



Managed Cybersecurity

Build a robust, fit-for-purpose cybersecurity defence that evolves with the specific threat landscape your business faces. Reduce unnecessary downtime, protect operations and data, and make cybersecurity spend work harder and smarter. Our proactive support **keeps cybercriminals out, and operations on** – so you can focus on being strategic



- ISO27001 accredited for data management
- UK helpdesk and engineers available 24/7
- Solutions by Darktrace, Bluedog, Mimecast, KnowBe4 and more
- Focus on driving business value from staying secure



Managed SOC

Reduce the time taken to neutralise security threats and prioritise incidents based on business impact. Managed SOC aggregates data from all IT infrastructure and correlates into alerts and comprehensive reports in one platform. Risks are rapidly analysed and escalated to Sentis or an automated countermeasure.



Managed Anti-ransomware

Avoid ransomware-induced failures, downtime and financial loss with the help of a fully managed anti-ransomware solution. Identify and block known and unknown strains across every networked device. Patch installation and management proactively seals cracks in networks.



Managed Antivirus

Protect data from loss, theft and corruption with an advanced business antivirus. Machine Learning and AI capabilities block day-zero and never-before-seen threats, and diffuse encrypted malware hiding in files. Monitoring and maintenance ensure antivirus is tailored to your threat level.



Threat Detection and Response

Achieve total security posture clarity by combing security activity and data from every resource in your IT infrastructure. Includes Endpoint Detection and Response (EDR), Network Detection and Response (NDR) and Security Information and Event Management (SIEM) to rapidly identify and isolate covert threats.

Managed Cybersecurity



Next Generation Firewall

Protect systems from being compromised with a business grade firewall configured to your operational set up. Includes VPN infrastructure for secure, private remote network access and activation on every networked device. Proactive maintenance from our experts ensures consistent high performance.



Application Whitelisting

Take total control over the workloads run on your system to minimise the security risks of shadow IT. Specify and enforce an approved index of applications or file types that have been vetted by you for business function and threat management. With breach monitoring and change management.



Threat Filtering

Make internet use safer by intercepting and blocking evasive threats hidden in emails and webpages. Prevent the internet from being an attack vector and protect staff from social engineering manipulation. Includes email security and web browser filtering with advanced sandboxing technology.



Identity Management

Prevent operational and data losses from user exploitation and misuse. Staggered, unique and automated authentication processes ensure you're in total control of who's doing what on your network. Includes MFA, Active Directory Management, BitLocker, Azure Identity and Access Management and more.



Staff Training

Defend your business from costly human error with security awareness training and accreditations tailored to your threat landscape, operations and user competency. Includes Guided Security Training Sessions, Phishing Simulation Testing via KnowBe4 and security certifications such as Cyber Essentials.



Patch Management

Maximise the lifespan, performance and security of IT infrastructure. Sentis deploys regular critical patch updates to servers, operating systems and apps to ensure infrastructure remains free from vulnerabilities and infections. Focus on strategic initiatives and leave the day-to-day to Sentis.