The SME Cyber Security Vendor Evaluation Framework

A Practical System for Choosing the Right Cyber Security Vendor

Executive Summary

SMEs face an overwhelming cyber security market filled with identical-sounding claims, inconsistent pricing, and unclear evidence. This framework provides a structured, defensible way to evaluate vendors based on business fit, technical capability, compliance, support, cost clarity, and long-term risk.

The framework includes three core guides plus an interactive scorecard:

- **Part 1:** Why Choosing a Cyber Security Vendor Is Hard
- **Part 2:** How to Compare Vendor Claims
- **Part 3:** Turning Evidence Into a Clear, Confident Decision
- **Interactive Scorecard:** A weighted scoring model SMEs can use immediately

Part 1 — Why Choosing a Cyber Security Vendor Is Hard

The SME Reality

- Vendors sound identical
- Claims are difficult to verify
- Pricing is inconsistent
- Support quality varies widely
- SMEs lack time and internal expertise

The Core Problem

SMEs are forced to make high-risk decisions with incomplete information.

Part 2 — How to Compare Vendor Claims

What to Ask For

- Evidence of capability
- Integration documentation
- Compliance certificates
- Support SLAs
- Pricing breakdowns
- Roadmap visibility

What to Watch For

- Vague answers
- Missing documentation
- Over-promising
- Hidden costs

Part 3 — Turning Evidence Into a Clear, Confident Decision

The Decision Model

1. Gather evidence
2. Score each category
3. Apply weighting
4. Compare vendors
5. Make a defensible decision

The Outcome

A structured, repeatable process that reduces risk and increases confidence.

Interactive Scorecard

A 7-category weighted model covering:

1. Business Fit
2. Technical Fit
3. Compliance
4. Support
5. Onboarding
6. Cost Transparency
7. Risk & Accountability

Conclusion

This framework gives SMEs a practical, evidence-based way to choose the right cyber security vendor — without needing technical expertise.