MDR SECURITY VENDOR CHECKLIST

Questions to ask when evaluating a managed detection and response (MDR) vendor

Finding the right MDR provider isn't just about choosing a vendor — it's about securing a true partner who empowers your team to focus on what matters most. Sophos MDR hits the mark on these key evaluation factors.

What security control points and attack vectors do the provider's analysts have visibility of?
Broader visibility means stronger protection against multi-stage attacks. Sophos MDR covers Endpoint, Network, Firewall, Cloud, Email, Identity, Backup, and Productivity tools.

Will their solution integrate with your existing IT tech stack and cybersecurity defenses?
Avoid costly rip-and-replace headaches — Sophos MDR offers 350+ integrations, including direct Microsoft compatibility, for seamless protection.

What is the typical response time for their team to remediate to threats?
Ransomware can unfold in minutes, turning delays into million-dollar losses. Sophos MDR's average time to detect, investigate, and remediate a threat is 38 minutes, 96% faster than the industry average in-house SOC.

What levels of service and interaction do they offer?
MDR isn't one-size-fits-all. Requirements vary by organization size, budget, industry, and team. Sophos MDR provides a range of service tiers and threat response modes to suit your needs.

Do they include comprehensive incident response as standard that fully remediates threats and provides root cause analysis?
Detection and alerting isn't enough. Swift action is needed to contain and fully remediate threats before they escalate. Sophos MDR includes unmetered full-scale incident response.

Ready to get started on your MDR journey? Visit sophos.com/stop-threats to speak to an expert now.

SOPHOS

2025-06-24 (MP)