Sophos XDR vs. MDR

When to position Sophos XDR vs. Sophos Managed Threat Response

Extended Detection and Response (XDR) Intercept X Advanced with XDR

Overview

- Do it yourself threat hunting and detection
- Built on the world's best endpoint protection
- Add expertise, not headcount with intelligent XDR
- First XDR build for security analysts and IT admins

Why Customers Choose Sophos XDR

- Believe they can conduct threat hunting and security operations in-house
- IT operations to maintain hygiene
- Move from reactive to proactive IT and security operations
- Less expensive than MTR

Proof Points and Stats

- #1 - Sophos XDR has more customers than anyone (over 15K)
- "With 51% of organizations using EDR, and another 31% considering doing so in the near future, it has become a core capability for endpoint security" – ESG Research[1]

Discovery questions

- Have you heard of EDR or XDR Are you familiar with threat hunting?
- If you haven't bought an EDR or XDR tool why not?
- Are you aware of managed detection and response (MDR) services?
- How big is your team? How many are dedicated to security?
- Do you have the resource to conduct threat hunts, investigations, and response actions to identified threats?
- If you were going to search for an active adversary in your network how would you go about that?
- How long does a typical response to a threat take you? What steps do you take?
- What happens if a threat hits at 3am on a Sunday morning?

Managed Detection and Response (MDR) Sophos Managed Threat Response (MTR)

Overview

- Threat detection and response done for you
- 24/7 human-led threat hunting
- Investigates suspicious activity, not just detections
- Others stop at notification, Sophos takes action

Why Customers Choose Sophos MTR

- Looking for the best protection available
- Lack time and expertise to conduct threat hunting and security operations in house
- Peace of mind knowing MTR team is monitoring
- Costs less than building their own SOC

Proof Points and Stats

- Overe 2,000 organizations protected
- "34% of organizations say their biggest challenge is that they lack skilled resources to investigate a cybersecurity incident involving an endpoint to determine root cause" – ESG Research[1]
- By 2025, 50% of organizations will be using MDR services (up from less than 5% in 2019) – Gartner[2]

[1] https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1

[2] Gartner, Market Guide for Managed Detection and Response Services, 26 August 2020, Analysts: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

SOPHOS