Richmond College gains visibility and secures all network devices

Richmond Upon Thames College (RUTC) is one of London's oldest established colleges offering a broad range of innovative courses for people from 14 years to adults and is home to over 3,500 students and 300 staff.

In Spring 2020, they moved into the first phase of a new 80M flagship campus facility, with phase two being completed in 2021. The project also includes the construction of two new secondary schools. As the campus and schools are being completed and the infrastructure to support the growth in students is nearing completion, the College is looking to address student, facility, and staff device network security.

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.

Stephen Hacon, RUTC's IT Manager explains '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'.

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'.

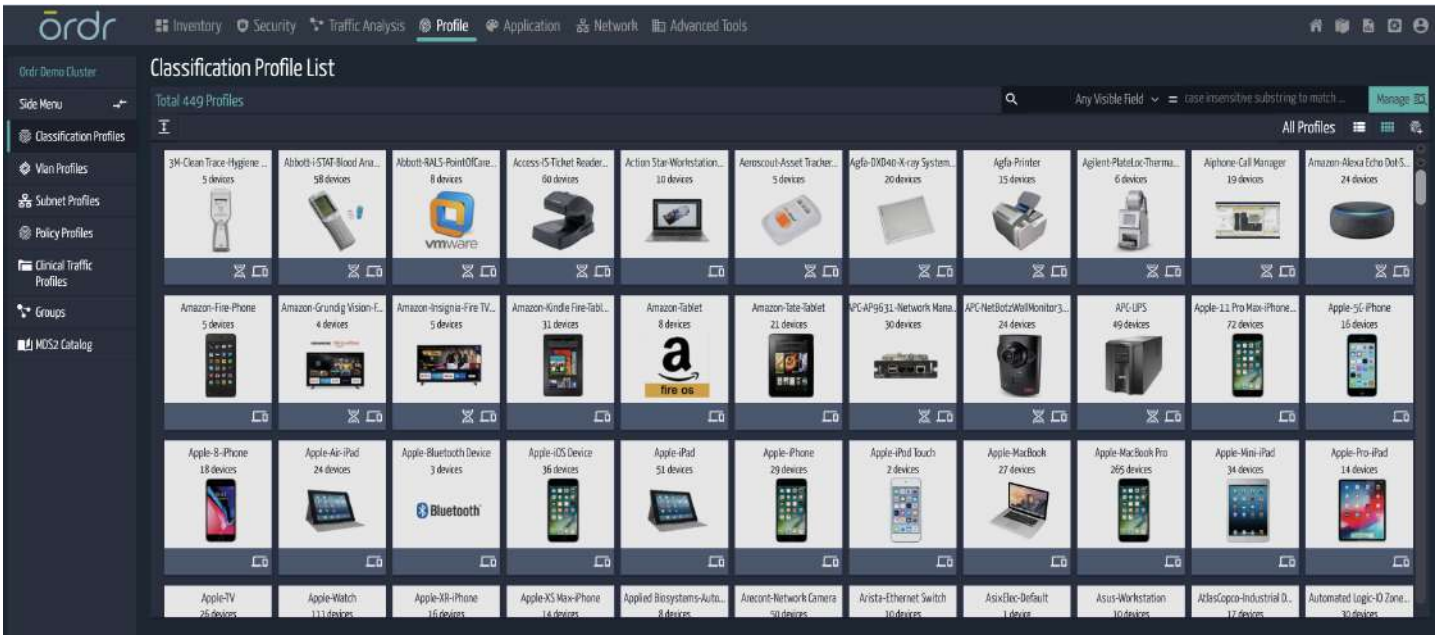
The Solution

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.

'With the Ordr user friendly dashboard, we are now able to identify potential security vulnerabilities, allowing us to effectively secure our network with just a few clicks,' said Stephen.

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.

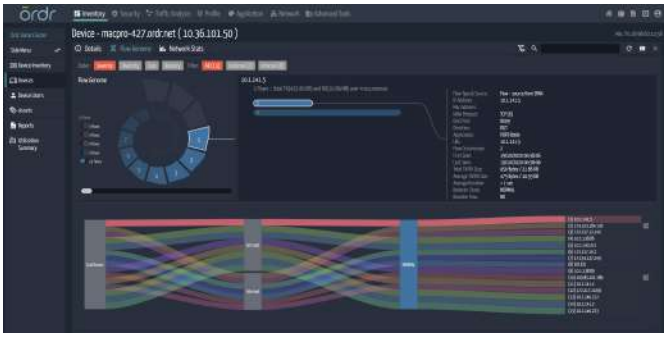


Screen showing profiles of attached devices

Summary

In addition to the rich device context for visibility and security, by adopting Ordr SCE, 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 SCE can stop the infection in its tracks by automatically creating segmentation policies to isolate the infected device and prevent lateral movement across the network.



'We have now regained full visibility of our infrastructure' explained Stephen; 'we are no longer blind'.

'Working with 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!'

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.