ORDR

Winning At Attack Surface Management

3 Reasons You Can’t Live Without Asset Intelligence

ordr.net

Highlights

WHY TRADITIONAL TOOLS MISS CRITICAL ASPECTS OF YOUR ATTACK SURFACE

THE ESSENTIALS OF ASSET INTELLIGENCE FOR PROACTIVE SECURITY

STEPS TO LEVERAGE ASSET INTELLIGENCE FOR REAL-WORLD SECURITY ACTIONS

Asset sprawl and hidden risks — are you prepared?

Connected devices are proliferating across your enterprise, and it's not just traditional IT assets like laptops and mobile phones. You're now confronted by a sprawl of specialized IoT, OT, and other connected devices — whether in hospital systems, retail stores, banks, manufacturing plants, or university campuses.

The challenge is that many of these devices can't have software installed, leaving them undetected by tools like EDR and MDM. This means you lack visibility into a significant portion of assets within your network — high-risk devices holding sensitive data, using default credentials, lacking proper security, and capable of halting operations if compromised.

As your asset attack surface expands, this buyer's guide will show you how to build comprehensive asset intelligence, empowering you to take action with confidence.

Asset intelligence 101: why you should care

Many enterprises still rely on spreadsheets or tools like a CMDB to track their asset inventory. However, the data in these manual operations are rarely up-to-date or accurate and often falls short when it comes to assessing security software coverage, patching vulnerabilities, or responding to incidents.

While IT and security tools may provide critical information, it's often fragmented. Even when you aggregate this data via API, major gaps remain — especially for IoT and OT devices that can't run endpoint agents or are fully owned by teams that don't communicate well with each other.

Asset intelligence is the glue that ties this fragmented data together. It starts with every CISO's goal: minimizing risk. It achieves this by first providing a consolidated view of all assets — IT, OT, and IoT. Then, it communicates this view to all stakeholders and solutions, offering actionable insights that create remediation workflows or even enforce policies in real time.

Do you have asset intelligence? Answer these questions:

Even if you have visibility into all devices, each one is more than just an IP or MAC address. To assess and prioritize security, you need additional data points such as user context, device manufacturer, installed software, and known vulnerabilities or recalls.

1

Can you track agentless devices?

Devices like IoT and OT can't enroll in tools like a MDM or EDR, leaving you blind to their presence and the risks they pose.

2

Can you precisely identify and classify all assets?

Vulnerability scanners may provide IP and MAC addresses, but in some cases, they don't reveal the device type, software, or other risk indicators.

3

Do you understand the business impact of each asset?

Different asset types have different impacts on an organization. Knowing this empowers you to prioritize which assets to secure and minimize risk.

Reason 1

Security gaps transcend individual tools

Tracking your assets using tools like EDRs, MDMs, or vulnerability scanners is a good start. However, many devices — on average, 42% according to Ordr data — cannot install endpoint agents.

These tools often don't know what they're missing. If there are devices that should have an agent installed but don't, or if an agent isn't functioning properly, there's no way to detect these gaps.

Asset intelligence operates at a higher level than individual tools. It provides a comprehensive snapshot of all assets, enabling swift action — whether that involves installing or troubleshooting endpoint agents or creating segmentation policies to isolate devices that can't be protected by agent-based solutions.

Do you have the right insights to close security gaps?

To effectively monitor and close security gaps across your organization, here are some must-have capabilities:

- **Insights into agent health:** It's one thing to install an agent, it's another to know whether it's working properly and communicating with the management console.
- **Keep track of assets that can't install agents:** A big chunk of any enterprise are assets that cannot enroll with your existing tools but need to be monitored.
- **Asset profiling data for informed actions:** Insights aren't useful if you can't take actions. Make sure you know the device owner, location, and other information so you can build workflows or enforce policies to close gaps.

of enterprise assets cannot install an agent, on average*

**OrdrAI Platform Data*

Reason 2

Managing risks requires a lot more than CVE scores

NIST's National Vulnerability Database recorded 29,065 new vulnerabilities in 2023 — averaging 2,400 each month. This volume creates a massive challenge for organizations managing tens to hundreds of thousands of devices. Tracking which devices have vulnerabilities is hard enough, let alone patching every single one. The problem is further complicated by assets like legacy medical devices, industrial systems, and banking machines that often have outdated, unpatchable software.

Asset intelligence provides an organization-wide view of your vulnerabilities with context. Instead of focusing solely on the severity of each CVE, it evaluates how each device — considering its function, the data it holds, and other factors — contributes to risk within the context of your organization.

Only by combining in-depth insights mapped to your specific risk tolerance can you begin to prioritize and take effective action, whether that's patching, real-time quarantining, or proactive segmentation.

The context you need for effective risk management

Comprehensive device profiling

Identify every device type, its function, and the software and vulnerabilities it carries to assess risk accurately.

Actionable remediation data

Having information on device ownership and location enables you to streamline and expedite remediation efforts.

Legacy and unsupported systems

Track all devices running obsolete or unsupported OSs to identify those requiring additional protective measures.

Reason 3

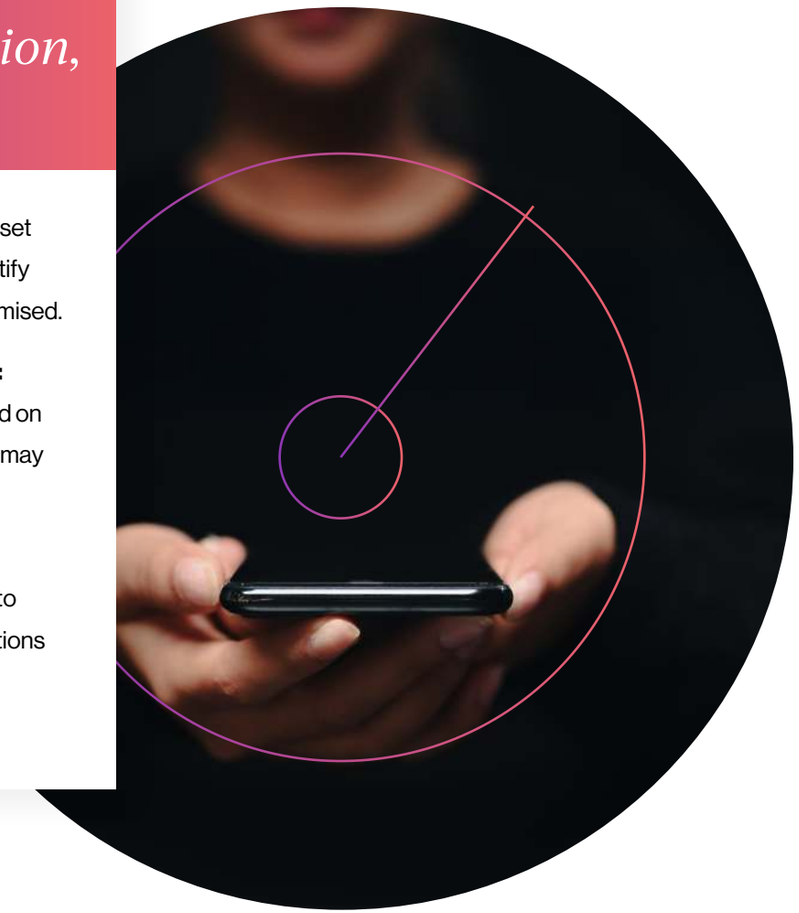
Lack of blast radius insights is hindering incident response

A significant part of incident response involves analyzing compromised assets and understanding their relationships with their surroundings. This can be a time-consuming task, often taking upwards of 24 hours as teams scramble to gather and correlate data from various IT and security tools.

Because asset intelligence provides always up-to-date insights into all assets, incident response teams are better equipped to dive directly into action — whether that involves quarantining a device or updating policies.

Critical intelligence for containment, eradication, and recovery

- **User interaction mapping:** Track every asset that each user interacts with to quickly identify affected assets when an identity is compromised.
- **Detailed software and vulnerability data:** Understand the software packages installed on each device and identify vulnerabilities that may have been exploited during the incident.
- **Internal and external communication tracking:** Monitor device communications to detect signs of lateral movement or interactions with phishing or malicious sites.



The asset intelligence checklist

Here are three tips to help you be able to obtain asset intelligence, so your team has ready-to-go insights to build and automate workflows, detect and respond to threats, or even create microsegmentation policies to reduce risk on high risk, highly vulnerable assets.

Develop primary sources for asset insights

Don't rely solely on existing tools like EDRs or MDMs. Many assets can't be enrolled in these solutions or install endpoint agents. Real-time monitoring of agentless devices is crucial for mitigating organizational risk.

Ensure precise device identification

Gain clear asset profiling and classification for each device, including its type, function, ownership, and location. Vulnerability scanners often only provide IP and MAC addresses on agentless devices. You need in-depth insights to effectively assess risk, create remediation workflows, and enforce policies.

Incorporate business context

Understand which device profiles, data, and behaviors have the most impact on your organization. Use this context to map each asset's risk profile and prioritize patching or protection measures.

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

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