SECURITY STACK COST REVIEW

COST CONSOLIDATION SCORECARD

VYFORITY
ARCHITECTING RESILIENCE
CAPITAL EFFICIENCY

10 QUESTIONS
Each "No" is a direct cost recovery opportunity.

SCORE BELOW 6?
An independent audit is worth the conversation.

Q 01–06 — STACK EFFICIENCY

Six categories of waste — most mid-market organisations carry at least three.

- ☐ **Q1. No Duplicate Capability**
  You can list every active security tool and confirm no two perform the same primary function. **Overlap is the most common — and easiest — waste to eliminate.**

- ☐ **Q2. All Tools Fully Deployed**
  Every licensed tool is fully deployed — none are partially implemented or still awaiting rollout. **Partial deployments cost the same as complete ones.**

- ☐ **Q3. No Zombie Subscriptions**
  You have cross-referenced your IT General Ledger against active log sources in the last 90 days to identify billing for inactive tools. **Ask your team — they'll name two immediately.**

- ☐ **Q4. Licensing Reflects Reality**
  Licensed seat counts and enterprise agreements reflect current active users and hybrid-workforce realities, not peak historical headcount. **Overprovisioning typically runs 20–30% above actuals.**

- ☐ **Q5. Mapped to Specific Controls**
  Every active tool is explicitly mapped to a specific, required security control or threat scenario. **Nothing exists merely "just in case" or because it is a current buzzword.**

- ☐ **Q6. No Premium Feature Bloat**
  You aren't paying for premium licensing tiers (e.g., Microsoft E5) for capabilities that remain unconfigured. **Downgrading tiers saves instantly.**

Q 07–08 — GOVERNANCE & ACCOUNTABILITY

Tools with no named owner cost the same as tools that are actively managed.

- ☐ **Q7. Every Tool Has a Named Owner**
  Each tool has a named individual accountable for maintenance, patching, and reviewing its outputs. **No owner means no one noticing the cost.**

- ☐ **Q8. Alerts Are Acted On**
  Every tool generating alerts has someone actively reviewing and acting on that output. **DLP and SIEM consoles with unread alerts are the most expensive shelfware.**

Q 09–10 — ADVISOR INDEPENDENCE

The advisor managing your stack has a financial interest in its size. Does yours?

- ☐ **Q9. Your Advisor Earns No Vendor Margin**
  Your MSP or IT advisor doesn't earn margin, referral fees, or vendor incentives on the tools they manage. **If they do, their recommendation and your cost optimisation conflict.**

- ☐ **Q10. Your Stack Has Had an Independent Review**
  The most telling question. Reviewed by an advisor with no financial relationship with any current vendor — whose only interest is your cost efficiency.

TYPICAL FINDINGS — WHAT AN AUDIT UNCOVERS

Three patterns appear in almost every mid-market stack review.

THE PHANTOM TOOL

A DLP, SIEM, or email platform generating alerts for months with no recipient acting on the output. The licence renews. **You are paying for the appearance of protection.**

THE MSP OVERLAP

Two endpoint protection platforms running simultaneously — one from the previous IT team, one added by the incoming MSP. **Combined waste: $20K–$40K per annum.**

THE FROZEN CONTRACT

An enterprise-tier contract signed three years ago for a headcount that no longer exists. Auto-renewal processed without review. **The vendor was not going to raise it.**

HOW DID YOU SCORE?

10/10	Exceptionally well-managed. Your stack is optimised.
6–9/10	Identifiable gaps. An audit will quantify the recoverable cost.
<6/10	**Active cost exposure. An audit will pay for itself.**

THE SECURITY STACK COST AUDIT

Structured, independent review of your entire security stack. Kill list & vendor negotiation brief delivered. **Fixed fee — $12,500.**

THE GUARANTEE: We identify at least $20,000 in annual savings, or this assessment is free.

SCHEDULE YOUR FISCAL AUDIT →

DEAN KASTELEC | FORMER ENTERPRISE CISO | KPMG DIRECTOR