ORDR

The Segmentation Playbook: 6 Blockers and How to Beat Them

Practical guidance to beat the risks, gaps, and complexity that's stalling segmentation projects.

What you'll learn

- ***Why*** segmentation efforts stall in IoT- and unmanaged device-heavy environments.
- ***How*** to move from visibility to enforcement without a complete overhaul.
- ***Steps*** to overcome common blockers and build momentum for segmentation.

Introduction: Why Segmentation Feels Hard— and Why It's Worth It

If you've tried to isolate unscannable medical devices, separate your POS from your HVAC, or build network zones in a plant, you've felt the friction. Across complex industries like healthcare, manufacturing, retail, and finance, segmentation isn't just a compliance checkbox — it's often the only practical way to protect high-risk, unmanaged devices.

The problem? Knowing you need segmentation isn't the same as being ready to implement it. Teams run into limitations with tools, visibility, and coordination, making it hard to turn intent into action. Even with the best intentions, the reality of existing infrastructure, vendor sprawl, and the fear of disrupting operations can stall progress before it even begins.

This guide is here to help you get unstuck. We'll explore the blockers that slow down segmentation and show how teams like yours are making practical, sustainable progress. With the right steps, you can reduce risk, support compliance, and keep your operations running, without needing a complete platform overhaul or a "perfect plan" before you begin.

Blocker 1 The Devices You Need Most Are the Hardest to Protect

Why this matters

Across hospitals, factories, and retail environments, many of the devices you rely on – HVAC systems, elevators, backup power, medical equipment – are unmanaged and can't easily be patched or taken offline for updates.

They're mission-critical, yet they become pivot points for attackers, leaving teams feeling stuck between maintaining uptime and addressing risk. The result? Organizations delay segmentation while exposure grows.

Common pitfalls

- *Ignoring high-risk devices* because they're hard to manage or patch.
- *Using VLANs alone* for segmentation without true isolation.
- *Waiting for complete inventories* instead of starting with what's known.
- *Failing to track and communicate progress*, stalling momentum and alignment.

Actionable Steps

- ***Use segmentation to protect high-risk devices*** while maintaining uptime and reducing risk.
- ***Identify unmanaged, high-risk assets early***, such as badge readers, imaging systems, POS terminals, and critical legacy systems.
- ***Build segmentation policies*** around device behavior, operational criticality, and exposure.
- ***Pair segmentation with patching efforts*** to protect devices that can't be easily updated.
- ***Start small to demonstrate progress*** by isolating a targeted group of high-risk devices and showing value.

IoT and unmanaged devices hold 64% of mid- to high-level enterprise risks.

- Rise of the Machines, 2024

Read Report

Blocker 2 You Can't Prove Control, So Compliance Gaps Persist

Why this matters

Regulatory frameworks like HIPAA, PCI, NIST, and ISO increasingly require proof of segmentation and least-privilege controls across critical assets. But in environments with unmanaged and IoT-heavy devices, many organizations struggle to demonstrate these controls during audits.

Without clear evidence of enforcement, audits become stressful and risky, leaving teams exposed to compliance gaps. The result? Organizations delay segmentation while compliance exposure grows.

Common pitfalls

- *Assuming visibility alone satisfies compliance* without demonstrating enforcement.
- *Delaying segmentation while waiting for complete coverage,* leaving audit gaps.
- *Lacking documentation of segmentation policies, baselines, and logs* required for evidence.
- *Treating compliance as separate from segmentation initiatives,* creating misalignment.

Actionable Steps

- ***Align segmentation with audit frameworks*** to document and prove control.
- ***Capture and maintain segmentation policies, baselines, and logs*** aligned with HIPAA, PCI, NIST, and ISO requirements.
- ***Collaborate with compliance teams*** to ensure documentation and evidence readiness.
- ***Launch targeted segmentation in prioritized areas*** to demonstrate measurable enforcement without waiting for environment-wide perfection.
- ***Show enforcement evidence, not just intent,*** to simplify audits and reduce compliance risk.

Blocker 3 Flat Networks Persist Without Proactive Controls

Why this matters

Visibility is essential for finding unmanaged and high-risk devices, but it doesn't reduce risk on its own. Without enforcement, risky devices remain exposed on flat networks, creating easy pathways for attackers to move laterally.

Many teams pause after achieving visibility, thinking they've reduced risk, when in reality, the work has just begun. Visibility without enforcement leaves gaps that attackers can exploit while giving a false sense of security.

Common pitfalls

- *Assuming visibility alone equals security,* without enforcing policies.
- *Relying on VLANs,* believing they provide effective isolation.
- *Treating segmentation as a one-time project* rather than an ongoing process.
- *Overlooking enforcement capabilities already available* (NAC, ACLs, firewalls).
- *Delaying action due to perceived complexity,* keeping networks flat and exposed.

Actionable Steps

- ***Enforce segmentation based on visibility findings*** to transform insight into action.
- ***Leverage NACs, ACLs, and firewalls you already have*** to begin policy enforcement.
- ***Use device profiling and behavioral data*** to build and refine segmentation policies that adapt to your environment.
- ***Audit VLAN configurations*** to find and close isolation gaps that visibility reveals.
- ***Treat segmentation as a continuous workflow,*** refining policies as devices and behaviors change to prevent your network from staying flat.

85% of healthcare VLANs are heavily polluted with mixed assets, exposing critical and legacy devices to broader risks.

- Rise of the Machines, 2024

Read Report

Blocker 4 Inflexible Policies Can't Stop Lateral Movement and Exfiltration

Why this matters

Attackers don't just move laterally within your environment; they also exfiltrate data across IT, IoT, and OT networks, exploiting flat or static segmentation to maintain persistence and evade detection.

Even when anomalies are detected, teams often lack the device context and flexible segmentation needed to quickly isolate threats, slowing containment and increasing incident impact.

Common pitfalls

- *Using segmentation only as prevention* without planning for active incident containment.
- *Delaying segmentation adjustments during incidents,* missing the chance to contain threats.
- *Lacking integration between detection, monitoring, and segmentation,* slowing response.
- *No traffic analysis,* leaving teams in the dark about how their devices behave in real time.
- *Failing to simulate east–west and north–south scenarios,* leaving workflows untested.

Actionable Steps

- ***Use segmentation for active containment*** to limit lateral movement and reduce blast radius during incidents.
- ***Leverage real-time behavior signals*** to adjust segmentation dynamically when threats are detected.
- ***Integrate detection and monitoring with segmentation*** for faster, automated containment.
- ***Apply asset context, device role, and typical traffic patterns*** for precise isolation during incidents.
- ***Test containment workflows*** using simulated lateral movement and exfiltration scenarios to refine readiness.

32% of enterprise assets connect to both the internet and communicates internally.

- Rise of the Machines, 2024

Read Report

Blocker 5 NAC Segmentation Stall in Complex Environments

Why this matters

Network Access Control (NAC) platforms like Cisco ISE and Aruba ClearPass are often positioned as key segmentation tools. However, NAC deployments frequently stall or remain incomplete due to profiling gaps, complex enforcement logic, and concerns about operational disruption.

Teams hesitate to enforce NAC policies in environments with diverse unmanaged, IoT, and OT devices, where a single misconfiguration can disrupt critical operations. This fear of "breaking something" keeps NAC initiatives stuck, leaving high-risk devices and vendor-managed assets unsegmented and exposed.

Common pitfalls

- *Treating NAC as the sole segmentation strategy,* especially in unmanaged and IoT-heavy environments.
- *Attempting broad NAC deployments* without scoping high-impact areas.
- *Relying on incomplete or inaccurate device profiling,* leading to unknown devices bypassing controls.
- *Using NAC only for wireless networks,* while wired enforcement stalls due to complexity.
- *Fearing operational disruptions,* leading to indefinite delays in NAC enforcement.

What works

- ***Position NAC as part of a layered segmentation*** strategy, complementing ACLs, VLANs, and firewalls.
- ***Scope NAC enforcement to targeted, high-impact use cases*** like vendor-managed IoT/OT zones and third-party access points.
- ***Refine NAC policies using accurate device profiling and behavior analysis*** to minimize bypasses.
- ***Pilot NAC on specific device groups,*** such as IP cameras or HVAC systems, to validate enforcement safely.
- ***Pair NAC with monitoring and detection*** to identify post-access threats and improve containment readiness.

40% of organizations citing implementation complexity as their primary barrier [to microsegmentation implementation].

- Cybersecurity News

Microsegmentation Technical Deep Dive into Network Security

Blocker 6 Tool Sprawl and Switching Architecture Add Drag

Why this matters

Organizations often face pressure to implement segmentation while simultaneously navigating firewall upgrades, NAC refreshes, or vendor transitions. Tool sprawl across visibility platforms, NAC, firewalls, and switches create confusion over where to start and which tools to use for enforcement.

Infrastructure refreshes and architecture debates can stall progress, leading to delays and uncertainty. While teams wait for the "perfect stack" or a consolidated environment, high-risk devices remain unsegmented, leaving organizations exposed while planning drags on.

Common pitfalls

- *Delaying segmentation until after tool migrations or infrastructure refreshes,* leaving devices exposed in the meantime.
- *Assuming a single vendor stack is needed* before segmentation can begin.
- *Overcomplicating tool selection and architecture decisions,* causing stalled initiatives.
- *Prioritizing architecture debates over risk reduction,* losing momentum toward tangible progress.

What works

- ***Anchor segmentation around clear, high-impact goals*** to reduce exposure now, even while broader plans are evolving.
- ***Align with IT and security teams*** to clarify current enforcement capabilities and where segmentation can proceed immediately.
- ***Treat segmentation as an iterative process,*** refining policies as infrastructure changes.
- ***Build a roadmap for tool and platform integration*** without letting it stall immediate progress on risk reduction.

Conclusion: From Stuck to Started

Segmentation can feel overwhelming, especially in environments filled with unmanaged devices, evolving threats, and tool sprawl. But you don't need a perfect plan or a complete platform overhaul to begin reducing risk.

Segmentation isn't a one-time project. It's a practical, evolving capability that grows with your environment and adapts as threats change. By shifting your mindset from planning to progress, you can build the confidence, alignment, and momentum needed to strengthen your security posture while keeping operations running.

Every step forward, however targeted, reduces exposure, supports compliance, and builds resilience. You can move from stuck to started, proving what's possible while preparing for what's next.

Key takeaways:

Segmentation is progress, not perfection. Each targeted step you take reduces risk and builds momentum.

Align efforts with compliance and operational needs to demonstrate measurable control.

Use visibility to inform action transforming insight into enforcement.

Keep segmentation adaptable refining as your environment and threats evolve.

Momentum matters. Starting now positions your organization to scale and strengthen resilience over time.

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

ordr.net

Follow Ordr on

Ready to take control of your attack surface?

Get a personalized demo to see how Ordr's Asset Intelligence can help you identify vulnerabilities, reduce risks, and enhance your security posture.

REQUEST A DEMO