



ART

AIR-GAP REGULATED TRANSFER



2U RACK-MOUNT APPLIANCE

Security and operations: the appliance and the Agent

From setting up the appliance to the key on the user's computer: security comes from structure and operation is painless by design, with guided setup, signed updates and simple recovery.

For: Security specialists and the operations team

In this catalog: The Agent as a security boundary, installing the appliance, commissioning, updating, and recovery

<https://www.bardin.tech/en/bardingate-art/>

In ART the security boundary includes the user's computer as well as the appliance's wall. No component inherits trust from its position and each authority validates its own input.



✗ **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.

The Agent is a boundary of its own



Key and identity

The Agent's key is made on the machine itself and kept in the operating system's secure store where the platform offers one. Enrolment is a certificate request plus an administrator's explicit approval, never a side effect of a successful install.



Encrypted spool

Each user's local copy is encrypted with a content key protected by the OS secure store and isolated by ACL; another user on the same computer cannot see it.



Channel

TLS 1.3 with mutual identity. Each Agent host has its own revocable device certificate; a hostname or IP is never an identity.



File integrity

Regular files only, links not followed; hashes at source and spool, quota, fixed destination roots, atomic publish and a final re-read. An arbitrary path never confers authority.

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.



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.

☰ 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.

✓ 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 Agent follows: your organization's signed package, a key made on the computer, the administrator's approval of enrolment, and a signed configuration bundle from the appliance. Installing the Agent is not approving its enrolment.

✦ Day to day: look, approve, that is all

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

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.

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.		
Replacement time target	8 hours from the moment hardware, packages, configuration and licence are available	Recovery point	The last verified configuration export
Not restored	In-flight transfers, retained content, active sessions and audit that was never exported	Senders	A request that never received a durable receipt may be sent again

The recovery time is a design target, not a measured commitment; it must be measured on your appliance before any contractual promise.

Trust is not inherited from one component's position to another; each authority validates its own input.

More about this product

CATALOG 1

Product overview

CATALOG 2

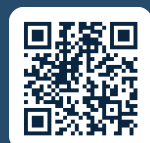
User experience

CATALOG 3

Content assurance

For advice, a demonstration and contact details:

<https://www.bardin.tech/en/bardingate-art/>



Specifications may change without notice.