Ordr Connected Device Security for Manufacturing and OT

See, Know, Secure Every Connected Device To Optimize Resiliency and Maximize Uptime

The ongoing digital transformation of manufacturing is having such a dramatic impact that it's been dubbed the 'fourth industrial revolution' (Industry 4.0). Operational Technology (OT) and Internet of Things (IoT) are changing the way manufacturing production environments and supply chains work by improving efficiencies, automating processes and adding intelligence. This revolution has led to a rapid co-mingling of traditional IT and OT environments blurring the once clear lines between production floor and carpeted area.

> ***"Once they enter the "Oh Wow!" Phase, organizations realize that security — whether IT, OT, physical or supply chain — needs a whole-of-enterprise focus. Historical IT and OT functional differences are becoming a liability when security is involved."***
>
> ***"By 2025, 75% of OT security solutions will be delivered via multifunction platforms interoperable with IT security solutions."***
>
> Gartner
>
> **Market Guide on OT Security**

Manufacturing organizations need multifunctional platforms focused on securing every connected device (whole enterprise focus), to fully realize the promise of digital transformation.

Introducing Ordr Connected Device Security

Ordr is the only purpose-built platform to discover and secure every connected device—from traditional IT, to IoT, IoMT and OT. Ordr will discover every connected device, profile device behaviors and risks, and automate response. Ordr not only identifies devices with vulnerabilities, weak ciphers, weak certificates, and active threats, but also those that exhibit malicious or suspicious behaviors. Ordr enables networking and security teams to easily automate response by dynamically creating policies that isolate mission-critical devices, those that share protected organizationally unique sensitive data or run vulnerable operating systems.

Ordr can be deployed on-premises or in the cloud, and offers a zero-touch, agentless deployment. Ordr has been effectively implemented at-scale to secure connected devices in large, complex networks in the manufacturing industry and and offers a zero-touch, agentless deployment on-premises or in the cloud.

Ordr provides the quickest time to value for every manufacturing organization worried about securing connected devices:

✓ **See every device and flow**

Ordr continuously analyzes network traffic to ensure an always up-to-date view of connected devices and organizational risk. Unlike periodic scans which can easily miss devices and ignore risk for weeks or months, Ordr provides real-time analysis to discover every device with granular details (e.g., make, model, serial number, operating system, software version) in addition to mapping all connectivity and communications flows.

✓ Know every vulnerability, risk, and anomaly

All security tools can generate data, but few generate security-relevant insights. By correlating granular device details with manufacturer and vulnerability databases, Ordr can identify devices with vulnerabilities, recalls, and risks such as weak passwords and weak certificates. A built-in threat detection engine and machine learning powered behavioral analysis allow the solution to identify both known and unknown threats such as zero-day attacks.

✓ Secure via automated policies

While Ordr's analysis is passive, it can automate the creation of policies to protect devices and mitigate risk. By baselining normal device communications patterns, the platform can create appropriate Zero Trust policies such as microsegmentation to reduce a device's exposure while ensuring access to essential services. Ordr policies can be used to proactively improve security, isolate vulnerable devices that cannot be updated, or quarantine devices that show signs of compromise. Policies created by Ordr are enforced with existing security and network infrastructure and can be manually reviewed before enforcement or pushed automatically.

Ordr Use Cases for Manufacturing

✓ Real-time Asset Inventory

As the decentralization trend in manufacturing organizations continues to grow in popularity, operational purchasing decisions, including connected devices, are made locally by multiple stakeholders across the organization. Ordr automatically discovers all IoT, OT, and other devices connected to the network and automatically classifies each device with granular details such as make, model, serial number, operating systems, network details, and location.

✓ Protect Against Cyberattacks

Manufacturing organizations are a top target for bad actors. Attacks such as ransomware can halt manufacturing operations and have significant impact to an organization's bottom line. Ordr identifies all connected devices, uncovers their risks, and can detect malicious activity with an integrated threat detection engine and behavioral analysis. Ordr baselines communication patterns for every device and alerts on anomalous activity as well as malicious activity such as communications to a command and control site. Ordr proactive, reactive, and retrospective capabilities enables team with dynamically created policies to segment, quarantine, or lock down a potentially compromised device.

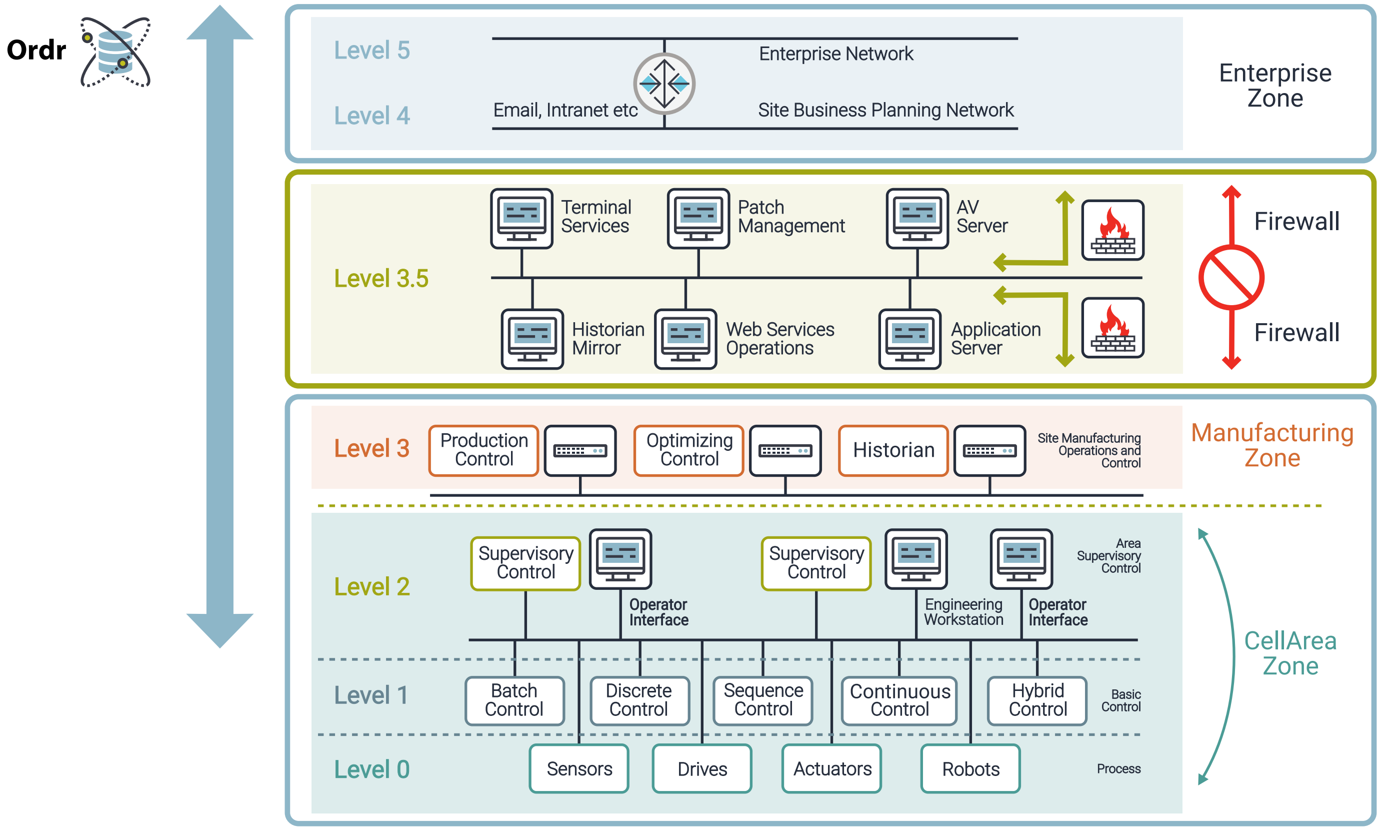
✓ Address Regulatory Compliance

With manufacturers, component suppliers, software developers, logistics companies, and systems integrators involved at various points in the manufacturing process, manufacturing organizations are faced with unique regulatory compliance standards that include ISO 9001, ISO 13845, IEC 61215, IEC 61646, IEC 62443, CGMP, PET and NIST 800-171. Clear visibility into how devices map to each regulatory compliance standard can expedite the governance, risk, and compliance process. Ordr provides a centralized view and a single source of truth for all connected devices and device risks to help address regulatory compliance requirements.

✓ Zero Trust Segmentation for Risk and Cost Avoidance

The livelihood of a manufacturing organization depends on maintaining production at maximum capacity. Business-critical devices such as workstations, pressure sensors, field devices, thermostats, and infrared thermography can provide years of service but often run obsolete operating systems that cannot be updated. Ordr can identify devices with older and obsolete operating systems and provide protection with microsegmentation policies. This enables potentially vulnerable devices to continue to be part of the manufacturing operations, even when patches are no longer available or possible, enabling operational expenditure savings.

Ordr maps to the Purdue Model



Case Study: Automotive Parts Manufacturer

A global automotive parts manufacturer serving more than 60 customers, including BMW, Ford, GM, Toyota, and VW, needed to address their connected device security risks. Their connected device environment spanned over 28 manufacturing plants, three technical centers, one software center, and 13 customer service centers with a broad range of devices from complex infotainment devices (i.e., in-car navigation and telematics) to fleet management and machine sensors.

Ordr was selected after mapping the solution's functionality to key pillars of the NIST framework: Identify, Detect, and Protect. Ordr delivered real-time visibility of all connected IoT and OT devices across all environments, identified their risks, uncovered vulnerabilities, and provided a map of device communication patterns. Additionally, Ordr helped the manufacturer achieve a Zero Trust architecture for their connected devices with the dynamic creation of policies to protect mission-critical operations.

Measurable benefits from deploying Ordr included:

- Unified security management across IT and OT environments
- Cyber-resilient manufacturing processes
- Proactive risk identification and mitigation
- Decreased audit preparation costs

About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information, visit www.ordr.net and follow Ordr on Twitter and LinkedIn.