Partner case study

# Protecting educational IT against a hostile threat landscape

**Company**
Chesterfield College

**Country**
England

**Industry**
Further Education

**Solutions**
WithSecure™ Elements

WITH secure | KryptoKloud

## Protecting an unusual and complex IT environment

Matthew Day, Head of ICT at Chesterfield College, and his team of 11 IT personnel, are tasked with keeping all of this secured and running smoothly. He says that while the college has yet to suffer a serious security incident itself, the team was conscious of the need to keep up with the changing threat landscape.

He comments: “There have been several high-profile cyber-attacks targeting the education sector, particularly since the first lockdown. This motivated us to re-evaluate our approach and further strengthen our security measures before we became a headline ourselves.”

Recent research from the UK Government reveals that around 88 percent of further education institutions in the UK have suffered a breach or attack in the last 12 months. Nearly half were negatively impacted by these incidents.

Day explained that, while there was nothing specifically wrong with their previous security provider, they proactively made the decision to move towards a greater level of visibility across their unorthodox IT estate. It was also critical that they could count on a real-time response to any emerging threats.

He elaborated: “Our IT environment is complex because we not only have thousands of standard devices, but also a lot of specialist technology to enable our students to learn cutting-edge skills. It’s essential that we have proper visibility of all these different systems and can spot anything unusual.”

## The search for the right security partner

To improve their levels of visibility and responsiveness, Chesterfield College sought to partner with a managed security service provider that could offer the right expertise and tools.

“To deal with the latest threats, we needed cyber security experts monitoring the estate 24/7; we determined it wasn't viable to staff this in-house, so needed to find a reliable security partner,” Day added.

In June 2021, the team began discussing its needs with other educational institutions with similar situations. The aim was to gather industry experience, good and bad, and discover which providers had the right capabilities and mindset for the job.

KryptoKloud and its security partner WithSecure™ immediately emerged as a favourite choice among industry peers.

Day explains: “We focused on word-of-mouth referrals so we could get a real representation of the best providers for what we needed. KryptoKloud and WithSecure™ quickly went to the top of our list as everyone praised their industry experience and the quality of the service.”

### About Chesterfield College

Chesterfield College is a general further education college located in north Derbyshire. A team of around 600 staff, support 10,000 learners across a huge range of courses, with the college providing apprenticeships, A-levels, degrees, electrical engineering, hairdressing, bricklaying, and everything in between.

Underpinning all of this is an IT estate of around 2,500 endpoints, including both standard computing devices and specialised equipment for the more technical courses. Alongside this, the site sees traffic from countless personal devices that connect to the network, from staff and students alike.

> “It’s a relief to know we have the proven ability to identify and stop cyber attacks. For example, we had a minor incident with a student testing out their skills and exploring our IT systems, trying to escalate privileges and maintain persistence.”

Matthew Day, Head of ICT at Chesterfield College

The positive buzz was backed up by a highly competitive quote for the services Chesterfield needed – an important factor in the education sector where budgets are always a concern.

Chesterfield College took on KryptoKloud as an MSSP providing 24/7 support through its Security Operations Centre (SOC).

WithSecure™ provided pre-selected Elements' technology to KryptoKloud's SOC team, namely Endpoint Detection and Response (EDR) and Vulnerability Management.

Day explains: "The partnership was perfect for our needs: KryptoKloud provided the expertise, and WithSecure™ ensured they had visibility into our network so that monitoring and response was possible in real time. If any issues arise, KryptoKloud's SOC team can react and triage them as needed, and then alert us to any follow-up actions that we need to take: they operate as a specialised extension of our in-house team."

## Delivering visibility and automation

Chesterfield College has seen a number of powerful benefits over the last year of working with KryptoKloud and WithSecure™, from a higher level of security confidence to simpler and more cost-effective  IT security management.

"It's a relief to know we have the proven ability to identify and stop cyber attacks," Day explains. "For example, we had a minor incident with a student testing out their skills and exploring our IT systems, trying to escalate privileges and maintain persistence."

He continued: "Using WithSecure's solutions, the KryptoKloud team were immediately able to identify this suspicious activity and alert us. Thankfully this was just a curious student and not a genuine threat actor, but it demonstrates we can reliably spot the increasingly common 'living off the land' techniques used by real attackers.

The Chesterfield IT team also immediately saw the benefits of having a single partnership cover all security needs across their IT estate. The approach provides a single pane of glass for the team to view the entire network and simplifies a number of processes, as well as being more cost effective.

Day explains: "As well as looking out for active threats, the partnership is hugely beneficial for our routine security needs. Things like software updates and patches are automatically applied, and we are alerted if there are any issues. This is a great help as it frees us up to concentrate on value-add activities: developing the College's IT to better serve our students, rather than just 'keeping the lights on'."

Finally, WithSecure™ also provides the capability for KryptoKloud to conduct both scheduled and proactive vulnerability scanning as needed. The team had previously relied on multiple third party solutions for this, so the consolidation enabled them to further streamline and reduce overheads.

"We maintain Cyber Essentials Plus certification and are working towards ISO 27001,"Day explains, "so the patching and vulnerability scanning functions are extremely useful for us. WithSecure™ makes it easy to create reports on our activity to demonstrate that we are proactively identifying and resolving issues."

He concludes: "KryptoKloud and WithSecure's partnership is a perfect match for securing our complex IT needs on a tight budget."

# 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