SOLUTION OVERVIEW

CLOSING THE ZERO-TRUST BLIND SPOT



How WanAware secures FDA-cleared medical devices without agents, scans, or disruption to patient care

You already know the problem: thousands of FDA-cleared IoMT devices, infusion pumps, patient monitors, telemetry systems, smart beds, that cannot run an agent or absorb an active scan, sitting outside the reach of every zero-trust control your team is trying to build. WanAware closes that gap with a platform that is agentless and scanner-free by design, nothing installed on a device, nothing actively probed. This overview covers what that platform actually includes, how it closes the gap in practice, and what to expect from deployment through to full visibility.

Want the full mission briefing?

Read the white paper on The Zero-Trust Blind Spot



WHAT WANAWARE DOES

Agentless discovery

Every device, medical or IT, is discovered from the network itself. Nothing is installed on an infusion pump, a monitor, or a smart bed, so nothing about its FDA-cleared configuration or warranty status is ever touched.

Passive, not active

Discovery observes what a device is already doing on the network. It does not probe, scan, or send devices unexpected traffic, so it carries none of the destabilization risk that keeps IoMT VLANs excluded from active scanning today.

The Relationship Graph

Every discovered device and every connection between devices is mapped into one continuously current graph, showing exactly what each device can reach and what can reach it.

Always current, not point-in-time

Visibility is not a scan that ages the moment it finishes. The graph updates continuously as the network changes, so the picture your team works from is always today's network, not last month's.

HOW IT WORKS



STEP 1

Passive observation

WanAware observes network traffic and device communications, agentlessly, across every connected device.



STEP 2

Identification

Devices are identified and classified from what they are actually doing, without installation or active probing.



STEP 3

Relationship mapping

The Relationship Graph maps every connection and dependency, medical and IT, into one continuously current model.



STEP 4

Continuous visibility

Security and biomedical teams get queryable, always-current visibility feeding zero-trust segmentation and incident response.

WHAT THIS SOLVES

Where you are today	What changes with WanAware
IoMT devices hide in plain sight, absent from the asset record IT and security actually use.	Every device is discovered continuously and agentlessly, medical and IT, in one inventory.
Zero trust cannot verify, segment, or police a device it does not know exists.	Every device is mapped and available to assign a least-privilege policy against.
Flat, unmonitored clinical VLANs are invisible until an incident proves otherwise.	**The Relationship Graph** shows exactly what each device can reach before an incident, not during one.
Blast radius is unknown when ransomware executes, costing hours in the worst possible moment.	**Blast radius** is already mapped, so containment and isolation start from a known picture.

PROOF IN DEPLOYMENT

These outcomes are consistent with what health systems report after deploying WanAware across multi-site IoMT fleets: full visibility achieved quickly, zero disruption to clinical operations, and a measurable improvement in how fast teams can answer the one question that matters most during an FDA cybersecurity recall: how many of these do we have, and where.

MISSION CONTROL: BY THE NUMBERS

- **100%** Device visibility within 10 days
- **Zero** Disruption to patient care during deployment
- **4.2x** Faster response time to FDA cybersecurity recalls

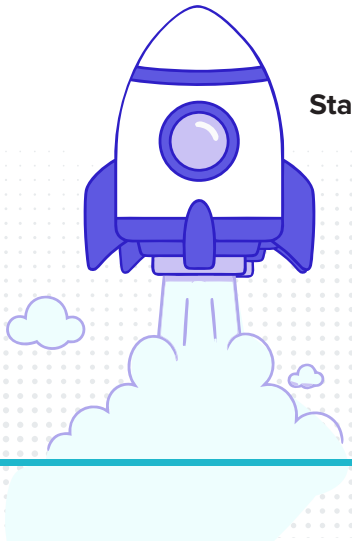


WHY WANAWARE

- **Agentless and scanner-free by design.** Nothing is installed on a device, and nothing is actively scanned or probed. Agent-based and active-scanning tools were never designed to touch FDA-cleared equipment safely. WanAware was.
- **One graph, not three inventories.** Biomedical engineering, IT, and security work from the same continuously current view instead of reconciling separate, aging records.
- **A foundation for zero trust, not a workaround.** Segmentation, least-privilege policy, and lateral-movement monitoring all depend on knowing a device exists. WanAware is the layer that makes that true for every device, not just the ones that could run an agent.

THE TAKEAWAY

Closing the zero-trust blind spot does not require touching a single pump, monitor, or bed. It requires seeing them, continuously, and WanAware is built to do exactly that.



READY FOR LIFTOFF?

Start a free trial or see a demo at wanaware.com.

FREE TRIAL SEE A DEMO