SOPHOS

Strengthen Microsoft Defender with Sophos MDR

Reduce cyber risk, increase the efficiency and impact of security investments, and improve insurability by strengthening Microsoft Defender with 24/7 human-led threat detection and response from the world's most trusted MDR service provider.

A Sophos Whitepaper. July 2023

Introduction

Endpoint security is an essential layer of protection, but it can't stop every threat. Today's sophisticated adversaries increasingly deploy stealthy tactics, techniques, and procedures (TTPs) to avoid being blocked by security technologies, including exploiting unpatched vulnerabilities, leveraging stolen credentials, and abusing legitimate IT tools.

To stop advanced ransomware attacks and breaches it's essential to supplement Microsoft Defender with 24/7 human-led detection and response. However, the sheer volume of alerts generated by Microsoft security technologies together with the complexity of the threat environment make security operations a resource-sapping uphill task for most companies.

As a result, organizations are increasingly turning to Sophos, the world's most trusted and highest rated Managed Detection and Response (MDR) provider, to strengthen Microsoft Defender. Sophos analysts monitor, prioritize, and respond to Microsoft security alerts 24/7, taking immediate action to stop confirmed threats. They also use proprietary Sophos detections, threat intelligence, and human-led threat hunts to detect and stop threats beyond Microsoft Defender.

Sophos MDR is designed to meet you where you are, working with your existing IT and security investments, and your in-house resources. Whether you're looking to supplement your internal team with additional expertise, extend your cyber defenses with full "out of hours" coverage, or fully outsource threat detection and response, Sophos MDR can help you achieve superior cybersecurity outcomes.

Strengthen Microsoft Defender with Sophos MDR

✓ Reduce cyber risk

- Stop advanced ransomware attacks and breaches, including human-led threats that bypass Microsoft Defender

✓ Increase efficiency and impact of security investments

- Free-up IT resources for strategic program delivery
- Reduce the likelihood of incurring major incident recovery costs
- Get more return from your existing investments

✓ Improve insurability

- Access improved insurance offers that recognize and reward your reduced cyber risk

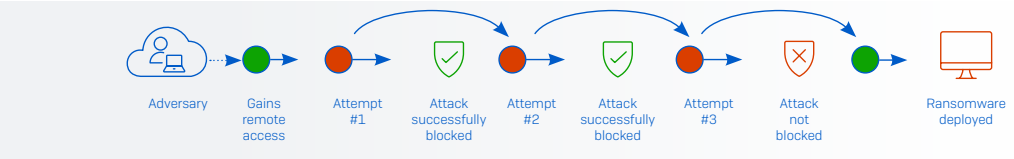
Adversaries Don't Break In – They Log In

The reality is that technology solutions alone, including Microsoft Defender, cannot prevent every cyberattack. Active adversaries are threat actors who adapt their tactics, techniques, and procedures (TTPs) on the fly using real-time, hands-on-keyboard actions in response to actions by security technologies and defenders, and as a means to evade detection.

These attacks, which often result in devastating ransomware and data breach incidents, are among the hardest to stop. They have also become highly prevalent, with 23% of small and mid-sized organizations reporting that their organization experienced an attack involving an active adversary in the last year. Reflecting the potential devastation of these attacks, 30% of IT/cybersecurity leaders consider active adversaries one of their top cyberthreat concerns for 2023[1].

Blocking active adversaries with security technology is not enough to thwart them. These skilled and persistent threat actors deploy multiple innovative approaches to achieve their goals, including:

- Exploiting security weaknesses to penetrate organizations and move laterally once inside the network, including stolen credentials, unpatched vulnerabilities, and security tool misconfigurations
- Abusing legitimate IT tools used by defenders to avoid triggering detections, including PowerShell, PsExec, and RDP
- Modifying their attacks in real time in response to security controls, by continuing to pivot to new techniques until they find a way to achieve their goals.



Example active adversary attack strategy

By emulating authorized users and taking advantage of weaknesses in an organization's defenses, malicious actors can avoid triggering automated detection technologies that struggle to differentiate between legitimate users and attackers.

Further compounding the challenge for defenders, today's well-funded adversaries also continue to innovate and evolve their business model. The recent rapid growth of the cybercrime-as-a-service model, including ransomware-as-a-service and phishing-as-a-service, has lowered the barrier to entry for would-be threat actors while making it easier to execute at scale and increasing the quality of attacks.

A consequence of these developments in the threat landscape is that the rate of data encryption due to ransomware is now at an all-time high, with cybercriminals succeeding in encrypting data in over three quarters (76%) of attacks[2].

The Reality of Ransomware

- 66% of organizations were hit by ransomware in the last year
- 76% of ransomware attacks resulted in data encryption
- 30% of attacks where data was encrypted also had data stolen
- #1 root cause of attack: exploited vulnerability (36%)
- #2 root cause of attack: compromised credentials (29%)

1 The State of Cybersecurity 2023: The Business Impact of Adversaries, Sophos.

2 The State of Ransomware 2023, Sophos.

24/7 Threat Detection and Response: A Modern Cybersecurity Essential

The good news is that by bringing together technology and human experts it is possible to stop advanced, human-led attacks. Every time an adversary takes an action, a signal is created. By combining human expertise with advanced AI-powered machine learning models and extended detection and response (XDR) tools, security analysts can leverage signals from security and IT technologies to detect, investigate, and neutralize even the most advanced human-led attacks, preventing ransomware and data breaches.

While 24/7 threat detection and response is now an essential part of any cybersecurity stack, most organizations are challenged to deliver it effectively, leaving them exposed to attack. The two most common barriers to success are a lack of expertise and a shortage of capacity.

Challenge #1: Lack of expertise

Threat detection, investigation, and response is a highly specialized activity that requires deep knowledge of attack techniques and investigation strategies, together with fluency in the tools used by defenders. Few organizations have this complex (and expensive) skill set in-house, with 93% admitting that they find the execution of essential security operations tasks challenging:

- 71% find identifying signals from noise challenging (i.e., understanding which signals/alerts to investigate)
- 71% are challenged to get sufficient data to identify if a signal is malicious or benign
- 75% say it is challenging to identify the root cause of the incident (i.e., how the adversary entered the organization)

The enormity of the challenge is made clear when you look at the data that defenders receive from their cybersecurity tools. This table contains a non-exhaustive list of Microsoft Defender events, and the event category.

Understanding the alerts is just a part of the threat detection and response process: defenders then need to apply contextual insights and threat intelligence to be able to fully understand the threat and identify the best course of action.

EVENT TITLE	EVENT TYPE
Suspicious URL clicked	Initial Access
Malicious files or network connections associated with the 3CXDesktopApp.exe process	Malware
New User Account Created	Persistence
TS_BL_Suspicious Eventlog Clear or Configuration Using Wevtutil	Defense Evasion
Process privilege escalation	Privilege Escalation
Attempt to turn off Microsoft Defender Antivirus protection	Defense Evasion
A file or network connection related to threat actor Storm-0867 detected	Credential Access
TS_BL_Script engines connecting to internet	Command and Control
Potential human-operated malicious activity	Suspicious Activity
TS_BL_Malicious Payload Download via Office Binaries	Execution
Emerging threat activity group DEV-0867 detected	Credential Access
Emerging threat activity group Citrine Sleet detected	Malware

Example case creation detections from Microsoft Defender

Challenge #2: Shortage of capacity

Threat detection, investigation, and response is a time-consuming activity. Illustrating this point, the median time to detect, investigate, and respond to an alert is nine hours in organizations with 100-3,000 employees, rising to 15 hours in those with 3,001-5,000 employees.

Dealing with security alerts consumes a huge amount of IT hours, while the urgent nature of the work can prevent teams from focusing on more strategic challenges. Plus, with adversaries executing attacks at any time of the day or night, threat detection and response needs to be performed 24/7/365 for maximum impact. Many, if not most, organizations struggle to secure the resources needed.

Solution: Supplementing defenses with Managed Detection and Response (MDR)

With 52% of IT/cybersecurity leaders saying that cyberthreats are now too advanced for their organization to deal with on their own, they are increasingly turning to specialist Managed Detection and Response providers such as Sophos to supplement and extend their in-house capabilities.

MDR Defined

Managed Detection and Response (MDR) is a fully managed, 24/7 service delivered by experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent.

Extended Detection and Response (XDR) is a platform that unifies security data from multiple sources to automate and accelerate threat detection, investigation, and response in ways that isolated point solutions cannot.

Sophos MDR analysts leverage the Sophos XDR platform to hunt for, investigate, and neutralize threats on your behalf. They leverage signals from across the IT stack, including firewall, email, cloud, and mobile security solutions, to accelerate threat detection and response.

Strengthen Microsoft Defender with Sophos MDR

Sophos MDR provides proven 24/7 threat detection and response for Microsoft Defender environments. Sophos analysts monitor, prioritize, and respond to Microsoft security alerts 24/7, taking immediate action to stop confirmed threats. They also use proprietary Sophos detections, threat intelligence, and human-led threat hunts to detect and stop human-led threats beyond Microsoft Defender.

The more we see, the faster we act. Sophos MDR leverages additional Microsoft Security event sources included in E3 and E5 licenses as well as signals from third-party firewall, cloud, email, identity, and network detection and response (NDR) investments to accelerate threat detection and response.

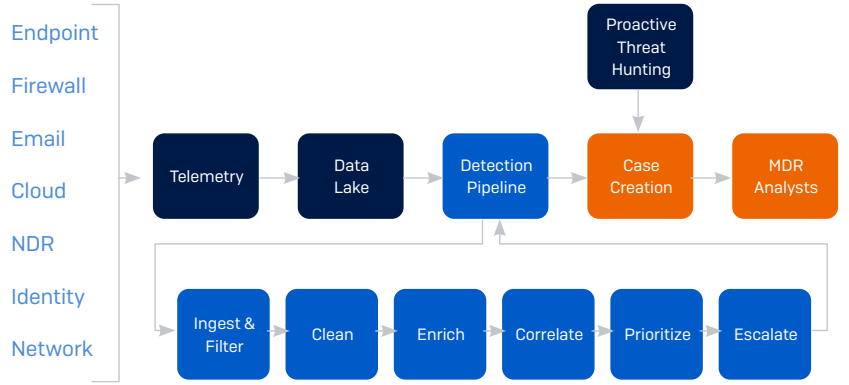
Microsoft Defender users enjoy immediate access to Sophos security operations experts by phone 24/7, as well as detailed reporting on threat activity in the Sophos Central platform.

Sophos MDR for Microsoft Defender is compatible with Microsoft Security Event Sources

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

Sophos MDR Security Event Flow

Our patented Security Event Flow is a key element of the Sophos MDR service. Telemetry from across the security environment, including Microsoft Defender, is ingested by the Sophos data lake and then processed through our detection pipeline, which converts the huge volumes of Microsoft and third-party alerts into usable, prioritized insights that enable us to investigate and respond effectively.



The Sophos MDR Security Event Flow

Ingest & Filter – Ingest telemetry and filter out unwanted noise

Clean – Transform data into normalized schema and map to MITRE ATT&CK®

Enrich – Add additional third-party threat intelligence and business context information

Correlate – Cluster alerts based on entities, MITRE ATT&CK categorization, and time

Prioritize – Score alerts and clusters to rank in order of prioritization

Escalate – Apply logic to escalates clusters into cases for investigation

24/7 coverage from seven global security operations centers (SOCs)

Threats are investigated and remediated by a global team of threat detection and response experts based out of seven global security operations centers (SOCs) across North America (Indiana, Utah, Hawaii), Europe (UK/Ireland, Germany), and Asia Pacific (India, Australia). With over 500 experts covering the entire threat environment, including malware, automation, AI, and remediation experts, Sophos MDR has a breadth and depth of expertise that is almost impossible to replicate in-house.

World-leading detection and response times

This unique combination of human, technology, and threat expertise enables Sophos MDR to deliver a world-leading incident response time of just 38 minutes that, in turn, drives superior cybersecurity outcomes:

- Mean Time To Detect (MTTD): 1 minute
- Mean Time To Investigate (MTTI): 25 minutes
- Mean Time To Respond (MTTR): 12 minutes

Who Uses Sophos MDR

Thousands of organizations across all sectors use the Sophos MDR service, from small companies with limited IT resources to large enterprises with an in-house SOC group. The three most popular Sophos MDR response models are:

- Sophos MDR completely manages threat response on behalf of the customer
- Sophos MDR works with the in-house team, co-managing threat response
- Sophos MDR supports and supplements the in-house team, alerting them to incidents that require attention and providing threat insights and remediation guidance

Threat Case: Leveraging Microsoft Defender to Detect Command-and-Control

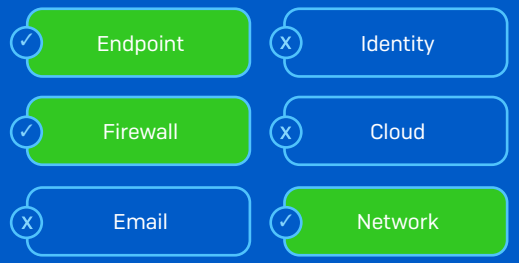
INDUSTRY
Professional Services

HEADQUARTERS
United States

EMPLOYEES
750

SERVICE TIER
Sophos MDR for Microsoft Defender

SOPHOS MDR INTEGRATED TELEMETRY SOURCES



What is Command-and-Control?

Command-and-Control (also called C&C or C2) consists of techniques that attackers use to communicate with and send commands to systems under their control within a victim network.

Command-and-control channels between a target environment and the attacker's infrastructure can be established in a variety of ways, including via phishing emails, social engineering, malware, holes in browser plugins, and more. Adversaries often use commonly available resources and mimic expected network traffic to avoid detection and suspicion.

DETECTION

Microsoft Defender generates an alert for communication to a malicious IP address.

The Microsoft alert is automatically correlated with events in the Sophos XDR data lake to determine if the attack was blocked by the customer's firewall, and whether it is impacting multiple endpoints.

INVESTIGATION

Sophos MDR analysts confirm that the malicious connection associated with the Microsoft Defender alert was blocked and the immediate threat is contained.

SophosLabs Intelix is used to identify the family of this attack, indicators of compromise (IOCs) and known IPs and domains used by the attacker.

The original Microsoft alert is enriched with this threat intelligence so it can be used for Root Cause Analysis.

RESPONSE

The compromised device is isolated, and the attack is contained.

Sophos MDR confirms initial access was achieved via email phishing. An investigation is performed to identify the composition of the phishing email and ensure no other user accounts are compromised.

Sophos provides recommendations to reduce the likelihood of successful phishing attacks in the future.

Customer Benefits

Whether you want to supplement and support your in-house security operations team or benefit from 24/7 expert-led detection and response without the operational burden of standing up your own SOC, Sophos MDR can help. Organizations that strengthen Microsoft Defender with Sophos MDR enjoy superior outcomes, including reduced cyber risk, increased efficiency and impact of security investments, and improved insurability.

Stop Advanced Threats with Microsoft + Sophos MDR

24/7 monitoring and response from a team of experts
Sophos MDR analysts monitor, prioritize, and respond to Microsoft Defender alerts 24/7, taking immediate action to stop confirmed threats

Detect and stop threats that bypass Microsoft Defender
Proprietary Sophos detections, threat intelligence, and human-led threat hunts add additional layers of defense

Enhance visibility and contextualize Microsoft Defender alerts
Integrate additional Microsoft Security event sources included in your E3 or E5 license

Get immediate access to security operations experts
Sophos MDR analysts are available by phone 24/7, and detailed reporting on threat activity is available in Sophos Central

Reduce cyber risk

One of the major advantages of strengthening Microsoft Defender with Sophos MDR is elevated protection against ransomware and other advanced cyber threats.

Sophos analysts have breadth and depth of experience together with fluency in using telemetry and threat hunting tools that is almost impossible to replicate in house. This enables them to respond quickly and accurately at all stages of the process — from identifying the signals that matter to investigating potential incidents and neutralizing malicious activities.

Sophos MDR secures more organizations than any other provider, enabling us to provide unrivalled 'community immunity'. Intel from defending one customer is automatically applied to all others with a similar profile, enabling us to proactively prevent similar attacks in that community.

★★★★★

"The pen testers were shocked they couldn't find a way in. That was the point we knew we could absolutely trust the Sophos service."

University of South Queensland, Australia

★★★★★

"With Sophos MDR, we have reduced our threat response time dramatically."

Tata BlueScope Steel, India

★★★★★

"We receive notification of any threats in real time."

Bardiani Valvole, Italy

Increase the efficiency and impact of your security investments

Sophos MDR enables you to increase the efficiency and impact of your people and your security tools.

Threat detection and response consumes vast amounts of IT capacity. Sophos MDR takes on this burden, freeing-up valuable IT resources for strategic program delivery. In parallel, 24/7 phone access to Sophos security operations experts and detailed reporting on threat activity via the Sophos Central platform accelerates in-house teams by enabling them to respond more quickly and accurately to alerts.

By using telemetry from your existing Microsoft and third-party security tools to accelerate threat detection and response, Sophos MDR elevates your defenses while enabling you to increase return on your existing investments.

Furthermore, with the average bill to remediate a ransomware attack now coming in at $1.85 million and 84% of ransomware victims saying the attack caused them to lose business/revenue[2], investing in a service such as Sophos MDR reduces the overall TCO of cybersecurity.

★★★★★

"Since implementing Sophos, we've managed to free up significant operational hours that have allowed our teams to focus on initiatives that have increased our student satisfaction."

London South Bank University, UK

★★★★★

"Sophos MDR's ability to remediate or remove threats in a swift manner and bring them to our attention frees us up to focus on high-value tasks."

Tomago Aluminium, Australia

Improve insurability

Sophos MDR enables organizations to achieve many of the cyber controls that are key to insurability and superior policy offers, including 24/7 detection and response, cyber incident response planning, logging and monitoring, and more.

Customers report improved access to insurance coverage as well as policies that recognize and reward their reduced cyber risk.

★★★★★

"Our decision to partner with Sophos for XDR and MDR was a big factor in achieving a decrease in cybersecurity premiums versus what we were told walking into this would be a doubling of those premiums. That's a big win that shows real value … I actually got a note from the CFO thanking our team for what we put together and MDR was a huge part of that."

Bob Pellerin, CISO, The Fresh Market, U.S.

2 The State of Ransomware 2023, Sophos.

The World's Most Trusted MDR Service

Sophos is the number one MDR provider globally, securing more organizations than any other vendor against ransomware, breaches, and other threats that technology alone cannot stop.

Sophos MDR protects many thousands of organizations across all industries around the world, giving us unparalleled depth and breadth of expertise into threats facing individual sectors. We leverage this extensive telemetry to generate "community immunity," applying learnings from defending one organization to all other customers with a similar profile, elevating everyone's defenses.

Of course, what matters most is the cybersecurity outcomes we deliver for our customers. Sophos is the highest rated and most reviewed MDR solution on Gartner® Peer Insights™ with a 4.8/5 rating across 300 reviews as of June 14, 2023 and 97% of customers saying they would recommend us.

Sophos is also named a leader in the G2 Grid® Reports for Managed Detection and Response, as well as being named a Leader for MDR in the G2 Overall, Midmarket, and Enterprise segments.

Most trusted
Over 17,000 organizations use Sophos MDR [Q2, 2023]

Highest rated
4.8/5 independent customer rating

Most reviewed
300 reviews on Gartner Peer Insights in the last 12 months

To learn more about Sophos MDR and how it enables Microsoft Defender users to reduce cyber risk, increase the efficiency and impact of security investments, and improve insurability visit www.sophos.com/mdr

Explore Sophos Endpoint Protection

Sophos Intercept X Endpoint Protection works for you and with you, adapting your defenses in response to an attack.

It is packed with powerful, multi-layered protection that provides superior protection against ransomware and advanced threats across all stages of the attack chain, including behavior-based ransomware rollback and 60 exploit mitigations that are enabled by default – no fine tuning required.

Our innovative Adaptive Attack Protection responds dynamically to a human-led attack, automatically deploying extra defenses to thwart the adversary and buy defenders time to respond.

Sophos MDR service users running Microsoft Defender can switch to Sophos Endpoint protection at any time, giving you complete flexibility while future-proofing your security deployments.

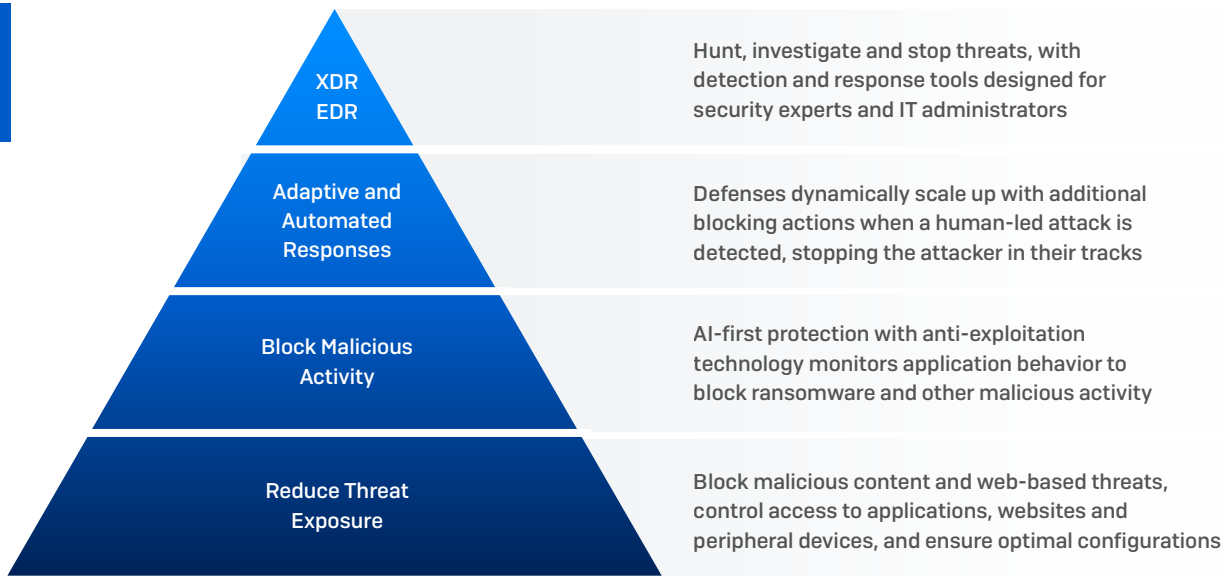
✓ Gartner Leader for 13 consecutive reports
Sophos has been named a Leader in the Gartner Magic Quadrant for EPP in every report since 2008

✓ Top rated on Gartner Peer Insights
4.8/5 independent customer rating

✓ G2 Leader for Enterprise, Midmarket, and SMB
Based exclusively on customer reviews

✓ 100% Protection Score – SE Labs
AAA rating for Enterprise and Small Business Security

To learn more and activate a free trial visit www.sophos.com/endpoint



Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Chris Silva, 31 December 2022
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, Magic Quadrant and PEER INSIGHTS are registered trademarks of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2023-06-27 (WP-NP)

SOPHOS