

The Network Digital Twin: 3D Physical Topology That Stays True to Reality

Every platform can draw a graph of what talks to what. WireTrace answers the question that graph cannot: where does everything physically live, how is it actually wired, and what changed since yesterday? The digital twin renders your buildings, floors, racked switches, device clusters and trunk cabling as a live, navigable 3D model, reconciled against discovered reality on every run.

WIRETRACE DIGITAL TWIN | VERSION 1.3 | 2026

3D + 2D
TWIN VIEWS

L2 + L3
PATH TRACING

LLDP / CDP /
SNMP
CABLE DISCOVERY

Drift log
EVERY CHANGE RECORDED

WHY "DIGITAL TWIN" AND NOT "NETWORK DIAGRAM"

A drawing shows what you believe. Discovery shows what exists. A twin earns the name by holding both at once and surfacing the difference. WireTrace keeps three things in one model:

Recorded intent

The placement and cabling your organisation believes it has: buildings, floors, subnet-to-location mappings, and links an engineer has confirmed as ground truth.

Observed reality

What discovery actually finds: assets identified passively from live traffic, and cabling walked over LLDP and CDP via SNMP from each placed switch.

The drift between them

Every discovery run reconciles the model instead of redrawing it. Links added, removed, or moved to a different port land in a change log with provenance, so a disagreement is a finding, not a rendering error.

Confirmed ground truth

One click marks a link as confirmed. Confirmed links are never auto-pruned, and if one ever disappears from discovery the twin flags it louder than ordinary drift.

HOW THE MODEL IS BUILT

LAYER	WHERE IT COMES FROM	YOUR EFFORT
Assets	Discovered passively by the sensor from real traffic: IP, MAC, vendor, device type, OT/Purdue level	None - automatic
Buildings & floors	You define your sites once	Minutes, once
Subnet mapping	You map each CIDR to a building or floor	Minutes, once
Placement	Auto-place drops every switch into the location whose subnet best matches (longest prefix wins)	One click
Cabling	Discover walks LLDP/CDP over SNMP from each placed switch and draws the real wires	One click

Honest by design. Which room a switch sits in is a fact about the building, not the network, so it enters the model through one-time operator input and is ranked above machine inference. Everything downstream of it stays current automatically. Asset capture is passive; cable discovery polls switches over SNMP from the management interface only, and is operator-initiated.

READING THE SCENE

The 3D view (Network Atlas) places a **boundary island** at the center: the Internet, edge and data-center firewalls, core switches and the VPN entry point. Around it, each building and floor becomes a **zone pad** holding its access switches and their device clusters, with trunks routed as bundled highways into the core. Switch tiers (core, aggregation, access) are inferred from real trunk counts. Color modes overlay Domain (IT/OT/IoT/IoMT), Risk (severity halos and alert beacons), or Purdue level (ISA-95 L0-L5 with segmentation-violation flags). Nothing on the island is invented: each node appears only when its underlying signal exists in captured traffic, configuration, or parsed VPN sessions.

PATH INTELLIGENCE

Alongside the 3D twin, a **2D diagram tab** gives engineers and auditors a tiered, placement-independent view of the same model. Pick any two assets and the twin reconstructs the path between them: layer-two hops from bridge tables and discovered links, and routed layer-three hops resolved by longest-prefix match across collected routing tables. Every hop carries its evidence source and a confidence rating, and every path states its coverage honestly; where visibility ends, the twin says so instead of guessing. The diagram exports as an audit-grade PDF, the artifact an IEC 62443 zone-and-conduit review asks for.

WHAT TEAMS DO WITH IT

Respond at the right cabinet

An alert names an asset; the twin names the building, floor, switch and port. Mean time from alert to hands-on drops when nobody is chasing a spreadsheet.

Physical blast radius

See what shares a compromised device's switch and rack, not just what it talks to, before deciding whether isolating it is safe.

Verify segmentation by looking

Zone boundaries drawn over physical placement make a violation visible instead of inferable from a table of rules.

Prove the control is in the path

Trace the actual L2/L3 path between two assets to show a firewall is genuinely in line, not merely configured.

Catch unauthorized change

A cable moved to a different port, a switch that vanished, a new uplink: the drift log records it with before and after.

Audit evidence on demand

Export the tiered diagram with coverage and confidence inline as a PDF for IEC 62443, ISO 27001 or internal review.

SETUP IN FOUR MOVES

Define buildings and floors. Map subnets to them. Click **Auto-place** to drop every discovered switch into the right room. Click **Discover** to draw the cabling. From then on the twin reconciles itself on every run and keeps the change log; the assets, tiers, risk overlay and drift tracking are automatic. Works across IT, OT, IoT and IoMT estates, fully on-premise, including air-gapped sites.