Ordr Software Overview: Foundation, Essentials, Advanced

Connected device security continues to be a major concern across all industries, and with more than 25 billion internet-connected devices operating today, the growing challenges of managing and securing these devices are daunting.

Ordr Connected Device Security Platform

Ordr is a connected device security platform that discovers every connected device, profiles device behavior, uncovers risk, and helps teams automate their response to threats. Ordr identifies devices with vulnerabilities, weak ciphers, weak certificates, active threats, and those that exhibit malicious or suspicious behaviors. Ordr also automates response for HTM, security, and networking teams by dynamically creating and enforcing microsegmentation policies or alerting and triggering specific security or operational workflows.

Ordr Software Packages

Ordr software packages are designed to guide users to the right features required for their specific needs and use cases:

Foundation

See every connected device

- Discover and profile every connected device in the network
- See granular details for each device beyond IP and MAC address
- Understand device connectivity status and activity
- Uncover device risk including vulnerabilities, recalls, and advisories
- Maintain a source of truth for asset inventory and enrich existing tools
- View detailed device information in dashboards and dynamic reports

Essentials

Know the risk of every connected device

- Includes all features in Ordr Foundation
- Assess your attack surface with customizable risk scoring
- Identify vulnerable devices based on passive and active data analysis
- Eliminate blind spots with complete N/S and E/W traffic visibility
- Uncover real-time threats with traffic analysis and threat insights
- Meet compliance with device communication and activity tracking
- Understand the retrospective impact of every new IoC detected

Advanced

Secure every connected device

- Includes all features in Ordr Foundation and Essentials
- Block malicious activity while letting devices perform core functions
- Define and apply proactive security across devices and environments
- Transform visibility into protection with automated policy generation
- Enforce policies on existing switches, NAC infrastructure, and firewalls
- Integrate with existing security infrastructure including EDR, firewall, NAC, and vulnerability solutions

Selecting The Right Package

The Ordr Foundation, Essentials and Advanced software packages are right sized for every user:

HTM/Clinical Engineering: Ordr Foundation is recommended for the operational lifecycle management of medical devices. This includes medical device asset inventory, vulnerability and risk management, traffic analysis and device utilization.

Networking: Ordr Advanced is recommended for networking teams interested in accelerating Zero Trust segmentation and NAC projects.

Operational Technology (OT) owners: Ordr Foundation is recommended for identifying industrial and facilities equipment and validating appropriate network connectivity. Ordr Advanced can be used to enforce proper network segmentation and to apply Zero Trust "air gaps" to proactively protect business-critical equipment in converged networks.

Security: Ordr Essentials or Ordr Advanced are recommended for security teams. Ordr Essentials includes the ability to identify all potential risks, including known and unknown threats. Ordr Advanced adds automated actions and advanced integrations with security and networking solutions.

Ordr Software Package Details

Platform Capabilities	Ordr Software Packages		
	Foundation	Essentials	Advanced
Ordr Software Package Details			
Device discovery	•	•	•
Device classification	•	•	•
Device location	•	•	•
Connection status	•	•	•
Device level flow visibility	•	•	•
Clinical details of medical devices	•	•	•
Medical device utilization	*sold as a separate license*		
Device Risk and Cyber Threats - Know your potential threats and business risk			
Device risk scoring	•	•	•
Device recalls and advisories	•	•	•
OS and firmware vulnerabilities	•	•	•
Behavioral analysis		•	•
Traffic analytics		•	•
Application destination URL visibility		•	•
Threat Intelligence feeds		•	•
Endpoint data retrieval using AD		•	•
User to device tracking		•	•
Ransomware detection		•	•
Lateral movement detection		•	•
Retrospective security			•
Active scanning			•
Policy Creation and Enforcement - Secure your environment			
Threat containment			•
Enhanced policy grouping			•
Segmentation policy creation & enforcement			•
Dashboards and Reporting - Operationalize device security and automate reporting			
Device dashboard and device reports	•	•	•
HTM dashboard and reports	•	•	•
Security dashboard and reports		•	•
Segmentation/security policy views and reports			•
Integrations - Integrate with existing security tools and infrastructure			
Syslog, SNMP, SMS, SMTP	•	•	•
Network Management System (NMS)	•	•	•
Microsoft Active Directory (AD)	•	•	•
Configuration Management Databases (CMDBs)	•	•	•
Computerized Maintenance Management Systems (CMMS)	•	•	•
IP Address Management (IPAM)	•	•	•
Medical servers	•	•	•
Network infrastructure	•	•	•
Security Information Event Management (SIEM) (device insights)	•	•	•
Security Information Event Management (SIEM) (security alerts)		•	•
Vulnerability scanners			•
Firewalls			•
Network Access Control (NAC)			•
Data center orchestration and segmentation			•

Ordr secures the millions of enterprise IoT and unmanaged devices such as manufacturing machines, building systems, medical equipment, printers and more that run within global networks. The Ordr Systems Control Engine uses machine learning to automatically discover and classify every IoT and unmanaged device, map all communications, detect and prioritize vulnerabilities, and then proactively secure each device through dynamic policy generation and segmentation. Organizations use Ordr to discover their devices, track usage, achieve proactive protection and compliance.
For more information about Ordr, go to ***www.ordr.net***