

Managed Protection Suite

Flexible, enterprise-grade cyber security packaged or built around your needs

Managed Protection Suite delivers enterprise-grade security backed by 24x7 SOC monitoring, managed detection and response (MDR) and identity protection. Choose a pre-configured tier or tailor a solution that aligns to your organisation's risk profile, helping keep your business secure and resilient at all times.

Who is this service for?

Managed Protection Suite is designed for organisations that want a structured, scalable approach to cyber security, without committing to a one size fits all solution.

- Organisations seeking a structured, scalable approach to cyber security
- Teams that want to avoid one-size-fits-all security packages
- Businesses balancing risk profile and operational priorities across multiple tiers
- Boards wanting clear, packaged starting points with room to grow

Three tiers of protection — pick a level, or build your own

Each tier builds on the last. Start where your risk sits today and scale up as your organisation's needs change.

Essential Protection

Continuous protection against common and emerging threats, with managed detection and response built in.

- 24x7 SOC monitoring to identify suspicious activity
- SOC-led response to contain and isolate threats
- Managed detection and response (MDR) on core systems
- Protection for identities and endpoints
- Visibility into security events and actions taken

Advanced Protection

Stronger defence against human-led attacks such as phishing and credential compromise.

Includes everything in Essential Protection, plus:

- Controls to reduce phishing and user-driven risk
- Behaviour-focused security layers to complement technology controls
- Enhanced reporting to support decision-making and governance

Complete Protection

For organisations with higher security, compliance or operational risk exposure.




Includes everything in Advanced Protection, plus:

- Controls designed to stop advanced attacks before they can execute
- Increased protection around privileged access and critical systems
- Stronger preventative measures aligned to zero trust principles

Build a tailored solution

Components from any tier can be mixed to create a custom package. Speak to your account manager to define the right approach for your business.

Business benefits

-  Faster detection and response to security incidents, reducing disruption, data exposure and overall business impact.
-  Lower risk from human-led attacks, minimising the likelihood of phishing, credential misuse and user-driven incidents.
-  Stronger protection for critical systems, safeguarding key applications, devices and user access from cyber threats.
-  Greater confidence in identity security, reducing the risk of unauthorised access and account compromise.
-  Earlier visibility of emerging risks, enabling quicker action before potential issues escalate.

Minimum 12-month term applies. Onboarding is scoped separately and dependent on your environment. Components can be mixed across tiers to create custom packages.

Why BCN?

Founded as a managed service provider, BCN is grounded in day-to-day delivery, keeping organisations secure, productive and supported. We're a leading Microsoft partner, and one of the first 35 globally to achieve Microsoft's Partner Designation for Support Services, recognising the strength of our service operations and our ability to support clients end to end.

