ORDR

Solution Brief

# ORDR + Cisco Identity Services Engine (ISE) Integration

## Segmentation Made Practical

Segmentation is the foundation of Zero Trust, lateral-movement containment, and cyber-resilience — but most organizations stall at isolated VLANs or NAC projects that never scale. Traditional approaches are too complex to operationalize.

ORDR and Cisco change that. Together we've delivered scalable ISE deployments that apply granular device context and full behavioral visibility to protect even the IoT, IoMT, BMS, and unmanaged devices that other tools miss. Security policies are created, simulated, and enforced automatically — without new infrastructure or operational burden.

## From Intelligence to Enforcement

The combined ORDR + Cisco ISE solution simplifies tasks that often overwhelm Zero Trust initiatives. ORDR automates the entire segmentation lifecycle — from discovery and classification to real-time policy enforcement — removing the guesswork and manual effort that slow or derail NAC projects.

- **Get accurate visibility of everything on your network** — ORDR's automated discovery and AI-powered classification engine identifies every device — including make, model, manufacturer, and OS — then groups assets by type, risk, location, and business function, not just IPs or VLANs. ISE admins can immediately leverage this deep context to define access policies. As new devices appear, they're classified and updated automatically, ensuring continuous visibility and consistent enforcement.

- **Detect and contain threats based on behavior** — ORDR baselines both North-South and East-West traffic to understand normal device behavior. Any anomalies or indicators of compromise are flagged in real time, allowing security teams to isolate or block malicious traffic instantly according to policy.

- **Generate and update dynamic policies** — Using real-time traffic data and AI/ML modeling, ORDR produces tailored segmentation policies in native ISE syntax for every device group, taking into account business role or location. Administrators get precise, context-aware recommendations they can apply with confidence.

- **Simulate and refine controls** — ORDR's AI-powered policy-matrix visualization maps how devices communicate at any level of detail — application, subnet, or business context. Teams can run "what-if" simulations to fine-tune rules, validate changes, and preview enforcement impact before going live.

- **Enforce and adapt automatically** — With a single click, ORDR pushes policies directly to ISE for enforcement. As devices appear, disappear, or change behavior, ORDR re-evaluates groups and automatically recalibrates policies so segmentation remains accurate and aligned with business goals — no manual upkeep required.

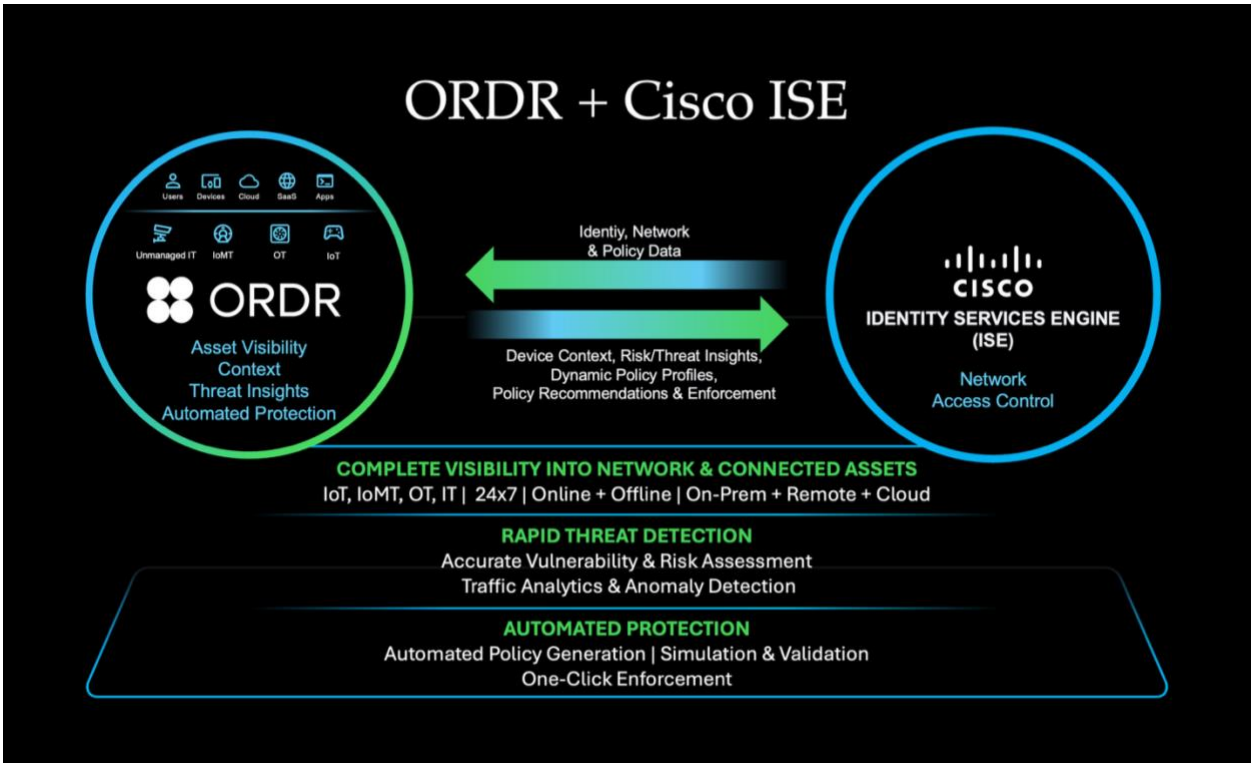
 

# How it Works

ORDR's turn-key, bidirectional integration with Cisco ISE collects, correlates, and deduplicates asset data to create a single source of truth.

- **Deduplication engine**: cleans and unifies all records whether they originate from ORDR, ISE, or other ecosystem tools.
- **Correlation engine**: merges identity, policy, and risk-posture data so each device record is complete and actionable.
- **Continuous feedback loop**: ORDR sends ISE advanced classification and risk posture for IoT devices, and notifies ISE when it detects compromised devices through behavior analysis. It also auto-generates policy recommendations that can be simulated, fine-tuned, and enforced automatically.

With this integration, organizations can gain complete visibility into every connected device and deploy microsegmentation in days — not months.




# ORDR Ecosystem Integrations

ORDR integrates with leading security, networking, infrastructure, IT, and clinical platforms to unify and enrich device context. All data is consolidated into the ORDR Data Lake, giving teams the most complete and accurate view of every connected device across the organization. These enriched insights improve security-team efficiency and strengthen the defenses of all integrated tools.

ORDR

# About Us

ORDR is the leader in AI-powered segmentation, securing some of the largest organizations in healthcare, transportation, manufacturing, and financial services. Having analyzed more than 100 million unique device types, the platform is purpose-built to solve the toughest security challenge: unmanaged and IoT assets that put business uptime on the line. By turning intelligence into swift, automated protection, ORDR helps teams contain threats, reduce exposure, and keep operations resilient — 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 Twitter and LinkedIn.

*For more information, visit ordr.net*

*Follow ORDR on*

Ready to bring ORDR to your chaos?

Request a demo