ORDR

SOLUTION BRIEF

Resilient, Secure Healthcare Starts with AI-Driven Segmentation

Why Healthcare segmentation stalls — and how ORDR delivers rapid, whole-hospital protection.

The Goal Is Clear. The Execution Isn't.

Healthcare security and network leaders know segmentation is essential for Zero Trust, containing lateral movement, and ensuring patient safety. Yet, despite years of effort, many healthcare organizations remain stuck with fragmented VLANs, stalled NAC projects, or exposed medical devices.

The reason? Healthcare environments are complex – with unpatchable medical devices, vendor-managed systems, and critical clinical workflows. Legacy tools can't keep up with the scale and sensitivity of modern healthcare networks, making segmentation too complex to operationalize effectively.

ORDR's Perspective: Make Segmentation a "Quick Win"

We believe segmentation in healthcare should be automated, adaptive, precise, and safe — protecting patient care and compliance without disrupting clinical operations. Instead of brittle ACLs and manual guesswork, organizations need:

- Real-time visibility into every connected device (IoT, IoMT, OT) with clinical context — no agents required
- Safe simulation of enforcement to avoid impacting patient care
- AI-driven policy recommendations based on device behavior and clinical function
- Native enforcement across existing healthcare infrastructure — segmentation isn't just a compliance checkbox — it's your first line of defence for patient safety and data security

Strategic outcomes you can expect

With ORDR, segmentation becomes a real control that protects patients, staff, and data:

- Enforce in days, not months
- Protect critical clinical assets without disrupting workflow
- Visualize and simulate coverage to ensure patient safety
- Deploy policies across your existing healthcare stack
- Prove HIPAA, HITECH, and NIST compliance with audit-ready reporting

Copyright © 2025 ORDR Inc.

6 Reasons Healthcare Segmentation Projects Fail (and How ORDR Solves Them)

Segmentation in healthcare often fails due to unique challenges in clinical environments. Below are six recurring issues — and how ORDR addresses them with precision, automation, and confidence.

Critical medical devices remain exposed

Legacy, and hard-to-patch IoMT devices (e.g., infusion pumps, MRI machines) can't be secured with traditional tools.

ORDR isolates them safely using policy-based enforcement — no agents, no disruption to patient care.

HIPAA and NIST audits demand proof of control

Visibility alone doesn't satisfy HIPAA, HITECH, or NIST.

ORDR maps and enforces least-privilege policies with detailed, audit-ready reporting for compliance.

Poor visibility leads to flat healthcare networks

Lack of insight into device behavior leaves critical systems exposed.

ORDR translates real-time discovery into actionable controls tailored to clinical workflows.

Static policies can't contain live threats

Attacks move faster than traditional segmentation can respond.

ORDR detects abnormal behavior and dynamically adjusts enforcement in real time.

Segmentation stalls in unmanaged clinical environments

Agent-based tools fail across IoT, IoMT, and vendor-managed systems like imaging equipment.

ORDR augments NACs and Firewalls with precise profiling and automated policy generation.

Teams delay due to complex healthcare stacks

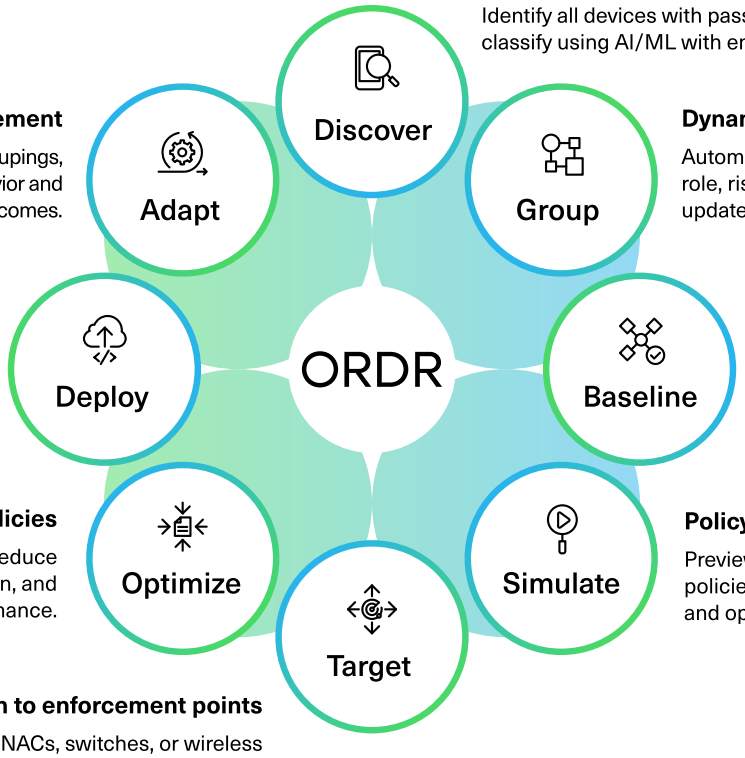
Tool sprawl and legacy systems slow down segmentation efforts in hospitals.

ORDR integrates with existing infrastructure, from EHR systems to network switches, and evolves with your environment.

Copyright © 2025 ORDR Inc.

How ORDR Automates Segmentation

Most tools stop at discovery. ORDR delivers end-to-end segmentation for healthcare with an AI-powered lifecycle, ensuring patient safety, compliance, and operational efficiency:



Profile, classify, assess

Identify all devices with passive, agentless discovery; classify using AI/ML with enriched attributes.

Dynamic segmentation mapping

Automatically group devices by business role, risk, behavior, function, and context; update in real time.

Actual, vetted communication

Monitor communication patterns to define normal behavior, surface anomalies, and inform policy creation.

Policy testing and governance

Preview enforcement impact and refine policies to meet regulatory, governance, and operational requirements.

Assign to enforcement points

Map policies to firewalls, NACs, switches, or wireless controllers for north–south and east–west protection.

Compress to streamline policies

Translate into native syntax, reduce complexity, eliminate duplication, and validate for scale and performance.

Real-time policy provisioning

Push policies to 3,500+ platforms in real time; adapt automatically as context and environments change.

Continuous refinement

Continuously update classifications, groupings, and policy logic based on observed behavior and deployment outcomes.

About Us

ORDR is the leader in AI-powered asset risk and exposure management, trusted by top organizations across healthcare, pharmaceuticals, manufacturing, and financial services. With insights from over 100 million asset types, ORDR's platform empowers security teams to identify their biggest risks and take swift, effective action. From maintaining security hygiene to real-time threat detection and protection using microsegmentation, ORDR makes action not just possible but automated and simple — bringing ORDR to chaos.

ORDR is backed by top investors including Wing Venture Capital, Ten Eleven Ventures, Battery Ventures, Mayo Clinic Ventures, and Kaiser Permanente Ventures. For more information, visit www.ordr.net and follow ORDR on X and LinkedIn.

For more information, visit **ordr.net**

Follow Ordr on

Ready to bring ORDR to your chaos?

REQUEST A DEMO