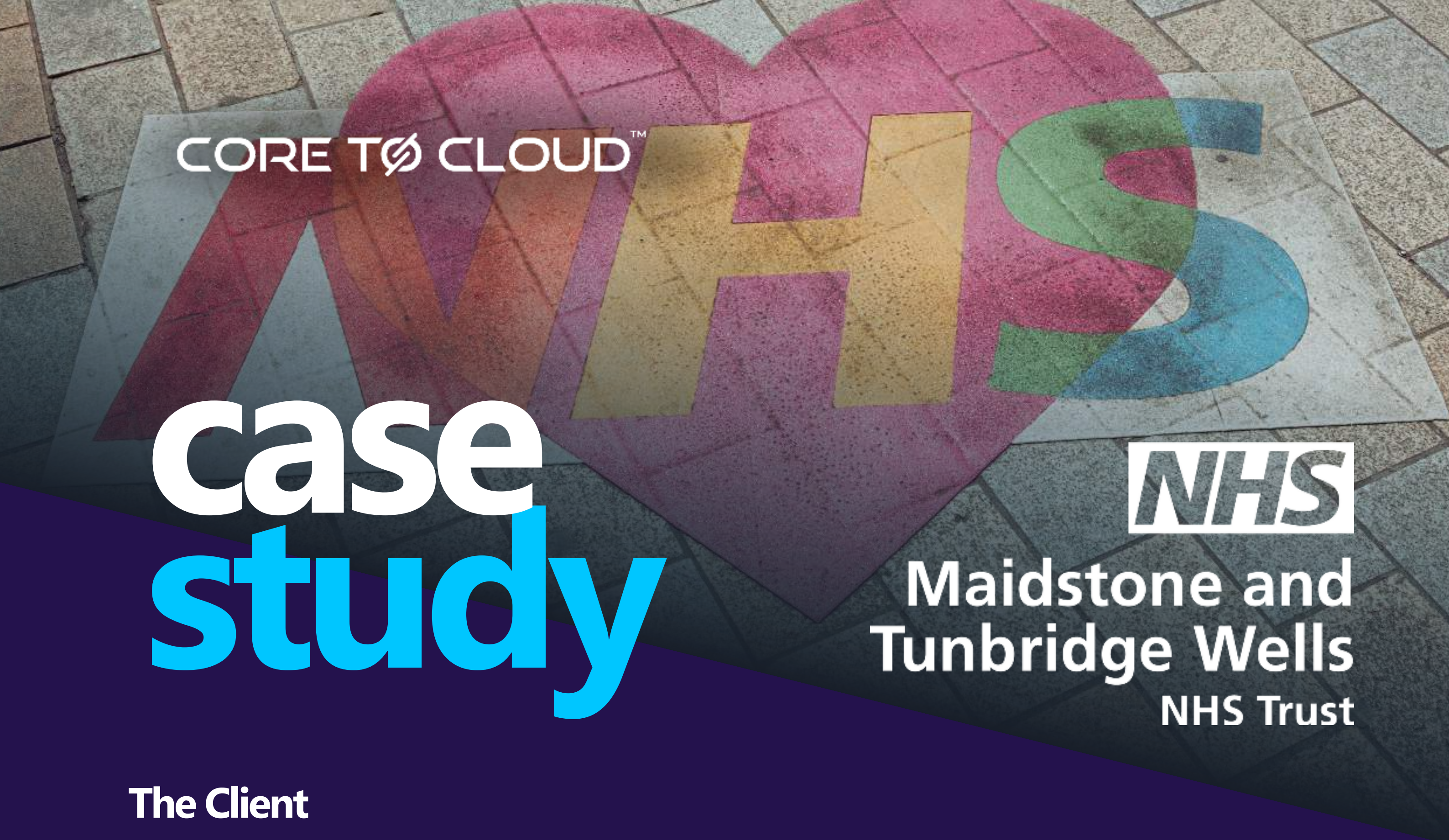

CORE TØ CLOUD™

case study

NHS
Maidstone and Tunbridge Wells
NHS Trust

The Client

Maidstone and Tunbridge Wells NHS Trust delivers acute hospital services to the local community, with a focus on high standards of patient care and operational resilience. The Trust's Cyber Security Architect leads a small team of three responsible for safeguarding critical systems, ensuring compliance, and meeting growing regulatory requirements. With increasing scrutiny under the Data Security and Protection Toolkit (DSPT), the Trust needed to gain clear visibility into the risks posed by its third-party suppliers, while ensuring limited internal resources could remain focused on wider security priorities.

The Challenges

Like many NHS organisations, Maidstone and Tunbridge Wells NHS Trust had no single, consolidated view of supplier risk. Supplier contact information was fragmented across inboxes and individuals, and there had never been a consistent process for gathering or validating information. As a result, understanding supply chain risk was slow, reactive, and resource-intensive.

At the same time, suppliers often presented lengthy governance documentation that claimed compliance and security best practice, but the Trust had no way of verifying whether those claims were accurate. With DSPT requirements demanding stronger oversight, the Trust needed a service that could test suppliers directly, provide independent validation, and highlight genuine areas of concern.

The challenge was further amplified by the size of the team. With only three people in the cybersecurity function, there simply wasn't capacity to manually review or monitor supplier assurance. The Trust needed a solution that could deliver accuracy and confidence without adding more strain to an already stretched resource. This made finding a trusted partner with both the expertise and capacity to help absolutely critical.

CORE TØ CLOUD™

> ***I honestly think every NHS Trust should speak to them — we've all got the same challenges, and Core to Cloud takes a huge amount of the burden away.***
>
> **Michael Valentine,**
> **Cyber Security Architect**

The Solution

Core to Cloud introduced Maidstone and Tunbridge Wells NHS Trust to its Third-Party Risk Management (TPRM) service. The engagement began with a small proof of concept covering two to three suppliers. The results quickly impressed the team, giving them the confidence to secure funding to expand testing across 25 key suppliers.

The service provides independent verification of supplier claims, ensuring that governance submissions reflect reality rather than unchecked promises. This has allowed the Trust to hold suppliers accountable, gaining assurance that critical partners are taking appropriate steps to secure sensitive data and infrastructure.

Onboarding was a challenge initially, as supplier contact data had never been centralised. However, working with Core to Cloud's team, the process was made straightforward and painless. The Trust described their support as answering "all our weird questions" and making the rollout smooth despite the complexities.

The Outcome

The TPRM service has fundamentally changed how Maidstone and Tunbridge Wells NHS Trust approaches supplier risk. By focusing on approximately 70% of its estate through carefully selected key suppliers, the Trust has achieved visibility where it matters most and can prioritise oversight on the highest-risk areas of its supply chain.

With Core to Cloud's independent assessments, the Trust can now challenge suppliers with confidence, verifying their security claims rather than simply taking them at face value. This new level of accountability has delivered assurance not only to the cybersecurity team but also to senior leadership, directly supporting DSPT compliance and wider regulatory expectations.

Most importantly, the Trust has gained confidence that if a supplier breach does occur, it will be far better positioned to respond effectively and minimise the impact.