Ordr Integration with Tenable

Managing Vulnerabilities with Rich Device Context

A proper vulnerability management program and the right tools are critical to help security and IT teams continuously identify, classify, prioritize, and remediate vulnerabilities to reduce risk.

These teams, however, are challenged when extending vulnerability management to IoT, IoMT, OT and other unmanaged devices such as building automation, security systems, medical devices, and manufacturing equipment. Unlike managed devices (e.g., servers, workstations, and laptops), unmanaged devices can be difficult to locate and are sensitive to active scanning leaving gaps in vulnerability insights. Additionally, these unmanaged devices 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 and Tenable.io or Tenable.sc.

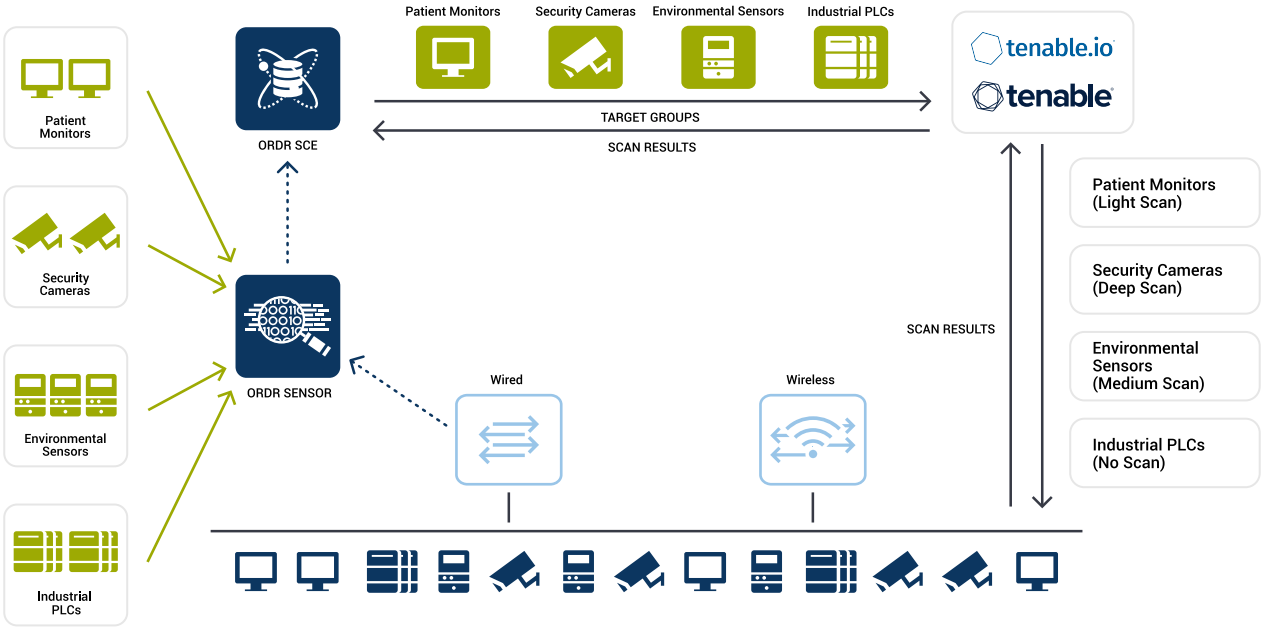
HOW ORDR AND TENABLE ENABLE COMPLETE VULNERABILITY MANAGEMENT

Ordr Connected Device Security Made Simple

Ordr discovers every connected device, profiles device behaviors and risks, and automates remediation responses. Ordr integrates with numerous IT systems such as Tenable.io and Tenable.sc for cloud or on- premise support, as well as asset management, firewalls, switches, and SIEMs to create a unified view of devices, risks, threats, and network behaviors.

Tenable.io & Tenable.sc Vulnerability Management

Tenable.io and Tenable.sc quickly identify, investigate, and prioritize vulnerabilities. Managed in the cloud or on-premise and powered by Nessus technology, Tenable provides the industry's most comprehensive vulnerability coverage with the ability to predict which security issues to remediate first.



Ordr automatically discovers and classifies all network connected devices and gathers granular context such as make, model, hardware, OS, and software versions by passively analyzing network traffic with deep packet inspection. Ordr can then send collected device details to a customer's Tenable.io or Tenable.sc instance, providing these tools with a detailed understanding of which assets to scan and the type of scan best suited to each device. Currently, organizations such as hospitals or manufacturers with devices that may be sensitive to active scans often exclude entire subnets from vulnerability scanning to avoid service disruption or impact to patient safety. This, however, increases 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 and enabling scanning without risk of disruption or impact to safety.

Ordr also learns from Tenable's advanced scanning engine to augment security analytics and insights. Tenable scan results are incorporated throughout the Ordr GUI and used in the calculation of device risk scores to enable a comprehensive view of risk for each connected device and your overall environment.

BENEFITS OF INTEGRATING ORDR WITH TENABLE

Ordr integrates with Tenable.io and Tenable.sc to provide connected device insights and enable organizations to close vulnerability scanning gaps with the ability to apply the right scan regardless of the device type, location, criticality, or role within the organization. Many vulnerable IoT, IoMT, and OT devices scanned by Tenable cannot be patched or updated. For these devices Ordr automates the creation of compensating controls such as segmentation to safeguard these devices by sending policies directly to firewalls, switches, wireless controllers, or NAC systems. Similarly, Ordr can quickly orchestrate the isolation of infected devices through integration with existing network and security infrastructure.

COMPREHENSIVE COVERAGE

Ordr's discovery and classification of all managed and unmanaged devices enables administrators to quickly exclude specific connected devices or device categories from active Tenable scans, opening previously excluded network segments to vulnerability scanning.

SMART SCHEDULING

Ordr tracks utilization patterns for critical devices, enabling vulnerability scans to be scheduled when devices are not in use, minimizing disruption and operational risk.

OPTIMIZED SCANNING

Ordr's detailed insight of device types, scan sensitivity, and role within the organization enable administrators to tailor Tenable scans to each device.

PROACTIVE PROTECTION

Rather than blocking or quarantining critical vulnerable devices, Ordr segmentation policies reduce the attack surface to prevent threats while still allowing essential communications.

ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing Venture Capital, Ten Eleven Ventures, Northgate Capital, Kaiser Permanente Ventures, and Unusual Ventures.

Learn more at www.ordr.net and follow Ordr on LinkedIn and Twitter