



# ARP

AIR-GAP REGULATED PIPELINE



2U RACK-MOUNT APPLIANCE

## Content assurance and quarantine: nothing crosses unchecked

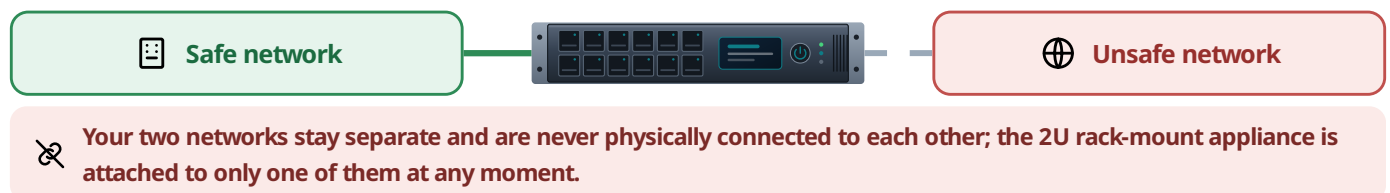
Before anything moves, every file passes two separate stages, deterministic validation and engine inspection. A check answers only yes or no, and every answer is recorded with the version that gave it.

**For:** Security specialists evaluating how content is checked

**In this catalog:** The seventeen validation rules, the three inspection engines, how a ruling is reached, quarantine, and the evidence that is kept

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

ARP treats filenames, extensions, declared types, archive structures and engine output as hostile input. Checks run only on the bytes hashed at admission and held inside the appliance, never on the source file, which is outside the trust boundary.

**2**separate stages:  
validation, inspection**17**deterministic validation  
rules**4**inspection engines: DLP,  
ClamAV, YARA, AI**0**bytes altered in the  
delivered file

### Two stages, two natures



#### Deterministic validation

Same input, same result. It asks "is the file what it claims, within what this route accepts?" It runs first, so a hostile archive never reaches an engine.



#### Engine inspection

Depends on installed signatures and rules: "is there something in this file we do not allow to cross?" Each engine is required or optional per route, and its version is recorded with the result.

### Yes or no, and no third answer

A check that ran has an answer. A check that did not run (engine crash, timeout) says nothing about the file; it is a mechanism failure and **never a quarantine**.

## Seventeen validation rules

| Group          | Rules                                                                                               | Protects against                                                                                                         |
|----------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Naming         | FilenameLength · IllegalChars · ReservedNames · MultiExtension · PathTraversal                      | Names that break, mislead or escape the destination filesystem, including reserved device names and traversal sequences. |
| Type           | ExtensionAllowlist · ExtensionBlocklist · MimeDetect · MimeExtensionMatch                           | Content that is not an accepted type, or whose detected type contradicts its extension.                                  |
| Size           | MaxFileSize                                                                                         | Files beyond what the route and the appliance are provisioned for.                                                       |
| Archive        | ArchiveDepth · ArchiveEntryCount · ArchivePathTraversal · ArchiveSymlink · ArchivePasswordProtected | Archive bombs, entries that escape extraction, outward links and encrypted contents that cannot be inspected.            |
| Active content | PdfActiveContent · OfficeActiveContent                                                              | Documents carrying embedded script or macros.                                                                            |

### “Encrypted” means “not inspectable”, not “malicious”

An encrypted archive is not judged malicious; it is content no engine can look inside. A route that accepts one has made a deliberate choice.

## Four inspection engines



### DLP

Four detector families: pattern, dictionary, label and entropy. It detects only, never masks or rewrites, and deliberately has no machine-learned scoring: results must be reproducible and explainable.



### ClamAV

Signature-based malware detection from a signed offline set; its version is recorded with every result.



### YARA

Rules for threats and prohibited content; signed sets, atomic activation and no mixing of versions.



### AI model

Runs on the appliance, offline, over what the fixed rules let through. It can hold a file back, never let one through; its version is recorded with every result.

## The ruling: from evidence to outcome

| What was found                                                             | Outcome                                        |
|----------------------------------------------------------------------------|------------------------------------------------|
| A CRITICAL, HIGH or MEDIUM finding                                         | Decided against: quarantine                    |
| The AI model judges the file malicious or out of place                     | Decided against: quarantine                    |
| Only LOW or INFO findings                                                  | Pass                                           |
| No findings, every required engine completed                               | Pass                                           |
| A required engine did not complete, was unavailable or ran out of attempts | Failed as a mechanism fault, never quarantined |

## Quarantine is terminal

A quarantined file is never delivered. It is enforced in several independent places so one mistake cannot open it: the transfer lifecycle has no way out of quarantine, the REST interface has no release endpoint, the permission list has no release permission and the console's quarantine page has no release button.

## What an operator can and cannot do

| Action                                                        | Available                    |
|---------------------------------------------------------------|------------------------------|
| See every contained item with route, reason and full evidence | Yes                          |
| Export a metadata and evidence report                         | Yes; never content           |
| Dispose of contained content early                            | Yes, with the reason audited |
| Read or download contained content                            | No; no route exists          |
| Release, override or reprocess                                | No                           |

An operator's job is to understand and escalate, not to overrule. A wrongly quarantined file is resolved by talking to the producer's owner and, if the policy was wrong, by an audited policy change; the source then re-sends.

### ✦ Nothing to tune day after day

You choose the profile for a route once and the checks run by themselves. Signatures and rules are updated with a signed offline data package, with no change to the software.

## ⚠ Four exceptional endings, four owners

| Ending                        | Meaning                                             | Whose problem                                                                |
|-------------------------------|-----------------------------------------------------|------------------------------------------------------------------------------|
| <b>QUARANTINED</b>            | Content assurance ruled against the file.           | The content: the producing system sent something this route does not accept. |
| <b>REJECTED</b>               | An approver rejected it, or nobody decided in time. | The process: a person declined or the organization did not act.              |
| <b>FAILED</b>                 | A mechanism failed and its attempts ran out.        | The appliance or environment: hosts, engines or capacity.                    |
| <b>Delivered, not settled</b> | The file arrived but source disposal failed.        | The source system.                                                           |

Because the four are never lumped into “errors”, the operator sees the signal: rising FAILED means fix the appliance, rising QUARANTINED means talk to the producer, and rising REJECTED for expiry means nobody is watching the approval queue.

## ☰ Evidence that lasts

### Every run leaves one immutable record

- What ran and at which version
- Against which content-set version
- The verdict, reason code and bounded findings
- Including runs that did not complete

### What is never kept

- Matched content beyond a bounded, masked context
- Signature or rule text
- Raw engine output and stack traces
- Absolute host paths

**A file that fails never crosses, and a file that was not checked is never reported as clean.**

More about this product

#### CATALOG 1

Product overview

#### CATALOG 2

Routes and policy

#### CATALOG 4

Security and operations

For advice, a demonstration and contact details:

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



Specifications may change without notice.