

CASE STUDY

RICHMOND UPON THAMES COLLEGE (RUTC)

From Device Sprawl to Precise Security

Richmond upon Thames College (RuTC) is one of London's longest-established academic and vocational colleges, serving 16-19-year-olds and adults. It caters to around 3,500 students and 300 staff members.

As part of its ongoing development, RuTC has been rolling out a new flagship campus facility that includes advanced STEM (Science, Technology, Engineering, and Mathematics) and Sports Centres. To support these expansions, the College is now focused on ensuring robust network security for all student, facility, and staff devices.



⚡ Challenges

The College identified the need to gather a full understanding of precisely what is attached to their network. They wanted visibility and security of every connected device – from traditional servers, workstations and PCs to newer and more vulnerable IoT devices. Many further education institutions also have a lack of visibility into their 'Shadow IT' devices – the practice of technology and devices that are deployed without the knowledge or approval of the IT department.

The provisioning of bring your own device (BYOD) added another security challenge with students bringing in devices that were not always fully updated and secure.

Stephen went on to explain that the College takes its duty of care to its students, faculty, and staff very seriously '... given that we have a significant proportion of under 18s, we have to be extra careful; safeguarding is key'.

“We had lost sight of all of the devices that were attached over the years – we needed to understand exactly what was connected to ensure no ‘back-doors’ or vulnerabilities could be exploited.”

Stephen Hacon
RuTC's IT Manager

Solutions

ORDR AI Protect for Segmentation uses deep packet inspection (DPI) and advanced machine learning to provide full visibility of all network-connected devices at a granular level, including make, model, serial number and location. ORDR also identifies device risks, including any inherent vulnerabilities and then continually monitors for behavioural changes via its Flow Genome and Traffic Analysis tool in order to actively prevent any threats that may arise.

The system is continuous, passive, and agentless. It requires no hardware changes to the network, integrating with the College's existing infrastructure to provide unrivalled device visibility and control for both managed and unmanaged devices.

ORDR also integrates with a comprehensive portfolio of existing security and IT solutions. ORDR was integrated with Splunk, the College's SIEM solution, enriching the Splunk system with real-time device visibility details and alerts on anomalous or malicious behaviour for further analysis by the security operations teams.

Summary

In addition to the rich device context for visibility and security, by adopting ORDR, the College is now also providing enhanced safeguarding by monitoring the real-time behaviour of staff, faculty, and students, and are notified immediately of any suspicious activity.

The new system has given the College continuous visibility into their network that was never possible before, protecting all wired and non-wired devices. Should a connected device such as a CCTV camera, door entry system, or an interactive whiteboard be compromised, ORDR can stop the infection in its tracks by automatically creating segmentation policies to isolate the infected device and prevent lateral movement across the network.

“With ORDR's user friendly dashboard, we are now able to identify potential security vulnerabilities, allowing us to effectively secure our network with just a few clicks,”

Stephen Hacon
RuTC's IT Manager



Working with ORDR has been a really positive experience where the system was installed quickly, giving us results from day one. We were a little surprised at what we found on the network, but I suspect we're not alone on that front!"

Stephen Hacon
RuTC's IT Manager

About Us

ORDR is the leader in AI-powered asset risk and exposure management, trusted by top organizations across healthcare, pharmaceuticals, manufacturing, and financial services. With insights from over 100 million asset types, ORDR's platform empowers security teams to identify their biggest risks and take swift, effective action. From maintaining security hygiene to real-time threat detection and protection using microsegmentation, ORDR makes action not just possible but automated and simple — bringing ORDR to chaos.

ORDR is backed by top investors including Wing Venture Capital, Ten Eleven Ventures, Battery Ventures, Mayo Clinic Ventures, and Kaiser Permanente Ventures. For more information, visit www.ordr.net and follow ORDR on [X](#) and [LinkedIn](#).

For more information, visit ordr.net

Follow Ordr on



Ready to bring ORDR to your chaos?

REQUEST A DEMO