Ordr Connected Device Security for Mergers & Acquisition

OVERVIEW

Performing due diligence during the M&A process is a complex endeavor that requires analyzing every aspect of a target organization. An important component of this process is assessing the IoT, IoMT, OT and other devices connected to the environment. This step is critical to understanding the assets and services included in the target organization, assessing the attack surface and potential risk, ensuring risk is addressed before integration, and services are not disrupted when environments are integrated. Having deep insights into connected devices can also provide an understanding of utilization to help with resource optimization and future operational planning.

Gaining an understanding and securing connected devices presents unique challenges that can slow the M&A process and impact outcomes.

CHALLENGES

- Gaining a complete view of all connected devices
- Assessing the attack surface and potential risk
- Ensuring risk is addressed before integration
- Ensuring services are not disrupted when services are integrated

ADDRESSING M&A CHALLENGES WITH ORDR

The Ordr connected device security platform helps teams overcome challenges during the M&A process with a granular view of every connected device, insights into vulnerabilities and risk, and capabilities to address risk and improve security.

GAIN A SINGLE VIEW ACROSS BOTH ORGANIZATIONS

Ordr addresses one of the most common M&A challenges of overlapping IP schemas when two organizations are combined. This challenge prevents teams from easily establishing a single view of both environments and can slow risk assessment and integration efforts.

Ordr overcomes these challenges by deploying lightweight sensors in each organization that tracks detected devices and appends each device with a unique identifier. This unique identifier enables Ordr to associate devices and communications to their proper organization for accurate visibility of the unique risk and security posture for each environment.

CREATE AN ACCURATE DEVICE INVENTORY

Ordr analyzes network traffic to automatically discover, classify, and gather granular details for every connected device without impacting device performance or availability. Within hours of deployment, Ordr provides accurate details on the make, model, operating system, serial number, application usage, port usage, and physical/network location for every device.

Ordr integrates with CMMS and CMDB tools to continuously enrich an existing inventory with missing devices and granular device details to create an accurate, and up to date inventory for all assets.

With a complete view of every device Ordr identifies devices with vulnerabilities such as an outdated operating system, unauthorized software, weak ciphers, and weak certificates. Ordr integrates with 3rd party sources to enhance vulnerability identification to include known vulnerabilities, unpatched software, and devices with FDA or manufacturer recalls and other threats.

MAP AND BASELINE DEVICE COMMUNICATIONS

By analyzing network traffic Ordr learns all communications between devices, device groups, and externally to the Internet. This insight helps identify devices using vulnerable protocols (e.g., SMB, RDP, Telnet), compliance violations, and external communications to risky destinations (e.g., Russia), or known malicious domains on the internet (e.g., command and control (C2) sites).

In addition, Ordr device communication insight can help to validate existing device deployments in VLANs and subnets, segmentation implementations, and ensure services are not disrupted when an acquired organization is moved or integrated post-acquisition.

Ordr also creates a baseline of normal communications for each device. Communications that deviate from their baseline help teams identify potentially malicious activity and active attacks.

Understanding device communications and baselines are also instrumental in enabling Ordr to dynamically create policy to respond to an active attack or to automatically create segmentation policy to proactively improve security.

UNDERSTAND CLINICAL RISK

Ordr calculates a risk score for each device to help teams understand risk to the organization, prioritize remediation efforts such as patching, and mitigation efforts such as quarantining, applying segmentation, or taking devices out of service. Each device risk score is a combination of:

- **Cyber Risk** – vulnerabilities, internal/external access, and criticality
- **PHI Exposure** – PHI presence, manufacturer disclosure (mds2), behavior, device portability, encryption at rest/in transit
- **Clinical Factors** – physical risk, equipment location, mission criticality (availability), mitigations
- **Environmental Factors** – VLAN pollution, last seen time, connection type, segmentation enforced
- **Customizable Factors** – severity adjusted on clinical impact, prioritized on business function, criticality based on business impact

UNDERSTAND DEVICE UTILIZATION

Ordr provides insight into medical device utilization to help identify areas of over or under usage and ensure data-driven optimization of devices. This helps teams understand how devices and services from a target organization might complement devices and services of the acquiring organization. For example, with Ordr device utilization insights an acquiring organization can understand how demand for services can be balanced across a target organization's device resources.

Device utilization insights can also help teams find windows of low usage to perform maintenance tasks and understand device capacity to inform budgeting, and future procurement efforts.

REMEDIATE RISK AND MITIGATE THREATS

Ordr provides insights to help teams identify risk and prioritize security efforts in addition to capabilities to help teams address threats with the right response. **For example, with Ordr you can:**

- Identify all devices with an outdated or unpatched operating system.
- Use the Ordr device risk score to prioritize security efforts and select the right mitigation or remediation action.
- Use utilization insights to plan patching or upgrade tasks to avoid peak usage time and service disruption.
- Use Ordr to automatically create segmentation policy to isolate vulnerable devices that cannot be updated/patched while keeping them operational.

  OR

- Identify active attacks based on traffic that deviates from the normal device baseline.
- Dynamically create policy to block attack traffic and/or quarantine the impacted device.
- Use Ordr physical location insights to direct a technician to the impacted device to service or reimage the device as needed.

Ordr includes native capabilities and supports integration with 3rd party tools to enable vulnerability management workflows and track vulnerability management tasks across teams.

ENFORCE ZERO TRUST SEGMENTATION

With automatic device discovery, classification, and communication baselining, Ordr can automatically generate Zero Trust segmentation policies to isolate and secure individual devices or fleets of devices based on nearly any device attribute. Policy created by Ordr is enforced using existing networking and security infrastructure to help simplify and accelerate segmentation efforts.

This capability can be used as a best practice to segment environments of an acquired organization and enable the secure integration of devices and services. Ordr segmentation policy can be adjusted over time to enable tighter integration between environments when required.