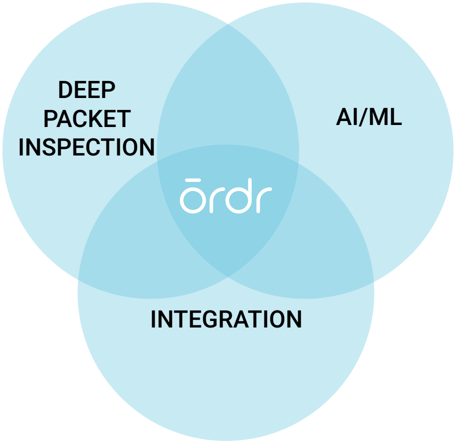
Delivering Asset Visibility at Scale

Using Deep Packet Inspection, Artificial Intelligence, and Machine Learning for Increased Accuracy of Device Identification

Having accurate and continuous visibility into connected assets is foundational to network hygiene. Gaining real-time knowledge of what devices are connecting to your network, if they are properly classified with make, location, operating system, serial number, and application/port usage, and ensuring that there is no impact to the device or the environment is critical. This requires the support of technology that reveals an assets unique identity and properties.

Ordr leverages Deep Packet Inspection (DPI), a technology that analyzes not just the packet header but also the application layer of its communication flow, retrieving key identifiers to categorize, classify, and group them into business or operational functions.

Traditional Network Access Control (NAC) vendors try to achieve similar function without DPI, and customers would immediately notice clear difference between technology that fully utilizes DPI and technology that mostly relies on non-DPI telemetry data.



The fundamental difference between DPI and non-DPI is an ability to see key device identifiers such as:

- ✓ Product model name (not model type)
- ✓ Serial number
- ✓ OS and software version
- ✓ Medical device modality type
- ✓ Study details
- ✓ Device utilization statistics
- ✓ Digital certificates
- ✓ User login/logoff patterns
- ✓ Accurately tracking supervisory protocols like SNMP, RDP, FTP, SSH, etc.

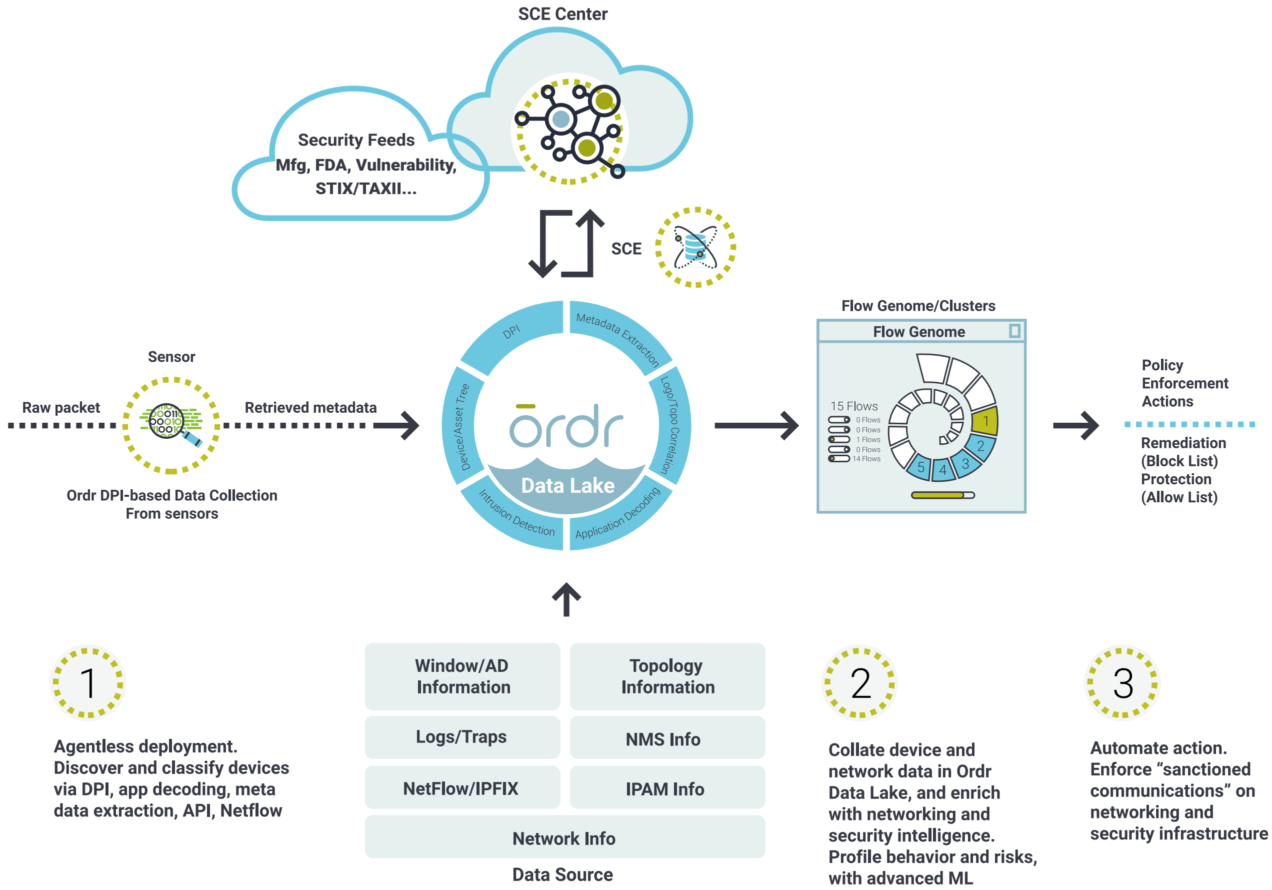
Non-DPI technology would not reveal such data which exists deeper in the application layer payload. If such identifiers are missing in the classification process, it would be extremely difficult to assess cyber security risk, because you cannot confidently tell whether your device has specific vulnerabilities related to the OS/patch level or whatever is disclosed by manufacturers or not. It would be challenging to match disclosed Common Vulnerability and Exposure (CVE) and Common Vulnerability Scoring System (CVSS) information to OS level of the device in the network.

The Ordr Systems Control Engine (SCE) platform with its high speed passive packet scanning technology also offers Intrusion Detection System (IDS) capabilities using threat feeds from multiple well-known providers. Ordr's IDS capability monitors for indication of an active threat and combined with known vulnerability detection, Ordr's DPI capabilities make our platform unmatched in the industry.

The Digital Transformation has brought on a massive amount of data that is generated by connected devices and with this tremendous growth, many organizations are experiencing lack of true network visibility. IT departments used to be responsible for all managed assets, yet today organizations have multiple teams that are responsible for devices, leaving large gaps and the inevitable unmanaged devices. DPI alone does not complete the Ordr classification engine. DPI disassembles device traffic and collects key pieces of data. The Ordr SCE platform uses its learning algorithms to group devices with similar characteristics. Such learning algorithms allow the Ordr platform to understand and correlate one device versus another device in a different location and create close match.

Artificial Intelligence (AI) and Machine Learning (ML) are other key technologies in Ordr platform to support hundreds of thousands of IT, OT, and IoT devices at scale, regardless of deployment type, on-prem or in the cloud.

Maximizing DPI Output by Automatically Training Classification Models



Agentless deployment. Discover and classify devices via DPI, app decoding, meta data extraction, API, Netflow

Collate device and network data in Ordr Data Lake, and enrich with networking and security intelligence. Profile behavior and risks, with advanced ML

Automate action. Enforce “sanctioned communications” on networking and security infrastructure

In a typical workflow, traffic from devices is sent to the Ordr sensor where a massive amount of traffic gets parsed and handed over to the Ordr DPI engine. Each piece data is sorted as attributes (300 ~ 400 attributes per device) and pushed to the Ordr Data Lake for AI/ML processing. Inside of AI/ML process, data goes through stages such as feature pruning, clustering, and classification. Ordr customers see this as a huge advantage – automation of the entire process to distill a massive amount of different device types connecting to the network and allow for workflow support with best in class data. This is exactly a reason why DPI technology alone does not scale, and the main reason why Ordr is a leader in both DPI as well as AI/ML technologies.

The platform keeps training its model that identifies similarities among devices. Without AI/ML technology, there is no global learning of devices. It learns similarities in the OS type, version, firmware revision, model name, its communication patterns, traffic destination, application type, and so on.

Enriching Additional Data via Integration

We have seen many cases where DPI does not see or cannot see enough data due to various reasons. It could be based on the way the network is architected or it could be a device itself is not sending enough data. The ability to ingest additional data including asset inventory data from CMDB/CMMS, device communication summary (e.g., raw NetFlow data), Active Directory data, Mobile Device Management (MDM) data, and vulnerability management data can be so crucial for data correlation and analytics. Typically, those 3rd party tools are integrated via API. In addition, our built-in Device Data Exchange (DDX) tool makes schema mapping flexible and easy for customers to ingest custom device attributes to the Ordr platform.

Whole Organization Monitoring

Ordr believes that every single connected device in an organization needs to be discovered and analyzed. For instance, in a healthcare organization the IT and facility devices are just as vulnerable as the medical devices. A vulnerability in the connected power generator is a huge risk toward business continuity. A vulnerability in an MRI can be as bad as a non-patched medical workstation. Once you have clear visibility and rich device context for the entire picture of connected devices in the entire facility, you have enough information to come up with appropriate risk mitigation plans and actions. If you only focus on one area of device discovery, you are completely blind to other risks, which might potentially bring operations in the entire facility down. The only way a system can reasonably classify the wide variety of devices in an enterprise that include smore than just medical is to use modern techniques like AI/ML and not just relying on attributes from DPI.

Ordr continues to work with our amazing customers to improve our platform and knowledgebase, understanding more proprietary and device specific protocols, training our AI/ML model based on the massive data we process every day, and increase accuracy and fidelity of our device classification technology, because we truly believe that this is going to help customers to fundamentally change their ability to protect their business, and the devices that enable it.

About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information, visit **www.ordr.net** and follow Ordr on **Twitter** and **LinkedIn**.