

Vulnerability Management

Qualys-powered scanning and remediation, before attackers can exploit weaknesses

BCN's Vulnerability Management service identifies security weaknesses across your environment before they can be exploited, helping you reduce risk, improve visibility and strengthen your security posture over time. The service is powered by Qualys, an industry-leading vulnerability scanning platform.

Who is this service for?

Vulnerability Management is designed for organisations that want greater control and confidence over their security posture, without adding unnecessary operational burden. It's well suited to organisations that need:

- Clear visibility of vulnerabilities across their full IT environment
- A risk-based approach to prioritising remediation
- Practical evidence to support Cyber Essentials, audits and security reviews
- Flexibility to choose between reporting-only or managed remediation
- Measurable insight into remediation progress and time to fix

Choose the right level of service

Two service tiers, both powered by Qualys, designed to match how much of remediation your team wants to keep in-house.

Scan and Report (Lite)

For organisations that want clear visibility and prioritisation, while keeping remediation within their own teams.

- Regular Qualys-powered vulnerability scanning
- Coverage across workstations, servers and public-facing assets
- Risk-based vulnerability assessment
- Monthly executive summary reporting
- Remediation guidance and prioritisation

Recommended

Vulnerability Management & Remediation (VMR)

For organisations that want vulnerabilities actively managed and resolved as part of an ongoing service.

- Initial vulnerability assessment and analysis
- Ongoing Qualys scanning and risk-based prioritisation
- Identification of end-of-life and unsupported software
- Tracked time-to-remediate targets
- Monthly executive reporting
- Ongoing remediation delivered as part of the service

Required for organisations pursuing Cyber Essentials Plus, where remediation must be evidenced.

Business benefits



Reduced business risk: proactively identify and address vulnerabilities before they lead to disruption, data loss or security incidents.



Improved operational resilience: regular scanning and prioritised remediation reduce avoidable outages and improve the stability of critical systems.



Better decision making for leaders: clear, prioritised insight into security risk helps leadership focus investment and effort where it has the greatest impact.



Lower burden on internal teams: structured vulnerability management removes the need for ad hoc investigation and manual tracking by internal IT.

Service scope and remediation coverage depend on your environment and agreed service boundaries. Onboarding and initial remediation scoping are completed at service initiation.

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.

