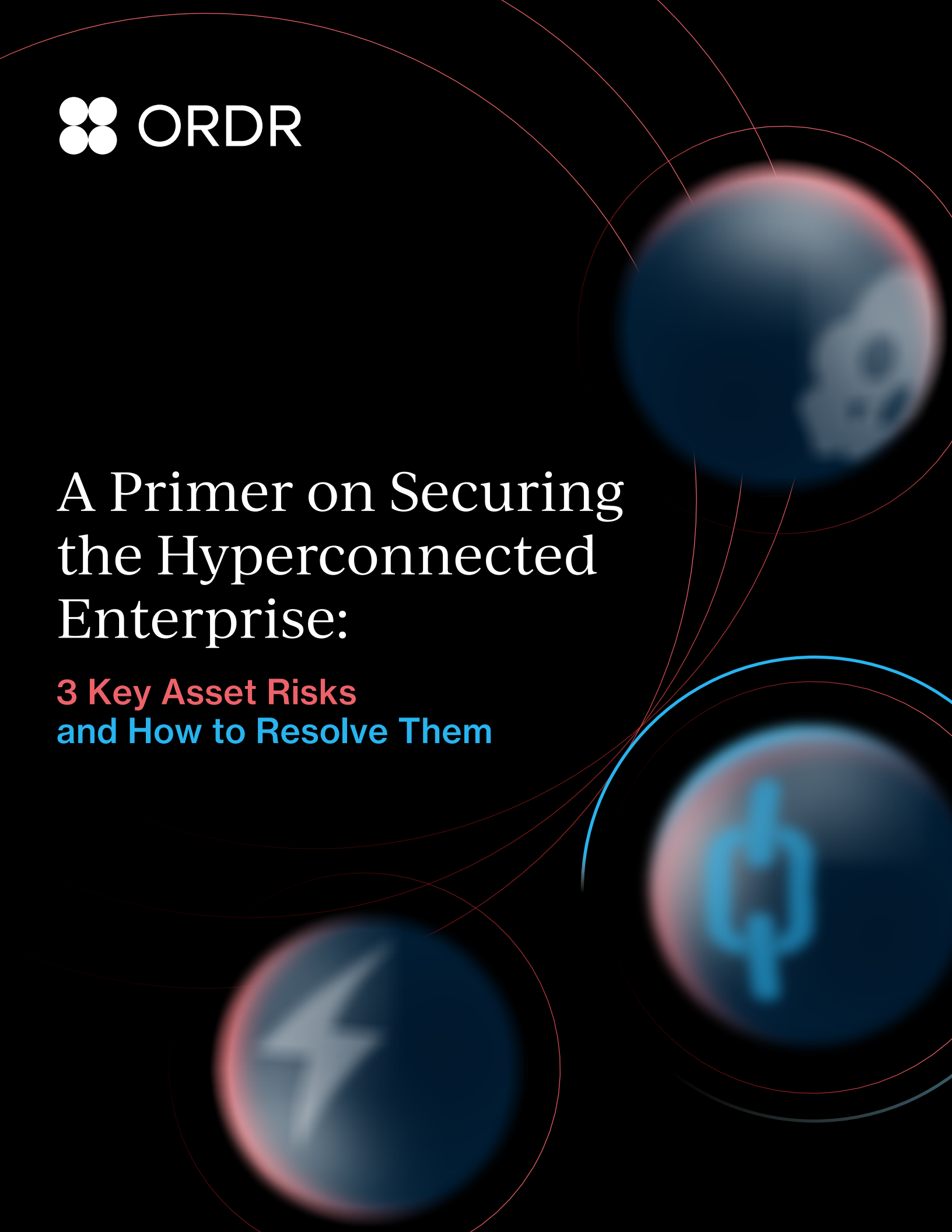
ORDR

A Primer on Securing the Hyperconnected Enterprise:

3 Key Asset Risks and How to Resolve Them



*"**Our nation's critical infrastructure**, the systems and services that Americans rely on every hour of every day for power, water, transportation, communication, healthcare, education, finance...and much more...**is, broadly speaking: highly digitized, highly interdependent, highly connected, and highly vulnerable.**"*

Jen Easterly

Director, Cybersecurity & Infrastructure Security Agency (CISA)

Safeguarding the Hyperconnected Enterprise: Key Risks and Realities

From the smallest sensors to large-scale industrial machinery, anything with a chip and an IP address is a connected device – and every one of them is a potential target for cyberattacks. With today's hyperconnected networks, a single compromise can affect your entire organization.

Yet keeping tabs on all these assets and understanding what they're doing is easier said than done, whether due to management process breakdowns or the devices' own limitations. Threats like ransomware, supply chain attacks, and nation-state actors are quick to exploit these gaps, all while compliance regulations and cyber insurance demands grow stricter.

Every asset you connect brings some level of risk; together, they create a complex web of exposure that's tough to understand, let alone control. That's why your cybersecurity and compliance strategy needs to account for every one of them. In this e-book, we'll walk you through the major risks to manage in today's hyperconnected world – and what you can do to stay ahead.

What you'll learn from this e-book

- THE MAJOR RISKS POSED BY CONNECTED DEVICES
- HOW CYBER ATTACKERS ARE TARGETING MISSION-CRITICAL ASSETS
- THE MOST COMMON REGULATORY REQUIREMENTS CONNECTED ASSETS
- PRACTICAL STEPS TO START TACKLING THESE CHALLENGES

Beyond IT: the hidden risks of increased connectivity

Connected assets come in all shapes and sizes. Sometimes they're categorized into IT, OT, or IoT buckets, or labeled as specialized devices for medical, industrial, or other purposes. But for most of us, they're simply "assets" that help run our organizations.

In many instances, different departments manage different devices, yet they all end up on the same networks. When security teams try to understand their asset attack surface, it's like looking into a fragmented mirror — only parts of the full picture are visible.

As the saying goes, you can't protect what you don't know exists. Departmental silos are one challenge. Blind spots in existing IT and security tools are another, as not every device can install security software or has patches available to cover its vulnerabilities.

To truly understand and prioritize which assets need protection, it's essential to think beyond IT, OT divides and the limits of existing tools.

How well do you know **your assets?**

Can you see every asset connected to your network?

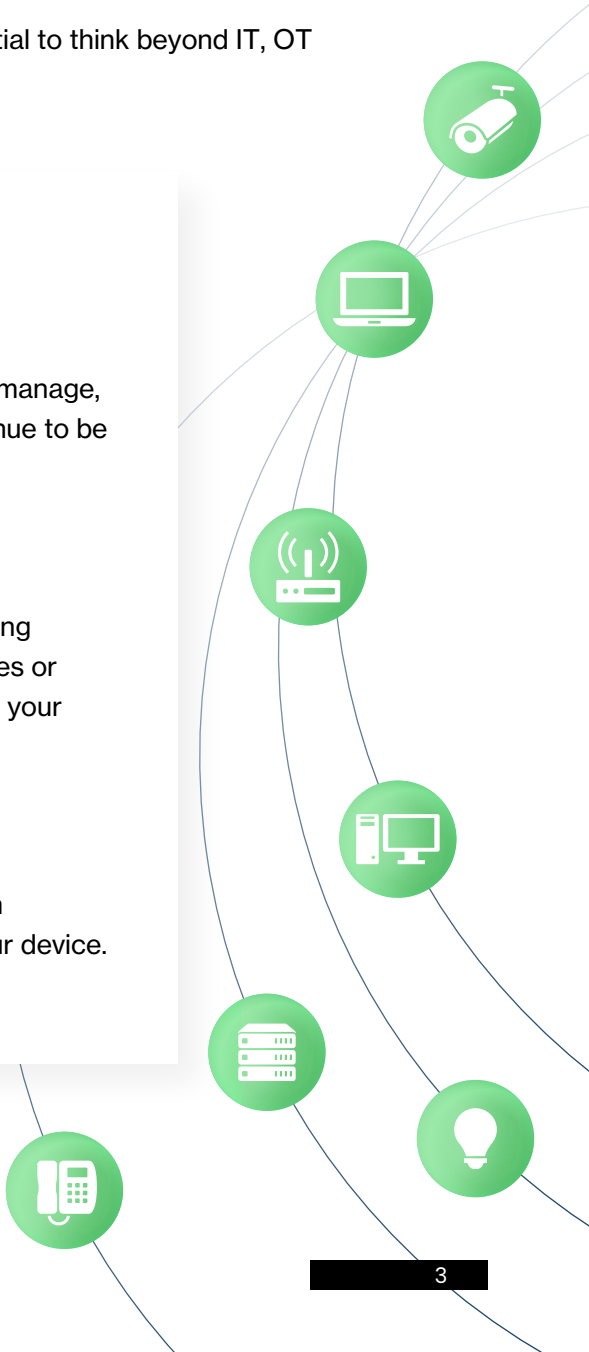
Understanding your asset attack surface starts with the devices you manage, but it can't end there. Despite your best efforts, new assets will continue to be added to your networks, and it's essential to keep track of them.

Can you gain visibility into the risks of your legacy devices?

Industrial devices are "built to last," but that often means their operating systems are decades old, preventing them from patching vulnerabilities or running modern security tools. Identifying and quantifying their risk to your organization is critical.

Do you have visibility into your supply chain risks?

Specialized industry devices frequently integrate niche software from third-party vendors. If that software becomes vulnerable, so does your device. Are you fully aware of the software in use across your devices?



Attackers are taking advantage of the hyperconnectivity

Cyberattacks are escalating in both scale and sophistication. Ransomware alone costs organizations millions each year, and geopolitical tensions have increased the risk of nation-state attacks, often aimed at critical infrastructure. Meanwhile, supply chain attacks expose just how difficult it is to detect vulnerabilities in third-party software.

With hyperconnected organizations, threat actors now have multiple avenues for gaining initial access, and once inside, they can easily navigate the network due to its interconnected nature.

Always assume that compromise is inevitable. What can attackers do once they gain access to your network? More importantly, how can you identify and protect your most critical assets before an attack occurs? Focusing on fundamentals – like identifying unmanaged and unpatched devices – is essential to minimizing risks before attackers strike.

Headline-grabbing **cyberattacks**

Ransomware

The Colonial Pipeline ransomware attack highlighted the vulnerability of critical infrastructure when it forced the company to halt pipeline operations.

Supply chain attacks

The SolarWinds compromise delivered malicious code to 18,000 customers, including the U.S. government, underscoring the danger of supply chain vulnerabilities.

Nation-state threats

The Chinese-linked Volt Typhon was discovered “living off the land” of critical infrastructure providers by targeting vulnerable devices instead of deploying malware.

The mounting pressure of cyber insurance and regulatory requirements

As the threat landscape expands, industry regulations tighten. Cyber insurance providers have also become more demanding, often asking adherence to common frameworks condition for coverage.

Audits are inevitable and rarely straightforward. Yet many organizations still rely on a fragmented view of their assets, using manual processes, or security or management tools that each have their own blind spots.

The good news? Many compliance regulations share a similar foundation. By consolidating data from your existing tools and gaining full visibility into what's happening on your network, you can stay ahead of compliance demands and improve your security posture.

Common **compliance requirements**

Maintain an asset inventory

Managing connected assets requires full visibility into what assets exist and where vulnerabilities may reside. For example, ISO 27001 requires organizations to monitor and report on risk, which starts with knowing what devices you have.

Vulnerability management and patching

Unpatched vulnerabilities in connected assets are frequently exploited in cyberattacks. Regulations like HIPAA mandate the monitoring and patching of IoT devices to mitigate this risk.

Incident response

With the expansion of the attack surface from connected devices, response plans must now cover IT, OT, and IoT incidents, including handling ransomware or supply chain attacks that could impact critical infrastructure.

Next Steps and Practical Tips for Managing an Expanded Attack Surface

The risks of connected devices, an aggressive threat landscape, and an entwined web of compliance can be as diverse as the assets themselves. There is no such thing as a one-size-fits-all approach to managing such a dynamic plane.

Philosophically speaking, the first step to overcoming these obstacles is an awareness that they exist. Practically speaking, you can gain device awareness by gaining in-depth intelligence into every single asset.

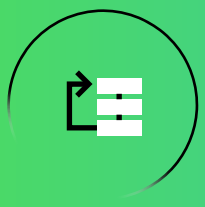
With complete knowledge of all assets connected to your enterprise, you're empowered to prioritize what matters most and take action. The north star for most organizations is to segment and isolate devices so that they don't affect each other. But security hygiene begins with knowing if your security and IT tools are correctly deployed and which vulnerabilities need patching first.

Ultimately, it's essential to gain intelligence across departmental silos. To minimize your attack surface, you need control over assets across your entire enterprise.

How to take control of your connected assets

Identify every device on your network

Developing and maintaining a comprehensive asset inventory is the foundation of cybersecurity and compliance. With complete intelligence into your assets, you can discover and monitor the unknown and unmanaged devices lurking on your network.



Prioritize risk management with mission-critical insights

An in-depth understanding of the OS and software installed on your devices as well as their function within your organization will enable you to prioritize which devices to deploy security to or to patch first.

Take actions to remediate and protect critical assets

Ultimately, you need to be able to take actions. It starts with figuring out which assets matter to you the most, deploying IT and security tools, and patching vulnerabilities. But the next step is to then monitor device behavior and communication to discover and respond to threats in real time as they move through the network, and eventually segment your assets so that your most critical systems are protected even if they cannot be patched or install security software.

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