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.

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

See every device and flow

Ordr constantly analyzes all available network traffic flows, all the time to ensure an always up-to-date view of the environment and organizational risk. Unlike periodic scans which can easily miss devices and ignore risk for weeks or months, Ordr ensures all analysis is in real-time, to discover every device at a granular level (make, model, serial number, operating system, software version and more), along with mapping its connectivity and communications flows.

Know every vulnerability, risk and anomaly

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

Secure via automated policies

While Ordr's analysis is passive, it can automatically take action to protect devices and mitigate risk. By baselining device communications patterns, the platform can create appropriate micro-segmentation and Zero Trust policies that reduce a device's exposure while ensuring access to truly vital services. Likewise, Ordr can create policies to isolate devices that have critical vulnerabilities or have shown signs of compromise. Policies can be set to be created for manual review or even pushed automatically.

Ordr Use Cases for Manufacturing

Real-time Asset Inventory

As the decentralization trend continues to grow in popularity in manufacturing organizations, multiple stakeholders across the supply chain are making local manufacturing and purchasing decisions. These decisions extend to the purchase of connected devices. Ordr can discover all connected devices including IoT and OT, managed and acquired by different teams, across manufacturing facilities all over the world. Ordr can automatically classify these devices, and deliver granular details such as make, model, serial number, operating systems, location and more.

Protect Against Cyberattacks

as ransomware that can halt operations, with significant impact to the bottom line. Ordr identifies all connected devices and their risks, and can detect lateral movement with an integrated threat detection engine. Ordr can baseline every communications pattern and alert on anomalous communications to a command and control. Finally, Ordr provides proactive, reactive and retrospective policies to segment, quarantine, scan or lock down a potentially infected device.

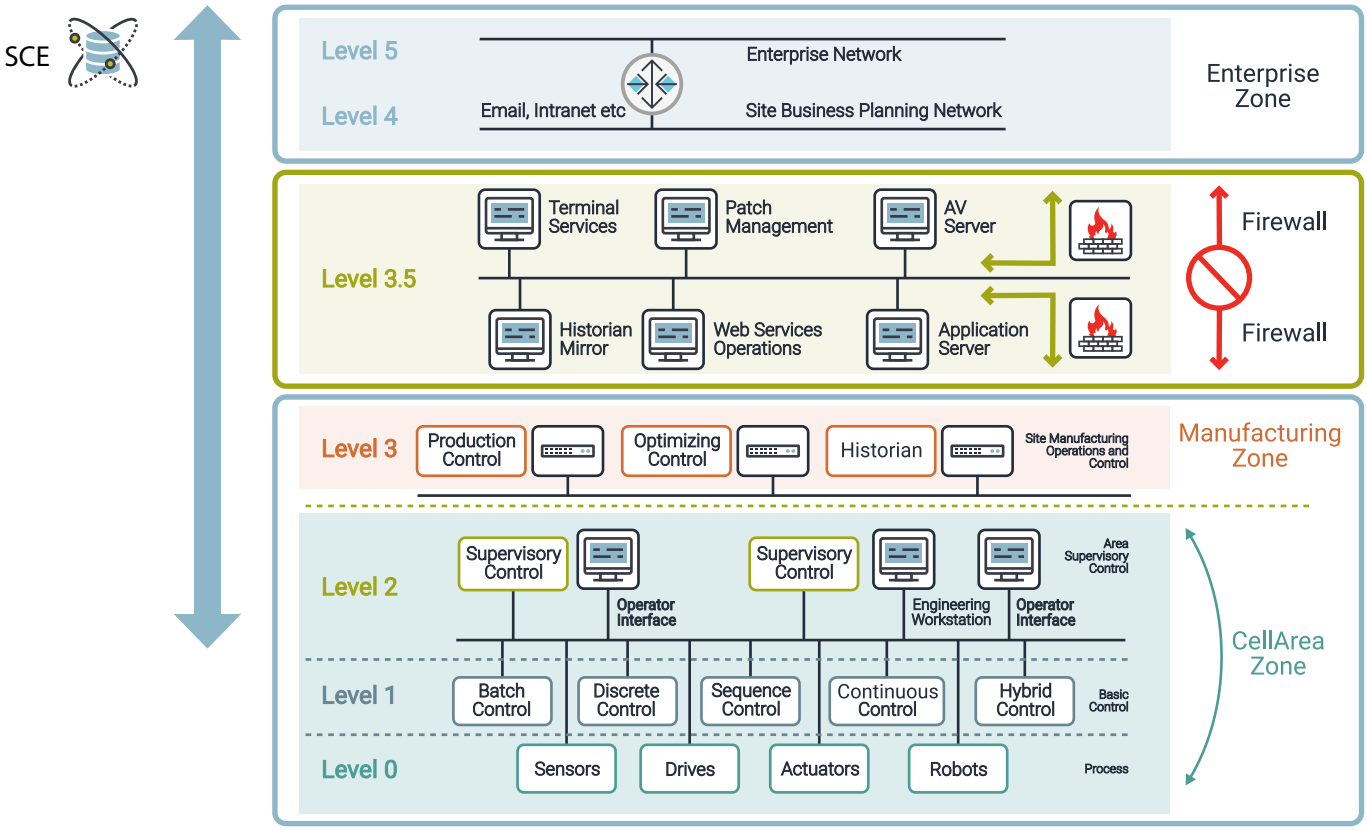
Address Regulatory Compliance

With manufacturers, component suppliers, software developers, logistics companies and systems integrators all involved at some point in the manufacturing process, the manufacturing industry faces some unique regulatory compliance standards. These include ISO 9001, ISO 13845, IEC 61215, IEC 61646, IEC 62443, CGMP, PET and NIST 800-171. Having clear visibility into which devices map to which regulatory compliance standard can expedite the governance, risk, and compliance process. Ordr provides the single asset inventory source of truth on assets and their risks, that are needed to address these regulatory compliance standards.

Zero Trust Segmentation for Risk and Cost Avoidance

The livelihood of a manufacturing organization depends on keeping facilities production at maximum capacity. Business-critical devices like workstations, pressure sensors, field devices, thermostats, infrared thermography, and more can be in service for years at a time, and often run obsolete operating systems. Ordr can identify devices with older and obsolete operating systems and ensure that they are secured via micro segmentation policies. This allows them 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 Manufacturer

An automotive parts manufacturer with more than 28 manufacturing plants, three technical centers, one software center and 13 customer service centers, serving more than 60 customers in every major region of the world including BMW, Ford, GM, Toyota and VW, needed to address their connected device security risks. Their connected device environment ranged broadly, from complex infotainment devices (ie. in car navigation, telematics, etc.) to fleet management and machine sensors.

The automotive manufacturer selected Ordr after mapping the functionality to the NIST framework of Identify, Detect & Protect. Ordr delivered real-time visibility of all devices across IoT and OT environments, identified risks and vulnerabilities associated with them, and mapped device communications patterns. More importantly, Ordr helped the automotive parts manufacturer embrace a Zero Trust architecture and dynamic creation of policies to secure mission-critical devices.

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.