ORDR

DATASHEET

ORDR AI Protect for Segmentation

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 ORDR AI Protect for Segmentation

ORDR AI Protect for Segmentation 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. "Segmentation" 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.

Maintain business productivity

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

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.

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.

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.

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 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.

THREAT/ANOMALY DETECTION & RESPONSE

Stay ahead of threats with real-time monitoring that detects and alerts on active threats, anomalous behaviors and risky communications.

ORDR Case Studies

ORDR secures over 100 million assets (2,500+ attributes each) and tracks 1.6 trillion device flows across all industries including healthcare, pharmaceutical, manufacturing, and financial services.

It’s eye opening when you put something like ORDR on your network. It has improved our incident response capabilities.

// Jay Bhatt, CISO

Franciscan Alliance

Franciscan ALLIANCE

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.

// Bob Ludecke, Chief Information Security Officer

Veritex Community Bank

VERITEX COMMUNITY BANK

About Us

ORDR is the leader in AI-powered asset risk and exposure management, trusted by top organizations across healthcare, pharmaceuticals, manufacturing, and financial services. With insights from over 100 million asset types, ORDR's platform empowers security teams to identify their biggest risks and take swift, effective action. From maintaining security hygiene to real-time threat detection and protection using microsegmentation, ORDR makes action not just possible but automated and simple — bringing ORDR to chaos.

ORDR is backed by top investors including Wing Venture Capital, Ten Eleven Ventures, Battery Ventures, Mayo Clinic Ventures, and Kaiser Permanente Ventures. For more information, visit www.ordr.net and follow ORDR on Twitter and LinkedIn.

For more information, visit **ordr.net**

Follow Ordr on

Ready to bring ORDR to your chaos?

REQUEST A DEMO