Ordr Systems Control Engine and Rapid7 InsightVM

Managing Vulnerabilities with Rich Device Context

Information technology and cybersecurity teams need a proper vulnerability management program and solutions in place to continuously identify, accurately classify, prioritize, and remediate vulnerabilities.

However, there are challenges when extending vulnerability management to unmanaged and IoT devices such as building automation and security systems, medical devices, and manufacturing equipment. Unlike managed devices (for example, servers, workstations, and laptops), unmanaged and IoT devices can be difficult to locate and are potentially sensitive to active scanning. Additionally, IoT devices are often the most vulnerable since they typically lack the protection of security agents and are in service for many years without regular patching, if patching is even supported!

The exponential rise in known vulnerabilities, threat vectors, and connected devices means that organizations must adopt a two-pronged, modern approach to vulnerability management: Ordr Systems Control Engine (SCE) and Rapid7 InsightVM.

How Ordr and Rapid7 Address Complete Vulnerability Management

Ordr SCE

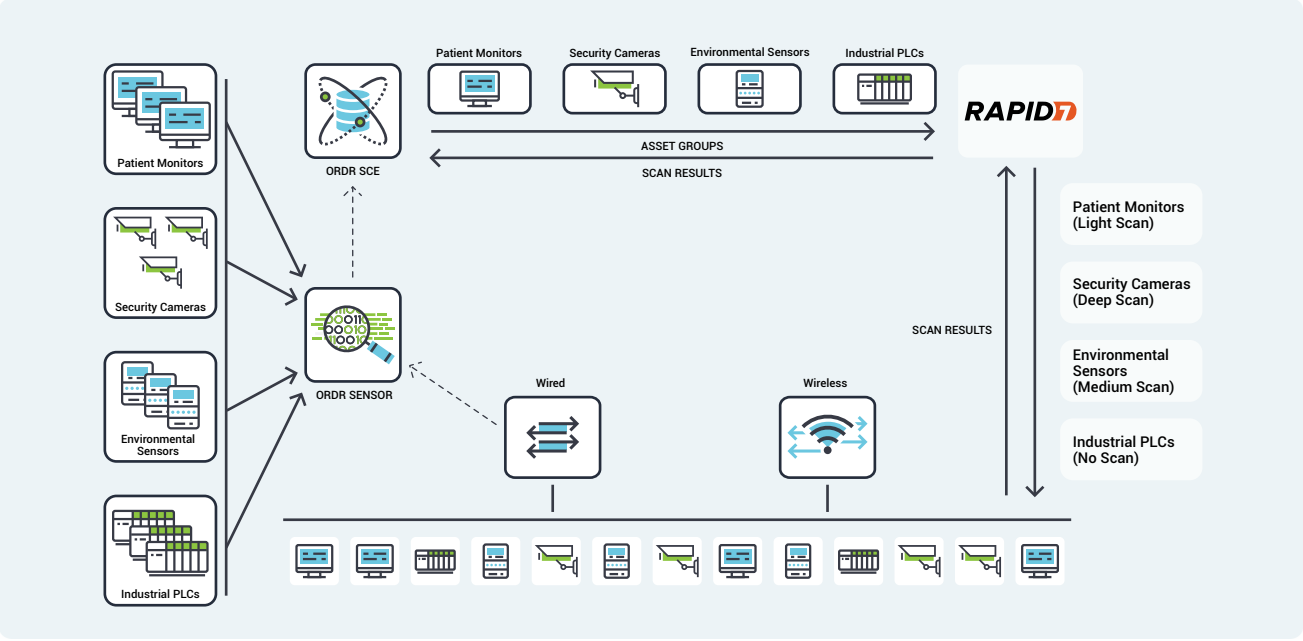
IoT Device Security Made Simple

Ordr SCE discovers every connected device, profiles device behaviors and risks, and automates remediation responses. Ordr integrates with numerous IT systems such as InsightVM, asset management, firewalls, switches, and SIEMs to create a unified view of devices, risks, threats, and network behaviors.

Rapid7 InsightVM

Vulnerability Risk Management

InsightVM not only provides visibility into the vulnerabilities in modern IT environments—including local, remote, cloud, containerized, and virtual infrastructure—but also clarity into how those vulnerabilities translate into business risk and which are most likely to be targeted by attackers.



Ordr automatically discovers and classifies all devices with granular context including make, model, hardware and software version info through passive monitoring and deep packet inspection. Ordr seamlessly sends this device intelligence and context to a customer's InsightVM instance, giving Rapid7 a detailed understanding of which assets to scan and the type of scan suited to each device. Currently, organizations with devices that may be sensitive to active scans, such as hospitals or manufacturers, often exclude entire subnets from scanning to avoid service disruption, increasing the risk of missing critical vulnerabilities. Ordr allows customers to open these subnets to scanning by creating highly granular and accurate device inclusion and exclusion lists, enabling assessment without risk of disruption.

Ordr also learns from Rapid7's advanced scanning engine to augment Ordr's security analytics. Ordr incorporates Rapid7 scan results into Ordr's device risk score and visibility dashboard to display a comprehensive risk assessment of each connected device.

Benefits of Integrating Ordr SCE with Rapid7 InsightVM:

Ordr works with Rapid7 to seamlessly discover all connected assets including IoT, IoMT, and OT devices. The joint solution enables Rapid7 to perform the right scan at the right time regardless of the device type, location, criticality or role within the organization. Many vulnerable IoT/OT devices discovered by Rapid7 cannot be patched or updated. Ordr automates the application of compensating controls to safeguard these devices by sending protection policies directly to firewalls, switches, wireless, or NAC systems. Similarly, infected devices can be quickly isolated through existing network and security devices.

COMPREHENSIVE COVERAGE

Ordr's identification and classification of lightweight, agentless devices allows administrators to quickly exclude specific IoT devices or categories from active Rapid7 scans, opening network segments to vulnerability scanning that had previously been excluded.

SMART SCHEDULING

Ordr tracks utilization patterns for critical devices, allowing administrators to schedule vulnerability scans for times when devices are not in use, minimizing disruption and operational risk.

OPTIMIZED SCANNING

Using Ordr's detailed insight into device types, scan sensitivity, and their critical role within the organization, Rapid7 scans can be tailored to each device.

PROACTIVE PROTECTION

Rather than blocking or quarantining critical IoT devices after infection, Ordr's segmentation policies create barriers that protect vulnerable devices while still enabling essential services.

Combining Ordr's unique device intelligence with Rapid7's advanced vulnerability intelligence provides organizations with the ultimate solution to efficiently manage risks while reducing service disruption and time to remediate.