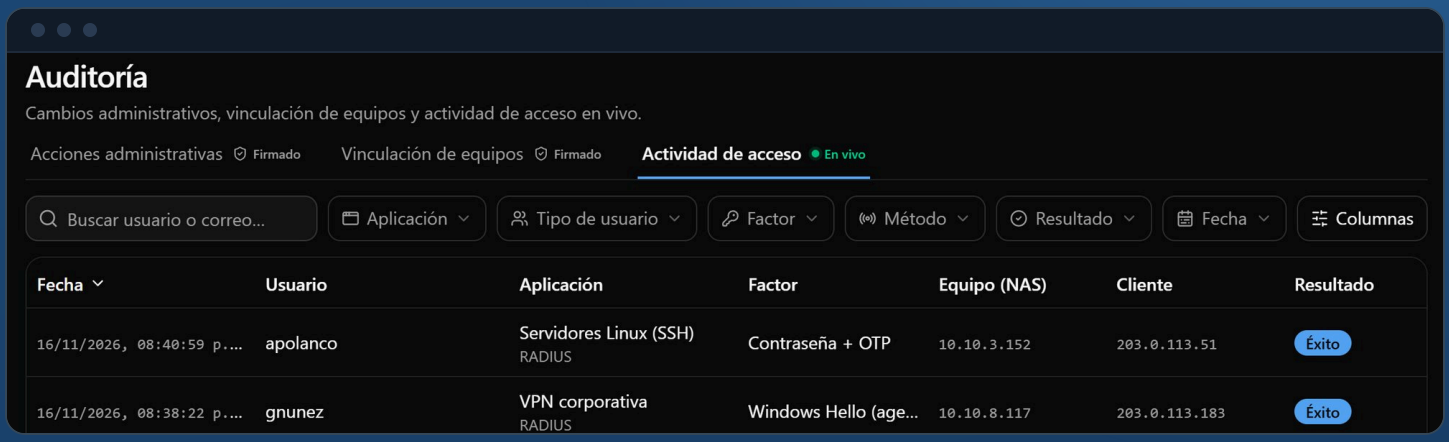
Installed in your infrastructure, even with no internet access. Your data never leaves your premises.

Traceable

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

THE CONSOLE

Every login, in plain sight.



Audit trail: who signed in, from where, to which device and with which factor. Screenshot with sample data, console shown in Spanish.

What it protects

- SSL and IPsec VPN
- Administrative access firewalls and network equipment
- Remote desktop RD Gateway · RD Web
- Windows sign-in local and RDP
- Linux servers SSH
- Web applications SAML 2.0

How it confirms

- App code TOTP
- Email approval
- Windows Hello with the Armor ID agent
- FIDO2 key console and portal
- Active Directory or LDAP users
- Local users external staff

Standards

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

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
SECURITY	Message-Authenticator required · secrets encrypted with AES-256 · chained log

Want to see it working with your equipment?

www.har-per.com