University of Warwick

THE UNIVERSITY OF WARWICK BUILDS A SECURE FUTURE WITH GRADIAN

The University of Warwick is a public research Russell Group university, located between the West Midlands and Warwickshire, England. Founded in 1965, the University is ranked 61st in the world and 10th in the UK. Some 92% of Warwick's research has been assessed to be 'world leading' or 'internationally excellent' in the Research Excellence Framework.

The University and the wider U.K. higher education (HE) community are at a security tipping point. According to the JISC 'Cyber Impact' report, it is no longer a case of 'if' a security incident will hit institutions – it's 'when'. JISC's Incident Response team, for example, is recording up to 6,000 incidents every year, including more than 1,000 denial of service attacks on the JISC network, targeting 236 members.

Moreover, Microsoft Security Intelligence reports that 87% of all enterprise global malware attacks have been against HE, including malware, advanced attacks, and phishing. Email platforms are under attack too: 96% of all phishing attacks are carried out via email spoofing.

HE institutions are struggling to keep up, JISC reveals. IT staff are being diverted from everyday tasks to resolve data breaches and incident recovery costs are spiralling. Another JISC report finds that recovery is challenging, time-consuming, and expensive. A lengthy rebuild of a digital estate could easily consume several million pounds, according to JISC.

Safeguarding The University of Warwick's Data

Common to the HE sector, the University of Warwick's email environment is subject to attack by cybercriminals. An abundance of devices, the value of students' personal identification information (PII), the University's intellectual property, and the rise of post-pandemic remote learning make the University's email platform a key target for malicious attacks.

"We have approximately 40,000 active accounts, across multiple domains," explains Des Butcher, Enterprise Application Director, University of Warwick. "Authentication is critical for us – not only to safeguard the email platform, but also to ensure critical emails are not blocked, such as the ones containing financial data or marketing campaigns."

The Challenge

The challenge for Butcher and his team was to take control of the authentication framework and prevent attacks infiltrating the University's systems. "SPF management was complex," he says. "We have many sending services to authorise, ongoing DNS updates, a need to ensure continuity of service and ensure configuration is correctly managed."

Moreover, the team needed to resolve DKIM (domain keys identified mail) lifecycle management. “With no means to authoritatively identify the sender, anyone could easily impersonate sending domains,” says Butcher.

Maybe the University could manually attempt to get visibility into the DMARC (domain-based message authentication, reporting, and conformance) standard reports and identify the services that were not authenticated? “Manual DNS changes were an unsustainable approach,” says Butcher. “It would have taken a long time and absorbed a significant amount of our resources – resources that would be better spent on value-add strategic security tasks. We needed a robust, automated DMARC policy without the headaches of the implementation.”

This is where Gradian comes in.

“We trust Gradian implicitly”

The Solution

This forward-thinking data protection consultancy proposed an innovative new approach to managing the University’s email security. Butcher again: “Gradian was the ideal partner to support our DMARC enforcement. Their managed service approach takes away the risk and the resources needed to implement successful defence against email attacks. Their depth of knowledge, proven track record, and professionalism mean we trust Gradian implicitly.”

Gradian deployed a Valimail DMARC enforcement platform at the University to eliminate domain spoofing and phishing. The highly automated solution delivers DMARC enforcement, easily enabling the University to auto-configure thousands of sending services. And integrated SPF technology dynamically overcomes the 10-domain lookup limit for every email – with 100% accuracy.

“With Gradian at our side, the implementation was straightforward. The team filled our resource constraints, knowledge gaps, and the risk of incorrectly configured enforcement. Very quickly, the University was benefiting from automatic DNS configuration, intelligent sender identification, and an easy-to-follow task list. One of the great features is the drill-down domain visibility. We have quantified evidence of the number of senders, the country of origin, and other insights. This was useful in developing the business case for enforcement.”

The Result

Almost eliminated phishing or spam campaigns

The bottom line? The University of Warwick now ensures only authorised senders can use the ‘warwick.ac.uk’ domain in the ‘From’ field of their email messages. “We have almost eliminated the frequency of successful phishing or spam campaigns purporting to be sent from the ‘warwick.ac.uk’ addresses. We have complete visibility into what’s happening, thereby stopping the mis-use of our domain.”

Gradian has also been instrumental in driving agile and effective change management. “Gradian has been vital in the change program. They worked with the different University stakeholders and departments ensuring they were on-board with the change. The Gradian team were proactive and skilled throughout, managing the process so our small team could concentrate on other priorities. With Gradian’s support and the innovative Valimail platform, the University of Warwick has a guaranteed path to fast, safe DMARC enforcement.”