Case Study

Industry: Financial Services

Financial services Leader With 788 Branches Across 17 States Selects Ordr for Connected Device Security

Texas-Based Financial Services Leader Chooses Ordr To Secure All Connected Assets

Leading financial services organization classifies all devices, baselines device behavior and significantly reduces time to respond to compromised devices using Ordr

A privately held financial services organization headquartered in The Woodlands, Texas, with more than 788 branches in 17 different states, had deployed a variety of connected devices ranging from video surveillance cameras, printers, PCs and ATM machines, The CISO for this organization was concerned that he did not have a real-time asset inventory, or visibility into what devices were actually connected to the network and what risks they brought. The CISO began the search for a cybersecurity platform that could champion his vision of visibility and security of all connected devices, but one that integrated with his existing security stack.

“My objective when entering the banking world 8.5 years ago was to make security more intelligent and efficient. A device as simple as a badge reader can be used to compromise an enterprise network. So the main thing we were trying to address was the security around a lot of these agentless devices. We started to search for an asset visibility and security platform that could help improve our security posture,” said the CISO.

“But the interesting thing as we dug into it a little bit more, and specifically looked at Ordr is that it is not just for IoT (Internet of Things) devices. It's anything that is connected to your network, and that's what I think makes Ordr special among peers. You do not realize how expansive your network is until you inventory every connected device.” continued the CISO.

Not Just IoT, Securing All Connected Assets Everywhere

Ordr is the leading platform for cyber asset and attack surface management. Within a few hours of deployment, using deep packet inspection, Ordr discovered every connected device including IT, IoT, IoMT, and OT, with granular context such as device type, manufacturer, serial number, operating system, location and more.

Challenges

- Distributed architecture with 788 branches in 17 states
- Lack of visibility into inventory of IT, IoT and OT assets on network
- Configuration Management Data Base (CMDB) not up to date
- Incomplete attack surface understanding for risk and security

Within the Ordr Data Lake, the device context is enriched with network topology details and threat intelligence data such as known vulnerabilities, ICS-CERT advisories and more.

“Asset discovery is extremely important but understanding what risks are around those assets is critical. Not all assets should be treated the same. If you don’t have an individual profile for each asset, your system treats them the same. Our core payment system is not going to be treated the same as another system that doesn't contain the same type of data, or the value data from a regulatory perspective. Understanding assets and their risks is how CSOs should approach security.” said the CISO.

Ordr also detects known and unknown threats. An integrated threat detection engine detects active threats, exploits and lateral movement such as attacker tools. In addition, Ordr Flow Genome uses advanced machine learning (AI) to map each device’s unique, customer-specific communications patterns, and baselines exactly how it should behave.

Unlike users, devices are deterministic, and have specific and predictable communications patterns. Baseline communications, for example, mapping

Ordr Results

- Comprehensive asset visibility–from laptops, workstations and ATMs to video surveillance cameras
- Delivered IT and security operational efficiencies with critical device insights
- Measurable risk reduction through identification of devices with vulnerabilities and outdated operating systems
- Proactive monitoring of communications flows for anomalies
- Accelerated Cisco ISE segmentation to isolate at-risk systems
- Maintained compliance via regulatory reporting on assets and risks

Key integrations

- Cisco ISE

how a video surveillance camera is behaving and what it is communicating to on the network, allows Ordr to surface anomalous behaviors such as devices communicating to command and control (C2) domains or moving laterally in the network. The baseline communications is also the foundation to implement Zero Trust policies for every device, allowing only "normal" communications and blocking everything else.

Ordr Is Delivering Business Outcomes and Value

"We talked about a visibility and security platform that would integrate with our entire security stack. This intelligent system is what I kept going back to - we need efficiency and security." said the CISO.

Ordr is designed to complement existing systems and existing infrastructure. In particular, this financial services leader wanted to accelerate Cisco ISE deployments using Ordr. Ordr maximizes Cisco ISE's powerful authentication and authorization features, addresses challenges with profiling and accelerates policy creation. In fact, Ordr has been able to reduce device

profile-oriented tasks by more than half, reducing this financial services leader's operational costs dramatically.

Ordr's comprehensive platform is delivering many benefits for this financial services organization. In addition to discovery and classification of all connected devices, with these insights shared with Cisco ISE, the financial services leader also uses Ordr Flow Genome to monitor and inspect the communications flows of its connected devices including ATM machines to detect suspicious and malicious behaviors.

> *"I will say from the get go that Ordr has done a fantastic job. From the on-boarding process, getting the information we needed from them, to the regulatory side where Ordr provides us with reporting that goes to regulators."*
>
> **CISO**

Aligning to Financial Services Leader’s Focus on Customer Success

One of the key values for the financial services organizations is its commitment to customers. This organization is a community bank built upon the needs of its customers, and these same principles are reflected in Ordr’s “customer first” philosophy.

“Ordr believes in customer success and has an executive devoted to customer success, which is very important. Three of my top vendors have great customer success teams and I would go to bat for each of those vendors anytime I'm asked to. Ordr fits in that same mode of believing in customer success, which is essential when you get the product and decide how you are going to utilize it.

Is it going to become shelfware, or are you going to be one of those companies that uses the system to its full potential,” said the CISO.

“In terms of surprises along the way; there haven't been any hiccups. You typically run into a lot of hiccups when you're implementing certain solutions, but it's been a successful journey so far and we look forward to continued success.” continued the CISO. “Ordr is a tool that can help your institution evaluate your risk, setting up your strategy. The world of IT is constantly changing. We are in an era of advanced threats in a dynamic environment, and you need Ordr as a critical part of your security stack”.

About Ordr

Ordr makes it easy to SEE, KNOW, and SECURE every connected device in your network—in real-time. Using a “whole enterprise” philosophy and the Ordr Data Lake, populated with a rich and growing library of millions of detailed device profiles, Ordr identifies every IT, IoT, IoMT, and OT asset, maps its attack surface, and protects each device with dynamic policies and automated enforcement. Organizations worldwide trust Ordr to provide complete asset inventory, address risk and compliance, and accelerate Zero Trust initiatives.