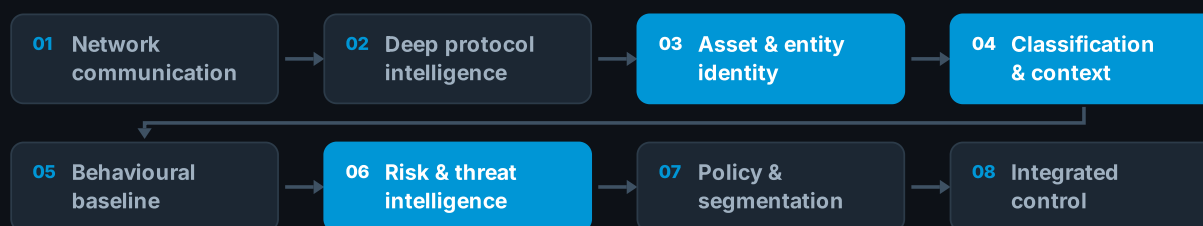


SOLUTION BRIEF: AIR-GAPPED AND DISCONNECTED OPERATIONS

Running WireTrace, and keeping it current, with no connectivity

Everything WireTrace needs to analyse your network lives on the appliance. Upgrades and intelligence refreshes cross the gap on your media, under your controls, and the appliance never connects out.



For: Government, critical national infrastructure, defence and OT operators

Most network security platforms can be installed on premises. The harder question for a disconnected site is what happens next: **does the platform still work fully with no internet, and how does it stay current?** This brief answers both, step by step, for WireTrace.

01 What runs on the appliance

WireTrace runs fully without internet access. Nothing it needs for day-to-day analysis is fetched from outside:

Analysis

Protocol decoding, identity, classification, detection, baselines, vulnerability matching, risk scoring, policies and reports all run on your WireTrace server and sensors.

Knowledge

Asset identity and classification knowledge, the application catalogue and end-of-life data ship on the appliance as versioned content.

Rumi, the AI assistant

Rumi runs entirely on the WireTrace server with no external AI service. It needs host resources of its own; the Deployment and Sizing Guide covers this.

02 Installing and upgrading offline

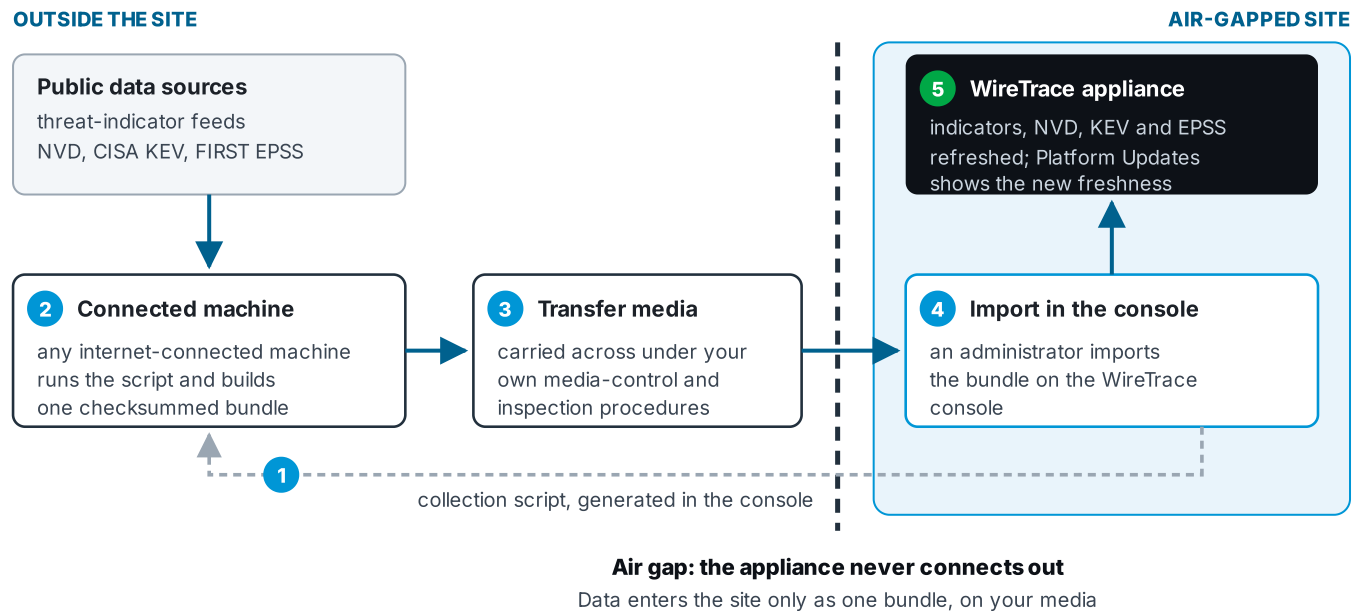
WireTrace installs from **one self-contained release package**, carried in on media under your own media-control and inspection procedures. Upgrades follow the same route, with no online step.

Each release also improves the knowledge the platform works from. It is maintained as versioned content, separate from product code, and every content change is tested, peer-reviewed and versioned before release.

Area	What improves with each release
Identity	The evidence rules and reference data that resolve observations into one durable identity per device.
Classification	Classification rules and the device taxonomy that assign domain, type, role and Purdue level.
Detection logic	Detection rules and their ATT&CK and ATT&CK for ICS mappings.
Application recognition	The catalogue of cloud, SaaS, vendor-cloud and infrastructure applications devices use.

03 Refreshing threat and vulnerability data

Threat indicators and vulnerability data change faster than releases. A disconnected site refreshes them with a **collection script** and **one checksummed bundle**, without the appliance ever connecting out.



The offline refresh flow. The console generates the collection script; each refresh is steps 2 to 5. The appliance has no network path to the outside at any point.

- 1 Generate** the collection script (Bash or PowerShell) in the console and take it to any internet-connected machine. It holds only the sources, a start date and any commercial-feed key of your own: no site data. Handle it as a credential.
- 2 Run** it there. It collects current threat indicators and NVD, CISA KEV and FIRST EPSS data into **one checksummed bundle**, which the console verifies on import.
- 3 Carry** the bundle across with the media controls, scanning and approvals you apply to any inbound file.
- 4 Import** it in the console.
- 5 Check Platform Updates** for the new versions and freshness.

04 Knowing how current you are

On a disconnected site the risk is not missing data but not knowing how old it is. The **Platform Updates** page shows the version, freshness and any action required for vulnerability data, threat feeds, classification and identity knowledge, the application catalogue and detection reference data, so stale data is visible rather than silently trusted.

05 Operating model and suggested cadence

Cadence is your decision, set by your transfer windows and risk appetite. A suggested starting point:

Activity	Suggested cadence	Notes
Threat and vulnerability refresh	Weekly, or at each scheduled transfer window	Shorten during periods of heightened threat or when a widely exploited vulnerability is announced.
Release upgrade	As releases become available, after your own acceptance testing	Brings the knowledge improvements listed in section 02.

06 The data that never leaves

Inventories, identity evidence, communication records, alerts, investigations, policies, reports and Rumi conversations stay on the appliance. The offline refresh is one-way: published threat and vulnerability data comes in, and the appliance makes no connection out.

Limits, stated plainly

- OT vendor advisories, CISA ICS advisories and some third-party feeds are online sources, not part of the offline bundle. Collection follows each feed's own terms of use.
- Improvements to identity, classification, detection logic and application recognition arrive with releases, not between them.
- Vulnerability results are only as current as the last import.

Plan a disconnected deployment

A technical session walks through installation, the offline refresh cycle and an operating cadence for your sites.

Book a demo at wiretrace.io/request-demo or email sales@wiretrace.io