ORDR

Solution Brief

ORDR + Splunk

Enterprise Security Operations Centers (SOCs) designed to detect and respond to cybersecurity issues are finding themselves limited by the lack of complete visibility across the organization. Physical security cameras, research systems, medical equipment, OT systems, printers, and other IoT devices were never considered in-scope traditionally.

But as cyber threats such as ransomware increase, it has become critical to ensure that security operations teams have an understanding of not just the risks from IT-managed assets, but also unmanaged IoT and OT.

ORDR and Splunk have partnered to expand the coverage of the SOC to include IoT and OT systems.

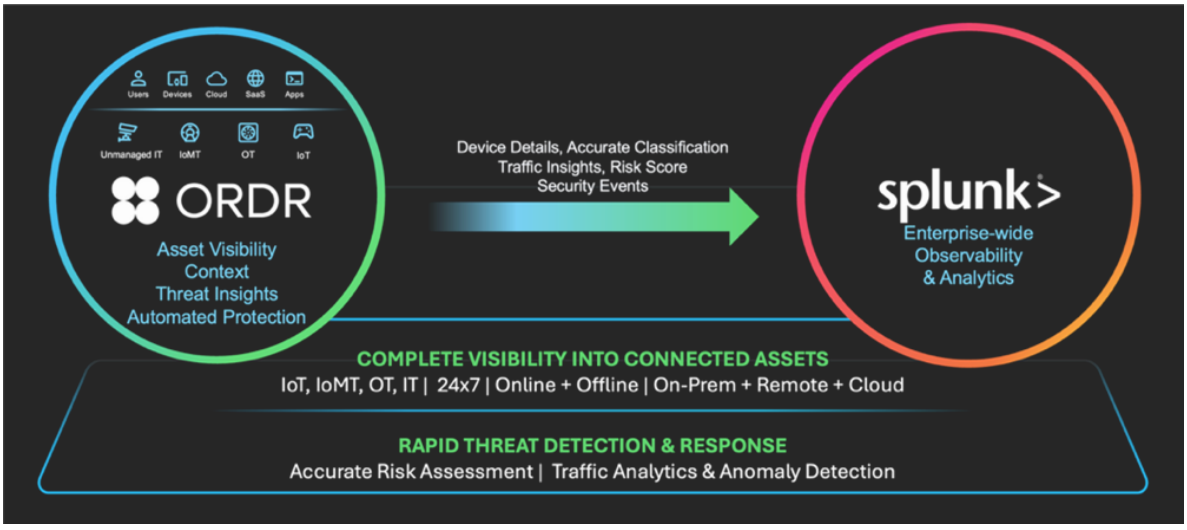
ORDR and Splunk

The ORDR AI Protect platform automatically discovers and classifies every device, identifies risk, maps communications, establishes baseline behavior, and provides protection with automated policies.

The device information is detailed and granular including make, model, software, and serial number. ORDR also learns where it is located, how and where it is connected, what it is doing, and continuously monitors threats and incidents based on extensive security intelligence.

This rich and accurate asset intelligence along with up-to-date security alerts can be sent to either Splunk Cloud or Splunk Enterprise platforms. This empowers SecOps teams to create custom risk and visibility dashboards, drastically improving how they investigate and respond to threats.

ORDR's integration with Splunk, designed to be turnkey with minimal configuration, makes it fast and easy to expand SOC coverage to include IOT and OT systems.



ORDR

Benefits of Integration with Splunk

- **Complete picture of every connected asset**: ORDR's AI-powered classification engine discovers every connected device including the make, model, manufacturer, and OS. For example, a security camera would be accurately identified as a physical security camera with the meta data. These details help SOC in easily investigating threats.

- **Threat detection based on anomalous behavior or other indicators of compromise**: ORDR's continuous traffic monitoring allows ORDR to detect malicious attacks in North-South and East-West traffic, including detecting behavior anomalies. For example, ORDR can build a baseline to POS systems in PIC network and detect anomalies as soon as a new anomalous or malicious pattern has been detected. These security events are shared with Splunk in real time.

- **Risk remediation and mitigation:** Speed up investigation and analysis with rich, accurate context necessary to contain suspicious activity quickly, including asset classification, device users, mapped events, and more.

ORDR Ecosystem Integrations

ORDR integrates with industry-leading security, networking, infrastructure, IT, and clinical solutions to unify device details, enrich device context, and extend the value of your existing technology investments. Data from integrations is combined in the ORDR Data Lake to create the most complete and accurate view of every connected device across your whole organization. ORDR also enriches these solutions with accurate insights, making security teams more efficient, and cyber defenses stron

ORDR

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 X and LinkedIn.

For more information, visit ordr.net

Follow ORDR on

Ready to bring ORDR to your chaos?

Request a demo