See, Know, and Secure Every Connected Device

OVERVIEW

Connected devices are now a significant part of the network eco-system across all industries. These IP-enabled devices can range widely, from cameras and payment card systems to business-critical devices such as infusion pumps and HVAC control systems. These devices cannot be taken out of service, even to be patched, and typically have an expected service life of more than 10 years, (far more than typical managed endpoints).

Often, these devices support rudimentary operating systems, can be difficult to discover via traditional asset inventory solutions, cannot be scanned via vulnerability management systems and cannot support corporate endpoint security agents. These devices can be business, IT and cybersecurity blind spots.

Introducing Ordr Connected Device Security

Ordr is the only purpose-built platform to discover and secure every connected device - from traditional servers, workstations and PCs to Internet of Things (IoT), Internet of Medical Things (IoMT) and Operational Technology (OT) devices.

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 proactive, reactive and retrospective policies. These include reactive policies to quickly mitigate risks during an attack, proactive policies to segment mission-critical but vulnerable devices, and retrospective analysis and policies to identify compromised systems based on new indicators of compromise.

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, across all industries.

CHALLENGES

1. Connected IoT, IoMT and OT proliferation introduces real-time asset inventory issues.

2. Devices running outdated operating systems increase an organization's attack surface.

3. Connected devices may be an initial threat vector into an organization.

4. To move from detection to response during an incident, device details — what it is, where it's located, what actions are possible — are critical.

5. Maintenance and procurement decisions require device utilization insights.

BENEFITS

INCREASE VISIBILITY INTO DEVICE RISKS

BRING DEVICES INTO COMPLIANCE

MANAGE PROCUREMENT AND CAPITAL SPEND

ACCELERATE THREAT DETECTION AND RESPONSE

IMPLEMENT ZERO TRUST SEGMENTATION

DELIVER DEVICE UTILIZATION EFFICIENCIES

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

SEE EVERY ASSET AND CONNECTION	KNOW ALL RISKS AND BEHAVIORS	SECURE EVERY THING
COMPREHENSIVE VISIBILITY	**ACTIONABLE RISK INSIGHTS**	**CYBER RESILIENT RESPONSE**
•Profile every asset in the network	•Known threats via threat detection engine	•Proactive Zero Trust policies on NAC, FW, switches
•Map every connection for every asset	•Unknown threats via baselining behavior	•Reactive policies for incident response
•Physical context: make, model, serial #	•Vulnerabilities, weak passwords, recalls	•Retrospective analysis for new IoCs
•Network context: MAC,IP, VLAN, subnet	•Anomalous behavior – C2, app anomalies	

Unify network and security infrastructure via enrichment and automated policies
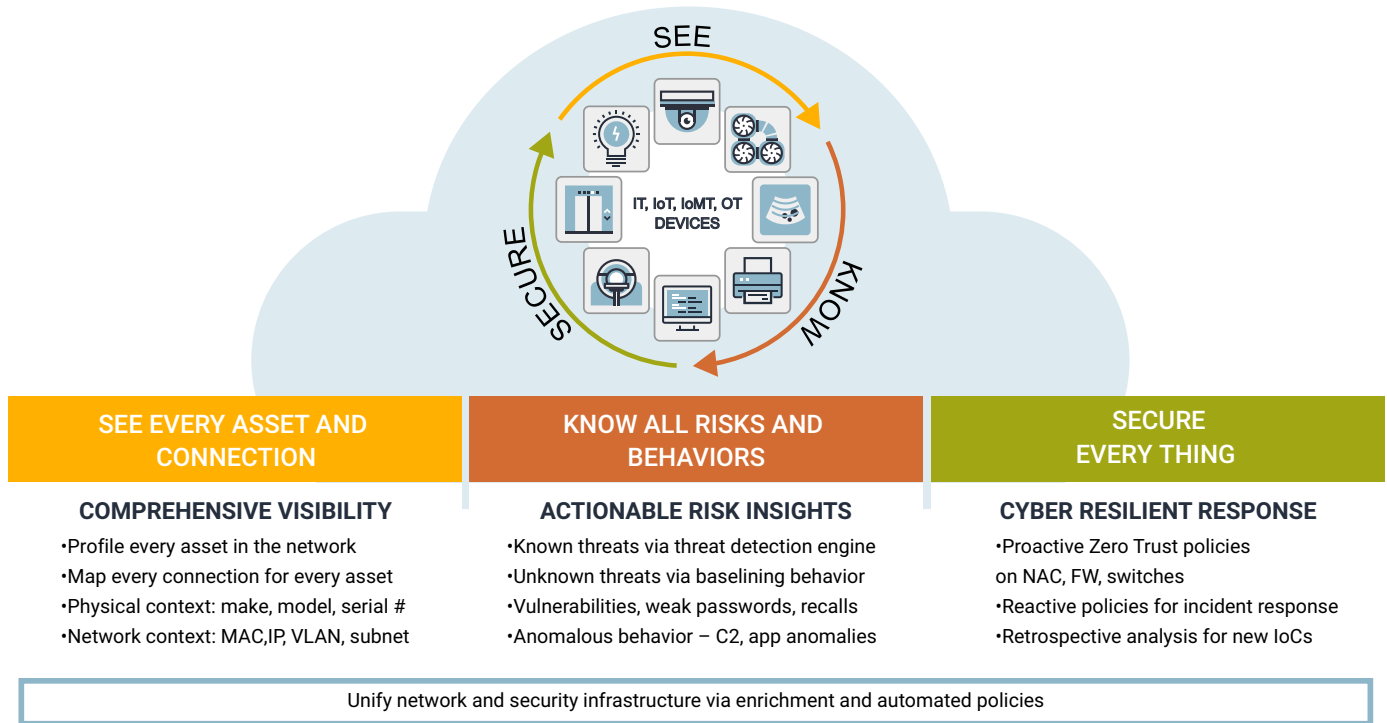
FIGURE 1: ORDR DEVICE SECURITY FRAMEWORK

Figure 1 describes the Ordr Connected Device Security Framework, comprised of the following pillars:

Comprehensive Visibility

Within a few hours of deployment - via a network TAP or SPAN - Ordr passively discovers high-fidelity context on every connected device, including make, model, operating system, location, application/port usage, and network connectivity. In addition, the Ordr Flow Genome uses machine learning to profile the behavior of every device and baseline communications patterns continuously. This comprehensive device, network and behavioral context is then enriched with threat intelligence, vulnerability data, FDA, device manufacturer alerts, CareCERT and incorporated into the Ordr Data Lake. Organizations can quickly identify devices with outdated operating systems, FDA recalls, on the CareCERT list, or banned by the U.S Commerce Department, and integrate inventory data with asset management systems. Organizations can also pinpoint where devices are located and establish what other systems they are communicating with at any point in time.

Actionable Risks and Threat Insights

The Ordr platform provides insights into both known and unknown threats.

Known threats: Ordr identifies risks such as devices with vulnerabilities, recalls, weak passwords and weak certificates. Vulnerabilities can be correlated with industry and manufacturer databases, and shared with vulnerability management solutions. Ordr also offers an integrated threat detection engine to detect threats across the kill chain, including East West lateral movement, exploits, attacker tools (eg Eternal Blue, Cobalt Strike) and more.

Unknown threats: Ordr's proprietary AI/machine learning-based engine baselines normal device behavior and identifies anomalies such as communications to a malicious domain or application anomalies for high-risk protocols (SMB, RDP, etc).

Security teams can customize their risk scores to ensure that all alerts are aligned to organization priorities. In addition, during a security incident, Ordr can track devices associated with a specific owner or identify the most recent authenticated login to a device via Active Directory/LDAP, WinRIM/WMI and Kerberos integration.

Automated Cyber Resilient Response

Ordr automates the appropriate proactive, reactive or retrospective response for device, networking and security teams. These policies can be created and enforced with one click of a button on existing switches, wireless controllers, and firewalls, or via NAC platforms.

Proactive Response:
Unlike users, devices are deterministic with specific behavioral patterns. Ordr automates proactive policies that only allow sanctioned communications flows for devices. For example, Ordr enables Zero Trust segmentation for devices with outdated operating systems that cannot be patched but need to safely stay in operations.

Reactive Response:
During an incident, Ordr automates the creation of NGFW policies, ACL blocks, quarantine VLAN assignment, port shutdown, or session termination to mitigate device risks. When a new device is detected on the network, Ordr can trigger CMMS or ITSM workflows.

Retrospective Response:
Ordr is the only connected device security vendor that offers a "time-machine" to analyze historical communications to newly announced Indicators of compromise. This provides forensic insights on a device that may have been compromised in a previously undetected security event.

KEY ORDR USE CASES

ASSET INVENTORY & MANAGEMENT

Real-time visibility and classification of all network assets. Identify devices with vulnerabilities.

COMPLIANCE

Continuous and real-time asset inventory, identify devices with legacy O/S or deployed in the wrong VLAN or subnet.

DEVICE UTILIZATION

Understand how devices are used to manage procurement, device maintenance and end-of-life.

NAC ACCELERATION

Complement and accelerate your NAC deployment by classifying devices and automating NAC policies.

THREAT DETECTION AND RESPONSE

Identify devices that are behaving abnormally, have vulnerabilities or weak passwords/certificates.

ZERO TRUST SEGMENTATION

Easily generate and enforce granular segmentation policies. Align with Zero Trust and CARTA frameworks.

Comprehensive Integrations

Ordr offers the most comprehensive integration in the market — extending IoT device context, addressing visibility and vulnerability gaps, and generating and enforcing policies to proactively harden the enterprise infrastructure against attacks. Ordr integrates with next-generation firewalls, network access controls, wireless LAN controllers, IT Services Management (ITSM), Security Information and Event Management (SIEM), Vulnerability Management and Configuration Management Database (CMDB) solutions in the market.

One Unified Platform for HTM, Security and Networking

Ordr Clinical Defender for HTM/BIOMED

• Inventory all IoMT devices, identify those with PII and risks

• CMDB lifecycle management and automation

• Cost avoidance via segmentation for devices with outdated O/S

• Optimize IoMT utilization & procurement spend

Ordr Connected Device Security for Security Teams

• Real-time inventory into devices, risks and flows for compliance

• Address risks and vulnerabilities to protect against cyberattacks

• Accelerate incident response

• SOC enrichment with threat intelligence integration

Ordr Connected Device Security for Networking Teams

• Discover, monitor and track all connected devices

• Map all device communications patterns

• Accelerate Zero Trust segmentation for vulnerable devices

• Accelerate NAC deployments (Cisco ISE, Aruba Clearpass)

Customer Success

Ordr prides itself on a customer-first culture. Ordr takes a whole-enterprise approach that allows for strategic dialog between IT and Security teams. The Ordr Customer Success team is led by industry experts that will augment teams during the onboarding process and guide networking, security, and device owners through the entire device security framework.

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**.