

CORE TO CLOUD™

case study

The Client

The Glasgow Organising Company was established to deliver the Glasgow 2026 Commonwealth Games on an accelerated timetable of less than two years. Its technology remit covered the systems needed to stage the Games, including timing and scoring, venue technology, corporate IT, cybersecurity and broadcast production.

As the organisation moved from mobilisation into live delivery, its workforce, supplier network and public profile grew rapidly. The cyber risk changed with that growth, creating a need for controls that could be introduced quickly and work within a complex, time-critical programme.

Working with Core to Cloud, Glasgow 2026 introduced Halcyon as a specialist layer of ransomware protection within its broader cybersecurity programme. The solution strengthened resilience while providing additional assurance to the Board and government agency partners.

The Challenge

Glasgow 2026 had to build its technology and security environment at exceptional speed. The risk profile moved quickly from the relatively contained bid and mobilisation phases to the high-profile delivery of an international sporting event.

A rapid influx of staff and suppliers created a period in which security mitigations had to catch up with organisational growth. At the same time, the team faced an evolving threat environment, increased public interest and a fixed budget. Ransomware was a particular concern because even a contained incident could affect confidence in the Games and the systems supporting them.

The chosen technology needed to:

- Provide specialist protection against ransomware
- Be deployed quickly within a compressed delivery timetable
- Work alongside the SOC and existing security controls
- Fit within the available budget
- Support Board and government stakeholder assurance
- Complement the work of Glasgow 2026 and its other security providers



CORE TO CLOUD™

> ***Your generous support in providing cutting-edge ransomware protection within our budget significantly strengthened Glasgow 2026's cybersecurity. This technology added an essential extra layer of security, helping us defend the Games against a constantly evolving and more complex cyber threat environment, and provided an additional level of assurance to our Board and government agency partners.***
>
> **Martin Fitchie**
> Chief Information Officer

Glasgow 2026 responded with a layered programme that included independent cyber advice, a cybersecurity working group, SOC capability, staff training, web application protection and specialist ransomware defence.

The Solution

Core to Cloud introduced Glasgow 2026 to Halcyon as a specialist response to the organisation's ransomware risk. The engagement moved quickly from an initial discussion of the requirement and budget to deployment, reflecting the limited time available before the Games.

Halcyon was added as a dedicated ransomware protection layer within the wider security environment. Its role was specific: to strengthen defence against ransomware without displacing the controls and providers already supporting Glasgow 2026.

The technology was embedded into Glasgow 2026's SOC operations, giving the team a practical way to incorporate the additional protection into day-to-day monitoring and response. Core to Cloud supported the process by understanding the organisation's objectives, working within the available budget and collaborating with the wider group of security providers.

Working Alongside Existing Security

Halcyon formed one part of a broader, layered mitigation programme. Glasgow 2026 had already begun strengthening its position through external cyber advice, a working group, SOC support, staff training and web application protection.
The objective was to address a defined gap rather than replace or duplicate the wider security architecture. By adding specialist ransomware capability, Glasgow 2026 strengthened a material area of risk while preserving the contribution of its existing controls and service providers.

This collaborative approach was important in a programme where decisions had to be made and implemented quickly. It helped the organisation improve resilience without creating unnecessary complexity during the final stages of Games preparation.

The Outcome

The additional ransomware protection strengthened Glasgow 2026's overall cybersecurity resilience and became part of its SOC operations. It gave senior stakeholders greater confidence that the organisation had taken practical steps to address one of the most disruptive cyber risks facing the Games.

> ***Halcyon was well received and embedded well within our SOC operations***
>
> **Martin Fitchie**
> Chief Information Officer

The threat became tangible during the Games when a subcontractor experienced a ransomware incident. There was no impact on Games delivery, but the event reinforced the reality of the risk and the value of the layered controls that had been put in place.

For Glasgow 2026, success was measured in the secure delivery of the event and the confidence it could provide to its Board, government agency partners and wider stakeholders. Core to Cloud's contribution supported that outcome by adding specialist capability at the point it was needed.

A Responsive Relationship

Alongside the technology, Glasgow 2026 valued the way Core to Cloud engaged with the programme. The relationship was straightforward and collaborative, with the team taking time to understand the organisation's objectives, financial constraints and delivery pressures.

Core to Cloud worked constructively with Glasgow 2026's other security providers rather than seeking to overstate its role. That approach helped the specialist ransomware capability fit into the wider programme and supported rapid decision-making in a high-pressure environment.

Martin Fitchie's formal thank-you recognised the wider Core to Cloud team's commitment to keeping the Games, its systems and its people safe, and the contribution made to a successful and secure Commonwealth Games.

Looking Ahead

Glasgow 2026 demonstrated how a major event can strengthen its cyber position quickly when security is treated as a layered programme rather than a single technology decision.

Specialist ransomware protection gave the organisation an additional level of assurance during its highest-risk phase. The technology complemented the SOC and other security measures, while Core to Cloud's collaborative delivery approach helped the programme move at the pace required.

The experience leaves a clear lesson for other time-critical, high-profile organisations: rapid growth does not remove the need for proportionate security. Clear priorities, specialist controls and providers who understand the wider objective can materially improve resilience without slowing delivery.

Want to learn more? Get in touch with us today
Protecting UK businesses since 2015
www.coretocloud.co.uk