Sophos MDR for Microsoft Defender

Expert-led Threat Response for Microsoft Environments

Sophos Managed Detection and Response (MDR) for Microsoft Defender extends your team with highly skilled experts who monitor, investigate, and respond to Microsoft Security alerts 24/7.

Maximize Your Microsoft Security Investment

Many organizations have invested in the Microsoft Security suite but may not have enough in-house expertise to effectively use Microsoft's multi-product technology stack to detect, investigate, and respond to hundreds of security alerts every day:

- The global shortage of cybersecurity practitioners has reached 3.4 million[1].
- 71% of security teams find it difficult to determine which security alerts to investigate among the noise generated by their tools[2].
- The median threat response time for organizations with a dedicated security operations team is 16 hours, leaving attackers significant time to operate within the network[3].

Sophos MDR for Microsoft Defender provides the most robust threat detection, hunting, and response capabilities available for Microsoft environments. Our analysts monitor, investigate, and respond to Microsoft Security alerts 24/7, executing immediate, human-led response actions to stop confirmed threats with an industry-leading average threat response time of 38 minutes—96% faster than the industry benchmark.

Detect and Stop Threats Beyond Microsoft Defender

With Sophos MDR for Microsoft Defender, our Microsoft Security experts detect, investigate, and respond to threats using security data from the following Microsoft products:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- 0365 Security & Compliance Center
- Microsoft Sentinel
- Office 365 Management Activity

In addition, our proprietary detections, world-class threat intelligence, and human-led threat hunts add additional layers of defense, identifying and stopping more threats than Microsoft Security tools can on their own.

Organizations can also integrate non-Microsoft security tools and telemetry sources from Sophos solutions or dozens of other vendors such as Palo Alto Networks, Fortinet, Check Point, AWS, Google, Okta, Darktrace, and more for complete visibility and protection.

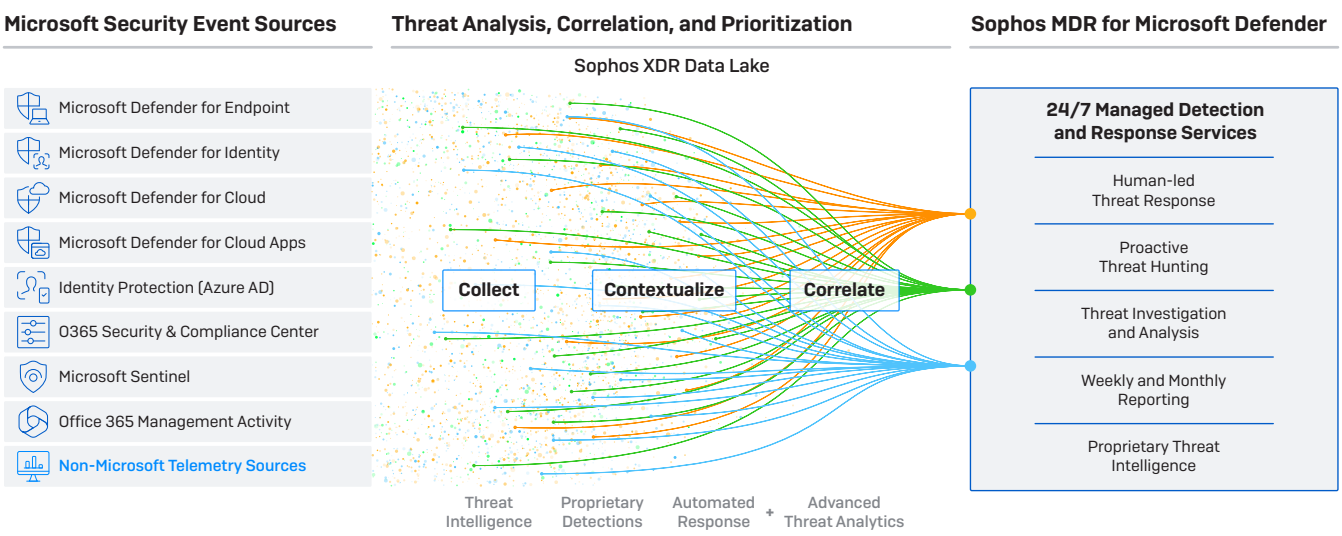
Highlights

- Sophos MDR analysts monitor, investigate, and respond to Microsoft Security alerts 24/7, taking immediate action to stop confirmed threats
- Service capabilities extend beyond Microsoft Defender for Endpoint and Microsoft Sentinel to provide coverage across the Microsoft Security platform
- When an active threat is identified, the Sophos MDR operations team can execute an extensive set of threat response actions on your behalf
- Proprietary Sophos detections, threat intelligence, and human-led threat hunts add additional layers of defense
- Integrate non-Microsoft tools and telemetry sources to stop attacks targeting your network, your users, and your customers

1 2022 Cybersecurity Workforce Study, (ISC)2
2 The State of Cybersecurity 2023: The Business Impact of Adversaries, Sophos
3 Gartner Cybersecurity Business Value Benchmark database, 2022

SOPHOS

Sophos MDR for Microsoft Defender: Key Service Capabilities



24/7 Threat Monitoring

Our Microsoft Security experts detect and stop threats before they can compromise your data or cause operational disruption. Backed by six global security operations centers (SOCs), Sophos provides around-the-clock coverage.

Human-Led Threat Response

The Sophos MDR team can execute an extensive set of threat response actions on your behalf to disrupt, contain, and eliminate attackers. Threat response actions can include:

- Isolating host(s) utilizing Sophos Central
- Applying host-based firewall IP blocks
- Terminating processes
- Forcing log off user sessions
- Disabling user accounts
- Removing malicious artifacts
- Adding malicious hashes to blocked items in Sophos Central

Proactive, Human-Led Threat Hunting

Proactive threat hunts performed by highly-trained analysts uncover and rapidly eliminate threats and identify attacker behaviors that evaded detection from deployed toolsets.

Compatible with Non-Microsoft Security Tools

Sophos MDR can integrate non-Microsoft security tools and telemetry sources to detect and stop attacks across your entire environment.

Weekly and Monthly Reporting

Real-time alerts, reporting, and management options are readily available in Sophos Central, while weekly and monthly reports provide insights into security investigations, cyberthreats, and your organization's security posture.

Monthly Threat Intelligence Briefings

Delivered by the Sophos MDR team, the "Sophos MDR ThreatCast" is a monthly briefing that provides insight into the latest threat intelligence and security best practices.

Proprietary Detections

Proprietary detections, advanced threat analytics, and world-class threat intelligence built into the Sophos platform add additional layers of defense, identifying more threats than Microsoft Security tools can on their own.

To learn more, visit:

sophos.com/microsoft-defender

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

23-07-10 DS-EN (DD)

SOPHOS