ORDR

Why Patching Alone Won't Save You

A Guide to 6 Segmentation Challenges in IoT-Heavy Environments

(And How to Overcome Them)

What you'll learn

- ***Why*** patching alone can't keep up with IoT and unmanaged devices.
- ***What*** makes segmentation practical and effective in IoT-heavy environments.
- ***How*** to reduce risk and protect critical devices without disrupting operations.

Why Patching Alone Won't Save You

Patching is typically the first step in security, and it works well in traditional IT environments with modern, managed devices. But in environments with IoT, such as medical devices and facilities systems, patching alone isn't enough. Many of these devices can't be patched quickly, if at all, and remediation often stalls due to vendor restrictions, operational needs, or outdated systems.

That's where segmentation comes in. Whether you're running a hospital, a manufacturing floor, or a retail space, segmentation is often the only realistic way to protect devices that can't be patched or taken offline.

The challenge is that segmentation has a reputation for being too complex or disruptive, often pushed to the end of the security roadmap — if it's considered at all. But it doesn't have to be this way.

In this e-book, you'll learn why segmentation efforts often stall, what it takes to make them practical, and how segmentation can become a scalable first line of defense for devices you can't patch or take offline.

IoT and unmanaged devices make ***up 42% of enterprise assets*** *yet represent* ***64% of mid- to high-level risks.***

- Rise of the Machines, 2024

Read Report

Challenge 1 Patching Can't Keep Up

Patching is often the first line of defense for security, and for many IT systems, it works. But in environments with a lot of IoT, facilities, and unmanaged specialty devices, patching isn't always practical. In industries like healthcare, manufacturing, retail, and transportation, patching either requires a lot of time or cannot be implemented at all.

What to watch out for:

For security leaders balancing risk reduction with operational uptime, patch management for non-IT devices comes with real-world challenges:

- *Sheer volume of vulnerabilities:* New vulnerabilities appear daily, creating a backlog while exposure windows stay open.
- *Cost/risk trade-offs:* Critical devices may be upgradeable, but the costs or operational risks are too high to justify patching.
- *Vendor/manufacturer dependencies:* Many devices require vendor coordination or government re-approval, delaying remediation even when patches exist.
- *Operational dependency:* Taking devices offline for patching or testing can disrupt patient care, production lines, or building operations.
- *Legacy and unpatchable systems:* Many industries rely on outdated but essential devices to achieve core business objectives, creating persistent risk as they remain online.

How to overcome:

Segmentation shouldn't be an afterthought. It can work alongside patching to restrict high-risk devices to only the communications they need while patching plans are in progress, protect systems waiting for vendor approvals, and secure legacy devices that can't be updated — all while maintaining uptime.

*40,009 CVEs were released in 2024, a **39%** increase from the previous year.*

- MITRE's CVE Program

Challenge 2 You Can't Segment What You Can't See

Visibility is the first step to segmentation, but it often falls short in environments with unmanaged, connected assets. Many of these devices can't run agents or authenticate securely, making them hard to monitor or control. At the same time, most CMDBs lack complete data on these assets, leaving them invisible to security teams. If you don't know what's on your network, you can't protect or segment it.

What to watch out for:

Traditional inventory tools fall short in IoT-heavy environments, creating challenges beyond basic discovery:

- *Blind spots in shared networks:* Devices like infusion pumps, badge readers, and HVAC controllers often run Windows OS and share VLANs with critical systems, creating lateral movement risks during an attack.
- *Incomplete context:* Even when discovered, devices may appear only as IP or MAC addresses, lacking details like type, owner, location, or function – making enforcement risky.
- *No user identity anchor:* Unlike managed IT devices tied to user identities and network authentication, IoT and BMS devices often lack both, removing an anchor for policies and secure access.
- *Dynamic environments:* Devices like portable X-ray machines and IoT sensors frequently move or change IPs, requiring continuous visibility to maintain accurate policies. Without it, teams resort to rigid network structures and manual processes that limit mobility.
- *Hidden risks in legacy systems:* Older devices with outdated software may not appear in inventories and often lack secure authentication yet remain connected and exposed.

How to overcome:

Visibility needs to go beyond discovery. Continuous, passive monitoring paired with accurate classification, contextual insights, and logical grouping helps build complete inventories across unmanaged devices in IT, IoT, IoMT, and BMS environments.

Using context and real-world behavior enables targeted, confident segmentation of high-risk, unmanaged assets – without disrupting operations.

*"If you don't have the visibility, everything else is **100**% more challenging.... whether that be managing vulnerabilities, whether it be segmentation."*

- Smitty Searless
IT Security Engineer, Emplify Health

Watch Webinar

Challenge 3 No One Owns Segmentation

Unmanaged devices, such as IoT, IoMT, and BMS devices, often fall between teams with unclear ownership and accountability. Without clear alignment across stakeholders, segmentation initiatives stall before they even begin. If no one owns it, no one drives it forward.

What to watch out for:

Segmentation requires cross-functional cooperation, but misaligned priorities and unclear ownership can create friction:

- *Enclaves vs. enclaves:* HVAC and building systems may be managed by facilities, medical devices by biomed or HTM, and networks by IT or security, leaving segmentation stuck between teams.
- *Mission vs. security tension:* Clinical and OT teams prioritize uptime and care delivery, while security teams prioritize reducing risk, leading to concerns that enforcement will disrupt workflows.
- *Budget and accountability gaps:* Security teams see the need for segmentation, but operational teams hold the budget and may deprioritize it, leading to gaps or wasted spend that doesn't serve broader organizational needs.
- *Different success metrics:* Facilities care about uptime, clinical teams focus on safety, and security teams focus on risk reduction, with no shared language to align priorities.
- *Fear of complexity:* Teams worry about managing policies, responding to alerts, and troubleshooting, making them hesitant to move forward.

How to overcome:

Segmentation isn't a burden — it's a way to protect uptime while reducing risk. Define shared success metrics like uptime, safety, and reduced exposure, then run targeted pilots on critical devices to build confidence and quick wins with minimal disruption. Early success creates cross-functional alignment before broader rollout.

"Early wins created momentum. Clinical engineering and networking teams saw tangible benefits and became eager to segment more devices."

- Smitty Searless
IT Security Engineer, Emplify Health

Read Blog

Challenge 4 Tools Don't Translate Insight Into Action

Visibility tools excel at identifying vulnerabilities and gaps. But without alignment with enforcement tools, segmentation stalls between "knowing" and "doing." Without coordination across NAC, firewalls, and inventories, high-risk, unmanaged devices remain exposed.

What to watch out for:

Enforcement gaps on unmanaged, non-traditional assets leave high-risk pathways unprotected.

- *Visibility without enforcement:* Inventory and vulnerability tools highlight unpatched, high-risk devices but can't isolate them, leaving insight without impact.
- *Controls lack context:* NAC and firewalls can enforce policies but often lack device classification, functional roles, or behavioral data needed to determine safe network access and segmentation.
- *Manual workflow friction:* Teams manually translate discovery insights into enforcement policies, slowing progress and introducing errors.
- *Policy misfires:* Enforcing segmentation without understanding device criticality, dependencies, and communication needs can disrupt operations, making teams hesitant to act.

How to overcome:

Insight only moves the needle if it drives action. By connecting asset intelligence — like device profiles, context, and behavior — with NAC and firewall enforcement, teams can turn visibility into precise segmentation. This enables safe, phased enforcement on high-risk devices while maintaining uptime and reducing exposure.

Challenge 5 Segmentation Feels Too Complex and Heavy

Manual segmentation often seems infeasible for large, diverse fleets of unmanaged devices. Overly manual efforts stall under scale or risk breaking critical workflows. For segmentation to succeed, it needs to be practical — and the process needs to be simpler, using intelligent automation to replace manual, error-prone steps.

What to watch out for:

Segmentation is often deprioritized because it's perceived as too heavy a lift:

- *Manual policy writing:* Creating zones and groups, VLANs or ACLs, and firewall rules for thousands of devices is slow, error-prone, and requires deep knowledge of device dependencies and communications.
- *Validation fears:* Teams worry that segmentation could block critical communications needed for patient care, manufacturing, or building operations, leading to cautious delays.
- *Resource constraints:* Segmentation projects compete with operational priorities and are seen as too resource-intensive.
- *Inconsistent enforcement:* Different teams apply segmentation differently, leading to policy gaps, overlaps, or drift.
- *Analysis paralysis:* The fear of "getting it wrong" prevents teams from starting, as they believe perfect policies and full coverage are needed before making progress.

How to overcome:

Segmentation doesn't have to be overwhelming. Start with policy simulation and targeted enforcement on high-risk areas to build confidence. By prioritizing automation and phased implementation, segmentation becomes practical, scalable, and aligned with operational priorities — not a side project that stalls.

Challenge 6 Trying To Do It All Stalls Progress

Segmentation projects often stall because teams try to do too much at once. Attempting environment-wide segmentation can overwhelm teams and paralyze progress. But segmentation doesn't have to be all-or-nothing to be effective.

What to watch out for:

Segmentation is often deprioritized because it's perceived as too heavy a lift:

- *Analysis paralysis:* Teams wait for perfect inventories or network overhauls before starting segmentation, delaying action while risk remains. Segmentation is a journey, not a one-time effort.
- *Scope creep:* Trying to segment every device, VLAN, or environment at once leads to bloated projects that stall before meaningful enforcement happens.
- *Operational disruption fears:* Teams worry that segmentation will block critical communications needed for patient care, facility operations, or production lines.
- *Lack of prioritization:* Without clear criteria, teams spread efforts too thin, addressing low- and high-risk areas simultaneously.
- *Unclear success metrics:* Teams stall when they don't define what "good enough" looks like for initial phases, preventing progress.
- *Undefined milestones:* Without clear milestones and target dates, segmentation projects lose momentum and fail to deliver results.
- *Resource allocation and commitment:* Top-down sponsorship, multi-team alignment, committed resources, and clear ownership are essential to execute any segmentation project.

How to overcome:

Segmentation succeeds when you start small and focus on what matters. Begin by isolating high-risk, unpatchable devices like legacy imaging systems or unmanaged HVAC controllers. Expand iteratively as confidence and visibility improves.

By setting clear, phased milestones, organizations can advance segmentation in practical steps while continuously improving over time — turning it into an achievable resilience strategy rather than an overwhelming ideal.

It's Time to Make Segmentation Work

In IoT-heavy environments, perfect patching is unrealistic. But reducing risk is still critical, and segmentation is the path to do that. When patching can't keep up, segmentation becomes the first and most practical line of defense, helping reduce exposure while keeping operations running.

Takeaways:

Resilience over perfection

Segmentation isn't a last resort. It's a practical, scalable strategy to reduce risk while maintaining uptime when patching falls short.

Start with high-risk assets

Isolate critical devices that can't be patched or taken offline, reducing exposure without disruption.

Complete the workflow

Visibility alone isn't enough. Pair discovery with profiling, policy creation, simulation, and orchestration to transform segmentation from theory into confident, practical enforcement.

Progress, not paralysis

Segmentation doesn't have to be all-or-nothing. A phased, targeted approach helps teams prove value, gain buy-in, and build momentum without overwhelming resources.

"Segmentation is not only possible, it's practical.... We were able to isolate high-risk devices, reduce our attack surface, and keep operations running. That's a big win."

- Smitty Searless
IT Security Engineer, Emplify Health

Watch Webinar

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