Sophos Managed Detection and Response
Extending protection beyond Microsoft Defender

Microsoft Defender

Endpoint Protection

- Antivirus protection for Windows
- Exploit mitigations
- Endpoint Detection and Response (EDR) tool
- Active adversary mitigations

Why you need it

- Endpoint protection is an essential foundation for effective cyber defense, automatically stopping threats from impacting your business.

MDR Sophos MDR

24/7 Monitoring

- 500+ threat and malware specialists supporting your organization.
- Follow-the-sun support from seven global SOCs (Australia, India, Europe, North America).

Why you need it

- Attackers work when you don't: 91% of ransomware attacks start outside business hours.*
- Attackers are *FAST*, taking on average 16 hours to reach AD (Active Directory).

Expert Threat Response

- Sophos analysts monitor, investigate, and respond to Defender alerts, taking immediate action to stop confirmed threats.
- Human-led threat hunting and Sophos threat intelligence add additional layers of defense.

Why you need it

- Threat response is HARD: 71% of IT teams don't know which alerts to investigate.**
- Threat response takes TIME: 64% of teams want to free-up time for strategic issues.**

Non-MSFT Telemetry

- Integrate telemetry from your non-Microsoft tools.
- Detect and stop attacks across your entire environment.
- Includes Email, Firewall, Identity, Network, Cloud, and Productivity integrations.

Why you need it

- Adversaries exploit any security weakness they can find and then move around your environment.
- Increase return on your existing security investments.

Gartner Peer Insights Customers' Choice 2023

The top-rated and most reviewed MDR service, and Gartner "Customers' Choice" for Managed Detection and Response Services

G2 Leader

The Overall Top-Rated Managed Detection and Response Service as rated and reviewed by customers on G2

MITRE ATT&CK

A top performing vendor in the MITRE ATT&CK Evaluations for Managed Security Services

SOPHOS