CMR Surgical - Case Study

CMR Surgical, a UK-based medical technology company, is redefining surgery through innovation. Known for making keyhole procedures more accessible and less invasive, the organisation's technologies continue to advance, gaining visibility across the healthcare sector.

But with innovation ultimately comes added complexity and increased demands, particularly when faced with maintaining and scaling a secure digital infrastructure across both cloud and on-premises environments in line with business objectives, highly technical operations, and ever-increasing regulatory requirements.

Operating with a lean but knowledgeable IT and security team, CMR Surgical recognised the need to ensure the continued security of its Microsoft environment, while also preparing for resiliency in the future. At the heart of this challenge was understanding the capabilities the organisation had access to, and prioritising knowledge growth in the most pressing areas, aligned to both best practice and real-world use cases.

> As noted by CMR Surgical's Group IT Director David Proctor:
>
> *"It's been really useful to have that external assistance where we know something's important, but we're just not in a position to sit down ourselves and say, 'Come on, we need to suddenly become experts'."*

While prior to their engagement with Threatscape CMR Surgical's team had made consistent progress on continually improving its cyber posture, a number of advanced capabilities within the Microsoft 365 suite remained underutilised. CMR Surgical appreciated that understanding and enabling these features would be vital to maintaining security as their operations developed and as compliance requirements, such as ISO 27001, became much more demanding.

Threatscape's Involvement

CMR Surgical engaged Threatscape to conduct a multi-phase programme, structured around Microsoft's suite of security tools. The collaboration began with a Microsoft-funded Overwatch assessment, delivered via Microsoft 365 Security and Compliance CSI funding secured by Threatscape on CMR Surgical's behalf. This initial step enabled both Threatscape and CMR Surgical to gain a clear, point-in-time understanding of their security posture.

This initial assessment led to further collaboration, with CMR Surgical participating in a series of Microsoft CSI-funded workshops delivered by Threatscape, including:

Mitigate Compliance and Risk

Protect and Govern Sensitive Data

Defend Against Threats with SIEM plus XDR

These workshops were tailored to support CMR Surgical's security strategy, offering hands-on enablement that helped the internal team to extract greater value and performance from their existing Microsoft 365 tooling.

In addition to funded services, CMR Surgical chose to invest directly in further engagements by commissioning Threatscape to deliver a Defender for Endpoint and Defender Hardening programme.

Ongoing Business Benefits

From the outset, CMR Surgical made it clear that they weren't simply conducting a box-ticking exercise. Rather, they were working to best align ongoing cyber security with the organisation's unique needs in terms of robust identity security and diverse environments, services, and tooling.

The most significant outcomes for CMR Surgical were improved clarity, prioritisation, and practical understanding. Conversations moved beyond the tools themselves to explore how specific changes would impact day-to-day operations while still reducing risk. With Threatscape's input, CMR Surgical was able to proactively map out a strategic development roadmap that addressed both immediate technical requirements and future business needs, and the team could now take an informed, confident approach to security planning and implementation.

Since their engagement with Threatscape, CMR Surgical encountered a scenario wherein the impact was significantly less than it would have been had the organisation not had access to Threatscape's expertise.

> *"It was a lot quicker to tidy up and deal with than it otherwise would have been."*
>
> **David Proctor**

This underlines the practical value of the organisation's time spent with Threatscape, not just in delivering configurations and point-in-time recommendations, but crucially in transferring knowledge to the internal team for ongoing enablement. By supporting the team with not just the *what*, but also the *why* of Microsoft's ever-increasing suite of security tools and their configurations, Threatscape helped to build long-term capabilities, and not just short-term results.

For CMR Surgical, the decision to work with Threatscape wasn't just about technical delivery. Threatscape's ability to secure Microsoft funding, tailor engagements to specific needs, and provide access to top-tier expertise (including multiple Microsoft MVPs within Threatscape's Microsoft Security Practice) set them apart. The relationship was defined by trust, flexibility, and a shared focus on outcomes. Rather than prescribing a generic approach, Threatscape worked closely with CMR Surgical to understand their unique environment and then acted accordingly, with speed, clarity, and precision.

Why Threatscape

We are one of very few specialised security companies with a dedicated Microsoft Security Practice. Our Microsoft consultants and engineers work exclusively within the Microsoft suite, guaranteeing a reliable depth of knowledge and technical excellence in a constantly evolving feature set.

As now five-time winners of the Microsoft Security Partner of the Year Award, including the global award in 2020, Threatscape's expertise in this space is backed by Microsoft's own stringent frameworks for partner success.

Threatscape's experience and technical capability has been validated through five Microsoft Advanced Specialisations, demonstrating the breadth of our Microsoft skill. Advanced Specialisations are subject to an external audit of subject-related processes, methods, documentation, and reporting, considering both the knowledge and professionalism of in-house staff, along with the organisation's overall expertise in relevant areas. In order to be awarded an Advanced Specialisation, all facets of the audit must be met, without exception.

We are also positioned to deliver Microsoft funding through the Partner Programme, including both FastTrack and the Partner Cybersecurity Investment Program, or CSI.

Microsoft's FastTrack programme assists customers in planning, onboarding, managing, and driving value and satisfaction from their Microsoft deployment. FastTrack partners are trusted by Microsoft, on the back of their engineering expertise and proven track record of delivering guidance and service enablement.

Similarly, CSI is an invitation-only programme created by Microsoft to offer funding to eligible organisations to enable them to expand their deployment through preliminary engagements with new services.

Where appropriate, Threatscape may deliver a Microsoft Sentinel Engagement, a Cybersecurity Assessment, a Threat Protection or Data Security Engagement, or a tailored Overwatch Initial Assessment, utilising our leading Microsoft Security technologies to create a real-time baseline based on 350+ security controls to enable prioritised, evidence-based security optimisation.

Contact Us