OrdrAI Protect

Protect Your IT, IoT, OT, IoMT with Advanced Threat Detection, Deep Behavioral Intelligence and Segmentation

The modern cybersecurity landscape is evolving rapidly, with attacks crossing traditional boundaries between IT, IoT, IoMT, and OT environments. Security teams struggle to gain visibility into all connected devices, including the 40% of devices that are unmanaged and go undetected creating security blind spots. Recognizing unauthorized data flows or Internet communications poses another challenge, as does identifying and mitigating against threats to mission-critical devices without disrupting essential operations.

Introducing OrdrAI Protect

OrdrAI Protect empowers security and IT teams with unparalleled granular insight into every asset including make, model, serial number, device owner, connectivity. Security teams can identify and prioritize vulnerabilities based on business relevance and detect advanced threats, anomalous behavior, and risky communications. OrdrAI Protect automatically generates policies—from reactive to proactive—to secure all assets, ensure compliance, and maintain operational integrity.

Key Benefits:

Eliminate blind spots: Discover high-fidelity asset context with highly accurate AI/ML powered classification of every asset including IT, IoT, OT and IoMT.

Reduce risks: Gain comprehensive visibility into vulnerabilities for both managed and unmanaged devices, then translate vulnerabilities into a prioritized action plan with risk scores and automated workflows assigned to the correct device owner. Ordr Flow Genome also profiles the behavior of every device and establishes baseline communications patterns.

Accelerate incident response: Quickly identify both known and unknown threats through an integrated intrusion detection engine and AI/ML-based anomaly detection. Accelerate response by generating policies to quarantine a device, block ports or terminate sessions on existing networking and security infrastructure. Share deep asset context with SIEM/SOC, create ITSM tickets, facilitating faster and more informed incident response.

Maintain business productivity: Confidently create Zero Trust segmentation policies to prevent lateral movement or isolate vulnerable devices based on baseline communications.

OrdrAI Protect Use Cases:

- **Asset inventory & management:** Automate hardware and software asset inventory across IT, IoT, IoMT, OT. Visualize asset connections and communications with detailed mapping, providing clarity on network interactions and potential risks.
- **Vulnerability management:** Prioritize vulnerabilities and assess the attack surface with customizable risk scoring aligned with business priorities. Quickly close vulnerabilities for IoT, IoMT, and OT devices with automated workflows assigned to the right owners.
- **Threat/anomaly detection & response:** Stay ahead of threats with real-time monitoring that detects and alerts on active threats, anomalous behaviors and risky communications.
- **Security and compliance gap:** Address compliance frameworks such as NIST-CSF, CIS Controls Cyber Essentials, CMMC, NHS DSP Toolkit, and more. Identify non-compliant devices like those running outdated OS or devices in the wrong VLAN/subnet.
- **NAC acceleration:** Accelerate Cisco ISE, Aruba ClearPass, FortiNAC projects with rich device context, and automated policies for connected devices.
- **Zero Trust segmentation:** Automatically generate dynamic policies for Zero Trust segmentation, ensuring that security controls allow only "baseline" device communications.
- **Accelerate incident response:** Share deep asset context with SIEM/SOC with automated workflows, facilitating faster and more informed incident response.

Ordr Case Studies

Ordr secures over 61 million assets (1000+ attributes each) and tracks 1.6 Trillion device flows across all industries including food and beverage, financial services, automotive, healthcare, and pharmaceutical companies.

"Within the financial services industry, there is a lot of governance. Having a solution like Ordr that can identify every "thing" on the network, including IoT and OT devices that are particularly challenging to categorize is important."

VERITEX® COMMUNITY BANK

// Bob Ludecke, Chief Information Security Officer, Veritex Community Bank

---

"It's eye opening when you put something like Ordr on your network. It has improved our incident response capabilities."

Franciscan ALLIANCE

// Jay Bhatt, CISO, Franciscan Alliance

For assistance with your asset visibility and security needs, visit ordr.net for more information or contact us at info@ordr.net.

ordr