



ART

AIR-GAP REGULATED TRANSFER



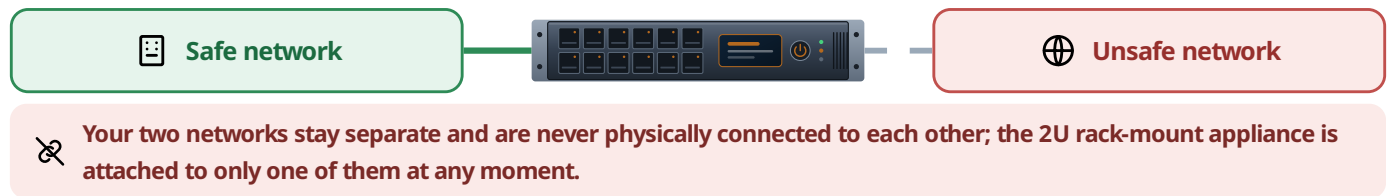
2U RACK-MOUNT APPLIANCE

Content assurance: from claim to evidence, before any delivery

Every Agent claim, file and piece of metadata is assumed hostile. The decision rests only on the bytes received, with named evidence and named versions.

For: Security specialists**In this catalog:** The ten checks in order, validation, offline anti-malware, and why anything unknown stops the transfer<https://www.bardin.tech/en/bardingate-art/>

ART never accepts that the file is what it is said to be. An Agent's claim serves only to reject the plainly forbidden early and never replaces the final check; the appliance always makes the final ruling on the stored bytes.



Ten steps, in order

1

Declared metadata

A cheap early refusal before receipt. Provisional.

2

Attestation

A signed statement from your own system, before receipt.

3

Durable integrity

SHA-256 is recomputed on the stored file.

4

Observed facts

Size, MIME type, archive and document structure; extracted once and shared.

5

Declared against observed

A mismatch is evidence; a claim never overrides what was observed.

6

Validation rules

Stateless rules over one immutable context.

7

Structured validation

JSON Schema 2020-12, XSD 1.0, CSV and field constraints.

8

bg-sign

The owner's detached signature, checked over the received bytes.

9

Inspection

ClamAV, YARA and the AI model in isolated workers.

10

Policy aggregation

Allow, reject, quarantine or approval; only policy decides.

No rule or engine rules by itself

Rules and engines only gather evidence. **Policy alone decides, and only the appliance's fixed process changes a transfer's state**, so no scanner, file reader or interface can declare anything clean.

Validation: what is actually checked

Area	Controls
Type and name	Extension and MIME are independent evidence; a mismatch is explicit and policy-controlled, and renaming never changes the observed type.
Archives	Nesting depth, entry count, expanded size, compression ratio, encrypted entries, path traversal, links and malformed structure. A limit breach fails without any unsafe extraction.
PDF and Office	Checked in an isolated process: active content, external relationships, macros, malformed parts and a failure to read the file are each recorded as a finding.
Structured data	JSON Schema 2020-12, XSD 1.0, a closed CSV schema and simple deterministic field constraints. These are validation, not DLP.
Resources	Every stage has time, memory and output limits. Running out of resources or failing to read the file is indeterminate, and the file does not pass.

Example: a "PDF" that is not a PDF

A file named .pdf whose bytes are not PDF is evaluated from the observed content and records a declared/observed mismatch as evidence; an Agent's early pass cannot make it valid.

Evidence is immutable and re-evaluation is additive

- Each evaluation is bound to the exact content, configuration, policy snapshot, profile, rule versions and input version. Publishing new configuration never rewrites a regulated transfer's evidence.
- A legitimate re-evaluation creates a new generation that links to the previous one and is audited; the previous stays.

ClamAV and YARA, offline



Signed sets

Signatures and rules are signed, versioned, immutable, activated atomically and recorded with every result.



One durable queue

Admission, persistence, restart recovery and backpressure live in one shared queue; there are no hidden queues inside engines.



Isolated workers

Rootless clamd on a local socket (no TCP); YARA with a limited number of parallel processes, one file at a time.

bg-sign signatures

A file's owner can place a detached signature in a filesystem attribute. The Agent only carries it and its claim is treated as hostile; the appliance checks the public key, the signer's authority and the signature over the SHA-256 of the received file. The private signing key never reaches the appliance.

When policy requires a valid signature, a missing, invalid, unsupported, untrusted or indeterminate one each has its own status, and the transfer does not go on.

External attestation

An organization can require its own system to have a say before a file is carried. That attester is outside the appliance and the Agent is only the carrier; the appliance verifies. The result acts before content is received and never loosens ART's own checks: even an acceptance does not make a file valid.

- The attested digest is compared twice with the file's: the second time before the durable receipt. An acceptance for one file cannot admit another.
- Absence and invalidity are different: an invalid one refuses under every mode.

A deterministic finding (ClamAV FOUND, YARA MATCH, a validation rejection) is never retried into a weaker engine or rule; an engine crash, timeout or malformed response is indeterminate, and the transfer does not go on.

✧ Nothing to tune day after day

Policy chooses which checks run and the checks run by themselves. Signatures and rules are updated with a signed offline data package, with no change to the software.

⊘ Anything unknown stops the transfer

Situation	Behaviour
Engine unavailable, crashed, timed out or answered malformed	Indeterminate; the transfer does not progress
The signature or rule set is incompatible with the engine	The appliance is not ready; admission waits
Required evidence is missing or its version unknown	Refusal, never a silent pass
An archive or resource limit was exceeded	Refusal with no unsafe extraction
A deterministic malicious finding	Quarantine; no retry with a weaker tool

🔒 The original stays out of reach

- Raw engine output, secrets, unrestricted rule internals and file content never appear in audit or user-visible errors.
- The sender gets the outcome and a reference code; an authorized role looks the evidence up by that code in the console, so the answer does not teach an attacker what passes.
- Safe preview shows only PNG pages made by an isolated worker; the browser never receives the original.

✓ What is tested

- Stage order, result uniqueness and a stable meaning whatever the order and parallelism of rules.
- A restart during inspection keeps one durable job and creates no duplicate outcome; a signature set is never mixed with another version within one attempt.

What could not prove itself does not cross; what crossed has proof.

More about this product

CATALOG 1

Product overview

CATALOG 2

User experience

CATALOG 4

Security and operations

For advice, a demonstration and contact details:

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



Specifications may change without notice.