CORE TO CLOUD™

THE CHALLENGE ORGANISATIONS FACE

halcyon

Ransomware incidents rarely begin with encryption. Attackers often establish a foothold, escalate privileges, and prepare for disruption long before encryption is triggered. Many organisations only become aware of an attack once systems are already unavailable, forcing urgent, high-stakes decisions under pressure.

A CHANGED RANSOMWARE THREAT LANDSCAPE

Modern ransomware is designed to evade controls and delay detection. Encryption is typically the final step in a multi-stage attack, and data theft or extortion pressure may begin before disruption is visible. The difference between a contained event and a major incident often comes down to whether ransomware activity is stopped before encryption or exfiltration.

WHAT HALCYON DELIVERS

Halcyon is purpose-built ransomware protection designed to stop attacks before they cause business impact. It focuses on ransomware-specific behaviours and execution paths, with the aim of preventing encryption and disrupting ransomware activity early, reducing the likelihood of downtime, recovery disruption, and extortion-led decision-making.

WHY PARTNER WITH CORE TO CLOUD FOR RANSOMWARE PROTECTION

Core to Cloud brings deep expertise in ransomware prevention and real-world attack disruption, helping organisations use Halcyon effectively to stop ransomware before encryption and business impact occur.

Beyond the technology itself, we provide commercial support and guidance throughout the journey, from early scoping and stakeholder alignment to deployment and ongoing optimisation.

Our role is to ensure Halcyon is implemented in a way that reflects how modern ransomware operates, so protection is put in place quickly, confidently, and with clear ownership, rather than treated as a standalone tool.

THE OUTCOME

With ransomware controls designed to operate earlier in the attack lifecycle, organisations reduce the likelihood of widespread encryption, prolonged outages, and crisis-driven decisions.