SOLUTION BRIEF

ORDR Integrations with Cisco

Cisco solutions are essential to connecting and securing modern IT environments. Internet of Things (IoT), Internet of Medical Things (IoMT), Operational Technology (OT), and other connected devices are increasingly found in these environments and can range from coffee makers and cameras to medical resonance imaging (MRI) scanners and manufacturing robots. These new connected devices enable new levels of automation and efficiency but also present new challenges for security teams.

Secure every connected device with ORDR and Cisco

ORDR's deep integrations across the Cisco portfolio add the visibility and insights needed to manage and secure the wide range of connected devices in today's environments. Powered by ORDR IQ, ORDR is the only purpose-built platform to discover, classify, and segment every connected device—from traditional servers, workstations, and PCs to IoT, IoMT, OT, and other connected devices.

ORDR discovers every connected device, profiles device behavior, uncovers risk, and enables automated, policy-based response. Using trusted asset intelligence, ORDR defines and simulates segmentation intent and informs enforcement through Cisco integrations, enabling consistent Zero Trust segmentation across distributed environments. This approach helps networking and security teams contain active threats, proactively segment vulnerable mission-critical devices, and perform retrospective analysis to identify compromised systems based on new indicators of compromise.

CHALLENGES

- Maintaining accurate device visibility
- Understanding unique device characteristics and vulnerabilities
- Identifying potential threats and active attacks
- Creating segmentation and zero trust policies to improve security

BENEFITS OF ORDR INTEGRATION WITH CISCO

Passively discover all devices

ORDR analyzes network traffic to discover every connected device and maintain an accurate, up-to-date catalog without the need for agents, scanning, or impact to mission critical devices.

Gain granular device visibility

ORDR uses deep packet inspection, API integrations, and application decoding techniques to identify, classify, and provide granular context for all connected devices.

Understand device behavior

ORDR anayzes device communications to create a baseline of normal device behavior and to identify and stop active threats.

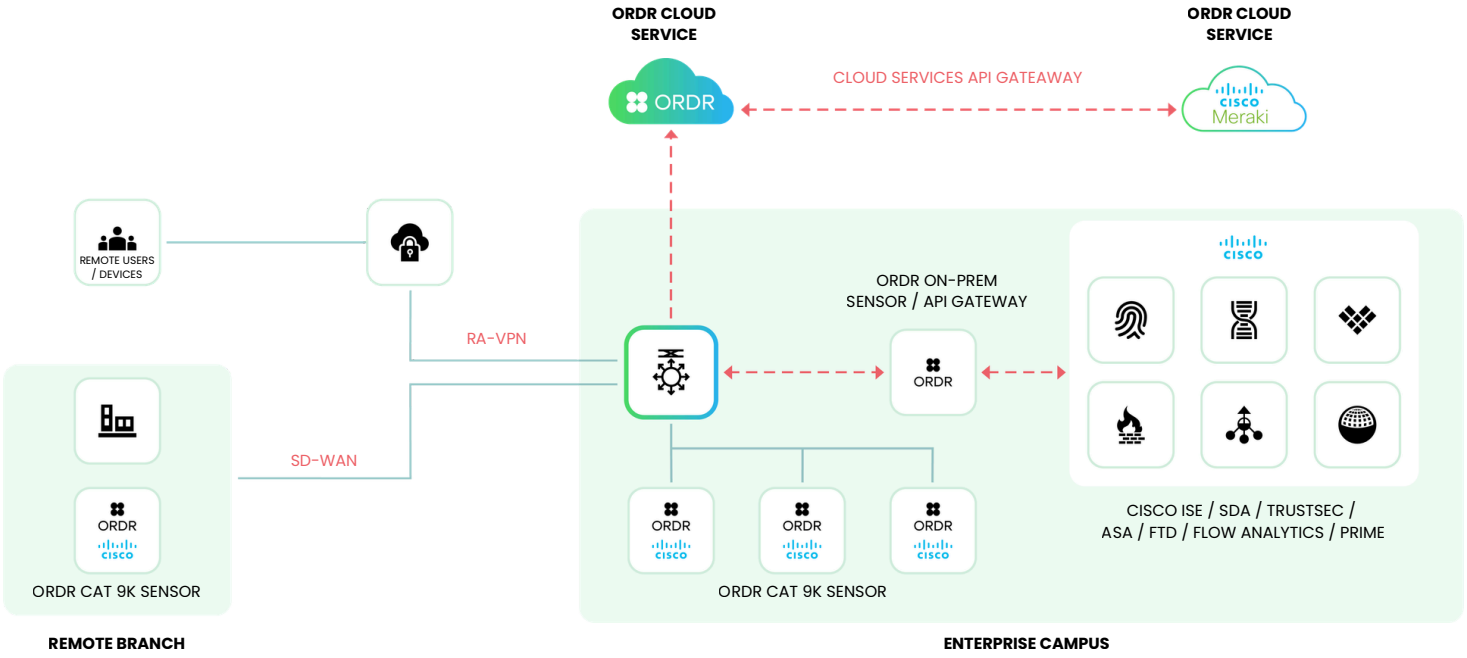
Accelerate segmentation projects

ORDR provides essential insights including device context and behavior to automate segmentation policies, accelerate zero trust projects, and improve security for connected devices.

ORDR integration with Cisco solutions

Cisco Healthcare: ORDR integrates with Cisco to discover and secure every IoT, IoMT, OT, and other connected devices in healthcare environments. ORDR provides healthcare IT teams with accurate and detailed information to discover, map, identify, and secure all connected devices. ORDR insights are used to dynamically generate Cisco ISE zero trust segmentation policies for threat mitigation and proactive protection.

Cisco IoT: ORDR integrates with Cisco to enable comprehensive visibility and security of every IoT device. ORDR automates discovery, provides granular classification, uncovers vulnerabilities, and monitors communications to identify potentially compromised devices. Ordr insights are critical to understanding device context and help to simplify and accelerate zero trust segmentation policy creation to improve security.



ORDR integration with Cisco products

Cisco Catalyst 9000 Series Switches: The ORDR Sensor for the Cisco Catalyst 9000 Series Switches leverages dedicated application hosting capabilities of the Catalyst 9000 to extend ORDR visibility to the access edge, branch offices, and other remote locations. The ORDR sensor collects network traffic directly from the Catalyst switch and provides high-fidelity visibility into all connected devices including device security risk, network connectivity, utilization metrics, and device behavior. ORDR insights gained from Catalyst 9000 switches simplify and accelerate device identification and creation of north-south and east-west segmentation policies for enforcement with Cisco ISE and SDA. ORDR can be deployed directly to each Catalyst 9000 switch or at scale to tens or hundreds of switches using Cisco DNA Center.

Cisco Identity Services Engine (ISE): ORDR integrates with Cisco ISE to significantly simplify and accelerate Cisco Software-Defined Access (SDA) segmentation for IoT, OT, IoMT, and other connected devices. ORDR automatically discovers and classifies every endpoint with high fidelity details and provides insights into essential and safe device behavior. Information from ORDR removes the guesswork and manual process of profiling unknown endpoints and provides necessary context to implement effective group-based segmentation. ORDR insights are used to dynamically generate Cisco ISE segmentation policies for proactive protection and ORDR's intelligent rule-based engine streamlines Cisco Adaptive Network Control (ANC) to rapidly contain active threats.

Cisco Meraki: ORDR integrates with Cisco Meraki to enable visibility of all IoT, OT, IoMT, and other connected devices across Meraki cloud-managed and Cisco enterprise networks. By analyzing data from Meraki Systems Manager, ORDR passively discovers all connected endpoints and provides a central view of every device with high fidelity details including device risk, normal and anomalous communications, and active threats. ORDR can automate proactive segmentation policies enforceable with Cisco ISE to prevent or stop the spread of an attack and improve connected device security.

Cisco Prime Infrastructure: ORDR integrates with Cisco Prime Infrastructure to centrally track every connected device and provide details such as physical location, device name, and other network connectivity information. ORDR combines these details with additional granular insights to ensure every discovered device is accurately mapped to its current network location and properly secured.

Cisco TrustSec and Software-Defined Access (SDA): ORDR complements Cisco TrustSec and Cisco SDA to accelerate effective group-based policy creation. ORDR seamlessly integrates with traditional networks and SDA fabric-enabled networks to automate discovery of all connected devices and provide rich contextual device classification and visual traffic modeling. ORDR insights help simplify and automate group assignments, group-based policy creation, and policy matrix provisioning to meet business requirements.

About Us

ORDR is the leader in AI-powered segmentation, securing some of the largest organizations in healthcare, transportation, manufacturing, and financial services. Having analyzed more than 100 million unique device types, the platform is purpose-built to solve the toughest security challenge: unmanaged and IoT assets that put business uptime on the line. By turning intelligence into swift, automated protection, ORDR helps teams contain threats, reduce exposure, and keep operations resilient — 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 **X** and **LinkedIn**.

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

Follow ORDR on

Ready to bring ORDR to your chaos?

Request a demo