



## The ORDR AI Protect Platform

# Segmentation Insights

*Identify VLAN mismatches and resolve them with confidence.*

## Rethinking Segmentation in the Age of Headless and Agentless Devices

As organizations adopt more headless and agentless devices across critical infrastructure, traditional segmentation strategies are being pushed to the limit. These devices — from medical systems to building controls — often can't be patched or monitored like standard IT endpoints. The result: networks with vulnerable devices intermingled with general-purpose endpoints, increasing lateral movement risk and complicating Zero Trust implementation.

Segmentation is no longer just a design principle — it's a security imperative.

But before enforcing policies, you need to see what's really happening across your network. That starts with understanding your VLAN topology.

## The Role of Segmentation Insights

The **Segmentation Insights dashboard** is a practical tool within the ORDR AI Protect platform that provides real-time visibility into how devices are distributed across VLANs, subnets, and physical locations. It helps security and network teams:

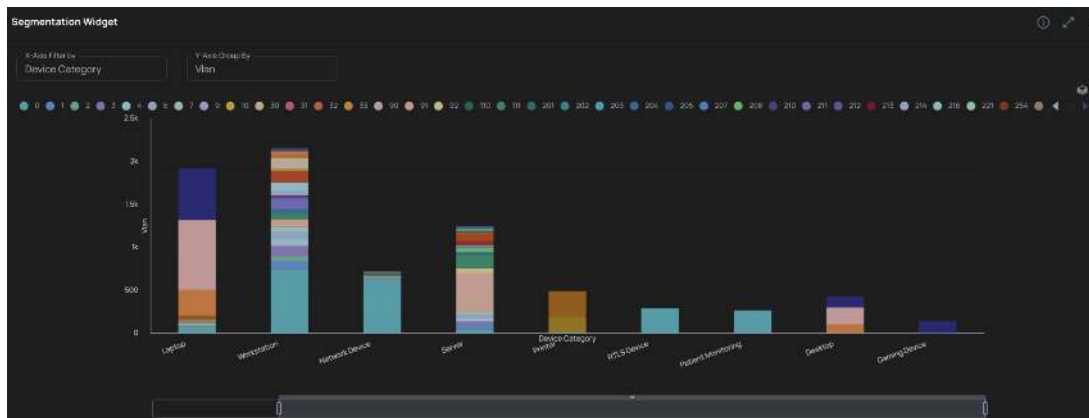
- Validate network design and identify segmentation gaps
- Pinpoint critical devices that may be co-located with standard endpoints
- Assess the risk of lateral movement within shared VLANs
- Understand device-to-VLAN relationships across all sites

By mapping the second layer of the network stack, the VLAN dashboard becomes a foundation for smarter segmentation and Zero Trust initiatives.

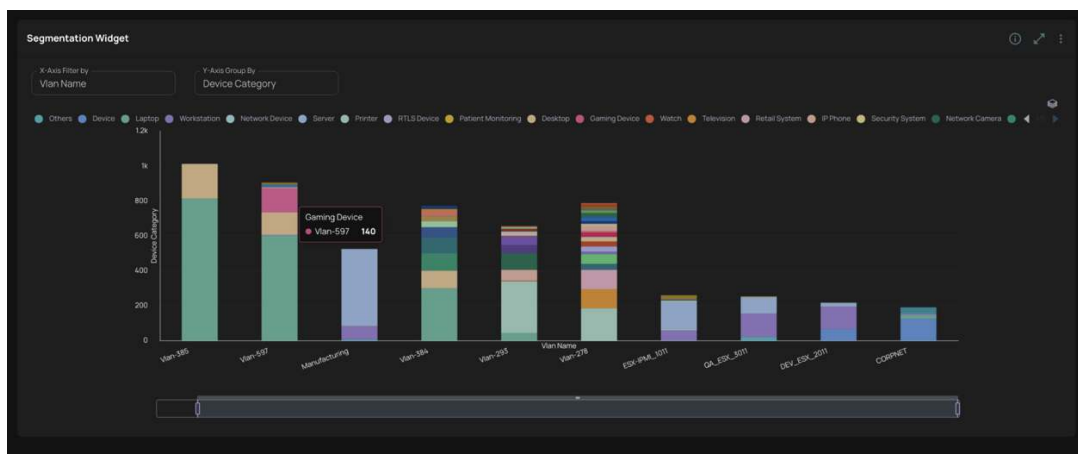
### Core Capabilities

- **Interactive VLAN and Subnet Mapping**  
Browse by VLAN, subnet, and site to see exactly how devices are grouped — and whether those groupings make sense.
- **Device Context and Grouping**  
View devices by group, category, or profile to see how medical, IoT, shadow IT, and managed devices are distributed across VLANs.
- **Exposure Analysis**  
Identify whether critical infrastructure is placed in flat networks alongside unmanaged or user endpoints.
- **Shadow IoT Pattern Recognition**  
Surface proliferation of unmanaged and agentless devices that may introduce risk.
- **Remediation Shortcuts**  
Initiate ticketing workflows, reassign VLANs, or adjust device attributes — right from the Explorer.

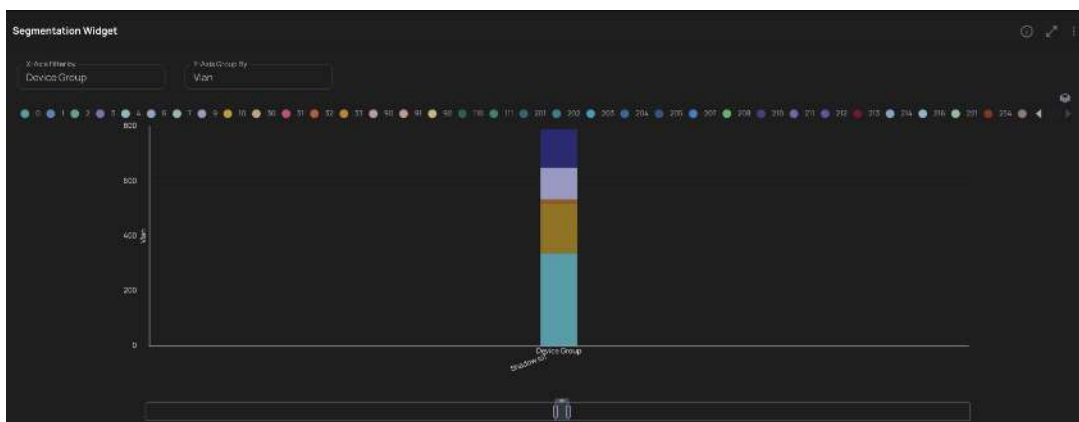
# Visual Insights



*Quickly spot at-risk VLANs where unmanaged or critical devices may be commingled — a common root cause of lateral movement exposure.*



*Validate whether your segmentation design reflects actual device use — ensuring VLAN policies align with real-world infrastructure.*



*Uncover device groups that span multiple VLANs, helping identify policy gaps or inconsistencies across locations.*

## Practical Questions It Helps Answer

These are the kinds of questions that often come up when reviewing segmentation posture or preparing to implement Zero Trust policies. The Segmentation Insights dashboard helps bring quick answers to the surface:

- Which of my critical devices share VLANs with standard endpoints?
- Are my security cameras and other agentless devices segmented appropriately?
- Where are shadow IoT devices most concentrated?
- How consistent is VLAN usage across my distributed locations?
- How many devices are associated with VLAN X or subnet Y?

## Built for Real-World Segmentation Challenges

Segmentation isn't just a policy — it's a moving target shaped by device sprawl, changing environments, and operational realities. The VLAN dashboard is designed to work with how teams operate today:

- **Supports remediation** via integrations with ITSM platforms and NAC/firewall vendors
- **Enables action**, not just visibility — assign tags, trigger workflows, or update policies in context
- **Used across dashboards** like Asset Insights, VLAN Distribution, and Medical VLAN Distribution
- **Scales across environments**, adapting to device population changes in real time

## Why It Matters

Gaining visibility into your VLANs isn't just about network hygiene — it's foundational to risk reduction, Zero Trust enforcement, and operational resilience. Whether you're reviewing segmentation posture, validating access policies, or preparing for an audit, ORDR's Segmentation Insights dashboard provides the clarity needed to act with confidence.

If you're aiming for practical segmentation — the kind that actually gets implemented — it starts here.

*To learn more or see your own VLANs in action, reach out for a personalized walkthrough.*



## 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](http://www.ordr.net) and follow ORDR on Twitter and LinkedIn.

*For more information,  
visit [ordr.net](http://ordr.net)*

*Follow ORDR on*



Ready to bring ORDR to your chaos?

[Request a demo](#)