



NAC SOLUTIONS OVERVIEW

ORDR + Your NAC: Agile, Targeted Segmentation That Works

AI-powered enforcement through the access infrastructure you already own.

Why NAC Stops Short of Segmentation

NAC was built for managed endpoints – not today’s explosion of IoT, OT, and legacy systems. Without real-time device intelligence, enforcement breaks workflows, policies sprawl, and segmentation never gets off the ground.

⚡ Why most NAC projects stall:

- Limited visibility into non-user devices like IoT, OT, and legacy systems.
- Static, manual policies that can break workflows or leave gaps.
- Enforcement that’s too rigid, too broad, or too risky to turn on.
- Rollouts delayed by cross-team friction and fear of disruption.

Bottom line: NAC gives you a control point but not the intelligence to use it.

How ORDR Makes NAC Smarter

ORDR transforms your NAC into a real segmentation platform – one that works in complex, dynamic environments.

Why ORDR



Enriches NAC with full visibility of unmanaged and agentless devices.



Auto-generates least-privilege policies in NAC-native syntax.



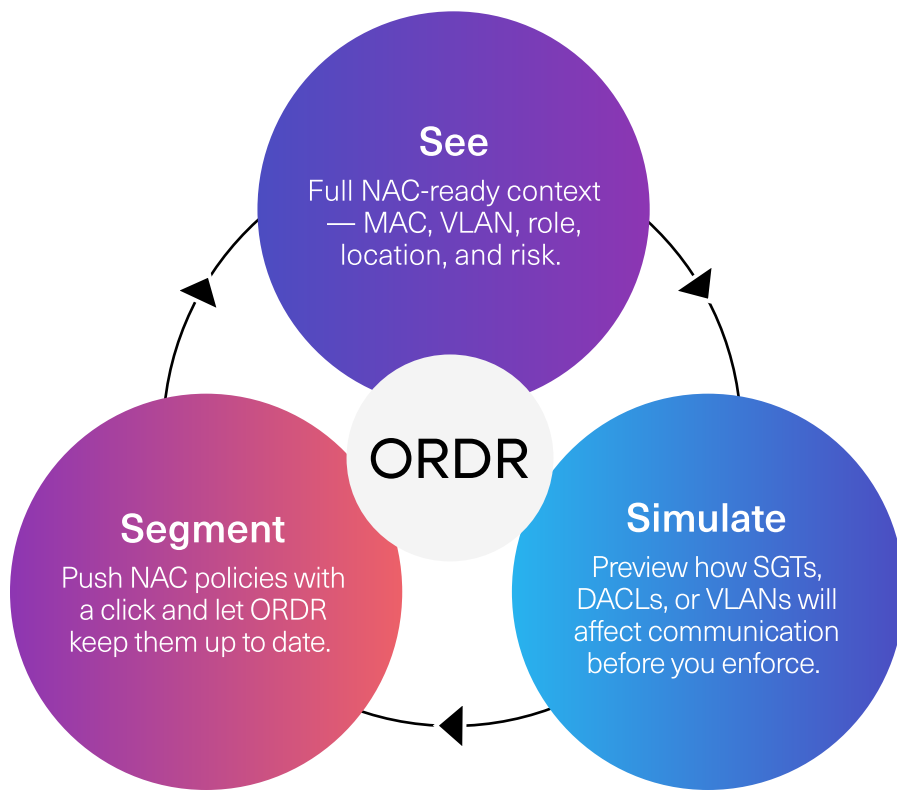
Keeps NAC policies accurate as devices move or change.

With ORDR + NAC, you can:

- ✔ **See everything:**
ORDR discovers and classifies every device — from infusion pumps to badge readers — no agents needed.
- ✔ **Enforce safely:**
ORDR auto-generates segmentation rules in your NAC's native syntax — then keeps them up to date as things change.
- ✔ **Understand behavior:**
We baseline how devices communicate, so you can build policies based on what's normal — not guesswork.
- ✔ **Respond fast:**
Detect threats or anomalies in real time and trigger NAC-based isolation with a click.

See. Simulate. Segment — Through Your NAC.

ORDR makes NAC enforcement viable — not just configured, but working in production. No guesswork, no policy sprawl, no breaking critical systems.



Built for the NAC You Already Use

ORDR integrates natively with today's leading NAC platforms — delivering dynamic, context-rich policies without needing to rip and replace.



Cisco ISE

Assign SGTs and DACLs based on ORDR's real-time classification and behavior modeling.

Eliminate ACL sprawl with dynamic, least-privilege policies.

Keep enforcement accurate as device roles and risks evolve.



HPE Aruba ClearPass

Assign roles or VLANs dynamically based on ORDR's risk and usage insights.

Push access policies for unmanaged devices with Aruba-native syntax.

Maintain segmentation as device states shift.



Fortinet FortiNAC

Build enforcement groups from ORDR's deep IoT, OT, and BMS profiling.

Automate policy push for high-risk or segmented asset types.

Quarantine suspicious devices using real-time risk triggers.



Forescout Platform

Enrich Forescout visibility with ORDR's business and risk context.

Auto-populate policy groups based on device posture and usage.

Adapt enforcement as the environment changes.



Extreme Networks ExtremeControl

Discover and classify every device — even those without agents.

Push segmentation rules across ExtremeControl infrastructure.

Respond to risk and behavior signals in real time.

What You Can Do with ORDR + NAC


ORDR turns your NAC from a gatekeeper into a full enforcement engine. No rip-and-replace – just smarter, safer segmentation.



Zero Trust enforcement
for unmanaged, high-risk, and unpatchable assets.



Threat containment
using behavior-driven NAC quarantine.



Operational segmentation
across cameras, HVAC, BMS, and clinical systems.



Safe rollouts
with phased segmentation by device type.



Audit-ready compliance
with HIPAA, NIST, PCI, IEC frameworks.

Smarter, Precise NAC Segmentation.

NAC wasn't built to understand every device – but ORDR was. By enriching your NAC with real-time intelligence, ORDR automates enforcement across every asset you care about, using the policies you already own.

Without ORDR	With ORDR
<ul style="list-style-type: none">• Visibility limited to managed endpoints• Static posture checks• Manual policy creation• Rigid enforcement approaches• Disruption-prone rollouts	<ul style="list-style-type: none">• Full context into IoT, OT, BMS, and clinical systems• AI-powered behavior baselining and risk scoring• Auto-generated, simulation-ready segmentation• Native NAC syntax: DACLs, SGTs, VLANs, roles• Phased, low-risk segmentation by business priority

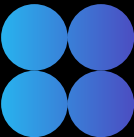
About Us

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