CASE STUDY

Richmond College Network Visibility and Security

Richmond College gains visibility and secures all network devices.

THE CHALLENGE

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 higher 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

"Working with inTEC EDUCATION and Ordr has been a really positive experience where the system was installed quickly, giving us results from day one' explained Stephen. '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

HOW WE DID IT

inTEC EDUCATION, the College's IT provider had already begun implementing their new wired and wireless network alongside a suite of other cyber security enhancements and recommended they deploy Ordr Systems Control Engine (SCE).

Ordr SCE 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. inTEC EDUCATION was able to integrate Ordr 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.

The new system has given the College continuous visibility into their network that was never possible before, protecting all wired and non-wired devices.

inTEC EDUCATION

Telephone: **0330 555 550**

Email: **enquiries@inteceducation.com**

www.inteceducation.com