How Ordr Works

The Ordr Systems Control Engine (SCE) is the only purpose-built platform to discover and secure all connected devices. Ordr uses a completely agentless approach, and can be deployed locally or in the cloud. The SCE passively analyzes network traffic to detect and classify all devices, and automatically find vulnerabilities, weaknesses, and threats. Every device is continuously analyzed to baseline appropriate behaviors, map communication patterns, and identify any malicious or anomalous traffic.

Ordr also takes action to mitigate risks. By learning the unique communication patterns of each device and class of device, Ordr can proactively create firewall, NAC, or other policies that ensure devices have the access they need while limiting unnecessary exposure. When threats or other incidents are detected, Ordr can likewise dynamically create segmentation policies to isolate or quarantine devices. Ordr also integrates with existing security and asset management workflows such as SIEM, CMDB and CMMS.

With this unique approach, Ordr ensures a single, complete view of all devices and their risks, and empowers teams to take quick action when required - all without the need for endpoint agents.

DISCOVER ALL DEVICES

- Agentless deployment
- Classify by make, model, serial number, location, O/S
- Vulnerabilities, exploits, industry-specific recalls
- Weak ciphers/certificates

PROFILE DEVICE BEHAVIOR

- Baseline communications
- Visualize via VLAN and subnet
- Identify anomalous and malicious communications
- Identify external communications

AUTOMATE ACTION

- Trigger workflows for SIEM, CMMS, CMDB
- Proactive segmentation and enforcement on NAC, FW, switches
- Incident response segmentation for vulnerable devices

Key Use Cases for Financial Services

Inventory and Management Of All Connected Financial Devices

Ordr ensures comprehensive coverage of all the many connected devices in financial environments. This includes traditional devices such as laptops, desktops, and servers, both locally or in the cloud. Ordr also ensures visibility of other connected devices that are often missed including BYOD and WFH devices as well as IoT and OT devices including ATMs, POS, security cameras, loss prevention devices, and building facilities assets.

Case Study: Regional Bank

A large regional bank with several hundred branches spread across 17 states recently needed to extend security to their many devices. The security team was facing a variety of challenges. The team needed to support a wide variety of devices including remote ATMs and loss prevention cameras in addition to traditional laptops and servers. The team was also having challenges related to their Cisco ISE NAC deployment. Specifically, many devices were only identified by their IP address forcing teams to create broad "allow policies" for NAC.

Ordr was able to come in and quickly solve these problems, while also uncovering risks that had previously gone unnoticed. Ordr provided visibility into all the organization's devices including their ATMs and other IoT and OT devices. By automatically identifying all devices, the security team was able to greatly enhance the NAC solution by applying policies based on specific device types and attributes. Ordr was also able to identify a variety of hidden risks including devices with expiring certificates as well as devices communicating with known malicious IPs and domains. With minimal time and effort from the security team, Ordr was able to establish a consistent approach to device security, extend existing security tools, and address risks that otherwise would have been missed.

About Ordr

Ordr secures the millions of enterprise IoT and unmanaged devices such as manufacturing machines, building systems, medical equipment, printers, and more that run within global networks. The Ordr Systems Control Engine uses machine learning to automatically discover and classify every IoT and unmanaged device, map all communications, detect and prioritize vulnerabilities, and then proactively secure each device through dynamic policy generation and segmentation. Organizations use Ordr to discover their devices, track usage, achieve proactive protection, and compliance. For more information about Ordr, go to www.ordr.net.