Solution Brief

Sophos MDR for Microsoft Defender
Expert-led threat response for Microsoft environments

Sophos Managed Detection and Response (MDR) for Microsoft Defender monitors your IT environment 24/7 to detect and stop sophisticated cyberattacks that bypass Microsoft security tools. Sophos threat analysts proactively hunt for signs of adversary activity and effectively respond to Microsoft security alerts, enabling your team to focus on initiatives that drive growth for your business.

Use Cases

1 | 24/7 THREAT MONITORING

Desired Outcome: Extend your in-house team with Microsoft Certified experts who respond to threats on your behalf.

Solution: The Sophos MDR team includes Microsoft Certified Security Operations Analysts specializing in detecting and responding to advanced cyberattacks using custom Microsoft response playbooks. Sophos provides the people, processes, and technology to monitor 24/7 and stop threats using data from your existing solutions, freeing up your internal teams to focus on business enablement.

2 | STOP THREATS MICROSOFT SECURITY TOOLS MISS

Desired Outcome: Detect and neutralize cyberattacks that Microsoft technologies alone cannot stop.

Solution: Sophos MDR uses proprietary threat detection rules and world-class threat intelligence to identify sophisticated adversary activities that may bypass Microsoft security tools. Using turnkey Microsoft integrations, Sophos can protect your organization from attacks including business email compromise (BEC) even without a Microsoft E5/A5 subscription.

3 | EXTEND VISIBILITY ACROSS ATTACK SURFACES

Desired Outcome: Integrate an extensive range of Microsoft and non-Microsoft solutions.

Solution: Leverage telemetry from Sophos products, Microsoft tools, and dozens of other vendors including endpoint, firewall, network, email, cloud, identity, productivity, and backup solutions, to extend visibility and stop attacks across your entire IT environment.
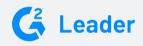
4 | DRIVE MORE BUSINESS VALUE

Desired Outcome: Balance cybersecurity risks and investments against business value and outcomes.

Solution: Sophos MDR for Microsoft Defender helps you balance the need to protect with the need to run your business. Get more ROI from your existing security investments and improve cyber insurance eligibility and premiums. Sophos helps meet essential insurance requirements such as 24/7 monitoring and Endpoint Detection and Response, mitigating risk to your business.

Gartner Peer Insights Customers' Choice 2023

A Customers' Choice in the 2023 Gartner®, Voice of the Customer for Managed Detection and Response Services report

G2 Leader

Rated the Number 1 MDR solution by customers in the G2 Winter 2024 Grid Reports

IDC

A Leader in the 2024 IDC MarketScape for Worldwide Managed Detection and Response Services

To learn more, visit
sophos.com/mdr-microsoft

SOPHOS