ORDR for Higher Education

Modern campuses never stand still. Students, faculty, researchers, medical centers, and athletic programs rely on thousands of connected devices—expanding the attack surface across sprawling, open environments. ORDR sees every device, understands its behavior, and secures the campus without slowing learning, research, or daily operations. With ORDR IQ, your team gains the intelligence and speed to outpace threats in environments where openness and security must coexist. This is security built for higher education—flexible, fast, and grounded in real network truth.

INTELLIGENCE: AI Protect for Security
See Every Device. Understand Every Exposure.

Campus networks are some of the most open and unpredictable environments in the world. Devices appear, disappear, roam, and rejoin across classrooms, labs, residence halls, stadiums, and research spaces — often without IT ever knowing. Traditional tools can't keep up with that level of churn.

ORDR continuously detects every device the moment it connects, automatically classifies it, and builds a living map of how it behaves. Instead of just showing what's on the network, ORDR shows what each device is doing — which systems it touches, which identities it uses, where it travels, and when its behavior starts to drift. This gives campus security teams something they've never had before: real-time, role-aware visibility across an environment that changes by the minute.

ACTION: AI Protect for Segmentation
Turn Intelligence Into Reliable Segmentation.

Campuses depend on availability and open access, making disruption unacceptable. ORDR delivers Zero Trust enforcement designed for distributed, mixed-use environments—academic buildings, research labs, medical centers, athletics complexes, residence halls, and remote sites.

With millions of flows analyzed daily and deep NAC and firewall integrations, ORDR makes segmentation predictable, scalable, and aligned with campus operations.

No agents. No device downtime. No interference with academic or research workflows. Just safe, repeatable Zero Trust enforcement across IT, IoT, OT, and research networks.

ORCHESTRATION: ORDR IQ
The AI Orchestration That Makes Teams Faster.

ORDR IQ uses ORDR's deep telemetry, device intelligence, and behavioral insight to deliver expert-level answers in seconds. It doesn't guess—it understands your campus.

Whether identifying exposed lab equipment, isolating compromised IoT sensors in residence halls, analyzing cross-campus communication patterns, or drafting segmentation plans for research data or clinical networks, ORDR IQ accelerates every workflow without adding agents or infrastructure. ORDR IQ gives your team the speed to outpace threats, not just react to them.

The Power You Experience with ORDR

ORDR protects every connected asset across the institution.
ORDR IQ gives your team the speed to outpace threats, not just react to them.
Together, they reduce breach risk, contain lateral movement, protect critical academic and research data, support key compliance needs, and strengthen campus resilience—without adding complexity.

Get Ahead. Stay Ahead.

Threats move fast. With ORDR IQ, your team can move faster. See what's inside your network before someone else does. One session often reveals what others miss.