

Managed security services checklist

A managed security provider watches your systems around the clock so you don't have to. These answers show which services you need and which you already have.

01 What is your biggest security concern today?

Ransomware, email fraud, data theft, compliance or remote workers.

02 How would a breach affect your business?

Lost revenue, customer trust, regulatory penalties or downtime.

03 Where does your sensitive data live?

Office servers, AWS, Azure, Google Cloud, Microsoft 365 or other cloud apps.

04 Which protections do you have today?

Firewall, endpoint protection, email filtering, web filtering, multi-factor sign-in or monitoring (SIEM).

05 Have you had a recent security audit, penetration test or vulnerability scan?

Yes, with results you could share later, or no.

06 Does your team have the time and skills to monitor alerts?

Yes, partly or no.

07 Do you have current security contracts, and when do they end?

Tools and providers often renew on different dates.

Rough answers are fine, and "not sure" is a useful answer. Please don't send account numbers, passwords or full bills; if we need to look at a contract, we'll arrange a safe way to share it.