

Ordr Systems Control Engine for the Financial Services Industry

Simplified Security and Compliance for All Connected Devices

The financial services industry faces extraordinary security challenges, and to keep pace, security efforts must be both comprehensive and efficient. In terms of threats, recent studies have found that cyberattackers hit financial services firms 300 times more than other sectors. At the same time, security teams must maintain and document regulatory compliance with a wide array of standards ranging from PCI-DSS, FNRA, and FFIEC. To make matters worse, teams need to secure a wave of new IoT devices that are often ignored by traditional security tools. Whether dealing with traditional laptops and servers, or ATMs, POS devices, security cameras and sensors, or connected facilities equipment, financial services security teams need to ensure that all their devices are safe and properly controlled.

Ordr arms security teams with the tools to easily maintain full visibility and control over all their connected devices. The platform ensures security and IT teams always have a comprehensive inventory of all assets, insights into the behavior, risks, and threats of each device, and the ability to take action and mitigate risks automatically. Whether for addressing regulatory compliance requirements, proactively managing risk, or enabling key security initiatives such as NAC deployments, micro-segmentation, or Zero Trust, Ordr ensures financial services organizations teams have visibility and control they need for unmanaged, IoT and OT devices.

Key capabilities include:



Real-Time Asset Discovery

Automatically detect and monitor all devices including traditional, IoT, OT, and BYOD devices.



Vulnerability and Risk Management

Find devices and vulnerabilities that are missed by traditional vulnerability scans.



Map Communications

Map and visualize connectivity and communication patterns for every device, including to external IPs.



Threat Detection

Find malicious traffic and devices that are exhibiting signs of compromise.



Regulatory Compliance

Accelerate regulatory reporting with complete visibility over every device and its security posture.



Automated Response

Automatically or manually segment and microsegment devices based on least privilege, and Zero Trust framework.

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.

Securing SWIFT environments

As of January 1, 2018, SWIFT requires all 11,000+ SWIFT member banks to comply with their Customer Security Controls Framework (CSCF) or risk non-compliance. The SWIFT CSCF is designed to drive security improvement and transparency, and includes broad requirements to secure member banks such as restricting Internet access, protecting critical systems from general IT environments, reducing the attack surface and vulnerabilities, and securing the environment. Ordr can help deliver complete visibility into financial organizations and their SWIFT environments, including discovery of all connected devices and monitoring these environments for anomalous traffic. The Ordr machine learning capabilities can baseline what is normal in the environment and create appropriate segmentation policies to secure unmanaged and IoT devices.

Regulatory Compliance

Ordr vastly reduces the time and effort needed to maintain compliance with a wide array of regulatory standards including the FFIEC IT Handbook, PCI-DSS, SOX, GLBA, NYCRR-500, FNRA, and more. Security and IT Teams can rest assured that they can provide comprehensive visibility and documentation of all their connected devices. Ordr also makes it easy to hone in on specific areas or attributes such as identifying whether devices with PCI cardholder information are in the same VLAN as other non-PCI devices. Additionally, teams can quickly focus on specific regulated device types or attributes such as ATMs, POS devices, or devices with outdated operating systems.

NAC Augmentation

Financial institutions are increasingly turning to NAC to help secure their environments. However, security teams can't enforce NAC policies until they are confident that they know what each device actually is. Without this insight, teams are often forced to create broad "allow policies" for devices, which often defeats the purpose of deploying NAC in the first place. Ordr provides the all-important prerequisite for NAC by automatically identifying each device in detail so that organizations can actually deliver on the promise of NAC.

Simplify Mergers and Acquisitions

Ordr brings clarity to the M&A process both before and after an acquisition. IT and security teams can quickly establish a comprehensive inventory of devices and automatically identify vulnerabilities and risks. Teams can quickly see devices and technologies by type to see where there is overlap or differences between the two organizations. If problems are uncovered, Ordr then allows teams to automatically create segmentation policies to mitigate the uncovered risk.

Microsegmentation and Zero Trust

Ordr lets financial organizations easily adopt modern security models and architectures such as microsegmentation and Zero Trust. Ordr automatically analyzes all traffic with machine learning to identify the unique connectivity needs of each device. This traffic mapping or "Ordr Flow Genome" provides the baselining of normal device behavior. This enables Ordr to automatically create segmentation policies to only allow access to the sanctioned devices and services needed. Policies can be manually reviewed by staff before enforcement on existing networking or security infrastructure. Policies can also be automatically deployed to ensure the fastest time to protection.

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.