BARDIN GATE
Secure data transfer between isolated networks

Catalog 4 of 4

ARP

AIR-GAP REGULATED PIPELINE

2U RACK-MOUNT APPLIANCE

Security and operations: an appliance that looks after itself

Security comes from the structure of the appliance and operation is painless by design: guided setup, signed updates with automatic fallback, and a unit that repairs itself.

For: Security specialists and the operations team

In this catalog: Commissioning, updating and rolling back, self-repair, replacement and recovery, and installing the appliance

https://www.bardin.tech/en/bardingate-arp/

ARP's security is not a feature on top of the product; it is the structure of the appliance. If any layer fails, the appliance closes rather than carrying on wrongly.

Safe network — — **Unsafe network**

Your two networks stay separate and are never physically connected to each other; the 2U rack-mount appliance is attached to only one of them at any moment.

Physical isolation

A physical switch inside the appliance joins one of the two networks at a time and fully disconnects the first before joining the other. At every start everything is disconnected first, and the disconnected state is proved by the switch's own feedback, not by a command having run.

Trusted start

UEFI Secure Boot, boot measured into a TPM 2.0 chip and a read-only system verified block by block with dm-verity. The boot chain is built once and is the same on every unit.

Data at rest

Data is encrypted from first boot with LUKS2 and AES-256-XTS. The key is released only to a start signed by the vendor, and the recovery secret is shown once to the commissioning operator.

Isolated inspection

Parsers and inspection engines run in rootless containers with AppArmor, seccomp, no network, a read-only root and resource ceilings. Every failure ends closed.

Intelligence on the appliance

Files are judged by their real bytes. An offline AI model can hold a file back, never let one through, and unusual flows raise alerts.

Identity and access

- **The appliance is the only authority.** The browser, imported files and everything else bring claims; none can grant authority.
- **The default is deny.** Roles carry an explicit scope, and a permission not written is a refusal.
- **Password, and the password again.** High-risk actions (roles, security policy, licence and update import, time correction, recovery, configuration import) ask for it again.
- **No back door.** There is no vendor master password, hidden account, email reset or unaudited bypass. Recovering the last administrator is a physical procedure at the unit.
- **SSH reaches only a restricted support account.** It returns reports, logs and status and nothing more; root has no SSH login and there is no routine shell or direct database access.

Audit and SIEM

Property	Value
Append-only, tamper-evident	Each event is chained to the previous hash; a segment closes at 10,000 events or one hour and its checkpoint is signed.
What is recorded	Every security, administrative and business-critical attempt and outcome, correlated; denied high-risk actions included.
Trusted time	Offline; the appliance keeps the security clock itself and a clock anomaly cannot extend a licence or retention deadline.
SIEM	One-way, typed export to your SIEM; TCP over TLS by default, optional mTLS, RFC 5424 JSON or CEF; addresses pseudonymized. Plaintext or UDP needs an acknowledged, audited warning.
Never exported	File content, credentials, tokens and private keys.

Day to day: look, approve, that is all

The operator looks at the dashboard and the approver approves. No SSH, scripts or schedules are needed; the appliance looks after itself as far as it can and, where it cannot, tells you why.

Commissioning, guided

1. **Rack it**
   Mount the 2U appliance and connect power and the Safe, Unsafe and management networks.
2. **Open the console**
   Open the console in a browser. A code on the appliance's own display proves you are at the unit.
3. **Guided setup**
   Steps run in order and each tests itself: hardware, time, network addresses and the first administrator.
4. **Accept**
   Take the signed commissioning evidence bundle; the appliance is ready for work.

The procedure is ordered and mandatory. The disk's recovery secret is shown once, on the commissioning page, to the person at the unit.

Updating and rolling back

- **Packages are signed and offline.** One without a valid signature, or below the recorded release sequence, is refused (anti-rollback); ordinary downgrade is prohibited.
- **Two slots.** An update is written to the other slot, booted once as a trial and committed only after health checks pass; otherwise the unit falls back to the previous version by itself.
- **Data is separate from software.** ClamAV signatures, YARA rules and validation schemas arrive in a data-only package that never changes software.

Self-repair

The appliance assumes nobody can reach it, so it repairs itself. It has no workstation, screen or routine SSH, and no recovery design may require reaching a failed unit.

Level	What it does	What survives
Soft reset	Returns software to the last known-good state; the same mechanism an update's fallback uses.	Identity, configuration, logs and audit
Hard reset	Returns the unit to its pre-commissioning state; it erases rather than restores.	Nothing; export the audit first

Replacement and recovery

Situation	The right path
One failed disk	Replace per the runbook; the volume stays healthy or recoverable.
Power supply or fan	Vendor procedure under maintenance, then re-check readiness.
Motherboard or security chip	The appliance asks for the recovery secret once, at the unit; it keeps its identity, configuration and licence.
Whole appliance lost	A replacement appliance: fresh commissioning, configuration import, secrets re-entered and endpoints re-established. The old identity is never cloned.

ARP's configuration file carries every route and policy but no secrets. After importing it, only the SSH keys need to be entered again and the hosts pinned again.

The appliance and installation

Item	What it means
The appliance	A 2U rack-mount appliance, ready as delivered. There is no server, operating system or extra software to choose or install.
Space and power	2U of space in a standard rack, and power.
Network	A connection to the Safe, Unsafe and management networks. The first two are never joined to each other.
Day to day	Just a browser. The console speaks fourteen languages, Persian included.
Internet	Not needed; licence, updates and signatures are offline and signed.

An appliance that must run where nobody can reach it has to repair itself, and know when it must not carry on.

More about this product

CATALOG 1
Product overview

CATALOG 2
Routes and policy

CATALOG 3
Assurance and quarantine

For advice, a demonstration and contact details:
https://www.bardin.tech/en/bardingate-arp/

Specifications may change without notice.