ordr

5 WAYS TO IMPROVE ASSET INVENTORY AND MANAGEMENT USING ORDR

© 2020 ORDR, INC.

Gaining visibility and control over an organization's many devices and endpoints is one of the most fundamentally important yet challenging tasks facing IT and security teams today. The number of connected endpoints has exploded both in terms of overall volume as well as diversity. In addition to traditional managed devices, teams must also corral a massive proliferation of unmanaged devices including IoT and OT, IoMT (Internet of Medical Technology) , and employee BYOD (Bring Your Own Device). Once identified, teams need to appropriately manage those assets based on their function, business role, and risk to the enterprise.

Using passive, agentless analysis, Ordr can automatically find and classify all connected devices whether managed or unmanaged. Each device is classified in granular detail including the make, operating system, serial number, application/port usage, location, and much more. The solution identifies security vulnerabilities, active threats, FDA recalls, manufacturing recalls, weak ciphers and certificates. Then, risk scores are provided to help prioritize devices that need to be taken out of service, patched, or quarantined based on the appropriate workflow.

With Ordr, teams alwayshave complete visibility of their devices at all times. And with full visibility over assets and risks, teams have the foundation and source of truth to power everything from better vulnerability management to network segmentation to NAC (Network Access Control) strategies and more. Let's briefly look at some of the specific ways that Ordr's approach to Asset Inventory and Asset Management can benefit organizations today.

1 UNIFIED VISIBILITY AND CLASSIFICATION OF ALL CONNECTED DEVICES

Much like a chess player needs to be able to see all the pieces on the board, IT and Security teams need to see all the devices on their network. Unfortunately, today that view is highly fractured with critical parts of the metaphorical chess board often being completely invisible.

Ordr brings all of an organization's many connected devices into a single unified context, including managed and unmanaged devices. In one view, staff can see traditional managed devices like laptops and servers as well as unmanaged devices of all types, IoT, OT assets, medical devices, mobile and personal devices, and more. Visibility into this latter category of unmanaged devices is particularly important as it is the area of the greatest growth in most organizations.

© 2020 ORDR, INC.

Ordr also automatically classifies each device in granular detail. By combining AI (Artificial Intelligence) and ML (Machine Learning) with DPI (Deep Packet Inspection), Ordr passively reveals a wealth of critical context for every device. This includes:

Device Type and Function

Instead of merely seeing an IP address, teams can quickly distinguish between laptops, security cameras, HVAC systems, or an infusion pump

Device Details

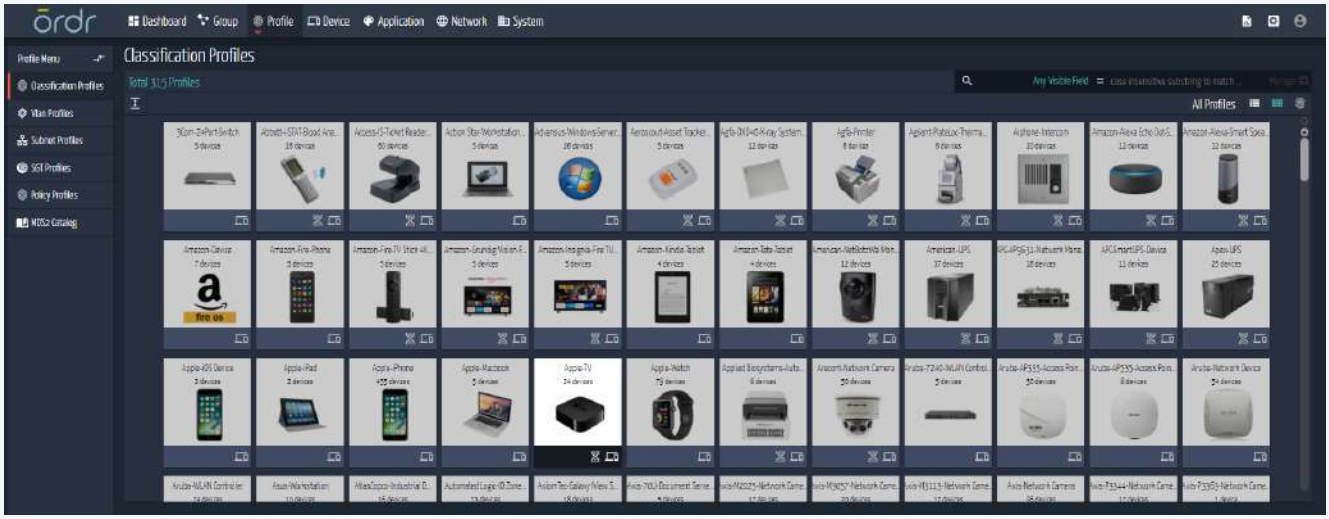
Find critical information on each device including the specific device make, model, serial number, OS version, and more

Network Context

See device network properties such as MAC/IP address, subnet, interface, VLAN, SSID, CDP/LLDP data, and other statistics

Location

Devices can be identified in terms of their location in the organization



© 2020 ORDR, INC.

2 ALWAYS-ON, REAL-TIME INVENTORY AND MANAGEMENT

For many organizations, inventory management is performed as a periodic point in time audit. This can lead to considerable gaps in visibility when devices are missed or offline during an audit or if there are significant changes between scans. These gaps can mean organizations are often exposed for weeks or even months before the problem is identified.

Ordr ensures that asset inventory and management is a continuous process so that information is always up-to-date. Since all traffic is continuously analyzed, Ordr detects new devices and can inform staff as soon as the device first connects. This real-time visibility allows staff to see a variety of devices that would typically be missed and left unmanaged including:

- **Employee laptops and mobile devices that are often out of the office**
- **Devices owned by visiting partners or contractors**
- **Devices that were temporarily offline**
- **New employees or newly deployed devices**
- **Changes in device configuration or security posture between regularly scheduled scans**

© 2020 ORDR, INC.

3 AUTOMATICALLY FIND VULNERABILITIES AND RISK

Next, teams need to identify any gaps that could put the security of the device or network at risk. Naturally, there is a wide range of factors that can contribute to a device's risk and many can be highly specific to the specific type of device in question. For example, in addition to traditional CVEs, staff may need to know that a medical device is part of an FDA recall or is communicating externally to known bad domains.

Ordr automatically checks the security posture of devices across a wide range of issues to proactively find potential problems. Ordr both includes its own built-in vulnerability scanner and integrates with an organization's existing scanners and patch management systems to ensure staff has a full view of all their vulnerabilities. Ordr identifies the following:

- **Vulnerable operating systems or applications**
- **Weak or default passwords even on agentless IoT devices**
- **Industry-specific recalls or vulnerabilities (e.g. FDA recalls, MD-Viper, etc.)**
- **Compliance violations via integrations with patch management systems such as winRm, BigFix, and SCCM**
- **Sensitivities to active scanning via a bi-directional integration with vulnerability manage-ment platforms such as Tenable or Rapid7 (e.g. devices that have not been scanned and optimal time to scan)**

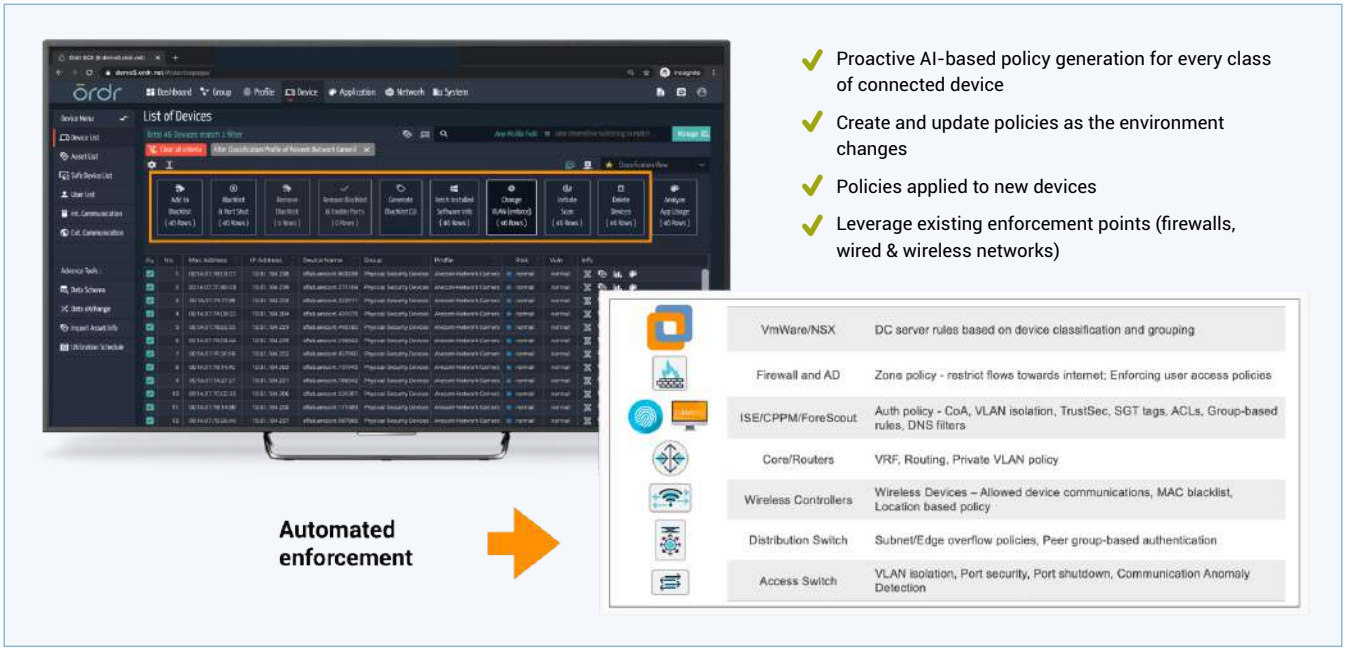
© 2020 ORDR, INC.

4 AUTOMATE WORKFLOWS

The speed with which organizations can find and mitigate weaknesses is often the difference between thwarting an attack or suffering a breach. However, the appropriate response and mitigations can vary widely based on the specific issue and management tools and systems that an organization has at its disposal.

Ordr provides a wide range of highly flexible workflow options that can be delivered natively through the solution or via integrating with existing tools and systems. All of the various rich device context described previously can be used to drive workflows that are appropriate to the specific device and its role in the enterprise. For example, with Ordr, teams can enact the following:

- **Trigger workflow to update weak or default passwords on devices**
- **Trigger workflow to track devices not communicating to A/V update sites**
- **Add a CMDB entry for newly classified devices**
- **Create an incident in the organization's ticketing or log management system**
- **Block, quarantine, or segment a device(s) at the network level**
- **Feed device details to a SIEM or other management system**
- **Integrate with IT tools like WMI, PowerShell, Linux SSH, and more**



© 2020 ORDR, INC.

5 ENABLE NEW SECURITY AND MANAGEMENT INITIATIVES

Once an organization has full visibility over their security and IT "chessboard," they can use that insight to drive a variety of strategic projects.

NAC AUGMENTATION:

Many organizations may be interested in deploying NAC-based controls for the network. However, without detailed visibility into the environment including each device's role and location, it can be almost impossible to establish appropriate NAC policies. Ordr can deliver value for existing NAC investments.

ZERO TRUST SEGMENTATION:

Similarly, many organizations aim to adopt increasingly segmented network architectures to protect internal assets and systems. However, this again requires that organizations know exactly what types of access a device needs in order to do its job. By classifying devices by their type and learning their unique traffic patterns, Ordr can automatically create Zero Trust segmentation and micro-segmentation policies that give devices the least amount of access without disrupting their approved functions.

DEVICE UTILIZATION:

Ordr enables device owners to understand utilization of devices, insights that may be important for healthcare organizations to maximize efficiencies and support purchase decisions. For example, in the healthcare vertical, the annual spend on medical devices run into multi-millions each year. Armed with real-time and accurate utilization from Ordr, medical device managers can confidently make decisions and optimize device usage for increased cost savings and a better patient experience.

VULNERABILITY MANAGEMENT:

While most modern organizations recognize the critical importance of vulnerability management, the sheer scale of the job can make it hard for staff to keep up. The growth of critical connected devices in organizations has added to an already complex landscape and created a new attack surface that is often invisible to traditional vulnerability management tools. Ordr automatically identifies vulnerabilities in IoT, OT, and IoMT devices that aren't seen by traditional scanners. Each vulnerability comes with deep insight into the device and clinical and threat-based contexts so that teams quickly find the devices that need priority attention. And with visibility into all connected devices, the platform makes the perfect complement to any existing vulnerability management program.

© 2020 ORDR, INC.

CONCLUSION

These examples are just some of the ways that organizations are using Ordr today. However, the solution's capabilities provide countless ways that teams can revolutionize the way they approach and use asset inventory and management. With a unified view, teams can ensure that all devices are in scope whether they are managed or unmanaged. Just as importantly, by understanding the type and function of each device, staff can ensure each device is managed appropriately based on its unique role in the enterprise. By continuously monitoring and analyzing the environment, teams can identify problems immediately and trigger workflows so that issues are fixed before they turn into incidents. And by integrating with an organization's many existing tools and systems, Ordr can help teams get more value out of the tools they already have.

To see a demonstration of the Ordr product or to test drive an Ordr Hands On Lab environment, please contact the Ordr team at

WWW.ORDR.NET