Report **2024**

ORDR

Rise *of the* Machines

The State of IoT, OT, and Agentless Devices

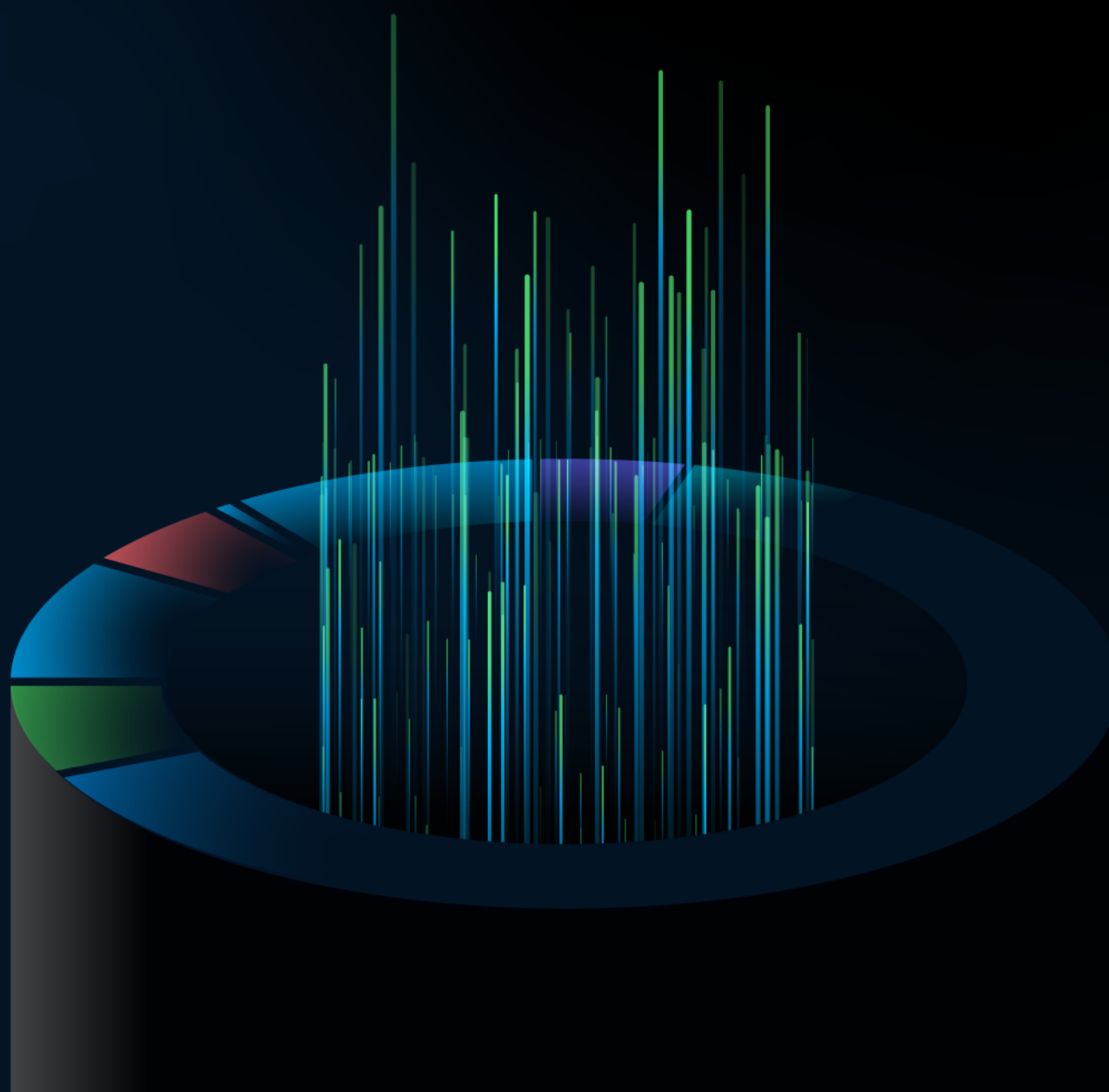


Table of Content

Executive Summary and Key Results 3

Why All Assets Matter: Washington University in St. Louis 4

Device Trends and Blind Spots 5

Beyond IT and Security Tools 6

The Most Overlooked Critical Assets 7

The Growing Threat of Shadow IoT 8

IT and Security Coverage Gaps 9

Vulnerabilities and Enterprise Risks 10

Overwhelming CVEs 11

Why Context Matters 12

Prioritization in Healthcare 13

Traffic Trends and Risks 14

Internet Connections and Threats 15

Internal Traffic Risks 16

The Path Forward: Reducing Agentless Exposure 17

An Asset Attack Surface Maturity Model 18

In Detail: Managing Attack Surface 19

Executive **Summary**

The Expanding Attack Surface of Agentless Assets

Cybersecurity is at a critical juncture. While attack surface management solutions are improving, unmanaged assets like IoT, OT, and other specialty systems remain a major blind spot and are rapidly multiplying in numbers. These devices, which account for **42%** of enterprise assets, often lack basic security controls and sufficient monitoring. Alarmingly, they represent **64%** of all mid- to high-risk assets.

Hostile actors, including nation-states like North Korea and Russia, increasingly exploit these vulnerabilities as the "path of least resistance." Over **14%** of agentless devices not only connect to the internet but also communicate laterally with an average of **six** other devices, creating extensive attack pathways.

Securing today's hyperconnected environments requires a shift from focusing solely on managed endpoints to addressing risks across all connected assets — especially those previously overlooked.

Key Results

Major Blind Spots

42%

of enterprise devices are agentless.

Higher Risk

64%

of mid- and high-level enterprise risks are associated with agentless devices.

Visible Attack Pathway

14%

of agentless devices connect to both the internet and internal networks.

Connected Blast Radius

6.2

is the average number of devices that an agentless asset communicates with.

Why Asset Management Across All Assets Matters: Washington University in St. Louis

Washington University in St. Louis (WashU), a private research university with over 20,000 staff and faculty and 15,000 students, spans networks that support both academic and specialized environments, such as healthcare. This diverse landscape of IT, facilities, medical, research, and BYOD devices presents unique challenges for asset and exposure management.

WashU

"In our diverse environment, unmanaged devices created serious blind spots. Asset classification and tracking gave us the visibility needed to assess risks, prioritize security, and strengthen our campus-wide security posture across WashU's complex networks."

— Joey Smith, Information Security Analyst, WashU

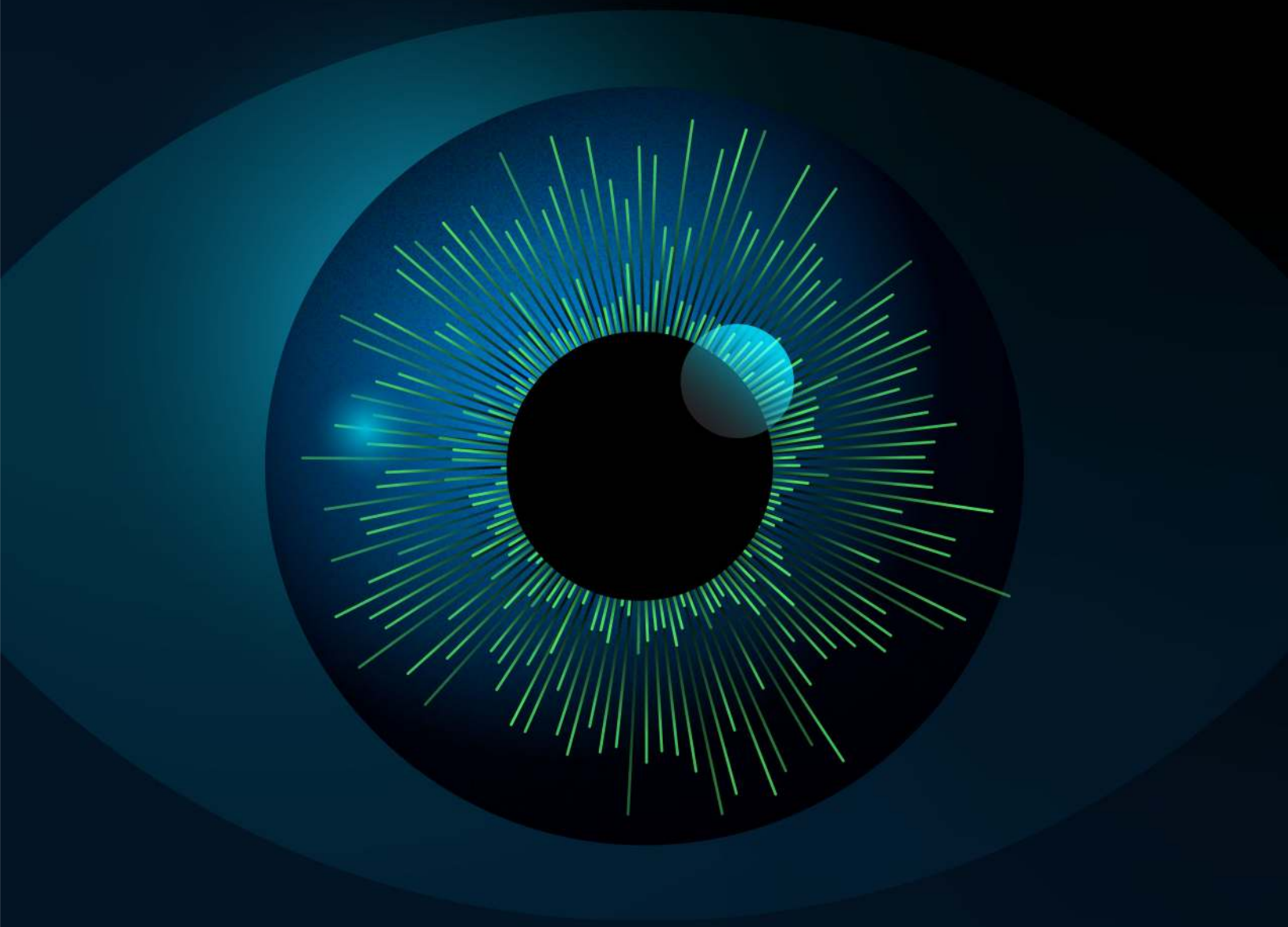
Challenges: Tracking Devices and Risks Across Campus

With its wide range of users, networks, and use cases, WashU found it difficult to centralize asset and risk management, leading to critical visibility gaps. Without clear device ownership in the inventory, setting up remediation workflows was nearly impossible.

Resolution: Improved Tracking for Streamlined Security

To strengthen security, WashU prioritized continuous monitoring across the asset lifecycle. Key steps included classifying each device, establishing department and business ownership, and cleaning up existing data, allowing for streamlined security policies and remediation workflows that align with the university's unique risk profile.

Device Trends: Persistent Blind Spots in Agentless Assets

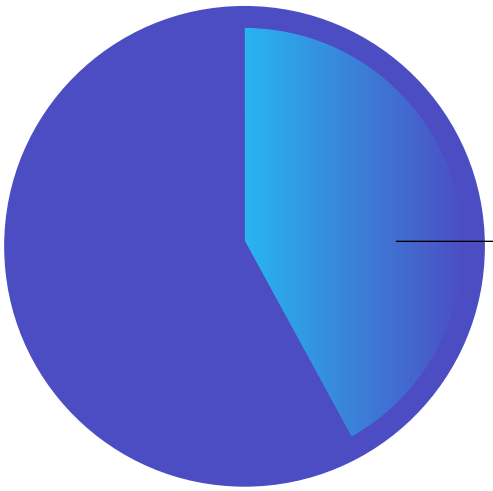


Unseen Risks: The Attack Surface Beyond IT and Security Tools

When assessing asset attack surfaces, the focus is often on managed devices — such as those protected by endpoint detection and response (EDR) or managed by device management solutions. Yet, **42%** of enterprise assets fall outside these systems. These unmanaged devices often lack users, proper onboarding, single sign-on, multifactor authentication, or even basic certificates to identify them, forming a "shadow network" of assets.

The challenge is even greater in specialized environments. For example, healthcare organizations rely on legacy medical devices, while manufacturing facilities depend on operational technology (OT) and industrial systems — both critical to operations but often lacking basic security protections. These unmanaged assets significantly expand the attack surface, making industries more vulnerable to breaches.

- *Shadow data take* ***26.2% longer to identify*** *and* ***20.2% longer to contain*** *(IBM 2024 Cost of a Data Breach Report).*
- ***34%*** *of enterprises experiencing breaches in IoT devices incurred cumulative costs between* ***$5 million and $10 million*** *(Forrester's 2024 IoT Security Trends)*



42%

of all enterprise assets are agentless

These include IoT, OT, facilities assets, and specialized devices in sectors like industrial, medical, and finance.

Breaking Down the 42%: The Most Overlooked, Yet Critical, Assets

Agentless devices are more than just unmanaged — they're often the backbone of operations, yet operate without basic security controls like authentication or encryption. Attackers exploit this lack of oversight, using these devices as entry points to bypass traditional defenses.

The Complexity of Agentless Devices

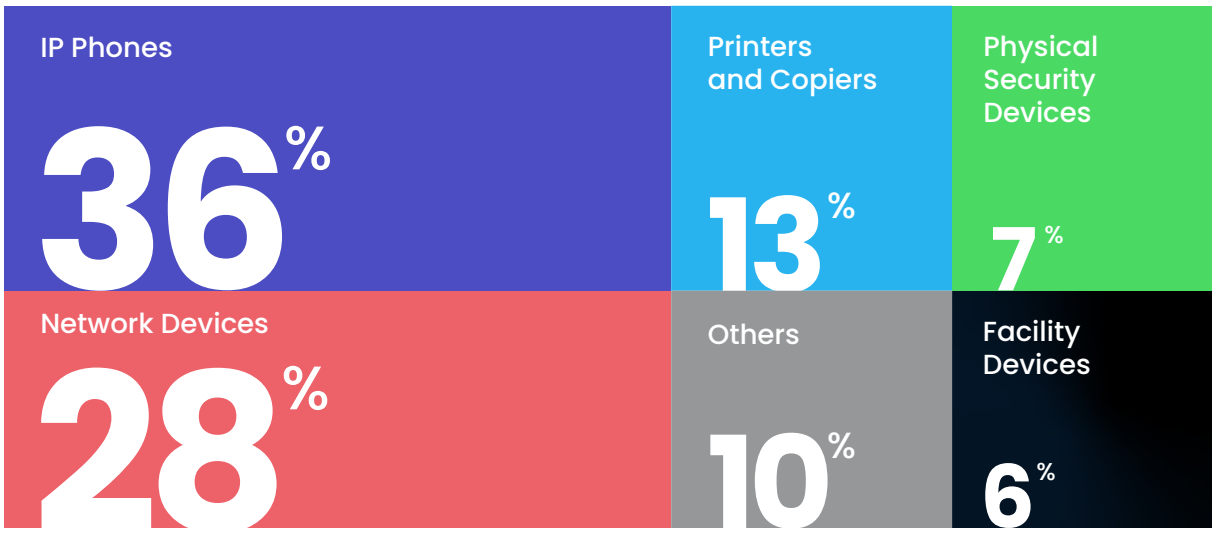
The sheer diversity of agentless devices complicates their management. From industrial sensors to facility equipment, these devices add layers of risk to enterprise security.

Examples include:

- ***Unmanaged operational equipment:*** *Industrial controls, HVAC systems, and UPS devices essential to operations.*
- ***Everyday devices with hidden vulnerabilities:*** *IP phones, digital displays, and printers that connect internally and externally.*
- ***Critical physical security devices:*** *Surveillance cameras and access controls, often outdated or unencrypted.*

Agentless Devices by the Numbers

A breakdown of the most common agentless devices highlights their pervasive presence across networks:



Untracked and Unseen: The Growing Threat of Shadow IoT

Shadow IoT devices are an escalating blind spot for enterprises, blending consumer-grade devices and banned or high-risk equipment along with business-critical assets. These unaccounted-for devices, such as smartphones, surveillance cameras, and networking gear, introduce compliance challenges and create unmonitored pathways that can lead to breaches, penalties, or operational disruptions.

The Internet of Stranger Things

An analysis of enterprise networks reveals surprising examples of consumer-grade devices operating alongside critical systems, often without proper segmentation. These devices, identified within customer environments, illustrate the scale of the Shadow IoT challenge:

Vehicles: Tesla, Ford

Gaming Consoles: Nintendo Switch and Wii, Microsoft Xbox, Sony PlayStation

Smart TVs & Streaming Devices: Vizio, Samsung, LG, Roku Stick, Nvidia Shield

Smart Watches: Samsung, Apple, Fitbit, Garmin

Exercise Equipment: NordicTrack treadmills, Peloton bikes

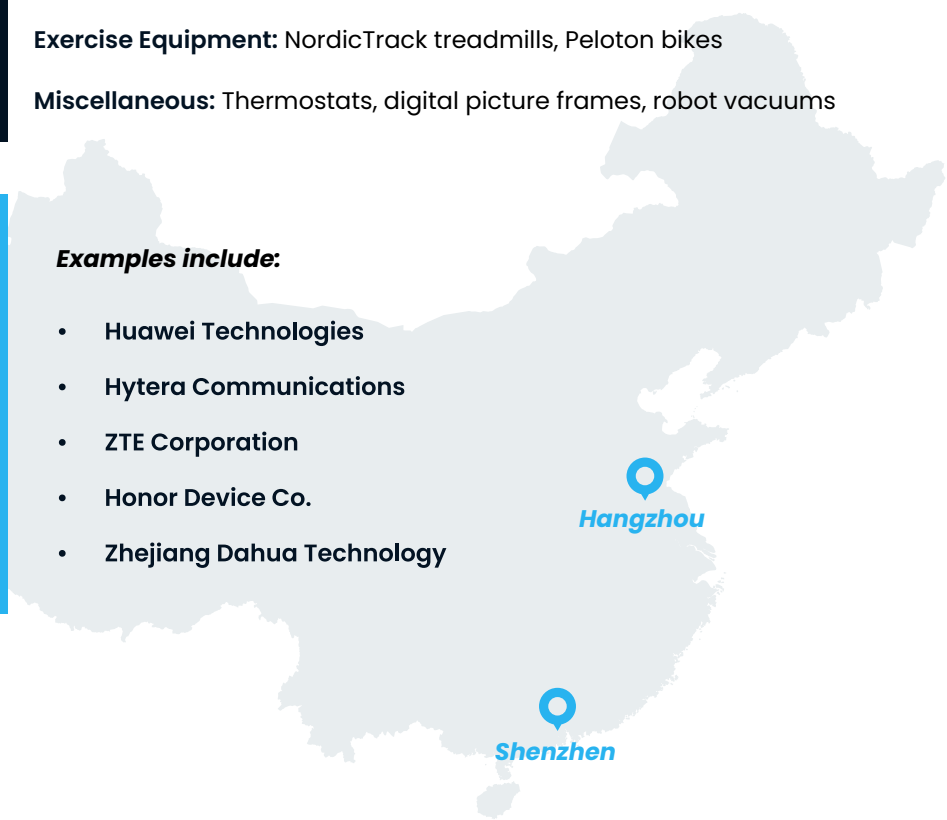
Miscellaneous: Thermostats, digital picture frames, robot vacuums

50+

is the average number of banned and high-risk devices found in an enterprise network.

Examples include:

- **Huawei Technologies**
- **Hytera Communications**
- **ZTE Corporation**
- **Honor Device Co.**
- **Zhejiang Dahua Technology**



IT and Security Tools: The Reality of Coverage Gaps

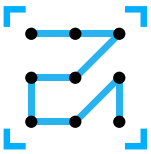
Even for managed devices, achieving full visibility remains a significant challenge. While IT and security tools offer robust insights and protection, only a fraction of enterprise assets are enrolled under them. This leaves considerable gaps, even among devices capable of being protected.

Effective attack surface management requires addressing both:

- **Security gaps** - devices lacking controls entirely.
- **Coverage gaps** - devices that could be protected but are not fully enrolled or monitored.

EDR Deployment

40% of devices support EDR, but only **84%** of them have EDR installed.



Scanning Gaps

Of the **58%** of devices capable of scans, **91%** are scanned.

Device Management

Although **57%** of devices can be managed, only **1/3** of those devices are managed.

Encryption Vulnerabilities

On average, enterprises have **380** devices out of encryption compliance, exposing sensitive data to potential loss.

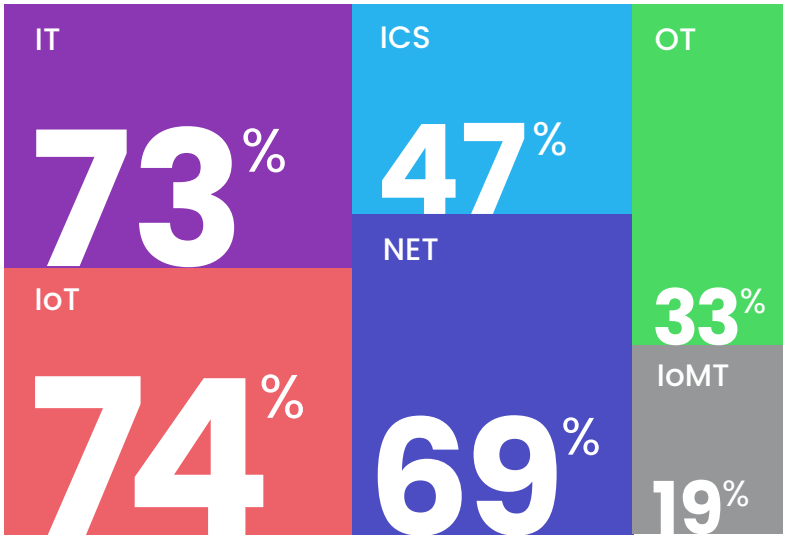
Vulnerabilities *and Enterprise* Risks

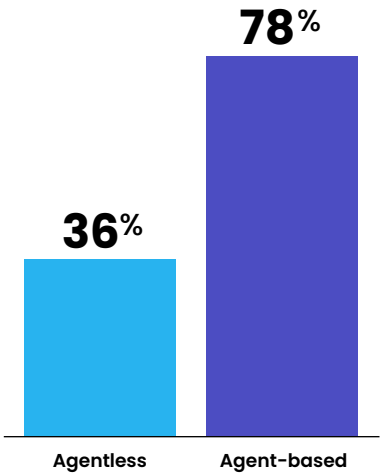
The Constant Challenge of **Managing Vulnerabilities**

Exploiting vulnerabilities remains one of the most effective ways attackers penetrate enterprise networks. However, the sheer volume of CVEs makes it difficult to identify which vulnerabilities matter most.

Hackers use high-impact entry points to exploit chains of vulnerabilities, moving laterally to compromise valuable assets. According to our analysis, **63%** of enterprise assets have critical CVSS scores of 9–10, underscoring the magnitude of the challenge.

Breakdown of Critical Vulnerabilities by Asset Type:





Windows Vulnerabilities

Legacy operating systems remain prevalent among agentless devices, often due to their specialized purposes in industrial or medical settings. These systems present significant risks:

10 7 XP

Windows 10

*Used by **80%** of Windows devices, with **3,373** known vulnerabilities to date. Its end-of-life is October **2025**.*

Windows 7

*Despite being end-of-life since **2020**, it still accounts for **1%** of Windows machines and has **1,499** known vulnerabilities.*

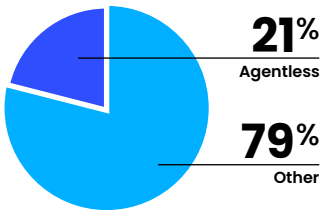
Windows XP

*While it accounts for less than **1%** of Windows devices, XP has **968** known vulnerabilities and has been end-of-life since **2009**.*

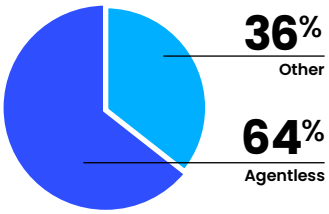
The Power of Context in Managing Vulnerabilities

While CVSS scores provide a starting point, not all vulnerabilities are created equal. Context — where a device is, how it's used, and its relationship to critical systems — determines its true enterprise risk.

Critical CVSS scores



Enterprise Risk



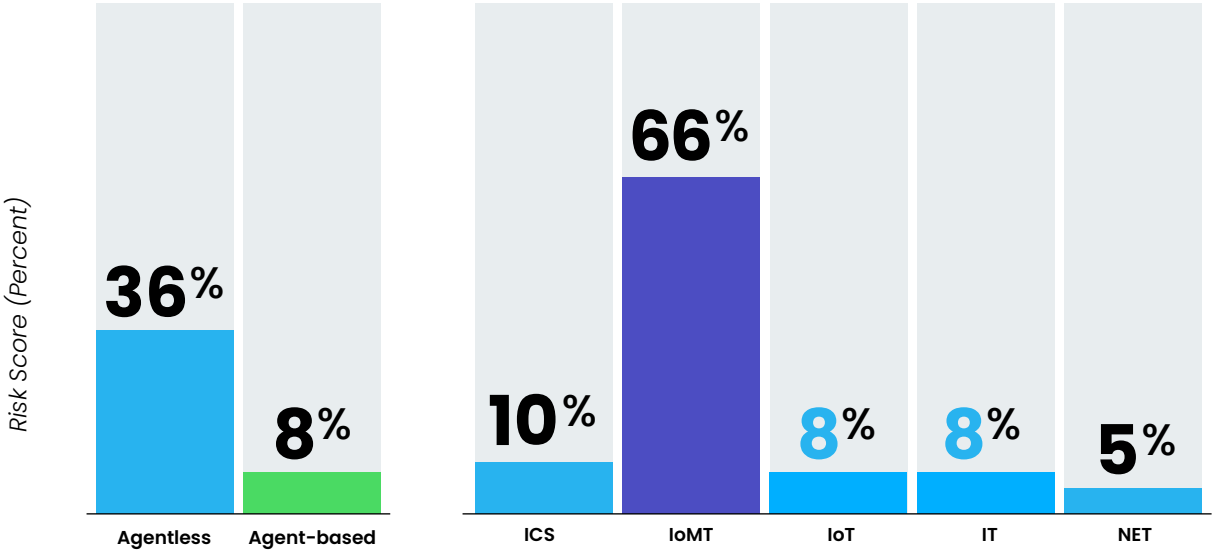
*While agentless devices comprise only **21%** of devices with critical CVSS scores, they account for **64%** of all mid- to high-level enterprise risks.*

Devices with Medium and High Risks

While IT and network devices contribute to risk scores, industrial control systems (ICS) and medical devices carry significant risks due to their critical roles. Medical devices, though fewer in number, have an even higher risk profile in healthcare environments.

Agentless devices, in particular, present distinct challenges that elevate their risk compared to agent-based devices. These can be divided into two key categories:

- ***Mission-critical devices:*** Essential assets like PLCs in factories or CT scanners in hospitals are critical to operations. Downtime or compromise can disrupt business continuity, requiring strong segmentation and protection.
- ***IoT devices:*** While less central to operations, IoT devices often serve as gateways for attacks or facilitate lateral movement, putting more critical systems at risk.



What is "Context"

Effective prioritization involves assessing:

Device type
Is it a critical medical device, a mobile device, or a desktop computer?

Ownership
Who is responsible for its maintenance and security?

Location
Is it in a high-priority area like a factory shop floor or on a guest network?

Patch status
Is it up-to-date or running outdated software/firmware?

Connectivity
Is it exposed to critical assets or external destinations?

Impact
How critical is the device to business continuity?

Healthcare Example: Why Context-Driven Prioritization Matters

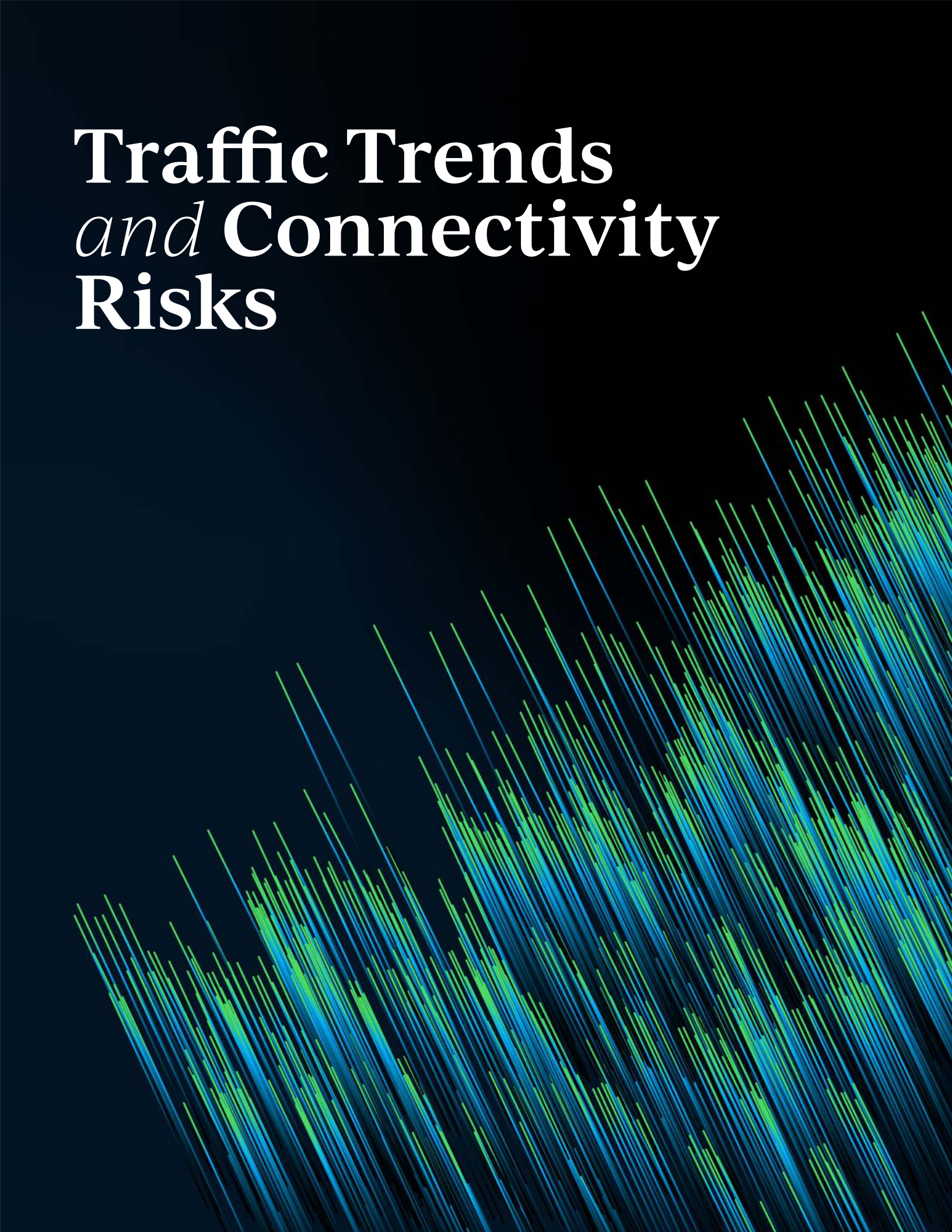
In healthcare, vulnerability prioritization is particularly crucial due to the varying impact of device roles and locations.

Our data shows: While medical devices account for only **19%** of all devices with critical CVSS scores, **66%** of them hold mid- to high-levels of risk when accounting for organizational risk context.

A CT scanner in a research lab presents minimal risk compared to one in a patient care setting, where it directly affects treatment outcomes.

A desktop computer inside an operating room is far more critical than the same device functioning as a kiosk in a breakroom.

Traffic Trends *and* Connectivity Risks



Internet Communications and External Threats

External connections are the primary entry points for attackers, providing opportunities to infiltrate networks and propagate internally to high-value assets. For example, we observed a spike in connections to Russia during the early days of the Ukraine war, highlighting how geopolitical events can amplify risks.

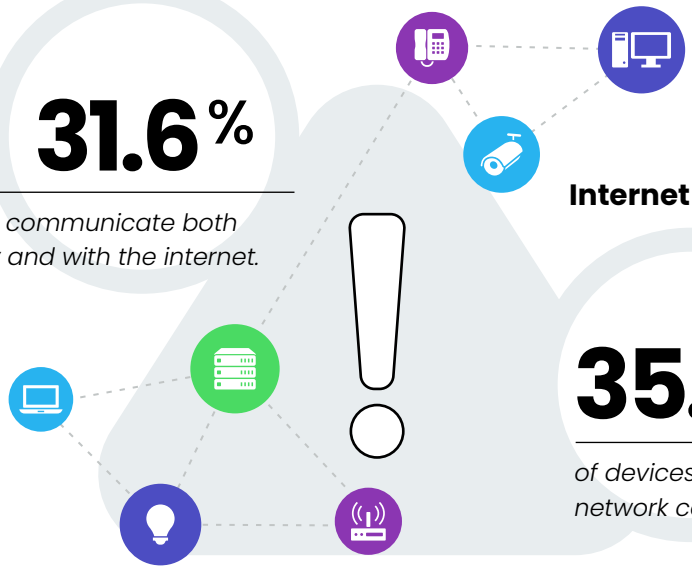
Emerging trends, such as communications with banned or high-risk countries like North Korea, Russia or even Iran, further underscore the importance of monitoring these interactions. Detecting suspicious activity early is essential for preventing unauthorized access and protecting critical enterprise data.

External Connectivity Risks

Total Blast Radius

31.6%

of assets communicate both internally and with the internet.

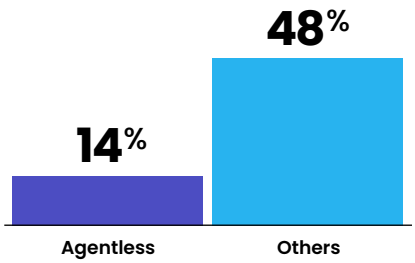


Internet Exposure

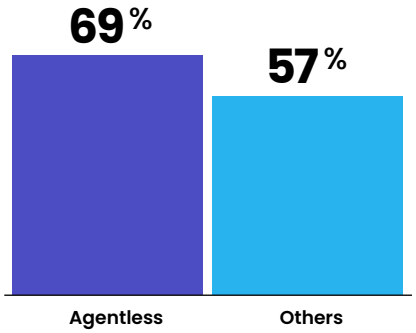
35.7%

of devices have external network connections.

Connects to internal systems



Connects with the internet

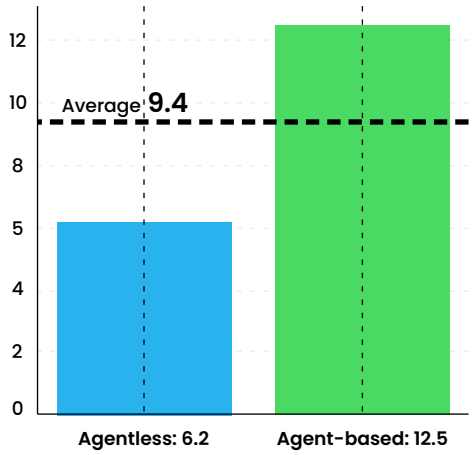


Internal Traffic Risks: Expanding the Attack Surface

In today's hyperconnected environments, internal communication between assets often creates hidden pathways for attackers to exploit. Once an attacker finds their way into an enterprise, they use internal connections to propagate across networks until they reach high-value targets.

Avarage Conections per Device

Agent-based devices, such as workstations, typically have more device-to-device connections but are protected by multiple IT and security tools. In contrast, agentless devices, often legacy and vulnerable, average over six peer connections, posing a greater risk.



Lateral movement

61% of assets have internal connections, providing attackers with pathways to move laterally and reach high-value targets.

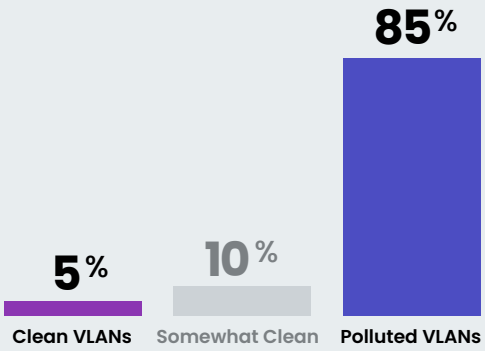
Lateral attacks

40K lateral movement attacks were detected in 2024

A Case Study: Healthcare VLAN Cleanliness

Healthcare, like other industries that rely on specialty devices, face unique connectivity challenges, where device segmentation can make or break security.

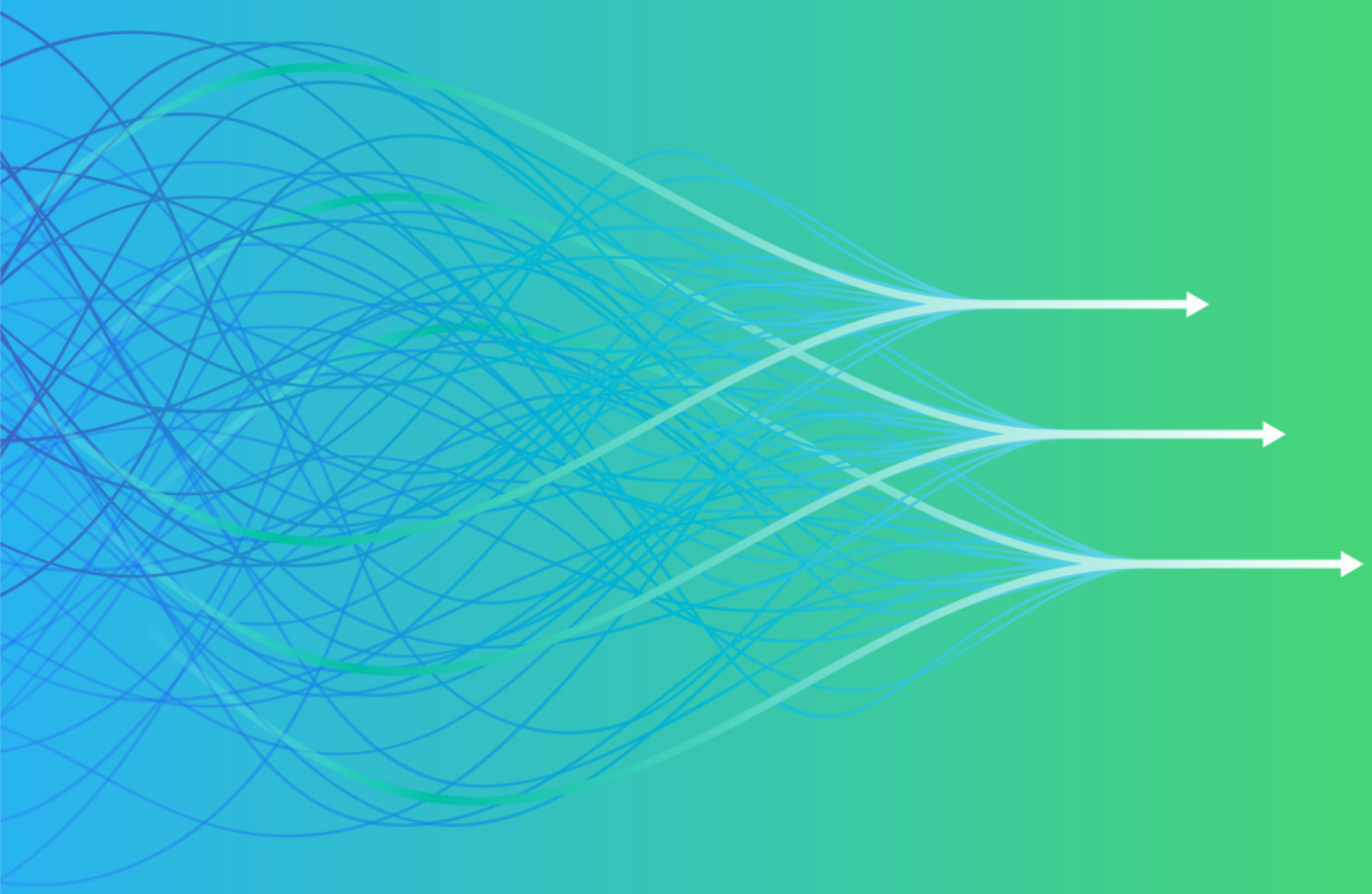
But ensuring VLANs are properly segmented is easier said than done, based on analysis of the "cleanliness" of healthcare organizations.



Clean VLANs: 5% *of VLANs contain only medical devices (100% clean).*

Polluted VLANs: 85% *of VLANs are "polluted" with mixed assets, exposing critical and legacy devices to broader risks.*

The Path Forward: **Reducing Agentless Exposure**



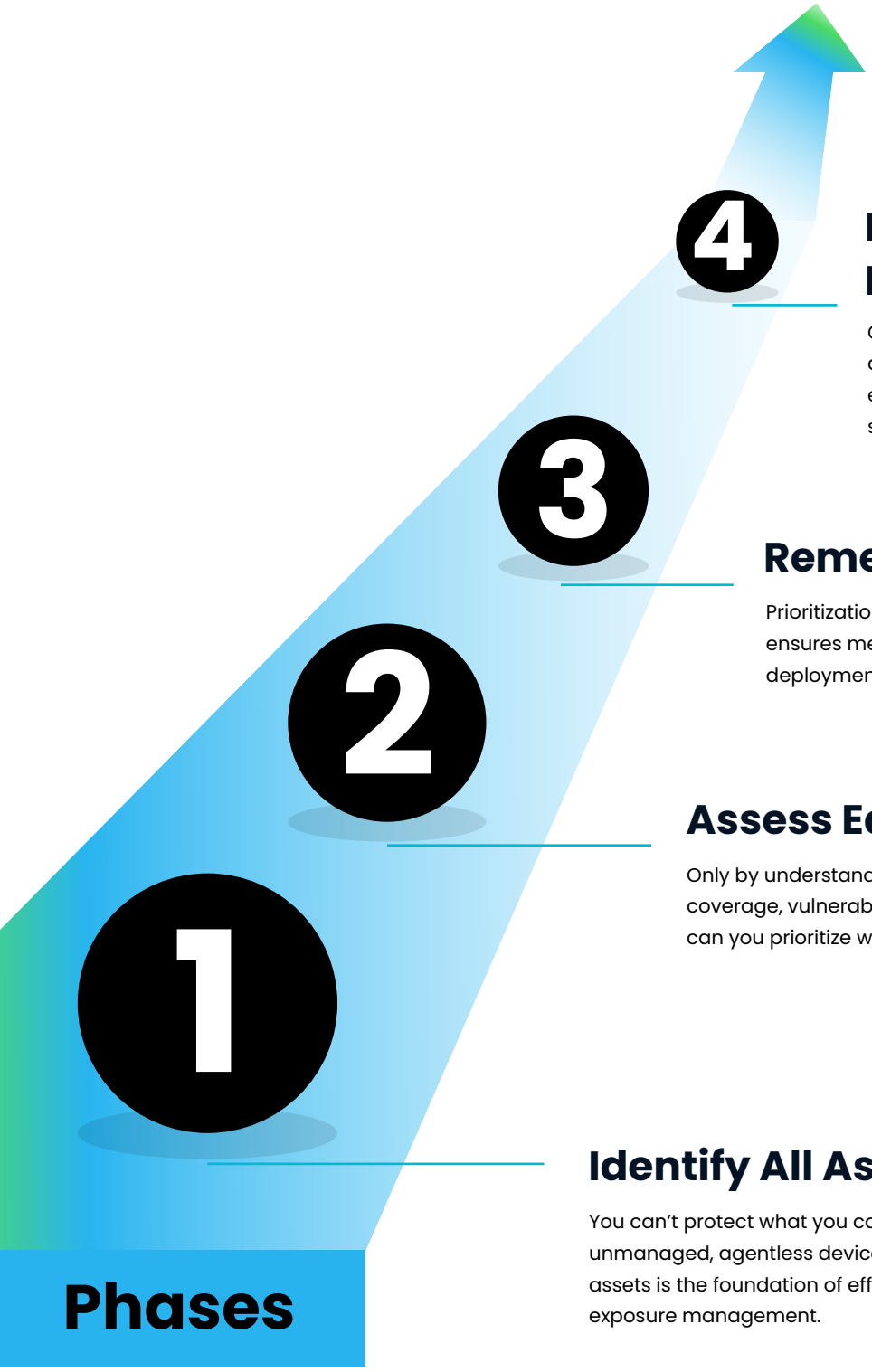
An Asset Attack Surface **Maturity Model**

Managing today's sprawling enterprise assets can feel overwhelming, with organizations juggling overlapping priorities. However, building a robust attack surface management program doesn't have to be daunting. By focusing on structured, incremental improvements, organizations can significantly reduce risks and enhance visibility.

We've created a maturity model with four critical phases to help organizations take control of their attack surface. These steps aren't one-and-done but form a cyclical framework for managing the entire lifecycle of your assets.

While these phases build upon one another, organizations can approach them simultaneously, depending on their unique needs and resources. On the next page, we'll explore each phase in detail.

In Detail: Steps to Managing Your Attack Surface



Identify All Assets

You can't protect what you can't see, especially the 42% of unmanaged, agentless devices. Achieving a full inventory of assets is the foundation of effective attack surface and exposure management.

Assess Each Asset's Risk

Only by understanding the context, such as security control coverage, vulnerabilities, and communications patterns, can you prioritize what matters.

Remediate Strategically

Prioritization is critical. Focusing on business-critical assets ensures meaningful risk reduction, whether it's tools deployment, patching, or VLAN isolation.

Implement Proactive Policies

Cybersecurity isn't static. Continuous monitoring and adaptive policies, such as micro-segmentation, ensure that even your most vulnerable systems are secure.

About Us

Ordr addresses the entire asset and attack surface management journey — visibility, risk-based vulnerability management, advanced threat detection and Zero Trust segmentation. By utilizing unified data discovery methods, combined with AI/ML analytics, Ordr effectively eliminates asset noise, prioritizes the top exposure to the organization, and delivers rapid threat containment using automated actions. Trusted by global enterprises, Ordr improves security hygiene, accelerates incident response, and facilitates Zero Trust initiatives. Ordr is backed by top investors including Battery Ventures, Wing Venture Capital, Ten Eleven Ventures, and Kaiser Permanente Ventures.

For more information, visit

ordr.net

Follow Ordr on

COPYRIGHT © 2024 ORDR, ORDR.NET