COMPETITIVE INTELLIGENCE

MANAGED DETECTION & RESPONSE COMPETITIVE OVERVIEW

Why managed detection & response (MDR)

- **Skilled resource gap** — Some threats can't be clearly defined as good or bad by even the best technology. MDR services can be a cost-effective way to access the necessary detection & response skills and resources without having to recruit, train, and retain internal talent.
- **Alert fatigue** — The number of alerts generated by security tools means that the humans involved fail to spot the important alerts among the noise. MDR services lend a helping hand to review, validate, and address alerts.
- **Time limitations** — Investigating alerts and hunting for undetected threats are time consuming. It takes additional time to respond effectively to a confirmed threat. With IT and security resources stretched thin, some organizations prefer to outsource these tasks, freeing up staff for other priorities.
- **24/7 coverage** — Few organizations have the in-house personnel to monitor for threats around-the-clock.

Identify the need - Use these questions to qualify MDR opportunities

- **Technology:** What solutions are you using to identify threat activity?
- **Resources:** Tell me about your security operations team.
    - Do you have resources dedicated for managing security events during nights/weekends?
    - How are you facilitating threat hunting inside the estate to look for behavior that would traditionally go undetected?
    - When you see a potential threat, what are your next steps following that detection?
- **Readiness**: Talk about your incident response preparedness plan. What do you do when a breach has occurred and unauthorized access to your hosts has been achieved?

Why Sophos MDR

- **Integration and protection –** Sophos offers a unique combination of integrations for the highest return on investment and leading native technology for the best proactive protection. Competitors typically offer one or the other, but not both.
    - **Integrations** – Sophos MDR integrates with the endpoint, network, firewall, email, cloud, and identity solutions an organization is already using – both Sophos and third-party. This means that customers do not need to rip and replace to benefit from Sophos MDR, while enabling them to get more detections and better returns from their existing security investments.
    - **Strong protection** – Sophos' combination of industry leading technology, multi-discipline human expertise, and breadth of experience enables Sophos MDR to deliver accelerated detection and response with an average resolution time of 38 minutes.
- **Instant SOC –** No need for an in-house Security Operations Centre.
    - **Fully managed response** — Sophos' response team can engage fully and take control of a threat, from detection through investigation to neutralization. Many other MDR services only notify customers of attacks or suspicious activities or require a response retainer for a limited number of response hours.
    - **Flexible response modes** — The MDR Complete response team can adapt its engagement depending on customer requirements. This means peace of mind for customers who know that they will get the help they need without any unwanted interference.
    - **Robust lead-driven and leadless threat hunting** — Sophos threat hunters use the latest intelligence and their expertise to proactively hunt for and validate potential threats.
- **Sophos Central** — Customers can view and manage their entire portfolio, as well as their MDR deployment and case history, from a single cloud-based portal.
- **Network Detection and Response (NDR)** – Sophos NDR brings in full visibility of network activity, leaving threat actors nowhere to hide. This visibility adds context and depth to investigations leading to faster resolutions and more accurate route cause analysis.

CrowdStrike (OverWatch, Falcon Complete [XDR])

Key weaknesses compared to Sophos

- **Integrations** – Sophos MDR can leverage telemetry from CrowdStrike and offer full scale incident response without having to replace the CrowdStrike products; CrowdStrike cannot offer full IR using third-party telemetry. Nor does it use it for detections. The exception is Falcon for Defender. Unlike Sophos MDR Essentials, CrowdStrike leaves remediation to the customer.
- **Proactive protection** – Sophos can provide stronger proactive protection than Falcon Prevent; the CrowdStrike team will have to spend more time addressing threats that got through.
- **Network enforcement** – Sophos Firewall not only acts as a network sensor but as a coordinated enforcement point. CrowdStrike lacks firewall appliances to complement endpoint security and would need to rely on third-party solutions for network enforcement. Note: CrowdStrike has an NDR product that it does not actively promote.

Watch out for

- CrowdStrike has strong EDR tools that allow customers with SOCs or skilled security analysts to perform their own investigations and hunting, as well as to see the same signals that the OverWatch team sees. Our XDR is already strong, with an aggressive roadmap to improve detection and investigation workflows. Meanwhile, most MDR customers will be happy to leave the more technical work to the Sophos MDR team.

SentinelOne (Vigilance Respond, Singularity MDR)

Key weaknesses compared to Sophos

- **Integrations** – Vigilance Respond doesn't support third-party product telemetry. While Singularity MDR *can* integrate with select 3rd party tools, it uses the additional data only to "enrich" its own 1st party detections.
- **Managed response** – Sophos MDR Complete includes unlimited IR at no additional cost, throughout the subscription term. 'Vigilance Respond' and Singularity MDR' SKUs provide only push-button response. 'Vigilance Respond Pro' and 'Singularity MDR + DFIR' SKUs include incident response, but only for a fixed number of hours that expire after a year. Both require installing additional tools to take advantage of IR.
- **Proactive protection** – Sophos Endpoint provides stronger proactive protection than SentinelOne. SentinelOne's MDR team will have to spend more time addressing threats that got through.

Watch out for

- SentinelOne is strong on automated remediation and rollback.

Arctic Wolf

Key weaknesses compared to Sophos

- **Native technology** – In addition to third-party integrations, Sophos MDR is fully integrated with the native Sophos endpoint agent, Firewall, Email, NDR, and Cloud Optix, easing deployment and enforcement. Arctic Wolf adds its own components that don't integrate with a customer's existing security solutions.
- **Managed response** – Sophos MDR always includes hands-on-keyboard remediation. MDR Complete also includes incident response. Arctic Wolf does not provide complete managed response, only recommendations and, with the optional Aurora EP/EDR, protection and push-button response.

Watch out for

- Arctic Wolf recently acquired Cylance which adds the Aurora endpoint.

Microsoft (Defender Experts for Hunting / XDR, Experts on Demand)

Key weaknesses compared to Sophos

- **Managed response** – Sophos MDR Essentials includes authorized response actions. The Defender Experts for Hunting service does *not* include managed response, only hunting/detection and alerting.
- **Incident response** – Sophos MDR Complete includes uncapped incident response. Microsoft Experts for XDR will not handle an active incident, this is handled by a separate IR service.
- **Instant SOC** – Sophos MDR can effectively play the role of an outsourced SOC. Microsoft assumes that a customer has its own SOC, Defender for Endpoint (formerly ATP) *and* premium support, which may be cost-prohibitive for some customers, on top of the cost of running own SOC
- **Third-party product support and NDR** – Unlike Sophos MDR, Microsoft will not offer detection and response based on third-party product data. Nor does Microsoft have the capability to add network detection and response for analyzing both clear and encrypted network traffic.
- **Detections -** Sophos MDR for Microsoft Defender allows customers who choose to continue using the Defender endpoint to gain additional detections from Sophos along with third-party product driven detections. This provides more detections with higher fidelity than Microsoft can offer.

Watch out for

- Microsoft Defender for Endpoint allow customers with existing SOCs or security analysts to perform their own investigations and hunting, as well as to see the same signals that the Defender Experts team sees. In addition, Microsoft aggressively promotes licensing bundles that include Defender for Endpoint.

For an MDR service to be truly effective in practice, it needs to cover several key areas. Any gaps could increase dwell time, reduce responsiveness, and impair visibility.

Capability	**Sophos**	Arctic Wolf	CrowdStrike	SentinelOne	Microsoft
Endpoint Protection (EP)	●	●	●	●	●
Cross-Layer Detection and Response (XDR)	●	●		●	●
Incident Response	●		+	+	+
Hands-On-Keyboard Remediation	●		●	●	+
Network Connector	+	+			
NDR	+	+			
MDR Third-party product integrations	●	●	●*	●#	

+ = elective components (requires add-on or separate product); *MS Defender and non-endpoint only, # Singularity MDR only

Watch out for: Guarantees and warranties

Some competitors attract customers with warranties that aim to instill a sense of confidence. These often come with fine print that makes them unlikely to pay out and, if they do, at a lower amount than advertised. Buyer beware!

Sophos Rapid Response

Sophos Rapid Response provides fast assistance with the identification and neutralization of *active* threats against any organization. After completion, the organization can seamlessly transition to become a Sophos MDR customer.

Why Sophos Rapid Response

- **Rapid identification and neutralization** — The Sophos RR team will get to work right away, often within hours, to identify and eject the adversary. Other vendors may take days.
- **Predictable pricing** — Rapid Response is sold as a fixed 45-day term license. This takes away the risk of hourly billing and runaway costs, as our incentives are aligned with the customer's: to get the customer out of danger as quickly as possible. Vendors who bill customers by the hour do not have the same incentive for swift action.
- **Post-incident threat summary** — The Sophos Rapid Response team provides you with a formal summary of its investigation, detailing the actions it took and the discoveries it made, as well as recommending long-term guidance on how to mitigate a reoccurrence of similar threats in the future.
- **Ongoing detection and response** — After remediating the initial threat, the Sophos MDR team continues to provide monitoring, detection, and response through the remainder of the 45-day term. Some competitors stop service when the incident is resolved or only provide detection (not remediation) for the remainder of the term.

Contact Sophos Rapid Response

rapidresponse@sophos.com

Australia: +61 272084454
Canada: +1 7785897255
France: +33 186539880
Germany: +49 61171186766
United Kingdom: +44 1235635329
USA: +1 4087461064

CrowdStrike (Endpoint Recovery Services)

Key weaknesses

- A shorter term (30-day) contract means customers will have a shorter period of post-remediation monitoring.
- Path to long-term managed service (Falcon Complete) may be more expensive and disruptive, as it requires turning over day-to-day management of endpoint protection to CrowdStrike.

Watch out for

The fixed-term model is similar to Sophos Rapid Response. CrowdStrike can also deliver additional incident response services with forensic evidence for insurance or legal claims (DFIR) at additional cost. Due to existing relationships, some insurers may prefer or recommend CrowdStrike.

Mandiant - Google Cloud (Incident Response Services)

Key weaknesses

- Only available on a per incident or per hour basis (or as a retainer)
- Single remediation response with no ongoing monitoring
- Due to the split from FireEye, Mandiant no longer can offer its own endpoint protection as part of MDR for customers that want to transition after the incident is complete

Watch out for

The Mandiant service is well-known and established. Responders are available in 30 countries around the world for on-site visits. Strong cloud expertise under new Google Cloud ownership.

Palo Alto Networks (Crypsis – Data Breach Response Services)

Key weaknesses

- Appears to provide only a single remediation response billed by period, not an ongoing contract
- Endpoint and response products are separate; the PAN endpoint product provides less effective proactive protection than Intercept X
- Crypsis teams are not fully integrated in Palo Alto technology or operations yet

Watch out for

Crypsis is a well-established player in the MDR and incident response market, with additional services such as litigation support available.