Case study

Protecting 40,000 students and 5,000 staff from cyber attacks

Company
Harris Federation

Industry
Education

Location
London and the Southeast UK

Solutions
Countercept MDR

WITH secure | Harris Federation

Preparing for a post-ransomware organization

Harris Federation, a Multi Academy Trust managing schools across the south east UK, suffered a ransomware attack and put in place a team, processes, and technologies to build out their defense in depth, aiming to set the example for in education, to make themselves resilient against further cyber attacks that could disrupt student outcomes.

An attack by a well-known ransomware gang in March 2021 – part of increased targeting of the UK education sector by ransomware groups[1] - shut down the Federation's IT systems for several weeks. At the time, the Federation had no dedicated cyber security capability. Jack Fowler, a cyber security specialist then working for the Open University, was hired shortly after as the Head of Information and Cyber Security to support the build out and maturity of cyber security at the Federation.

"One of the first things I did was to look at who had our back – who was defending our corner – in the event of a cyber-attack. It was evident the Federation was alone; we needed a long-term strategic partner whilst we built out our security maturity," says Jack. "We started looking for that strategic managed security capability we could call upon: a team that understood education. The emphasis was on identifying a partner, rather than a supplier, and for something better than a bundle of tools and add-ons.

About Harris Federation

Harris Federation is an education charity that, through its 5,000 staff, teaches and cares for upwards of 40,000 students between the ages of four and 18 years spread across more than 50 Primary and Secondary schools in London and Essex. The Trust is estimated to teach one in 40 children in London, and its approach to public education has seen its school places oversubscribed at a rate of four to one.

1 Support for UK education sector after growth in cyber attacks - NCSC.GOV.UK

The Managed Detection and Response difference

Most Managed Security Service Provider (MSSP) offerings failed to make the cut, but a Managed Detection and Response (MDR) service was a better fit. As a Microsoft 0365 and Defender customer, Harris had the basics in place, but it needed more than that. Spread across more than 50 locations, and with tens of thousands of users of hugely varying experience, intentions, and skills. However, its scale as a MAT is significant, and this in some ways gives Harris an advantage with its economies of scale. However, it also means a successful attack has a large impact on many students, and an attractive target for malicious actors.

Co-securing the Federation

“I say we were looking for a partner because we needed something effective fast, but we also wanted to achieve several more things in the future – and that called for more than a transactional relationship,” says Fowler. “With WithSecure, and with Countercept, we got that working partnership. It wasn’t a huge ecosystem with lots of add-ons and bolt-ons: it’s a service that works exactly as advertised, and people that help.”

WithSecure’s approach made a big difference.

“We felt we could have an honest and open conversation, and that showed in how WithSecure approached the challenges we were facing. There was no hiding behind spec sheets, and the people were open and easy to talk with. Finally, the research – in the form of papers and projects across a wide range of different security practices and also in threat intelligence – gave us confidence that we were going to be dealing with a company that cared.”

Spending wisely

Jack Fowler began his career with the Open University straight out of school, adding to his qualifications on the job, and experiencing the Open University as both an employee and a student of this unique institution. It’s made Jack an educationalist through and through.

“Every time I make a budget request, I have to think in terms of how we as a Trust use resources; there’s nothing unusual in that, and it's a common consideration for any business,” says Fowler. “But that also translates into: how does this benefit the pupils? I might want a shiny new tool or service, but is that money well spent, when it could go towards hiring more teachers, or getting a learning resource for the students. The decisions we make about IT and Cyber Security have a real-world effect on pupil outcomes.”

Managed Detection and Response is not known for being a bargain-basement cyber security capability. It calls for vast amounts of expertise, tooling, and practice, always calling for highly skilled analysts and threat hunters available – and at a high level of training and preparation. So how did Harris and WithSecure make this work?

Education is quite different from more mainstream enterprises, and as a charity, we're hyper cost-conscious," says Jack. "Looking at this from the perspective of seat- or endpoint-based pricing wasn't going to work. Of our tens of thousands of endpoints, many are unused for big chunks of time, and so we were able to work out how to make the cost work for us and for WithSecure, which understands how endpoints are utilized within the education sector.

Putting Countercept to the test

WithSecure's ability to deliver much more than a collection of tools and alerts was soon tested in an incident that, while minor in cause, could have had a massive knock-on effect on Harris' main mission of teaching.

"Microsoft Defender went ballistic one evening. One vague Microsoft alert, and our entire O365 tenancy was blocked," says Jack. "I was pretty sure it was a false positive – but I also needed to be certain. In the meantime, we were shut down – no external email… but that was the least of our worries. Come the morning, if we'd not resolved this issue, no-one would be able to send externally, within Education - this is hugely disruptive for operations".

With no actionable evidence from Defender, and no-one from Microsoft or its partner to provide that assurance quickly as the Federation isn't a premier support customer, Jack was faced with a long night of raising, escalating, and chasing a support call.

"Without enough information, making the call to remove the restriction left us with a huge dilemma – leave it in place, and school operations are disrupted for 40,000 children. Take it away, and we might have an incident on our hands," says Jack. "It was quicker to go through WithSecure, and that's exactly what we did."

"A WithSecure expert got straight on to a video call – at 11pm, no less – and provided me with the assurance we needed that we were looking at a false positive, validating our findings. That's the value we get from them."

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure