Enabling Zero Trust for Connected Devices

OVERVIEW

Internet of Things (IoT), Internet of Medical Things (IoMT), Operational Technology (OT), and other connected devices are now a significant part of the network eco-system across all industries. These IP-enabled devices range widely from cameras and payment card systems to mission-critical devices such as infusion pumps and HVAC control systems. Many of these devices are business-critical, cannot be taken out of service even for patching, and can have an expected service life of more than ten years - far more than a typical managed endpoint.

Connected devices are often built on rudimentary operating systems, can be a challenge to manage, cannot be scanned, and do not support endpoint security agents. Given the limitations, connected devices are blind spots for security and IT teams and create significant risk for your organization.

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 IoT, IoMT, and OT devices.

See

- Every connected asset
- Every device flow
- Every network connection

Know

- Every vulnerability
- Every risk and exploit
- Every anomaly

Secure

Every thing

- With proactive, reactive, retrospective response
- Unify existing security and networking infrastructure

Ordr collects nearly 1000 attributes to classify every connected device accurately, profile behavior, and uncover risk. Ordr insights not only help you identify devices with vulnerabilities, weak ciphers, weak certificates, and active threats, but also those that exhibit malicious or suspicious behaviors.

With deep device context, we simplify policy creation to accelerate threat response and improve your security posture. Dynamically created policies help you react quickly to stop the spread of an attack and proactively improve security with segmentation for mission-critical devices. Retrospective analysis identifies compromised systems based on new indicators of compromise (IOCs) to help you understand the impact and align protections.

Ordr has been effectively implemented at scale to secure connected devices in large, complex networks across all industries. Our solution is delivered as a cloud service and offers a zero-touch, agentless integration with any environment.

Ordr Use Cases

THREAT DETECTION & RESPONSE

NAC ACCELERATION

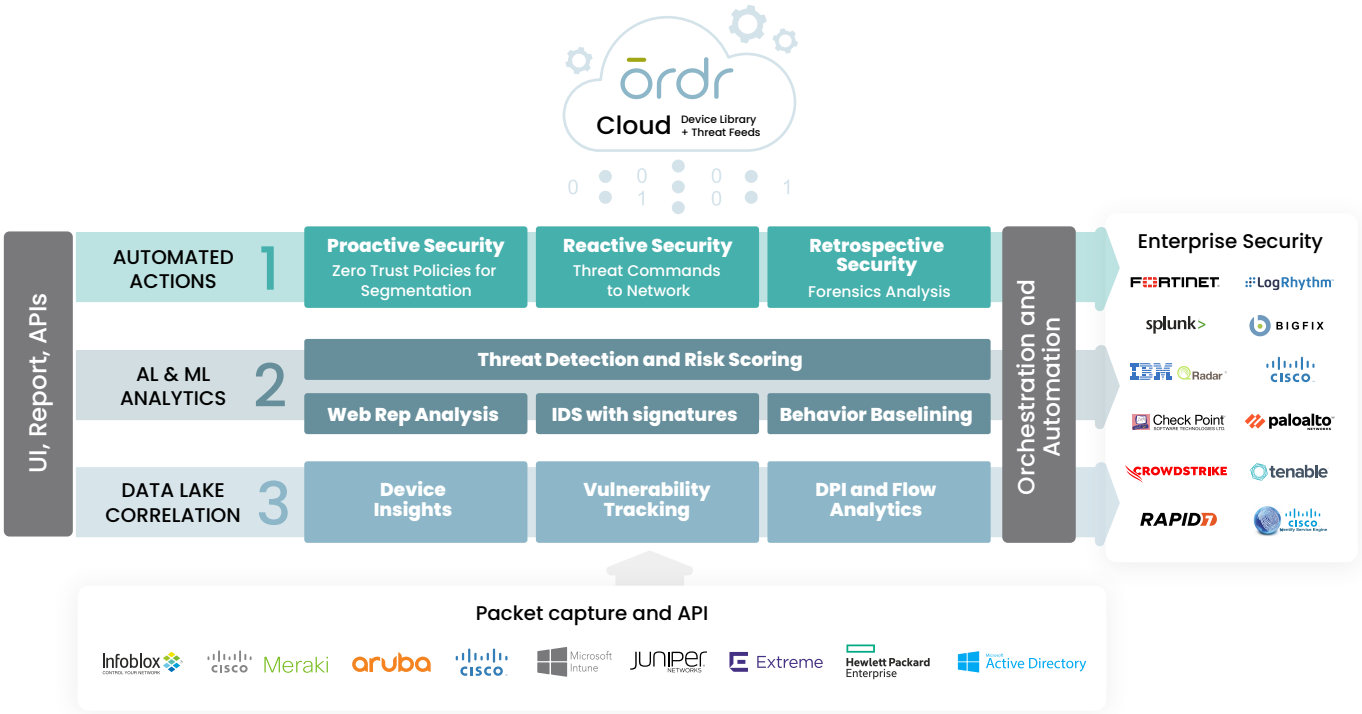
ZERO TRUST SEGMENTATION

INVENTORY & MANAGEMENT

DEVICE UTILIZATION

COMPLIANCE

How Ordr Works



Packet Capture and API

• Ordr integrates with network infrastructure, APIs, and deep packet inspection (DPI) to collect device flow data and send it to the cloud hosted Ordr Data Lake for correlation and analysis. These passive data collection options enable granular device insights without agents or scanning, so there's no impact on device operations or performance.

Data Lake Correlation

• Flow data is analyzed with DPI and correlated to accurately identify and classify every connected device with details including the device MAC, IP, make, model, operating system, location, application/port usage, and network connectivity. Device details provide insights into risk such as outdated OSs or weak passwords and can be enriched with 3rd party data to identify devices with known vulnerabilities and recalls. With Ordr you'll maintain an accurate, up-to-date device inventory and understand the potential risks to your organization.

AI & ML Analytics

• Ordr further analyzes device flow data to understand internal and external device communications, establish a baseline of normal communications for each device, and assess communication risk. Each baseline is compared with similar devices in your environment for an understanding of normal activity for each class of device. Multiple factors are combined including device vulnerability based on the OS and firmware, and communication insights to establish a risk score for each device. Ordr can uncover active threats by identifying deviations from each device's baseline and by using a signature-based IDS to identify and stop known malicious attack traffic.

Automated Actions

• Ordr leverages deep device context to dynamically create policies that improve your response to threats and reduce risk. Reactive policies can isolate devices with segmentation to stop the spread of attacks and proactive policies help accelerate NAC and zero trust projects to improve your security posture. Our retrospective capabilities aid forensics efforts and provide insights into potential exposure when new indicators of compromise (IOCs) are discovered.

Orchestration and Automation

• Ordr policies are created using native commands and syntax of popular security and network devices. These policies can be reviewed by security teams and enforced with existing security and network infrastructure with the push of a button. Ordr has over 70 integrations with security, network, and other IT tools to ensure tight and efficient integration into your environment and current workflows.

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.