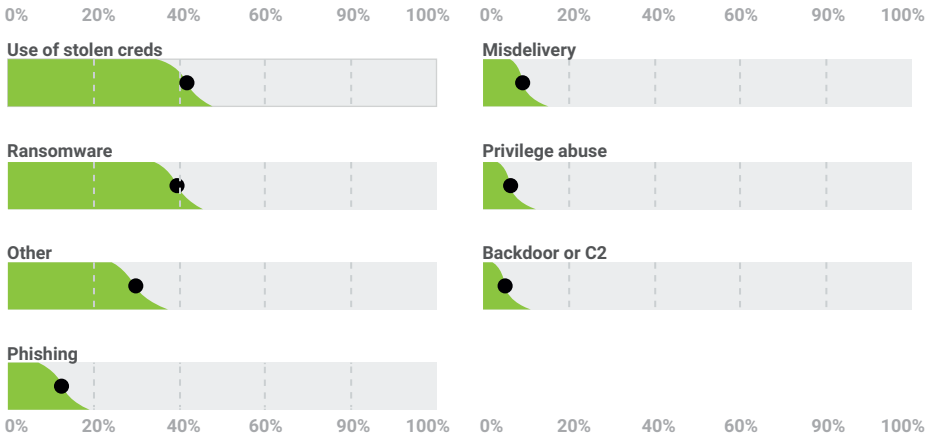
Ordr for Higher Education

Complete Visibility and Security of all Connected Devices

Universities, polytechnics, colleges, vocational schools, and other higher education institutions are the epicenter of innovation in laboratory science, mathematics, cognitive science, computer science, policy reform, technology, and more. In driving advanced innovation in areas vital to our world, our health and our intellectual life, higher education institutions are facing significant security risks.

Advanced research with confidential data and smart campus initiatives to bring more connectivity to students, educators, and faculty, also increases the likelihood of threat actors having more attack vectors to gain access to an institution's networks. In recent years, we have seen a spike in the number of higher education attacks, from ransomware to unpatched systems vulnerabilities and application vulnerabilities.

According to the 2022 Verizon Data Breach Investigations Report, **"Educational Services follows an eerily similar trend to the majority of the other industries; it is experiencing a dramatic increase in Ransomware attacks (over 30% of breaches). In addition, this industry needs to protect itself against stolen credentials and phishing attacks potentially exposing the personal information of its employees and students."**



Top Action varieties in Educational Services breaches (n=218)

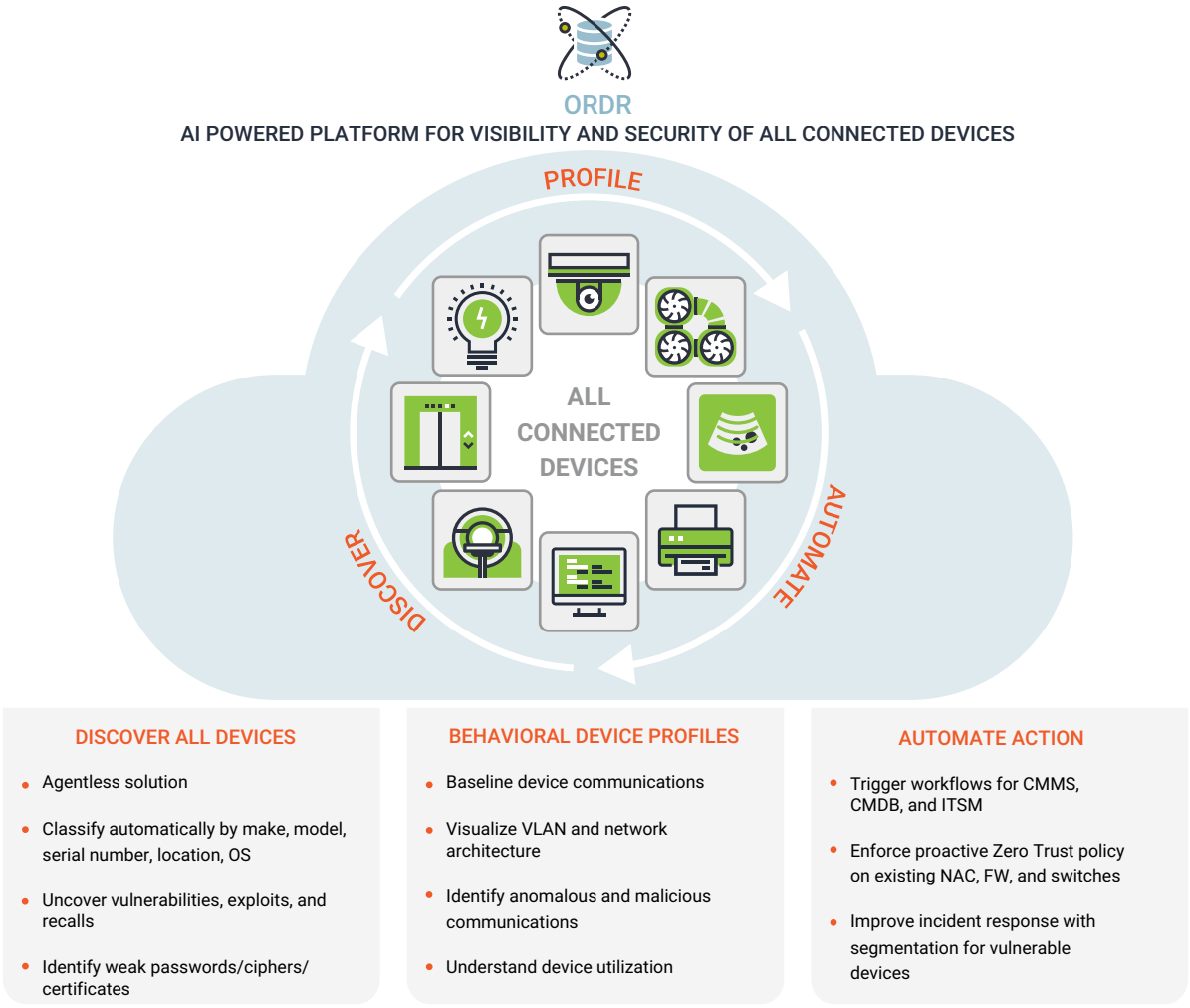
Introducing Ordr

The digital transformation in higher education campuses worldwide has led to the inevitable explosive increase of connected devices. The scale and diversity of these devices, and the capacity for network connectivity introduces risks. Every single device is a potential attack vector and must be secured.

Ordr helps you SEE, KNOW, and SECURE every connected device, everywhere -- from traditional servers, workstations and PCs to Internet of Things (IoT), Internet of Medical Things (IoMT), and Operational Technology (OT) devices. Ordr discovers and automatically classifies all devices on the network, profiles device behavior, uncovers risks, and can automate the appropriate action. Ordr is deployed in the cloud, offers a zero-touch, agentless deployment, and has been effectively implemented at-scale to secure connected devices in complex networks in higher education environments.

Real-Time Visibility and Classification of All Connected Devices

You can't protect what you can't see. Within minutes of deployment – via a network SPAN or TAP – Ordr automatically discovers and accurately classifies every device, complete with granular details such as make, model, operating system, serial number, location, and application/port usage. This visibility is continuous and in real-time to create a single source of asset inventory truth that can be integrated into your existing CMDB, CMMS, and ITSM solutions.



Profile and Baseline Device Communications

Using the built-in intrusion detection system (IDS), integration with threat feeds, and manufacturer databases, Ordr continuously monitors devices for risks, identifying those with vulnerabilities/exploits, manufacturer recalls, and using weak passwords, ciphers, and certificates. Ordr also analyzes and fully maps every device communication using advanced machine learning. This unique capability, called the Ordr Flow Genome, establishes a baseline of communications for every device so suspicious and anomalous behaviors, such as communications to a command-and-control (C2) server, can be identified. Ordr Traffic Analysis view also provides traffic constellation visualization for groups of devices across VLANs, subnets, security group tags (SGTs) and other network dimensions etc.

Proactive Enforcement via Fully Supported Integrations

Ordr not only identifies vulnerabilities, risks, and active attacks – the platform also creates policies to protect your connected devices. By baselining “normal behavior”, Ordr can dynamically create positive security policies to only allow “sanctioned communications”; this enables devices to remain in operation and communicate as need while limiting unnecessary exposure. Ordr dynamically generates these Zero Trust policies and enforces them on existing network and security infrastructure such as switches, firewalls, wireless LAN controllers, and more. Ordr also integrates with incident response and asset management tools to enable workflows across the entire lifecycle of vulnerabilities and threats.

Case Study: Higher Education Institution

A large higher education institution with more than five undergraduate campuses serving over 10,000 students needed a solution to enable visibility and improve security for their connected devices. Their environment included a variety of unique devices, from wireless routers, wireless disk drives, gaming consoles, and video streaming players to robotic arms, ultra-low freezers, workstations, and tablets. The team needed clear and continuous visibility of these devices, including network details such as device communications within and between VLANs. Ultimately they needed insights to enable proper segmentation across their environments.

Ordr met all their crucial security requirements, including alignment with NIST and MITRE security frameworks, and helped them adhere to regulatory compliance standards such as FERPA, GLBA, FISMA, HIPAA, HEA, and SAIG when triaging an incident. Ordr provided automated and continuous visibility into all their connected devices, helped them visualize all device communications, and baselined device behaviors. With this insight, the team used Ordr to automate group policy creation for expedited and informed segmentation enforced on their network access control (NAC) solution.

When faced with an incident, the team leverages granular device context from Ordr to quickly identify high-risk devices and pinpoint their exact location, including VLAN and associated switch port. Ordr capabilities have saved full-time employee (FTE) hours for their cybersecurity incident response team (CSIRT), reduced their mean time to respond (MTTR), and have overall improved the visibility and security of their connected devices.

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 Venture Capital, Ten Eleven Ventures, Northgate Capital, Kaiser Permanente Ventures, and Unusual Ventures. For more information, visit **www.ordr.net** and follow Ordr on **Twitter** and **LinkedIn**.