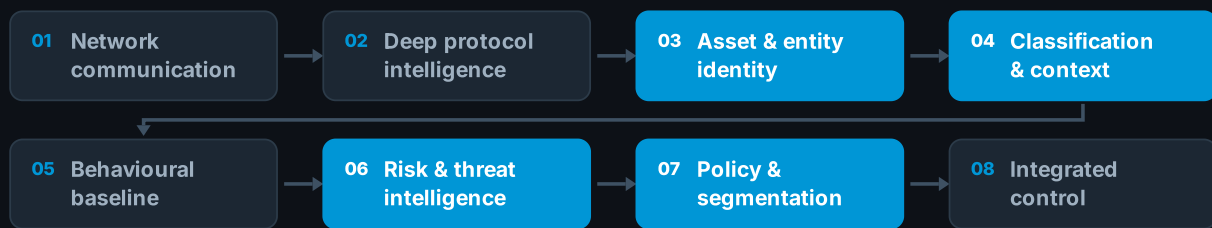


SOLUTION BRIEF

Risk & Exposure

What puts your devices at risk, what to fix first, and how to show it is fixed: exposure, vulnerability and asset risk grounded in what each device actually is and states on the network.



For: CISOs, vulnerability-management and exposure teams, OT security

Exposure and vulnerability programmes usually stop at the edge of what can be scanned. The controllers, building systems, cameras and embedded devices beyond that edge are often where the risk sits. WireTrace works from what devices state and do on the network, and **every finding says how it was reached, how strong the evidence is, and whether the vulnerable version is confirmed on that device.**

KEV + EPSS

vulnerabilities prioritised by known exploitation and exploit likelihood

3 lanes

Now, Next and Later, with owners, SLAs and change windows

0-100

Asset Risk Score per device, with a separate confidence indicator

Offline

vulnerability data refresh for air-gapped sites through a customer-run collector

01 Three questions, one evidence base

WireTrace is a **Deep Protocol & Asset Intelligence (DPAI)** platform. It decodes the protocols devices use, down to the payload, and builds one durable identity per device across IT, OT, IoT and IoMT. Risk and exposure work starts from that identity, so a finding is attached to a device you can name, with its classification, Purdue level and communication peers, not to an address.

What puts my devices at risk?

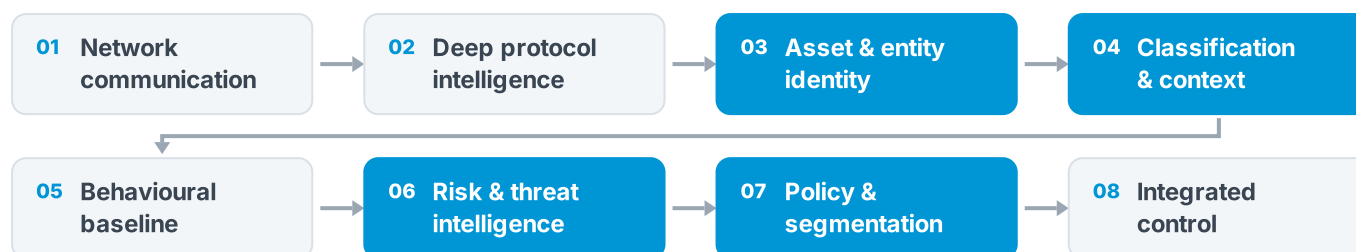
Exposures seen in traffic, vulnerabilities matched to identified software and firmware, and end-of-life products.

What do I fix first?

Findings ranked by exploitation, match strength, exposure and device role, in the Asset Risk Score.

How do I prove it is fixed?

A fix is verified when the vulnerable version is no longer observed; accepted risks expire.



The WireTrace platform flow. Highlighted layers are the subject of this document.

02 Exposure: what the network already shows

Many of the weaknesses that matter most need no vulnerability database at all. They are visible in the traffic itself. The **Risks & Exposures** view brings them together, alongside ransomware activity, and exports to CSV for your own tracking. Exposures are standing weaknesses, tracked separately from alerts.

Exposure	What WireTrace finds
Clear-text credentials and legacy authentication	Account names and credentials exposed by clear-text and legacy authentication, so weak practices can be fixed. Revealing a captured secret is restricted to authorised roles.
Weak cryptography and certificates	Weak cryptography in use, with TLS client fingerprints and certificate details recorded for identity, hygiene and threat matching.
Exposed services	Services exposed by devices, seen in observed communication rather than inferred from a port list.
OT exposure	Exposure of industrial devices and services, read from the industrial protocol traffic itself.
Network integrity	Adversary-in-the-middle techniques: TLS interception, TCP reset injection, layer-2 and name-resolution poisoning and DNS manipulation.

Active threat detection is covered in the *Threat Detection & Security Analytics* brief; this brief stays with standing conditions and what to do about them.

03 Vulnerability intelligence that states its evidence

WireTrace matches each device's identified OS, software, firmware and OT product to the NVD and OT vendor advisories, prioritised with CISA KEV (known exploited vulnerabilities) and FIRST EPSS (exploit prediction). **Every finding states how it was matched, how confident the match is, and whether the vulnerable version is confirmed on that device.** That distinction is what separates a confirmed exposure from a possible one, and it is shown rather than hidden.

Where version evidence comes from

A precise match needs a version. WireTrace is passive by default, and version evidence arrives through three routes:

- 1 What devices state.** Where a device states its model, firmware or serial number, as many industrial controllers, IoT and network devices do, WireTrace records it with its source. Operating systems are inferred passively with a stated confidence.
- 2 Switch and router polling.** With read-only SNMP access, WireTrace adds hardware details from switches and routers.

- 3 Optional credentialed collection.** Optional, administrator-governed active enrichment adds installed software, services and exact OS versions for the IT hosts an administrator chooses to scan. It needs defined scopes and read-only credentials, runs from the management interface, and an OT-safe profile keeps probes away from industrial and medical devices unless explicitly allowed.

Passive observation alone does not produce version-precise findings on devices that state no version. Such a device may receive a product-family match, labelled as the weaker match it is, or no match at all. For each device, WireTrace states which kinds of evidence are present, missing or stale, and an empty result is never presented as a clean one.

WireTrace observes

- A Purdue level 1 controller states its order number and firmware version in its protocol identity record
- An OT vendor advisory covers that product and firmware range, and the vulnerability is listed in CISA KEV
- The controller accepts sessions from an engineering workstation in the IT zone
- The vendor has no patch the plant can apply before the next shutdown

WireTrace produces

- **version confirmed** a finding with a strong match and its source evidence
- A higher Asset Risk Score, with known exploitation, exposure and control role shown as factors
- A remediation item in the **Now** lane, and a containment entry for the period until the patch can be applied
- Once segmentation intent is declared for the controller's conduit, traffic that breaks it is raised as a violation

WireTrace observes

- A Windows workstation whose operating system family is inferred passively
- No exact build or installed-software evidence: the host is outside any credentialed scan scope
- Advisories exist for that product family

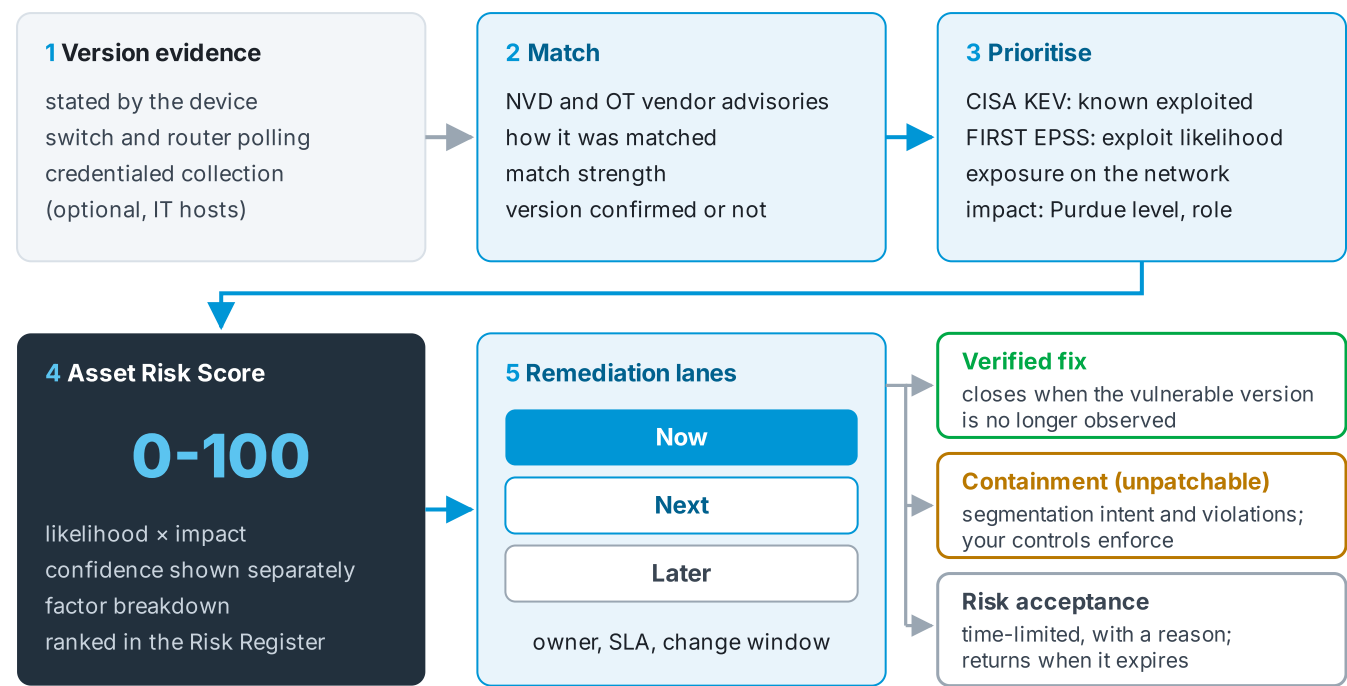
WireTrace produces

- **possible match** findings labelled with the weaker match strength, not presented as confirmed
- Visibility assurance showing that version evidence is missing
- If an administrator adds the host to a credentialed scope, the exact version is added and matching can confirm or rule out each finding

End-of-life intelligence

WireTrace flags operating systems and products past vendor end of life, using lifecycle data that also works offline. Coverage depends on the product being identified, and OT firmware lifecycles are not completely covered.

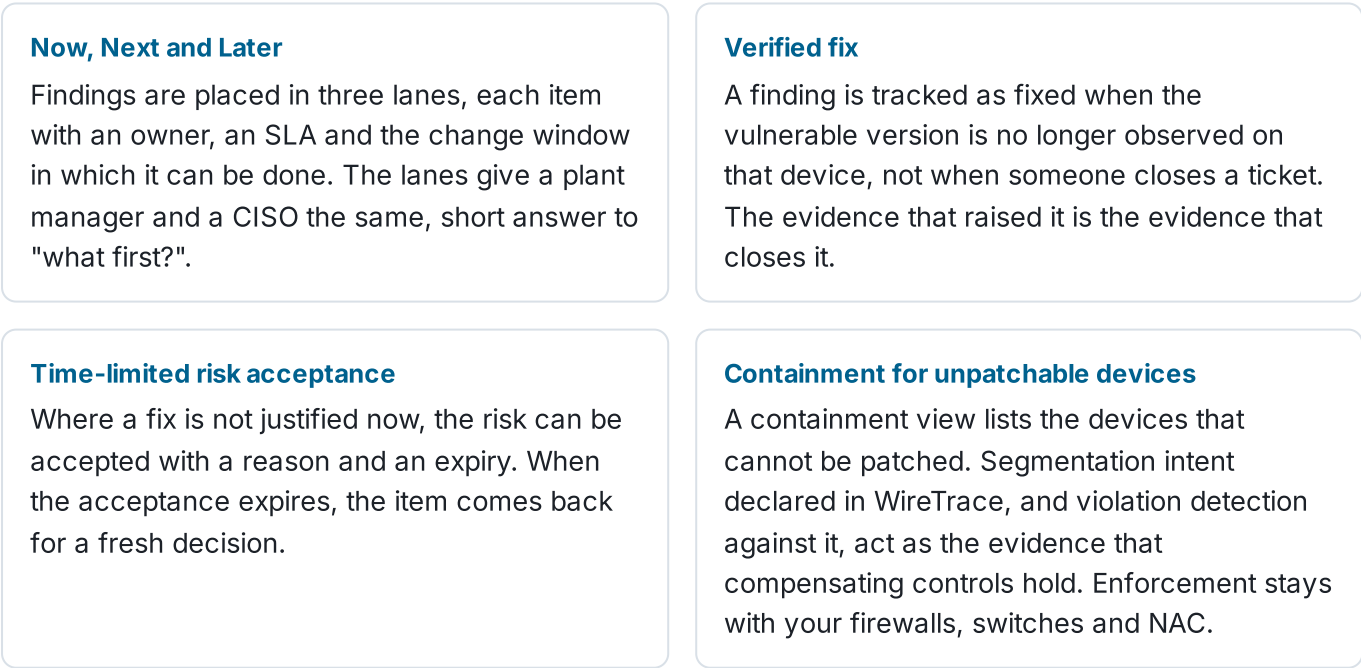
04 From evidence to a ranked fix list



Prioritisation in WireTrace. Version evidence is matched with its strength stated, prioritised by exploitation, exposure and impact, scored per device, and worked through Now, Next and Later lanes until the fix is verified, the device is contained, or the risk is accepted for a limited time.

05 The remediation workspace

The remediation workspace turns findings into work that a vulnerability team and plant or IT owners can agree on:



06 Asset Risk Score and Risk Register

Every device receives a 0-100 **Asset Risk Score**, calculated as likelihood × impact, with a separate confidence indicator and a factor breakdown, so a score built on thin evidence does not look as certain as

one built on confirmed versions.

Component	What it draws on
Likelihood	The most serious applicable vulnerability, weighted by KEV, EPSS and match strength; exposure; active threats; end-of-life status; hygiene; protocol deviations; policy violations.
Impact	The device's Purdue level and its safety or control role.

The **Risk Register** ranks devices by score with the factor breakdown, supports time-limited risk acceptance, and lets an owner override a device's criticality where the organisation knows better than the network. It is an asset-level register for security and operations teams, not an enterprise or GRC risk register.

07 Keeping vulnerability data current, including air-gapped

Connected appliances refresh vulnerability and threat-intelligence data automatically on their own schedules. Air-gapped sites refresh vulnerability data with a collection script run on any internet-connected machine: the checksummed bundle carries NVD, CISA KEV and FIRST EPSS data, is moved through the customer's own transfer process, and is imported in the console, which verifies it on import. The appliance never connects out. ICS and OT vendor advisories are online sources, not part of the bundle; end-of-life data works offline.

Limits, stated plainly

- Vulnerability findings are only as precise as the version evidence. Passive observation alone does not produce version-precise findings on devices that state no version; product-family matches are labelled as weaker matches, and some will not apply.
- Definitive patch status for IT hosts relies on credentialed collection and optional online advisory sources, which are off by default.
- End-of-life intelligence does not completely cover OT firmware lifecycles. The offline bundle carries NVD, KEV and EPSS data; ICS and OT vendor advisories need a connected appliance.
- WireTrace does not patch devices and does not enforce containment. Compensating controls are enforced by your firewalls, switches and NAC; WireTrace states the intent and detects violations.
- The Risk Register is an asset-level register, not an enterprise or GRC risk register. No accuracy or coverage figures are claimed.

Bring one question you cannot answer today

Pick the device class that worries you most, controllers, cameras or unmanaged hosts, and a WireTrace evaluation shows what the network says about its exposure and vulnerabilities, and how strong that evidence is.

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