ENABLING DIGITAL TRANSFORMATION IN MANUFACTURING ENVIRONMENTS WITH ORDR

ordr

EXECUTIVE SUMMARY

Manufacturers are facing unprecedented cybersecurity challenges. Digital transformation is changing manufacturing for the better, making operations more agile, efficient, and data-driven. However, the convergence of IT and OT has also led to converged risks. Operations increasingly rely on a wide range of IoT, IIoT, OT, and Cyber-Physical Systems devices that can't be managed or secured by agents. Yet, these devices increasingly need a broad range of connectivity both within the enterprise and externally to the cloud. At the same time, a broad set of attackers have shifted their sights to manufacturers to steal proprietary IP or disable operations with ransomware or other destructive malware.

To keep pace with these changes, security teams need visibility, intelligence, and controls that can span both traditional IT assets as well as the growing fleet of agentless assets used in both the IT and OT environments. The Ordr SCE provides this needed layer, bringing a unified, consistent approach to security that is continuous and automated. As IT and OT converge, Ordr offers an agentless converged approach to security that allows manufacturers to safely enable their digital transformations while mitigating the risks.

MACRO TECHNOLOGY TRENDS THAT ARE TRANSFORMING MANUFACTURING

Today's manufacturers sit at the confluence of 3 major technological trends. Each of these trends is driving the digital transformation of manufacturing in unique ways:

INDUSTRY 4.0 - Major advancements in automation are transforming how facilities work, making operations more efficient and agile while reducing costs. This move to "smart" operations is largely enabled by a new wave of OT devices and cyber-physical systems (CPS).

THE RISE OF CONNECTED DEVICES - Modern facilities rely on a wide range of "things" that are increasingly connected by default. This can include literally hundreds of types of IoT and IIoT devices including phones, time clocks, security cameras, HVAC systems, environmental systems, and much more. While many of these devices are not directly operational in nature, they can easily disrupt operations if they aren't available.

CONVERGENCE OF IT AND OT - Finally, all of these technologies are converging to a common infrastructure. IT, IoT, OT, and CPS all need connectivity to share data, telemetry information, and receive ongoing management and updates. While this connectivity could be to internal systems and servers, devices increasingly also need external access to cloud-based services.

> **By 2025, 75% of OT security solutions will be delivered via multifunction platforms interoperable with IT security solutions.**
>
> **- Gartner Market Guide for Operational Technology Security 2021**

Any one of these trends could potentially overwhelm an organization on its own. Yet unlike traditional enterprises that may only be dealing with one of these issues at a time, manufacturing environments must face them all simultaneously. The organizations that can take advantage of these trends while mitigating their risks will have a competitive advantage in the market.

RISKS AND CHALLENGES

Changes in technology often come with new risks, and the digital transformation of manufacturing is certainly no exception. More connected devices, sharing more data is a good thing for the facility -- but it also creates additional attack surfaces that need to be monitored and protected. And while many enterprises are struggling to manage their digital transformations, there are several security challenges that are specific to manufacturing and industrial logistics environments.

MANY DIFFERENT DEVICES WITH MANY DIFFERENT SECURITY PROFILES

The convergence of IT and OT environments brings together a wide variety of devices, often with wildly different risk profiles and security challenges.

TRADITIONAL IT DEVICES - Much like the IT side of the house, manufacturing environments will have laptops and servers that support a variety of manufacturing, operational, and supervisory control systems. Needless to say, these systems are high-value, high-risk assets and warrant strict monitoring and protection.

IoT/IIoT DEVICES - OT environments also have a wide range of IoT and IIoT devices, which often pose unexpected risks and challenges. Typically they cannot support a security agent and thus lack many of the protections that are taken for granted by laptops and servers. Yet IoT/IIoT devices can still have an incredible impact on a facility's operations. For example, something as simple as a time clock going offline could have a major impact on a plant that relies on union employees. Likewise, disruption to HVAC systems, temperature or environmental sensors, phones, building security systems, or cameras could all indirectly impact operations.

OT DEVICES - Naturally, OT environments can include a wealth of operational technologies including SCADA systems, PLCs, CPS, and a wide variety of other robotic and automation systems. Like IoT devices, these systems often can't be managed via traditional security agents.

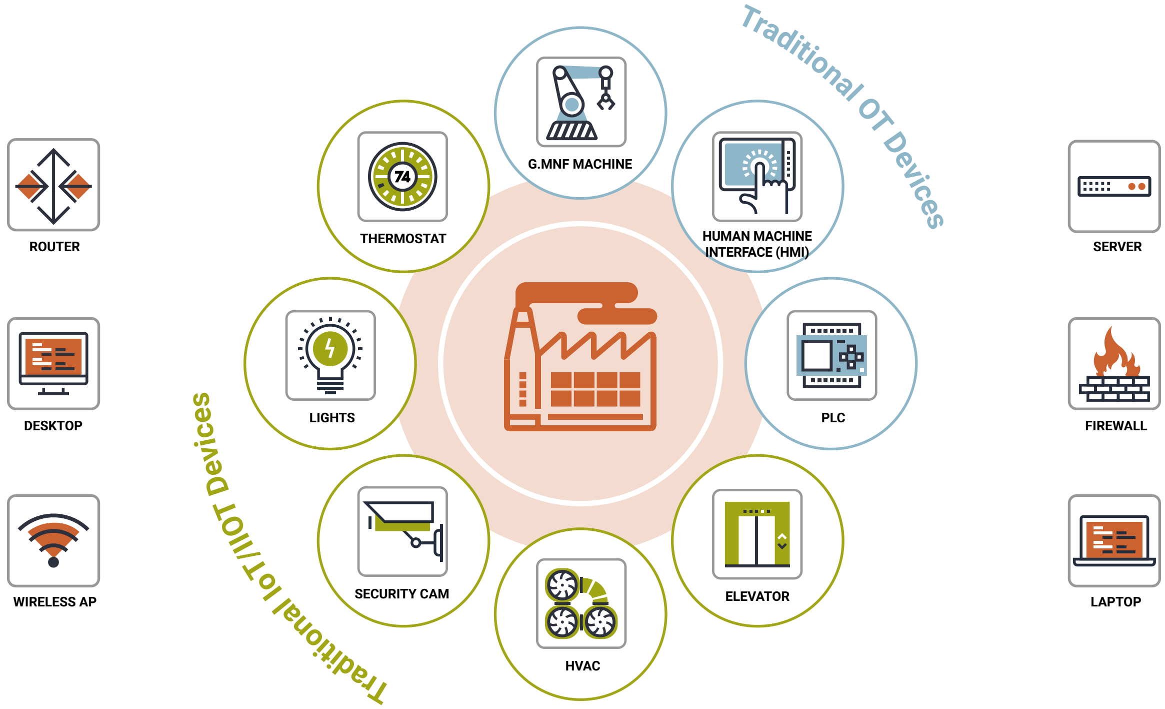


Figure 1: Manufacturing Attack Surface Spans more than SCADA/ICS Devices

The differences in these devices go well beyond whether or not they can support a security agent. They typically have very different risk profiles and face different types of threats and threat actors. Laptops and servers tied to plant operations are high-value targets and face the pervasive threat of criminal ransomware campaigns as well as more targeted attacks. IoT devices are often not updated and can contain vulnerabilities that attackers can use to disrupt devices, establish persistence, or use for spreading or ongoing command and control. OT devices are often targeted in order to cause disruption or damage, often by highly sophisticated state-based threat actors.

As these environments converge, security teams need a cohesive way to maintain visibility and control over all these devices, while applying security controls that are appropriate both for the unique needs of each device and the risks they face.

VISIBILITY CHALLENGES

Converged environments require converged visibility. For many manufacturers, this is the most fundamental and challenging aspect of their digital transformation. With many types of devices belonging to many organizational units, it can be difficult to even establish an inventory of what devices are in use and where. Then for each type of device, organizations will need to know their security posture, how they communicate, what connectivity they actually need versus what is unnecessary risk. There are several needs that organizations will need to be prepared for:

VISIBILITY OF ASSETS - Converged environments will often require security teams to establish a unified view of devices and assets that were previously within organizational silos. Naturally, individual teams may retain ownership and operational control over their devices, security teams will need new perspectives that include physical security, facilities management, supply chain, and more. What devices are deployed? What is their function? What teams are they owned by? How does the device impact facility operations? What rogue or shadow IT devices are in an environment that teams don't even know about?

VISIBILITY OF RISK - Once teams know what devices they have, they will need to know which devices have weaknesses. Different types of devices will have different needs and challenges in this regard. IoT devices may have unique vulnerabilities that are not seen by traditional scanners. Additionally, staff may not want to do traditional scans of IoT or OT devices due to stability concerns. This can create a more fundamental question of how to ensure only appropriate devices are scanned while others are not.

VISIBILITY OF BEHAVIOR - Next, organizations will need visibility into what devices actually do. Cyber-physical systems and even IoT devices need to generate, share, and consume data in order to be useful. This may require connectivity to internal systems and servers or the cloud. Likewise, systems need connectivity to be managed and updated. Security teams need to be able to ensure they have the appropriate visibility to know what each type of device truly needs in order to create appropriate control policies. Teams will also need this ability in order to recognize if a device exhibits any malicious or abnormal behavior that could indicate a compromise.

GROWING AND DIVERSE REAL-WORLD THREATS

As with any industry, it is important to look at risk in the context of real-world attacks. And if we look at the data, it is clear that manufacturers have become one of the most prized targets for attackers. Just as importantly, we can see that manufacturers face an incredibly broad set of threats that extend well beyond direct attacks on SCADA systems.

MANUFACTURING BECOMES A TOP TARGET - The 2021 IBM X-Force Threat Intelligence Index found that manufacturing was the 2nd most attacked industry after financial services. This was a significant jump compared to 2020 when manufacturing was the 8th most attacked industry. Manufacturing accounted for 17.7% of all attacks across all industries, compared to only 8.1% the previous year.

RANSOMWARE LEADS THE WAY - Additionally, the IBM report found that ransomware was the top threat in real-world manufacturing attacks, followed by data theft, and business email compromises. This aligns with analysis from Dragos which found that ransomware was the top threat followed by the theft of intellectual property and proprietary manufacturing processes. This serves as an important reminder that the threat landscape is evolving quickly, and SCADA is just the tip of the iceberg when it comes to a manufacturer's risk management.

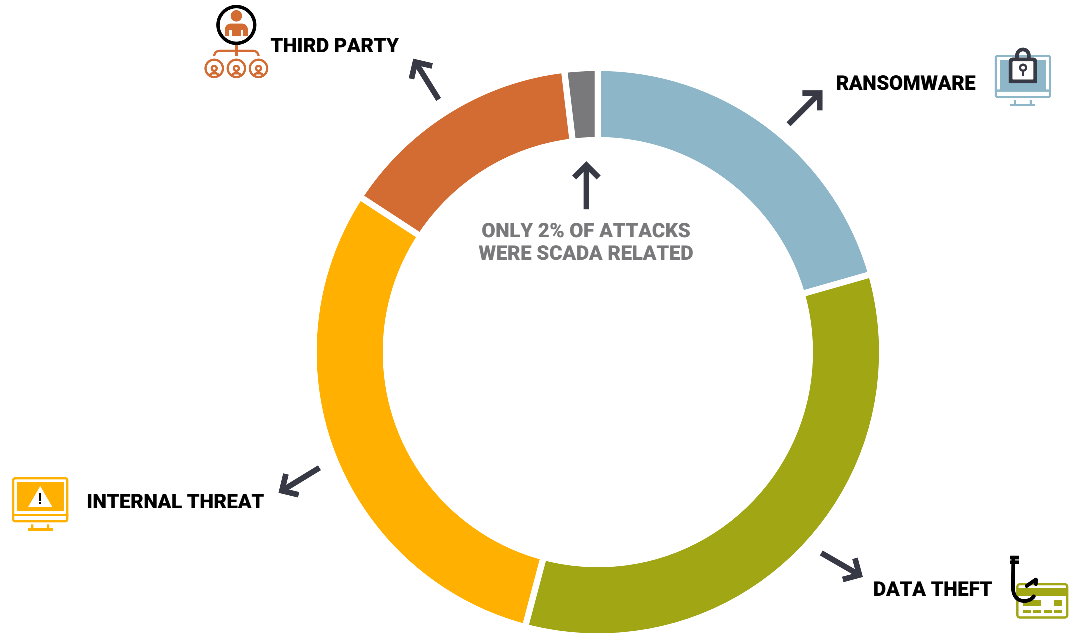
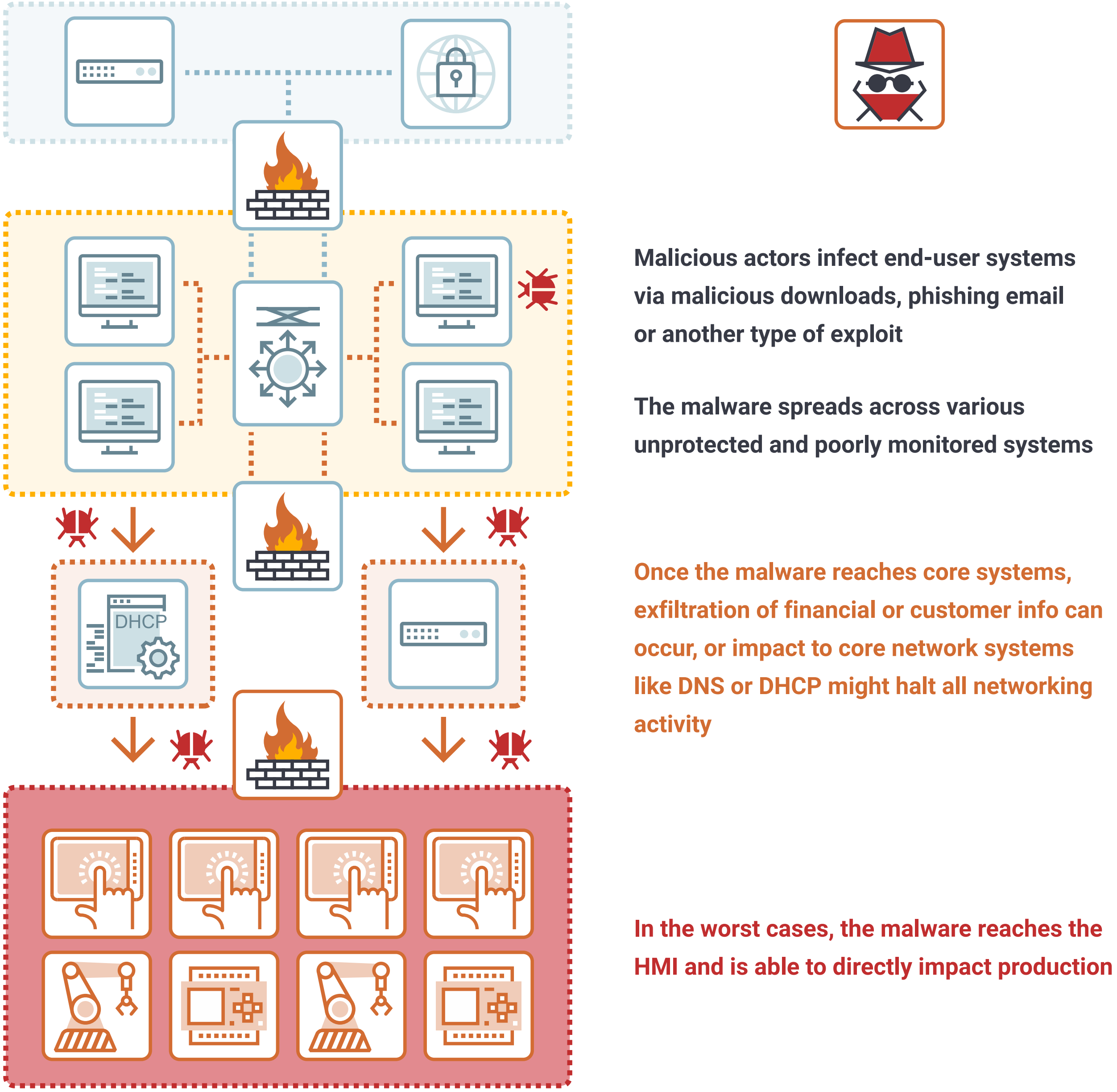


Figure 2: Manufacturing Attack Statistics

* Statistics compiled from IBM X-force 2020 Threat Intelligence Index, and Dragos Manufacturing Sector Threat perspective 2020

OT ATTACKS COME THROUGH ENTERPRISE NETWORK - Attacks on OT assets are often the final step of a complex malicious operation. For example, attackers may gain initial access via a malicious email on the enterprise network, then progressively spread to the operational network, and finally impact OT assets. See Figure 3. Once again the data supports this as the IBM report found that manufacturing had 4x as many business email compromises compared to other industries. This means that often the best way to protect OT and SCADA systems is often to protect upstream assets and detect and stop attackers before they ever reach the operational environment.



Malicious actors infect end-user systems via malicious downloads, phishing email or another type of exploit

The malware spreads across various unprotected and poorly monitored systems

Once the malware reaches core systems, exfiltration of financial or customer info can occur, or impact to core network systems like DNS or DHCP might halt all networking activity

In the worst cases, the malware reaches the HMI and is able to directly impact production

Figure 3: Cyberattack Progression in a Manufacturing Environment

DEFENDING MANUFACTURING ENVIRONMENTS WITH THE ORDR SYSTEM CONTROL ENGINE (SCE)

The Ordr SCE brings simplicity and consistency to the convergence of IT and OT, ensuring that manufacturing security teams always have full visibility and control over all their connected devices. Ordr deploys easily without impacting existing operations and without the need for agents. All analysis is continuous with built-in intelligence to detect and classify all devices, and automatically find vulnerabilities, weaknesses, and threats.

AGENTLESS AND PASSIVE DEPLOYMENT WITH IMMEDIATE VALUE

Unlike many traditional security tools, Ordr offers a completely agentless approach, and can be deployed locally or in the cloud. This means security teams can address the security of any type of connected device including traditional laptops and servers, as well as IoT, IIoT, or OT devices that will never support a security agent.

Ordr's architecture ensures that the solution is easy to deploy and can start delivering value quickly. Ordr works via passive, deep-packet inspection (DPI) of network traffic, and can often be installed within minutes or hours. Passive analysis ensures that teams don't need to worry about impacting existing operations. As soon as the platform is installed, Ordr DPI and proprietary artificial intelligence engine goes to work automatically identifying devices, detecting risks and threats, and analyzing behavior. While the solution will continue to baseline and learn more about the environment over time, teams can start getting insights into their converged environments almost immediately.

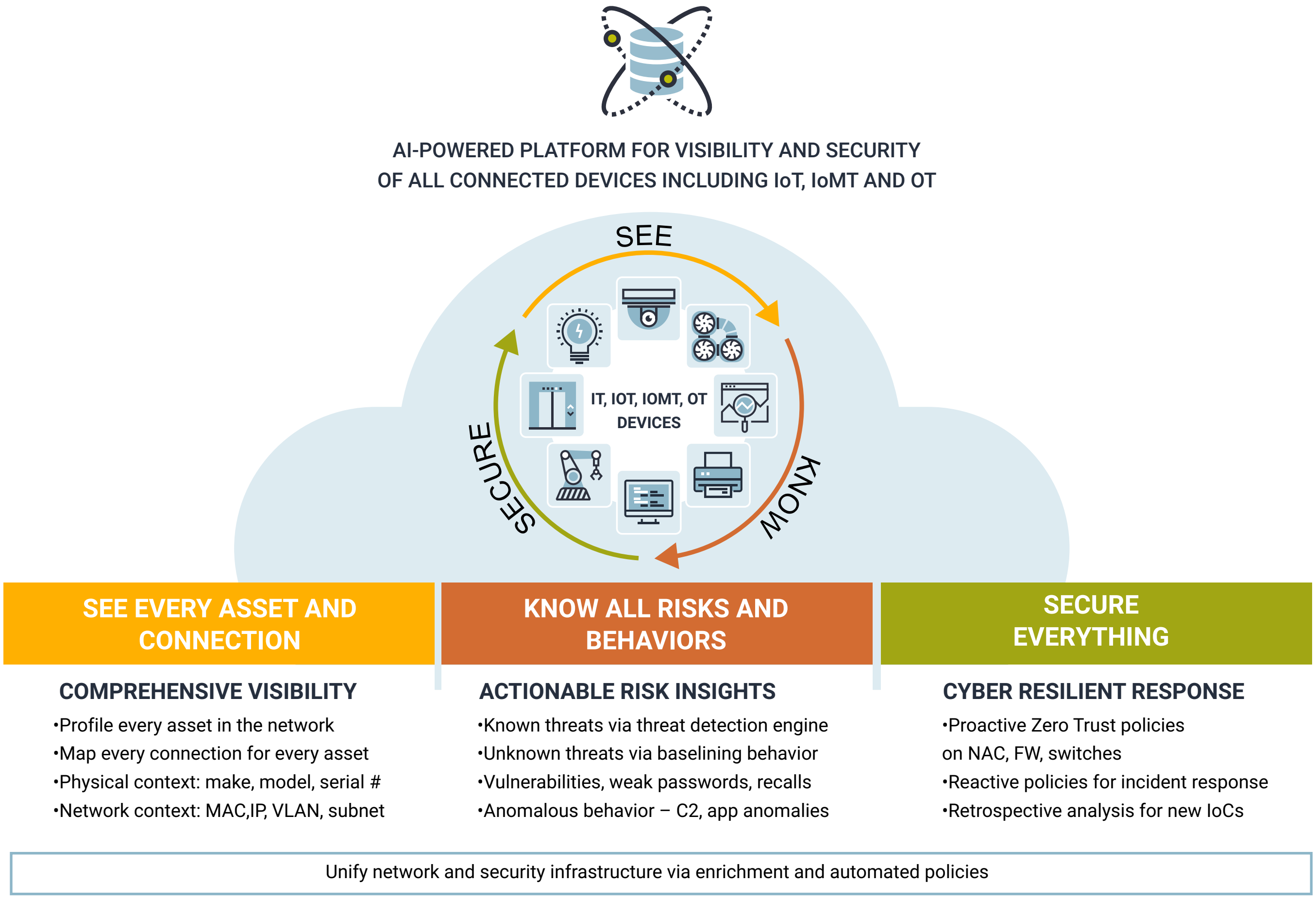
SEE, KNOW, SECURE EVERY CONNECTED ASSET IN MANUFACTURING

Ordr provides the quickest time to value for every manufacturing organization worried about 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 the devices and mitigate risk. Based on observing devices, 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.



AI-POWERED PLATFORM FOR VISIBILITY AND SECURITY
OF ALL CONNECTED DEVICES INCLUDING IoT, IoMT AND OT

SEE EVERY ASSET AND CONNECTION

COMPREHENSIVE VISIBILITY

•Profile every asset in the network
•Map every connection for every asset
•Physical context: make, model, serial #
•Network context: MAC,IP, VLAN, subnet

KNOW ALL RISKS AND BEHAVIORS

ACTIONABLE RISK INSIGHTS

•Known threats via threat detection engine
•Unknown threats via baselining behavior
•Vulnerabilities, weak passwords, recalls
•Anomalous behavior – C2, app anomalies

SECURE EVERYTHING

CYBER RESILIENT RESPONSE

•Proactive Zero Trust policies
on NAC, FW, switches
•Reactive policies for incident response
•Retrospective analysis for new IoCs

Unify network and security infrastructure via enrichment and automated policies

Figure 4: Ordr Platform - Visibility and Security for IT, IoT, IIoT and OT devices

KEY CAPABILITIES

Ordr provides a strong security foundation that applies to a variety of security functions including asset identification and inventory, vulnerability management, threat detection, behavioral analysis, policy creation, enforcement, and a variety of additional orchestrated responses.

REAL-TIME ASSET IDENTIFICATION AND CLASSIFICATION - Ordr brings together a unique combination of traffic analysis and AI to automatically discover and classify every device on the network. This includes high-fidelity information such as make, classification, location, and application/port usage. This visibility is continuous, real-time, and provides a single source of truth for network asset inventory.

DYNAMIC VULNERABILITYAND RISK MANAGEMENT Ordr delivers a variety of unique capabilities in the area of vulnerability management. The platform includes a built-in vulnerability scanner to identify devices affected by a variety of industry-specific security alerts or recalls. Ordr also complements traditional scanning tools with bi-directional integrations that allow staff to identify devices that may have been missed by previous scans. The solution can also be used to create customized scans that specifically include or exclude devices of a certain type - which can be critical to maintaining business operations.

ADVANCED THREAT DETECTION VIA BEHAVIOR PROFILING AND MACHINE LEARNING - Ordr includes a built-in IDS engine to detect threats and devices that are under active attack. Ordr also automatically learns every device's unique communication patterns, known as its Ordr Flow Genome. This provides a baseline that can be used to find suspicious and anomalous behaviors that could be the sign of an unknown threat.

RESPONSE ORCHESTRATION THROUGH EXISTING IT INFRASTRUCTURE - Ordr can automate controls both to proactively reduce the risks of a device as well as to isolate devices with detected risks or threats. By baselining device behavior, Ordr can dynamically create segmentation policies such as firewall rules that provide devices with necessary access while limiting unnecessary exposure. Policies can be dynamically generated and enforced on a variety of infrastructure including switches, firewalls, wireless LAN controllers, and more. Ordr also integrates with incident response and asset management workflows and can be used to quarantine compromised or high-risk devices.

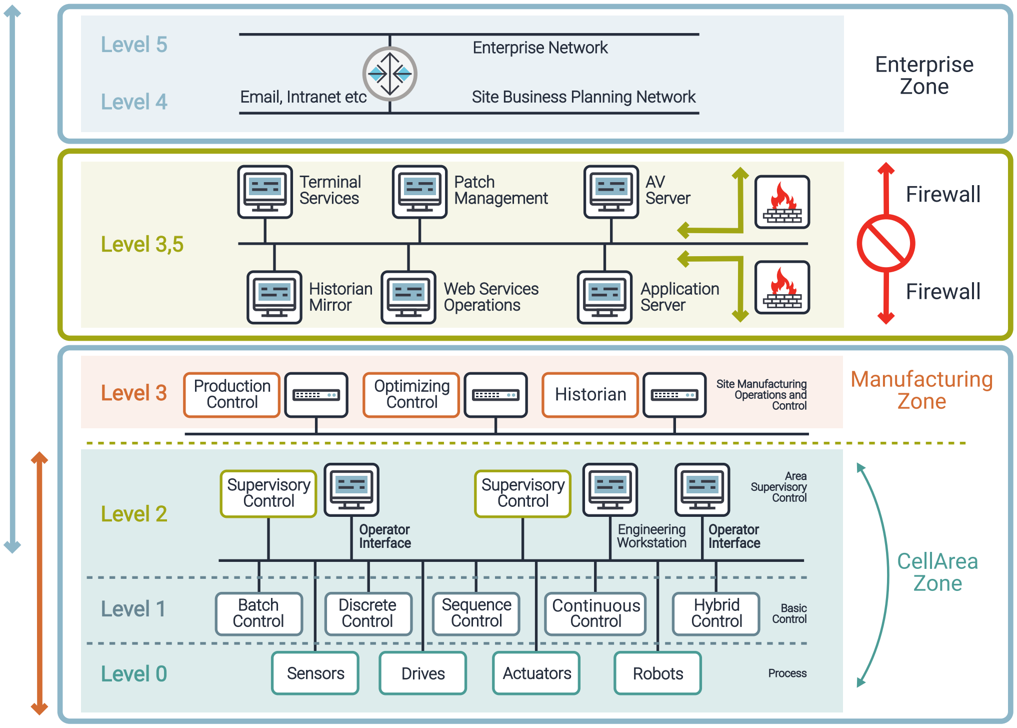
ORDR IN THE MANUFACTURING ENVIRONMENT

With Ordr, manufacturing security teams can ensure they have a unified and automated approach to visibility, detection, and enforcement that applies both to the enterprise and the manufacturing sides of their environments.

This provides a converged view of the organization's many connected assets that includes traditional devices as well as agentless and unmanaged devices. Most importantly, Ordr can create Zero Trust or least-privilege policies for unmanaged devices based on the actual observed communications needs of each device type. This ensures that IoT, IIoT, and OT technologies can deliver their value while keeping their exposure and risk to the bare minimum.

Naturally, no product is a security silver bullet, and the Ordr SCE is designed to work with and extend the value of other tools in the environment. Ordr can work with traditional vulnerability scanning tools to identify IoT-specific vulnerabilities, and to create custom vulnerability scanning jobs to cover devices that may have been missed, or to avoid scanning sensitive IoT or OT devices. Ordr can incorporate threat intelligence findings from external tools such as Anomali to enrich its ability to detect threats in the organization.

The platform also integrates with the organization's other enforcement tools such as switches, firewalls, and NAC tools to automatically enforce policy. Security teams can also push Ordr logs and alerts to SIEMs and ITSM tools. The platform also naturally complements OT-specific security tools which focus on the lowest levels of OT devices. As shown in Figure 5, Ordr supports Purdue models 2-5.



Single entity to monitor and manage any number of agentless or traditional endpoints

Least privilege policy and monitoring for HMI and other unmanageable OS platforms to mitigate risk

OT specific vendors focus on lower levels

Figure 5: Ordr supports Purdue Model levels 2-5

CONCLUSION

Manufacturers are facing a uniquely challenging security environment. The convergence of IT and OT technologies has introduced new complexities, and a new wave of threats have arrived to take advantage of any mistakes. The Ordr SCE offers a platform that is uniquely suited for these challenges. With the ability to bring visibility, detection, and response to all devices (agenteable or agentless) and all segments of the network, Ordr provides teams with the right foundation for securing their converged environments and enabling digital transformation.

To learn more about the Ordr SCE and how the solution can apply to your environment, please contact the Ordr team at WWW.ORDR.NET