Article

Mar 2026

What are your technical security assessment options?

A penetration test can be a great way to identify security vulnerabilities or misconfigurations on an organisations network through a controlled cyberattack simulation, where security experts act as attackers.

However, for smaller organisations penetration tests can be expensive and not always the most cost-effective solution to improving security posture. Setting effective test objectives is challenging for those new to testing, and it can be difficult to decide which of the various type of penetration test is most appropriate (network, web application, breach attack simulation, etc.) and aligns with business priorities.

An alternative assessment

This doesn't mean organisations shouldn't conduct technical testing, potentially leaving themselves exposed to unknown risk – just find an alternative that works for them.

A technical security assessment can be an affordable, targeted alternative to a first penetration test, providing assurance and identifying improvements to an organisation's security posture through automated scans and targeted manual testing.

A technical security assessment typically covers:

- External network vulnerability assessment
- Cyber Essentials Plus-aligned service review
- Internal authenticated network vulnerability assessment
- Active Directory configuration review
- Microsoft 365 configuration review

This assessment provides a holistic review of your technical security controls, with a final report identifying risks and actionable steps to enhance security and implement an effective risk remediation strategy. The results can also be used to inform future testing objectives and scope for technical assessments including full penetration tests, ensuring that those tests deliver the maximum value with the low hanging fruit already identified and remediated.