See 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, cannot be scanned via vulnerability management solutions and cannot support corporate endpoint security agents. These devices can be business, IT and cybersecurity blind spots.

Introducing Ordr Systems Control Engine (SCE)

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 Technologies (OT) devices.

Ordr Systems Control Engine (SCE) 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 (PCI, PHI, PII) 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, across all industries.

CYBERSECURITY BLIND SPOTS

1. Insecure or improperly segmented devices increase the attack surface of the internal network.
2. Corporate IoT devices such as unsecured conference room phones and smart televisions are susceptible to industrial espionage.
3. Communications and information sharing between devices in a network can be targeted in a data breach.
4. Unmanaged and IoT devices can be taken over as botnets as experienced with Mirai and Dark Nexus attacks.

BENEFITS

INCREASE VISIBILITY INTO DEVICE RISKS

BRING DEVICES INTO COMPLIANCE

MANAGE PROCUREMENT AND CAPITAL SPEND

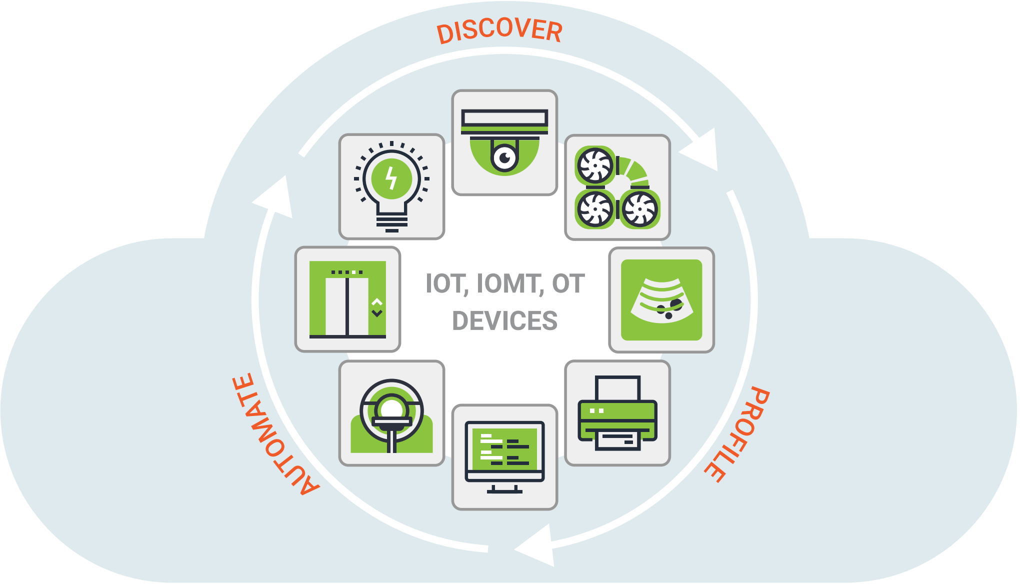
ORDR CORE AND PREMIUM

Ordr offers a foundational and premium software package for organizations:

- ✓ **Ordr Core** software delivers foundational device discovery, classification, and behavior analysis as well as risk profiling functionality.
- ✓ **Ordr Premium** includes all of Ordr Core features in addition to automated actions to address risks, and advanced integrations with security and networking products.

ORDR SCE:

AI-POWERED PLATFORM FOR VISIBILITY AND SECURITY
OF ALL CONNECTED DEVICES INCLUDING IOT, IOMT AND OT



DISCOVER ALL DEVICES

- Agentless deployment
- Classify by make, model, serial number, location, O/S
- Identify devices with vulnerabilities, exploits, FDA, recalls, CareCERT
- Identify devices with weak ciphers/ certificates

BEHAVIORAL PROFILE DEVICES

- Baseline communications
- Visualize via VLAN and network architecture
- Identify anomalous and malicious communications
- Understand utilization

AUTOMATE ACTION

- Trigger workflows for CMMS, CMDB, ITSM
- Proactive segmentation and enforcement on NAC, FW, switches
- Incident response segmentation for vulnerable devices
- Scan or quarantine devices, or block device communications

FIGURE 1: ORDR DEVICE SECURITY FRAMEWORK

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

Discover All Network Devices

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, and application/port usage. This device context is then enriched with threat intelligence, vulnerability data, FDA, device manufacturer alerts, CareCERT and incorporated into the Ordr Data Lake. This provides organizations with granular, high-fidelity classification into every device in their network. 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.

Behavioral Profile Devices and Risk

Ordr Flow Genome uses machine learning to profile the behavior of every device and baseline communications patterns. This allows Ordr to deliver deep understanding of behavior insights--from identifying anomalous or suspicious behaviors, such as communications to external malicious domains, to understanding device utilization. Device utilization patterns can identify areas of over or under use, to optimize device efficiencies, or support procurement decisions as teams scale their capacity. Communications to other IP/VLAN segments within the organization can be easily visualized, as well as communications to external networks. Ordr can also extract the latest authentication information via Active Directory/LDAP, WinRM/WMI and Kerberos to identify device users so organizations can locate devices associated with a specific owner, or identify the most recent authenticated login to a device during a security incident.

Automate Action

Ordr automates the appropriate response for device, networking and security teams. These include the automated creation and enforcement of segmentation policies, or alerting and triggering a specific security or operational workflow.

Proactive Segmentation:

Unlike users, devices should only communicate with specific systems. By learning device communications patterns, Ordr can dynamically create policies to allow only appropriate communications while limiting exposure. These policies can be automatically enforced on existing infrastructure - firewalls, switches, NAC and wireless LAN controllers.

Operational Workflows:

When a new or unknown device is discovered, Ordr can trigger a centralized workflow with a CMMS or CMDB to ensure proper inventory, authentication, and routing to the right device owners. Ordr can also initiate scans or open an ITSM ticket.

Security and Incident Response:

In the event of a security incident, or if devices have triggered an alert (known vulnerability, weak cipher, weak certificate, active threat, or malicious/suspicious behaviors) Ordr can push alerts to a SIEM, block traffic, or automatically segment the impacted device.

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 AUGMENTATION

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

THREAT DETECTION

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

SEGMENTATION

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

Platform 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.

Ordr Deployment Options

Ordr supports multiple deployment models including SaaS delivered, fully on-premises, private cloud, MSP hosted and multitenancy. There are three key components of the system:

Systems Control Engine:

SaaS managed service in the cloud or on-premises/ private cloud-hosted hardware appliances or software appliances in the data center that performs behaviour analisis, identeties anomalies, and is the core for management and policy decisions.

SCE Center:

Ordr operated cloud service that helps in zero-touch provisioning of each deployment and keeps it up-to-date with the latest threat feeds and device profiles.

SCE Sensor:

Hardware appliances or software appliances that are deployed at the access, distribution or core layer of the network and receive SPAN, tap, or flow data.

Sensors and on-premises appliances can be delivered as software images or preinstalled on appliances.

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**.