ORDR

SOLUTION BRIEF

Rethinking Segmentation: Turning Risk into Resilience with AI

Why segmentation efforts stall — and how ORDR gets you the quick win

The Goal Is Clear. The Execution Isn't.

Most security and network leaders know segmentation is critical for Zero Trust, lateral movement containment, and resilience. Yet despite years of effort and investment, few have moved beyond isolated VLANs or stalled NAC projects.

The reason? Environments have evolved — but tools haven't. Segmentation fails not because of poor strategy or lack of effort, but because it's too complex to operationalize at scale using legacy methods.

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

We believe segmentation should be automated, adaptive, precise, and safe — all delivered through a well-defined, easy-to-use workflow. Instead of brittle ACLs and manual guesswork, organizations need:

- ⊘ Real-time visibility into every connected device with deep context — no agents required
- ⊘ Safe simulation of enforcement before changes go live, so you understand the impact
- ⊘ AI-driven policy recommendations based on behavior and business function
- ⊘ Native enforcement across your existing infrastructure — without rip-and-replace

Segmentation isn't just a checkbox — it should be your first line of defense.

Strategic outcomes you can expect

With ORDR, segmentation moves from a stalled initiative to a real control that protects your business:

- ⊘ Enforce in days, not months
- ⊘ Protect critical assets without operational risk
- ⊘ Visualize and simulate coverage before enforcement
- ⊘ Deploy policies across your existing stack
- ⊘ Prove and track enforcement for auditors with confidence

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

Despite strategic intent, most segmentation efforts fail to deliver at scale. Below are six recurring challenges — and how ORDR addresses them with clarity, automation, and executional confidence.

Critical, high-risk devices remain exposed

Unpatchable systems like medical devices or building controls can't be secured with traditional tools.

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

Compliance audits demand proof of control

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

ORDR maps and enforces least-privilege policies with audit-ready reporting.

Poor visibility means flat networks

Insight without enforcement leaves exposure wide open.

ORDR translates discovery into action through infrastructure-native controls.

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 stall in unmanaged environments

Agent-dependent tools struggle across IoT, OT, and vendor-managed systems.

ORDR augments NACs and Firewalls with precise profiling and automated policy generation.
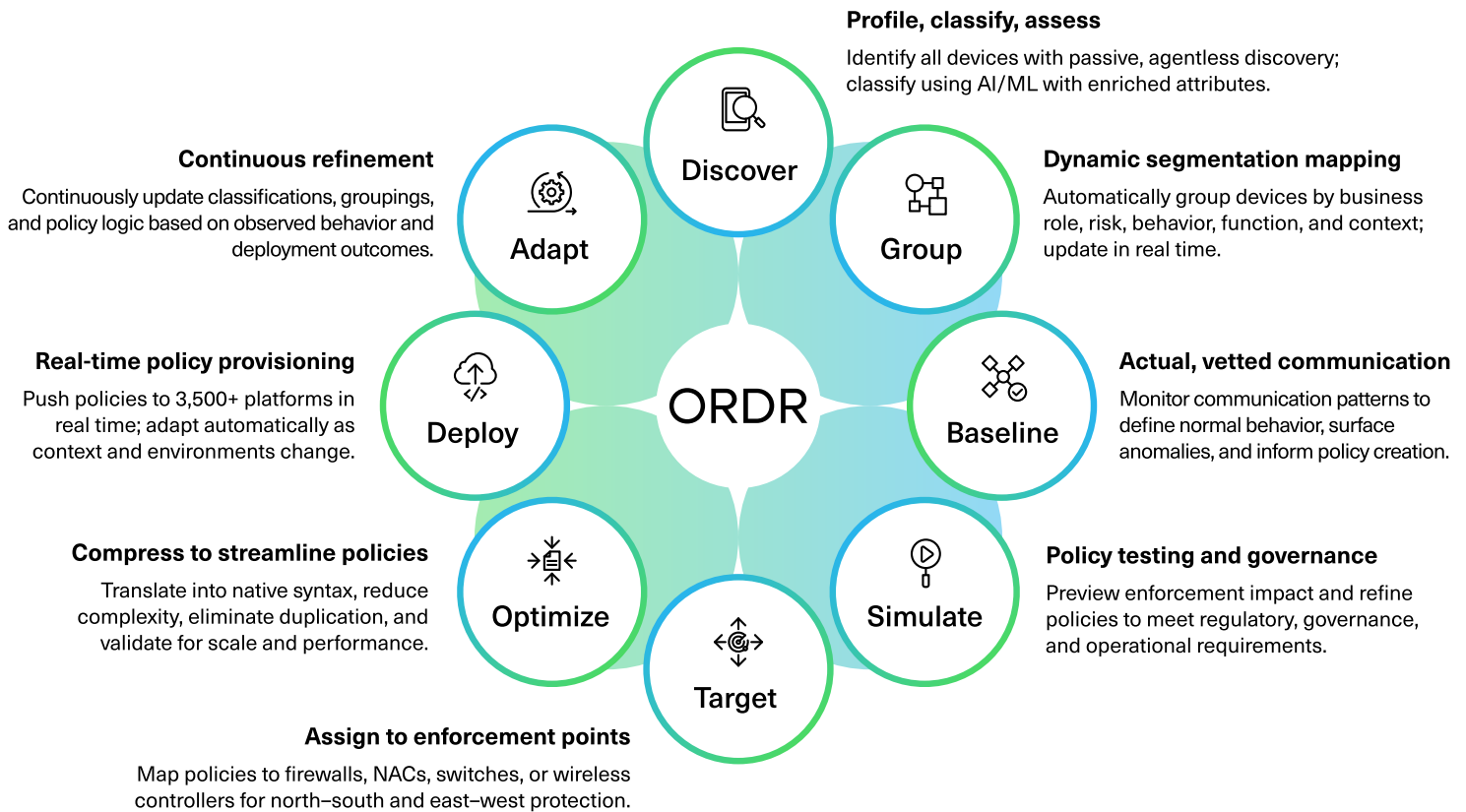
Teams delay while waiting on architecture changes

Tool sprawl and platform migrations slow down segmentation efforts.

ORDR works with your existing infrastructure — and evolves as you do.

:: ORDR

How ORDR Automates Segmentation

Most tools stop at discovery. ORDR delivers true enforcement with an end-to-end lifecycle powered by AI with streamlined workflow management and audit capabilities:

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.

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

Discover

Adapt

Group

ORDR

Deploy

Baseline

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

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

Optimize

Simulate

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

Compress to streamline policies
Translate into native syntax, reduce complexity, eliminate duplication, and validate for scale and performance.

Target

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

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

(X) (in)

Ready to bring ORDR to your chaos?

REQUEST A DEMO