ORDR

SOLUTION BRIEF

AI Protect for Segmentation

Contain lateral movement. Protect Uptime. Enforce Zero Trust.

Microsegmentation built on unrivaled asset intelligence

In today's environment, many of the highest-risk assets can't be patched quickly—or at all. Unmanaged, IoT, OT, and legacy devices often operate continuously, use specialized protocols, and support critical operations.

So when risk appears, security teams face a hard truth: if you can't remediate fast, you need to contain fast. That's what true microsegmentation is for.

Security that acts before incidents happen

ORDR AI Protect for Segmentation helps organizations take action by turning device intelligence into enforceable, least-privilege access—without slowing down the business.

Why Segmentation Fails

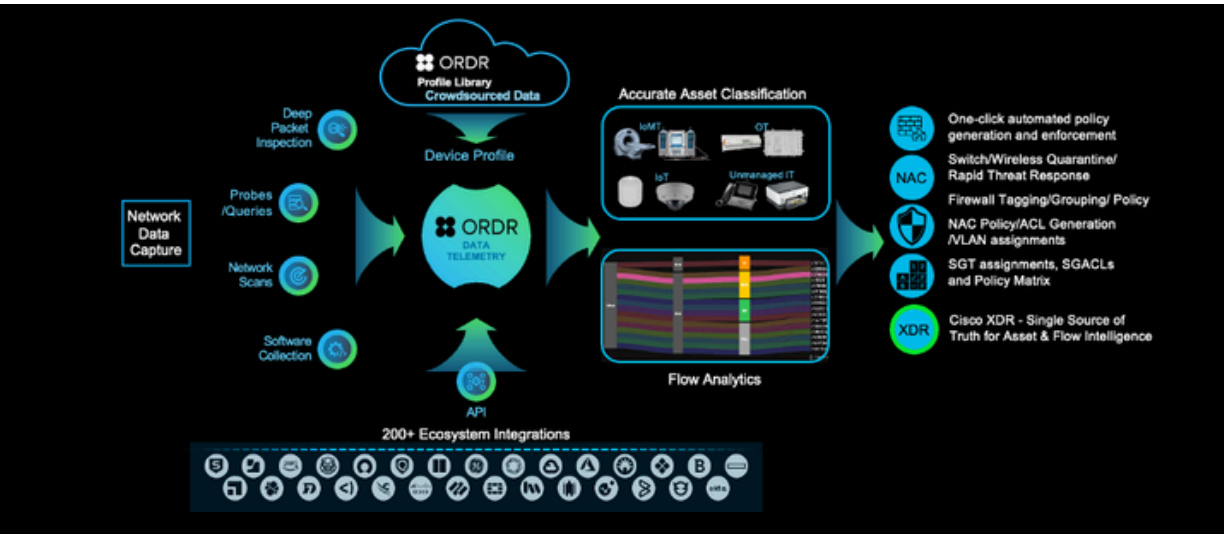
- Policies take months to build manually
- Teams fear breaking clinical or operational workflows
- Networks weren't designed for microsegmentation
- Rules become brittle (IP/VLAN-heavy and hard to maintain)
- Enforcement doesn't scale across unmanaged devices
- Zero Trust stays "planned" but not "proven"

"It's eye opening when you put something like ORDR on your network. It has improved our incident response capabilities."

— Jay Bhatt, CISO, Franciscan Alliance

ORDR removes the friction—so segmentation becomes a repeatable action, not a stalled project.

Segmentation Simplified with ORDR



ORDR AI Protect for Segmentation integrates into enterprise environments to operationalize enforcement through existing network and security controls.

Segmentation enforcement across common infrastructure, including:

- NAC platforms
- network access and switching
- wireless infrastructure
- firewalls and policy engines

You don't need a redesign to take action.

Segmentation without agents or redesign:

- no new inline hardware
- no VLAN redesigns
- no complex manual ACL work
- disruptive re-IP projects

Action happens faster—and enforcement is easier to sustain.

What ORDR Does Differently

ORDR accelerates segmentation by using real observed behavior to recommend policies quickly, validate safely, and enforce through existing infrastructure.

A faster path to enforcement, days, not months:

- Observe device behavior and communication
- Recommend least-privilege policies
- Validate safely (before enforcement)
- Enforce at scale across the environment
- Adapt as devices and risk change

What You Can Achieve with ORDR Microsegmentation

1. **Contain threats faster**
   Reduce lateral movement pathways and isolate risk before it spreads.
2. **Protect uptime**
   AEnforce least privilege in operationally sensitive environments without disruption.
3. **Reduce exposure from unmanaged and unpatchable assets**
   OTake action when remediation isn't possible.
4. **Accelerate Zero Trust outcomes**
   Make Zero Trust measurable through enforceable access control—not just frameworks and dashboards.
5. **Scale enforcement across the enterprise**
   Apply consistent controls across IT, IoT, OT, BMS, and IoMT.
5. **Simplify day-to-day policy management**
   Reduce complexity and keep policies aligned to reality.

Build policies on identity and purpose, not brittle network constructs

ORDR segmentation is driven by what devices are and what they need to do, including:

- device type and role
- location and function
- required services and dependencies
- real communication patterns

So policies hold up even when environments change.
Result: fewer broken rules, less maintenance, more reliable enforcement.

Validate before you enforce, to move with confidence

ORDR helps teams validate what will happen before it happens—so enforcement doesn't come with unnecessary risk.
Result: confident action without disrupting care delivery, production, or uptime.

Dynamic microsegmentation that stays current as risk changes
Your environment changes every day—and segmentation has to keep pace. ORDR keeps segmentation operational as new devices appear, workloads shift, risk posture changes, and abnormal behavior emerges. With ORDR, segmentation stays effective over time, evolving with your environment instead of getting stuck in a one-time project plan.

Why Now
Today's attacks move fast and spread faster. Segmentation is how you stop lateral movement and limit blast radius—protecting critical systems without disruption, so the business keeps running while risk is contained.