

ORDR for Healthcare Technology Management (HTM)

ORDR gives HTM teams a live, network-verified view of every connected device: **what it is, where it is, what it runs, and whether it is at risk**. That data flows straight into the CMMS your team already works in.

Every connected device: verified, located, and in your CMMS.

The problems HTM teams tell us about

The CMMS doesn't match reality

Devices land on the network without incoming inspection; retired assets stay active.

IT fields are blank or stale

IP, MAC, hostname, OS, and VLAN are rarely captured at intake and drift after every move.

Devices go missing

Pumps, telemetry packs, and portable monitors wander, delaying PMs, recalls, and survey prep.

Software is tracked by hand

OS versions, patch levels, and end-of-support status live in spreadsheets, if anywhere.

Recalls are matched manually

FDA and CISA advisories are cross-referenced against the inventory one model at a time.

Two teams, two lists

HTM and IT security work from different sources of truth and argue over whose is right.



Connected device inventory

ORDR finds every device on the network passively, with **no agents and no active scans touching clinical equipment**, and identifies it down to manufacturer, model, and device type.

- **Discovery from traffic, not data entry.** Sensors on SPAN/TAP and flow data see every device that talks, including ones that skipped incoming inspection.
- **Medical-grade classification.** Infusion pumps, patient monitors, imaging, lab analyzers, and surrounding IoT are profiled with make, model, and serial where available.
- **Reconciliation against the CMMS.** ORDR flags devices on the network that aren't in the CMMS, and CMMS records that haven't been seen on the network.
- **Utilization.** Active-use patterns help right-size fleets and support capital and replacement planning.



IT information on every asset

Every device record carries the network and security detail HTM is usually missing, updated as the device moves or changes. **A tech no longer has to walk to the device to read its software version.**

What ORDR captures	Why HTM cares
IP, MAC, hostname, DHCP history	Ties the CMMS record to the device IT sees; survives re-IPs
VLAN, subnet, wired or wireless	Confirms the device is on the right clinical network
OS type and version, end-of-life status	Spots unsupported Windows/Linux before an audit does
PHI handling, open ports, protocols	Answers security questionnaires and MDS2 follow-ups
CVEs and risk score	Prioritizes which devices need a patch or compensating control
First seen / last seen	Proves a device is in use, idle, or gone

When an FDA recall or CISA advisory lands, HTM can pull **every affected device with its IP and location in one query** instead of a model-by-model hunt.



Location identification

ORDR tells HTM where a device last connected, **down to the switch port or wireless access point**, and translates that into a building, floor, and unit.

- **Wired devices:** the exact switch and interface the device is plugged into.
- **Wireless devices:** the access point and controller it is associated with, pulled from wireless LAN controller integrations.
- **Human-readable location:** rules map subnets, VLANs, switches, or APs to site, building, floor, and department, so records read "4 West ICU" instead of an IP range.
- **Last-seen timestamps:** narrow the search for a missing pump or telemetry pack before it becomes a lost-asset write-off.

ORDR complements RTLS rather than replacing it. It covers every networked device with no tags to buy, and fills in where tags were never attached.



ORDR Software Inventory Collector (OSIC)

OSIC fills in what network traffic alone can't show: **installed software, patches, and security settings** on Windows, macOS, and Linux-based devices that can't take an agent or a vulnerability scan.

Imaging workstations, lab systems, and modality consoles often run a standard OS, but vendors forbid agents and active scans. OSIC uses a **lightweight, read-only, OS-native script** that reports to ORDR without consuming device resources.

OSIC collects	HTM use
Model, serial number, manufacturer, BIOS	Matches the device to its CMMS record with certainty
OS version, third-party software, end-of-life status	Tracks vendor-approved builds and EoS deadlines
OS patches and hotfix IDs with install dates	Verifies vendor patches were actually applied
Antivirus product, version, and status	Confirms vendor-validated AV is present and current
Disk encryption, local firewall, running processes	Evidence for HIPAA and security reviews; flags unauthorized software
IP-MAC binding, including VPN-connected devices	Keeps identity accurate as addresses change

Because CVEs are matched to software actually installed, vulnerability lists reflect **the device in front of you, not a guess based on its model**. OSIC also reaches devices on private or non-routable networks that sensors can't see directly.



Connecting to your CMMS

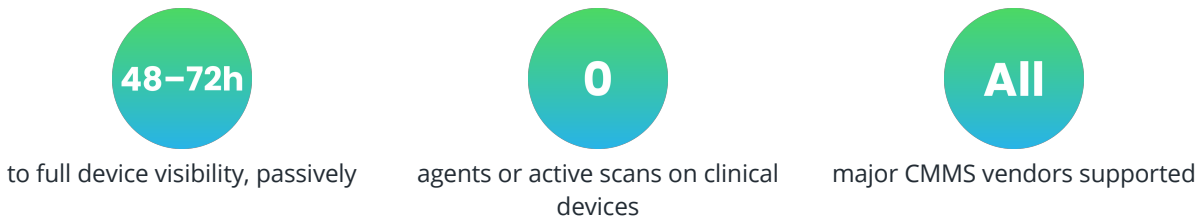
ORDR connects to all major CMMS vendors used by healthcare HTM teams. The CMMS stays HTM's system of record; ORDR feeds it.

Step	What happens
Pull	ORDR imports existing asset records from the CMMS
Match	Records are matched to discovered devices by serial, MAC, and model
Reconcile	Unrecorded devices and unseen records are flagged for review
Enrich	IP, MAC, OS, software version, location, vulnerabilities, and utilization are written back to each asset
Act	Rules can open work orders when a device hits a critical CVE, EoL OS, or recall

The same integrations extend to enterprise CMDBs, so HTM and IT security share one device record. What changes day to day:

- **No more re-keying IT fields.** IP, MAC, OS, and location update in the CMMS automatically.
- **Work orders from risk.** A new critical CVE or an EoL OS can open a ticket against the right asset.
- **One-click recall response.** Every affected device, with IP and last location, from the asset record HTM already uses.
- **Patch windows aligned with PMs.** Security fixes ride along with scheduled maintenance instead of pulling a device twice.

Why ORDR for HTM



- **One device record for HTM and IT security,** so both teams stop debating whose list is right.
- **Clinical context before any enforcement.** When security needs to isolate a vulnerable device, ORDR builds the policy from the device's real traffic and simulates it first, so a pump or monitor never loses the connections it needs for patient care.
- **Works with what you own:** your CMMS, your network gear, your RTLS.

A good first step

Export your CMMS inventory and let ORDR reconcile it against the network for one site. The gaps on both sides usually make the case on their own.

ordr.net/request-a-demo