WHITEPAPER

THE ZERO-TRUST BLIND SPOT

Stopping ransomware and lateral movement across FDA-cleared medical networks



TABLE OF CONTENTS

01: EXECUTIVE SUMMARY	3
02. THE IOMT FLOOD NO ONE CAN FULLY SEE	3
03. WHY YOU CANNOT JUST INSTALL AN AGENT	3
04. UNMANAGED MEANS INVISIBLE TO ZERO TRUST	4
05: HOW RANSOMWARE MOVES THROUGH THE BLIND SPOT	5
06. WHY ACTIVE SCANNING IS NOT THE FIX	5
07: THE WANAWARE APPROACH: AGENTLESS DISCOVERY AND THE RELATIONSHIP GRAPH	5
08: FROM BLIND SPOT TO BLAST-RADIUS CONTROL	6
09: THE TAKEAWAY	7

01. EXECUTIVE SUMMARY

Hospitals are flooded with Internet of Medical Things (IoMT) devices: infusion pumps, patient monitors, smart beds, and telemetry systems, all connected, all networked, and all multiplying faster than most security teams can inventory them. Traditional IT monitoring agents cannot be installed on FDA-cleared medical equipment without voiding the manufacturer's warranty or risking patient safety. The result is not a small gap. It is a category of connected asset that hides in plain sight, visible on the network and invisible to security.

Zero trust promises to verify every device, grant only the access it needs, and assume breach at every step. None of that is possible for a device your tools cannot see. This paper is about that blind spot: why it exists, how ransomware exploits it, and what it takes to close it without touching a single piece of life-supporting equipment.

02. THE IOMT FLOOD NO ONE CAN FULLY SEE

The infusion pump at the bedside, the telemetry monitor on the wall, the smart bed that reports patient position, the portable ultrasound wheeled between units: every one of them is a networked computer, and every one of them was cleared by the FDA as a medical device, not sold as general-purpose IT equipment. Hospitals add these devices continuously, unit by unit, vendor by vendor, and few of them are ever reconciled against the same asset inventory that tracks laptops and servers.

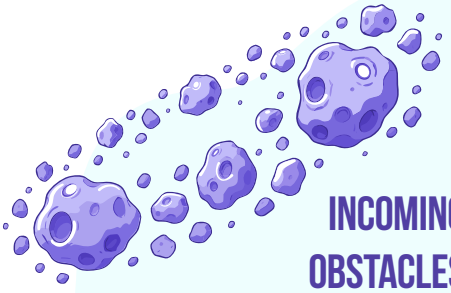
- **Volume without visibility.** A mid-size hospital can have thousands of connected medical devices across dozens of manufacturers, most of them never touched by the standard IT asset discovery process.
- **Networked by design, secured almost by accident.** IoMT devices are built to transmit data continuously. Security was rarely the design priority, and it is rarely added after the fact.
- **Every new device widens the gap.** Each additional pump, monitor, or bed is one more asset that exists on the network and nowhere in the inventory that is supposed to describe it.

03. WHY YOU CANNOT JUST INSTALL AN AGENT

An infusion pump is not a laptop. It is a regulated medical device, and its FDA clearance describes the device as validated, including its software configuration. Installing a third-party monitoring agent can alter that configuration,

which can void the manufacturer's warranty and, in the more serious cases, invalidate the clearance itself.

Even where that is not a concern, many of these devices run on aging, resource-constrained operating systems that were never built to host an additional running process without risking instability, on a machine that may be keeping a patient alive.



INCOMING OBSTACLES

Security teams are asked to secure devices they are explicitly told not to touch. That instruction is correct. It is also why the blind spot exists, and why closing it requires a different approach than the one used for every other endpoint on the network.

04. UNMANAGED MEANS INVISIBLE TO ZERO TRUST

Zero trust is not a product, it is a set of operating assumptions: verify every device explicitly, grant only the access each device actually needs, and assume that a breach has already happened somewhere on the network. Every one of those assumptions requires knowing the device exists in the first place. A device that never appears in an inventory cannot be explicitly verified, cannot be assigned a least-privilege policy, and cannot be watched for the anomalous behavior that would reveal a breach in progress. It simply is not part of the model.

Zero-trust principle	What it requires	Where unmanaged IoMT devices fail today
Verify explicitly	Every device authenticated and known to the security stack.	Most IoMT devices are invisible to IT and security tooling entirely.
Least-privilege access	Devices restricted to only the systems and data they need to reach.	Often placed on flat, under-segmented clinical VLANs by default.
Assume breach	Continuous monitoring for anomalous lateral movement.	Unmonitored devices generate no anomaly signal at all.

05. HOW RANSOMWARE MOVES THROUGH THE BLIND SPOT

Ransomware rarely starts where it does the most damage. An attacker typically gains an initial foothold through a phishing email, a compromised remote access account, or a vulnerable internet-facing system, then spends time moving laterally in search of a path to the systems that matter: the EHR, backup infrastructure, domain controllers. Unmanaged IoMT devices, sitting on flat or loosely segmented clinical networks and monitored by nothing, are an ideal stepping stone. They are rarely patched on the same cycle as IT assets, rarely watched for unusual traffic, and often sit closer, network-wise, to critical systems than anyone accounted for when the network was designed.

An attacker compromises a vendor's remote maintenance account and lands on a subnet shared with a dozen infusion pumps. Nothing about that subnet is monitored for lateral movement, because nothing on it was expected to be a target. From there, the path to the EHR is a matter of which flat VLAN connects them, not a matter of skill.

06. WHY ACTIVE SCANNING IS NOT THE FIX

The instinct once a gap like this is identified is to scan it: run the same vulnerability and discovery tools used everywhere else against the IoMT subnet. Active, credentialed scanning sends unexpected traffic and probes to devices that were never tested against it, and on fragile clinical equipment that can mean a frozen pump, a dropped telemetry feed, or a device that needs to be manually restarted at the bedside. Because of that real risk, most security teams simply exclude IoMT VLANs from active scanning altogether.

That exclusion is the correct call given the tools available, and it is also how the blind spot becomes permanent. Every scan that skips the IoMT network reinforces the boundary between what security can see and what is actually running. The gap does not shrink over time. It calcifies.

07. THE WANAWARE APPROACH: AGENTLESS DISCOVERY AND THE RELATIONSHIP GRAPH

WanAware discovers IoMT devices the same way it discovers carrier-grade network equipment: **agentlessly,** without installing anything on the device and without the active probing that puts fragile clinical equipment at risk. Discovery is built to observe what a device is doing on the network, not to interrogate the device itself, which means it can map an infusion pump or a telemetry monitor without touching its FDA-cleared configuration or its warranty status.

The result is a **Relationship Graph** that shows exactly what every device, medical or IT, can reach and what can reach it. That is the specific input zero trust and ransomware containment both depend on: not just a list of devices, but a map of blast radius, built continuously, without ever requiring a scan window on the units least able to absorb one.

Total infrastructure visibility without installing a single agent

Read the White Paper



08. FROM BLIND SPOT TO BLAST-RADIUS CONTROL

	Without visibility	With WanAware
Device inventory	Unmanaged IoMT devices hide in plain sight, absent from the asset record.	Every device is discovered continuously and agentlessly, without installing anything on it.
Zero-trust readiness	You cannot verify, segment, or police a device you do not know exists.	Every device is mapped and available to assign a least-privilege policy against.
Lateral movement exposure	Flat, unmonitored VLANs are invisible until an incident proves otherwise.	The Relationship Graph shows exactly what each device can reach before an incident, not during one.
Incident response	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.

09. THE TAKEAWAY

The instruction to leave FDA-cleared medical equipment alone is not the obstacle. It is correct, and it is not going away. The obstacle is trying to secure a zero-trust network with a blind spot built into it by design. Closing that gap does not require touching a single pump, monitor, or bed. It requires seeing them, continuously, without ever asking them to run something they were never built to run.

READY FOR LIFTOFF?

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

FREE TRIAL SEE A DEMO