SOPHOS

Securing Microsoft environments with Sophos

How to increase your profitability while elevating your customers' defenses

PARTNER BENEFITS

Why sell Sophos solutions into Microsoft environments

INCREASE YOUR PROFITABILITY

With Sophos solutions, you enjoy generous, lucrative margins, enabling you to see more reward for your effort.

EXPAND YOUR SECURITY FOOTPRINT

Sophos provides protection capabilities not available with Microsoft, enabling you to gain a bigger share of your customers' security budget.

INCREASE BUSINESS RESILIENCE

Diversifying your portfolio with Sophos solutions reduces your exposure to market volatility and change.

ENHANCE YOUR TRUSTED ADVISER POSITION

By enabling customers to take advantage of Sophos integrations with Microsoft, you demonstrate how you are delivering better RoI.

SOPHOS

SOPHOS CENTRAL PLATFORM

Managed by Customers | Managed by Partners | Managed by Sophos

SERVICES

MANAGED SERVICES

- MDR
- Incident Response
- Vulnerability Management
- Professional Services

ADVISORY SERVICES

- Penetration Testing
- Security Assessments
- Red Team Exercises
- Incident Readiness

THREAT PREVENTION AND CONTROLS

CONTROLS

- Endpoint
- Firewall
- Identity
- Email
- Network
- Web Browser

INTEGRATIONS

350+ Third-party integrations

SECURITY OPERATIONS

- XDR
- SIEM
- EDR
- ITDR
- NDR
- SOAR

THREAT INTELLIGENCE

SOPHOS X-OPS

- Adversary Tracking
- Threat Research
- Breach Forensics
- Malware Analysis
- Industry Collaboration

AI, AUTOMATION & ENGINEERING

- Adaptive Attack Protection
- Critical Attack Warning
- Security Analytics
- Detection Logic
- Threat Protection

DATA LAKE

AI-ASSISTED & AGENTIC WORKFLOWS

Your trusted security partner for Microsoft environments

SOPHOS

Sophos in Microsoft environments

600,000+
Microsoft environments secured

Providing unmatched insights into attacks in Microsoft environments. Learnings from defending one Microsoft user are automatically applied to all.

23,000
Advanced attacks detected by Sophos MDR in 2025

Sophos MDR leverages extensive telemetry from Microsoft tools to detect sophisticated attacks in Microsoft environments. 4,800 automated response actions to neutralize these attacks were executed in 2025 alone.

12 min
Sophos MDR response time

Sophos MDR leverages AI, automation and deep human expertise, enabling us to respond with speed and precision – at scale.
(H2 2025)

Verified. Integrated. Certified.

Member of Microsoft Intelligent Security Association

MISA Verified

SOPHOS INTELIX | Microsoft 365 Copilot

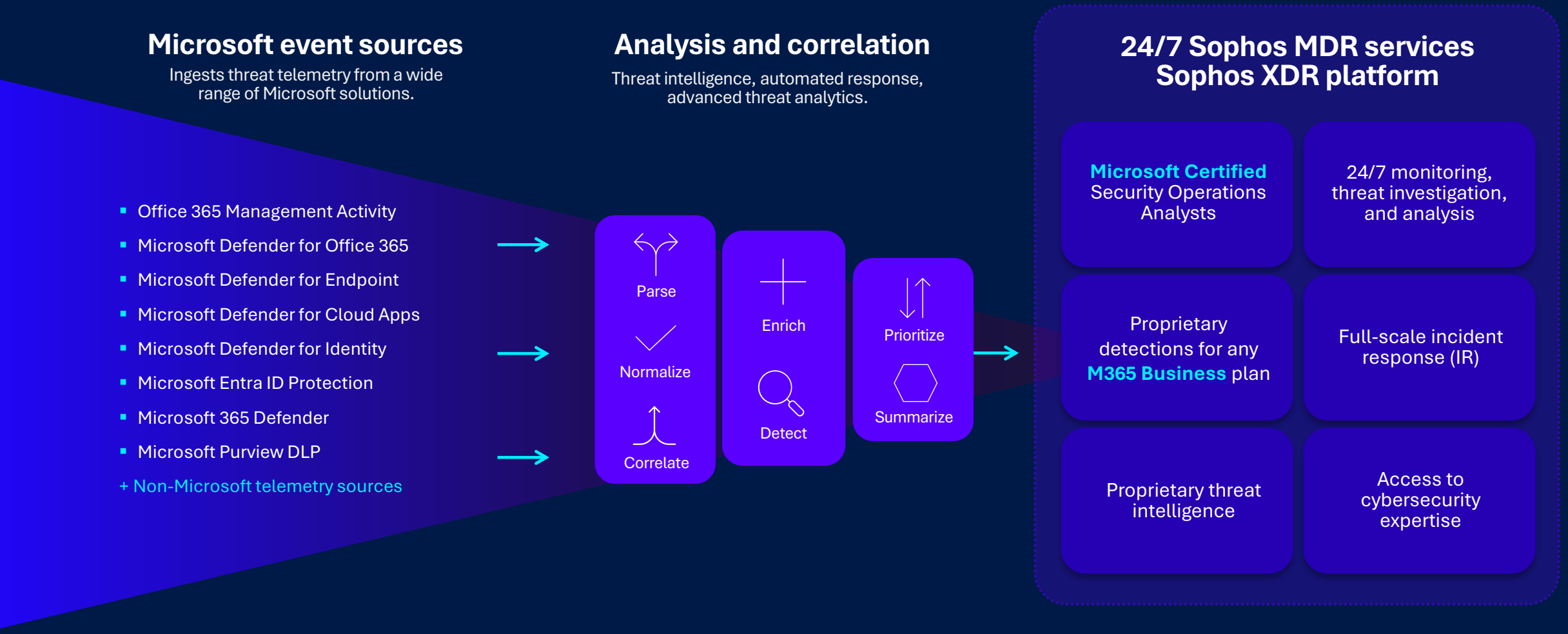
Copilot Security Integrations

Microsoft

Certified Security Operations Analysts

SOPHOS

Sophos deeply integrates with the Microsoft ecosystem



Democratizing security with the Management Activity API

- Most MDR and XDR providers rely on Microsoft's Graph Security API to get threat telemetry from Microsoft solutions.
- The Graph Security API provides strong detection value – but only for customers with an E5 license.
- For other customers – including those with M365 Business Basic, Business Standard and Business Premium plans – the Graph Security API provides minimal telemetry.
- In addition to the Graph Security API, Sophos also extensively leverages Microsoft's Management Activity API
  - Provides rich audit logs from Exchange Online, SharePoint, and other Microsoft solutions.
  - Included with nearly all Microsoft 365 license tiers.

Through the Management Activity API, Sophos surfaces thousands of threats each month that would go undetected without an E5 license.

EXAMPLE SCENARIO

- User clicks a phishing link, completes MFA, and an attacker hijacks the session.
- The attacker creates hidden inbox rules to delete or redirect emails that would otherwise alert the user to suspicious activity such as invoice fraud.
- Sophos ingests all the Microsoft 365 audit logs via the **Management Activity API**.
- Sophos applies threat intelligence to the audit logs to detect abnormal behavior.
- Activity is flagged for investigation by Sophos MDR or in-house analysts using Sophos XDR.

SOPHOS

The Microsoft-optimized MDR service

Sophos MDR provides superior threat detection and response for Microsoft environments

41% of Sophos MDR threat cases are triggered by telemetry from Microsoft tools.

Strongest foundations

At the start of customer engagements, our Microsoft-environment onboarding specialists work with customers to optimize configuration with Microsoft technologies.

Maximum inputs

In addition to Microsoft's Graph Security API, Sophos MDR also uses the Management Activity API, enabling us to surface thousands of threats each month that would otherwise go undetected.

Extensive response actions

Sophos MDR doesn't just notify of attacks; it stops them with automated and human-led response actions. Our Microsoft certified analysts specialize in detecting and responding to attacks using custom Microsoft playbooks.

Community immunity

Sophos MDR secures more than 35,000 Microsoft environments. Learnings from defending one customer are automatically applied to all, elevating protection for all customers.

SOPHOS

Sophos MDR Threat Case | Stopping a BEC attack

Threat detected

- Detection indicates a compromised user via a phishing campaign using WikiKit/Sneaky2fa toolkit
- Sophos MDR observed successful authentication using valid session tokens, indicating that the user's credentials had been harvested and reused to gain unauthorized access.

Threat remediated

As the response mode was 'Authorize', Sophos MDR:

- **Blocked user sign-ins for the compromised account.**
- **Revoked all current sessions.**

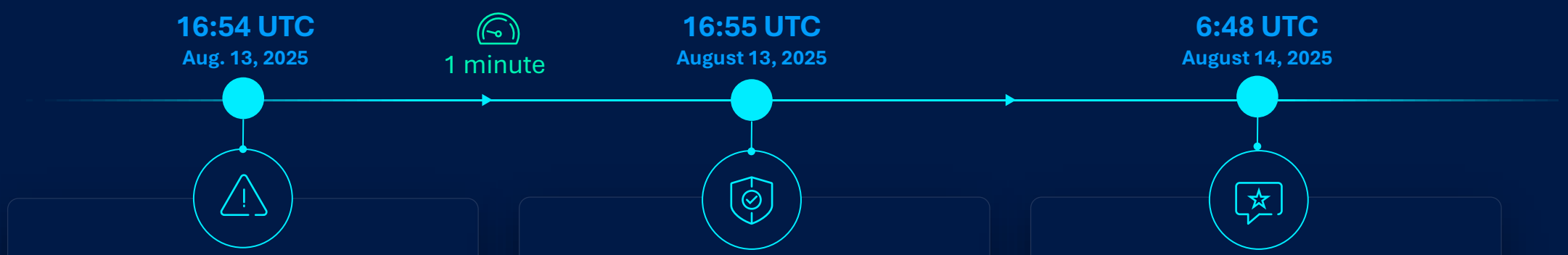
Sophos MDR also **revoked all active sessions in Entra ID**, preventing the attacker from regaining entry even if the account is later re-enabled.

Guidance provided

- Sophos MDR notified the customer and provided recommendations for further steps that can be taken to enhance security posture and prevent a repeat occurrence.

SOPHOS

Sophos MDR Threat Case | Adversary-in-the-Middle attack



Threat detected

A proprietary Sophos detection rule identifies an Adversary-in-the-Middle attack (Axios user agent).

Threat remediated

Microsoft O365 response actions are automatically executed, **disabling sign-in and terminating active sessions** for the compromised user account; the activity is immediately escalated to the customer.

Normal order restored

Once the customer confirms that the user's password has been reset, the Sophos MDR analyst re-enables user sign-in to restore access to the O365 account.

SOPHOS

The Microsoft-optimized firewall

Sophos Firewall is designed for Microsoft environments

Microsoft Azure

Microsoft Hyper-V

Flexible deployment

Includes hardware, virtual, and cloud deployment options.

Supports Microsoft Azure cloud and Hyper-V virtual deployments for any hybrid network requirements.

Device protection

Microsoft Server and platform signatures are constantly updated to detect and block vulnerability attacks.

Entra ID integration

Includes tight integration with Microsoft Entra ID for:

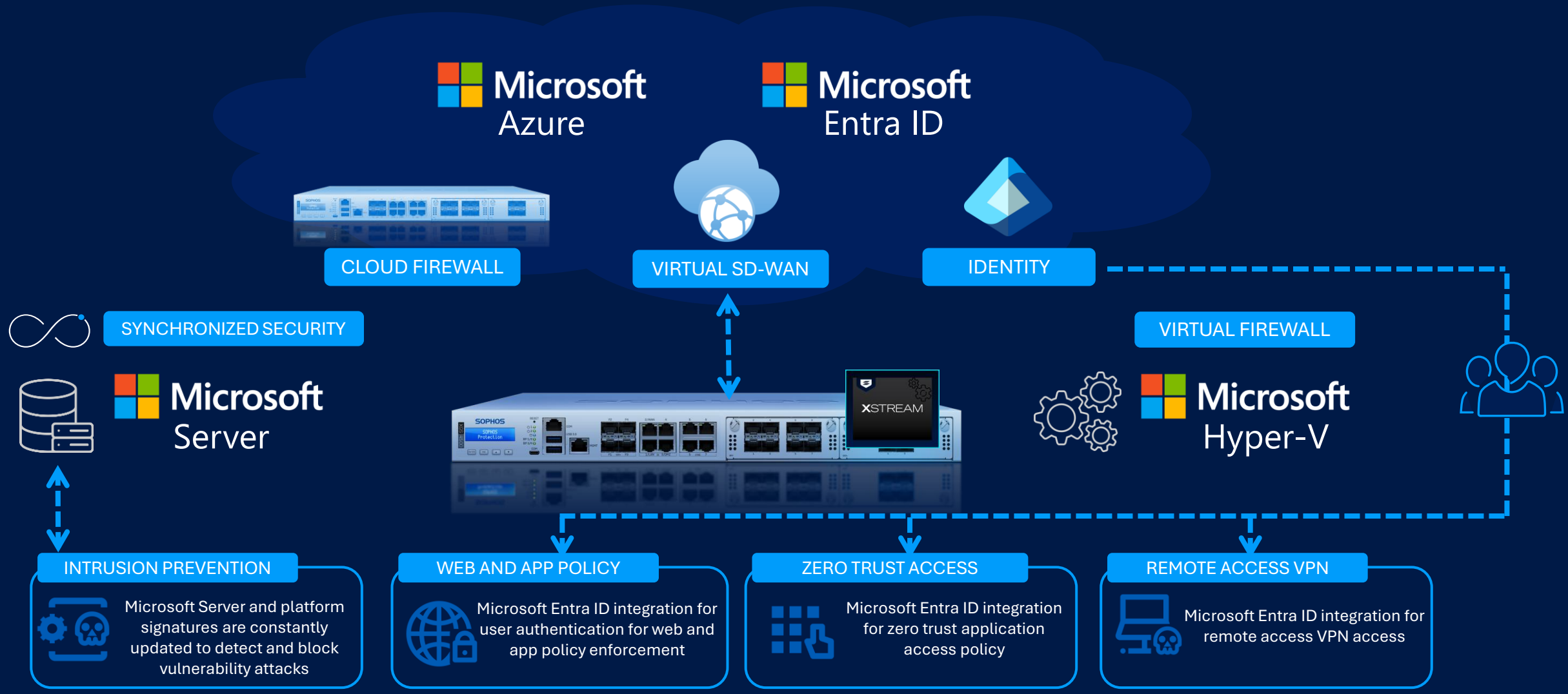
- User authentication for web and app policy enforcement
- Zero trust application access policy
- Remote access VPN

Virtual WAN

Integrates with Microsoft Azure Virtual WAN to make SD-WAN overlay network deployments easy and affordable.

SOPHOS

Sophos Firewall works better together with Microsoft



Threat intelligence trusted by Microsoft for Copilot

The Sophos Intelix threat intelligence service integrates with Microsoft Security Copilot and Microsoft 365 Copilot

SOPHOS INTELIX | Microsoft Copilot

SOPHOS INTELIX FOR MICROSOFT SECURITY COPILOT

Brings Sophos X-Ops' global threat intelligence directly into Microsoft's generative AI assistant for security teams, turning intelligence into faster, more confident decision-making.

SOPHOS INTELIX FOR MICROSOFT 365 COPILOT

Enables security and IT professionals to query Sophos Intelix in natural language from within Microsoft 365 apps, including Teams and Outlook, to investigate threats, analyze URLs or files, and get instant insights.

SOPHOS

Sophos selling motions in Microsoft Environments

SOPHOS

Two ways to sell Sophos into Microsoft environments

OPTION 1

Align to Microsoft plans

We have products and services that complement every Microsoft plan, from Business Basic to E5.

OPTION 2

Align to security challenges

Position and sell a combination of Sophos and Microsoft solutions — plus your own services — to enable customers to address their top security issues.

SOPHOS

OPTION 1

Sophos solutions complement every Microsoft plan

MICROSOFT 365 LICENSING

M365 BUSINESS BASIC | M365 BUSINESS STANDARD | OFFICE 365 E1 | OFFICE 365 E3 | ENTRA ID P1 | ENTRA ID P2 | DEFENDER FOR ENDPOINT P1/P2 | M365 BUSINESS PREMIUM | M365 E3 | M365 E5

CUSTOMER USES

Microsoft productivity tools

Office 365 tools including Word, Excel, PowerPoint, Teams, Outlook, OneDrive

COMPLEMENTARY SOPHOS SOLUTIONS

- **Sophos Endpoint**, inc. legacy platform support – Essential defense for Microsoft environments.
- **Sophos MDR** – Uses Microsoft telemetry to detect and stop advanced threats.
- **Sophos Email** – Great value email security for Office 365.

CUSTOMER USES

Microsoft Entra ID

Entra ID purchased standalone or as part of a bundle

COMPLEMENTARY SOPHOS SOLUTIONS

- **Sophos MDR** – Stops identity-based attacks, faster.
- **Sophos ITDR** – Leverages Entra ID to reduce identity risk.
- **Sophos Firewall** – Entra ID integration simplifies day-to-day management.

CUSTOMER USES

Microsoft security tools

Microsoft Defender solutions, inc. for Endpoint, Cloud Apps, and Identity.

COMPLEMENTARY SOPHOS SOLUTIONS

- **Sophos MDR** – Stops threats that tools alone cannot prevent.
- **Sophos Advisory Services** – Proactively identifies weak spots in organizational security posture.
- **Sophos Email Monitoring Service** - Detects threats that other email security solutions miss.

SOPHOS

OPTION 2

Sophos and Microsoft solutions address top security needs

IDENTITY THREATS

Identity-based threats, where adversaries impersonate legitimate users to compromise an organization, are on the rise - 79% of data breaches are identity-related.

SOLUTIONS:

- **MS Entra ID + Sophos MDR**
- **MS Entra ID + Sophos MDR + Sophos ITDR**

RANSOMWARE

70% of human-operated ransomware attacks used remote encryption*. Ransomware recovery costs organizations, on average, $1.53 million.

SOLUTIONS:

- **Sophos Endpoint + Sophos MDR**
- **MS Defender for Endpoint + Sophos MDR**

CYBER RISK REDUCTION

Prevention is the best option. By proactively testing their cyber defenses through pen testing and assessments organizations can identify and fix gaps before attackers exploit them.

SOLUTION:

Sophos Advisory Services

Followed by **Sophos, Microsoft, and partner-led services**

BUSINESS EMAIL COMPROMISE (BEC)

AI and automation have made it easier for attackers to execute sophisticated BEC scams, impersonating senior leaders to trick employees into giving them money or sensitive information.

SOLUTIONS:

- **Microsoft 365 Email + Sophos Email**
- **MS Entra ID + Sophos MDR**

** Microsoft 2024 Digital Defense report*

SOPHOS

Sophos solutions complement every Microsoft plan

SOPHOS

Why use Sophos solutions alongside Microsoft productivity plans

Microsoft productivity tools

Office 365 tools including Word, Excel, PowerPoint, Teams, Outlook, OneDrive

Productivity plans include:

M365 Business Basic
M365 Business Standard
Office 365 E1
Office 365 E3

- **Get business-level defense against cyber threats**
  - Productivity plans only include Microsoft Defender Antivirus, the basic, free, pre-installed antivirus software for Windows – not business-level endpoint protection.
- **Stop remote ransomware from encrypting your files**
  - Microsoft Defender cannot stop remote encryption in real-time, the approach used in 70% of successful human-operated ransomware attacks. *Source: Microsoft Digital Defense report*
- **Elevate protection against advanced email threats and phishing**
  - Microsoft Exchange Online only includes foundational spam and malware protection.
  - Microsoft Exchange Online does not include phishing simulations or user awareness training.
- **Get 24/7 threat monitoring and response**
  - 88% of ransomware attacks start outside standard business hours.

SOPHOS

Sophos solutions to complement Microsoft productivity tools

Microsoft productivity tools
Office 365 tools including Word, Excel, PowerPoint, Teams, Outlook, OneDrive

Recommended plan alignment:	M365 BUSINESS BASIC	M365 BUSINESS STANDARD	OFFICE 365 E1	OFFICE 365 E3

Sophos Endpoint

Advanced protection from cyber threats for Windows desktops, laptops, and servers.

Securing Microsoft environments

- **Protects current and legacy Windows operating systems**, including Win 7, Win 8.1, Win Server 2008 R2, Win Server 2012/2012 R2.
- **Unmatched ransomware protection**, including stopping remote encryption – used in 70% of success attacks in Microsoft environments*.
- **User-based licensing** increases customer value when running multiple Microsoft devices.

Licenses to sell

- Sophos Endpoint
- Sophos Endpoint 100 (term licenses only)
- Sophos Endpoint for Legacy Platforms

Sophos MDR

A 24/7 cybersecurity service that hunts for, detects and neutralizes advanced cyber threats.

Securing Microsoft environments

- **Uses threat telemetry from Microsoft solutions**, including Office 365, to detect advanced, human-led attacks that tools alone cannot stop.
- Sophos analysts can **execute Microsoft response actions** to neutralize attacks directly within the customer's Microsoft 365 environment.
- **Sophos' proprietary detection rules** based on Microsoft events accelerate threat response.

Licenses to sell

- Sophos MDR Essentials (with Sophos Endpoint (included) or Microsoft Defender)
- Sophos MDR Complete (with Sophos Endpoint)

Sophos Email

Comprehensive, great value defense against email-based threats for Exchange Online users.

Securing Microsoft environments

- **Integrates with M365 Email in minutes** for easy set-up, mail flow and day-to-day management.
- **Enhances and extends the foundational Exchange spam and malware protection** with email filtering, AI analysis, advanced threat protection, DLP and content control.
- **Reduces cyber risk** with built-in user awareness training including phishing simulation testing.

Licenses to sell

- Sophos Email

** Microsoft 2024 Digital Defense report*

SOPHOS

Why use Sophos solutions alongside Microsoft Entra ID

Microsoft Entra ID	**Entra ID P1 and Entra ID P2 available as standalone subscriptions** **Entra ID P1 included in M365 E3 and M365 Business Premium** **Entra ID P2 included in M365 E5**

- **Entra ID is NOT a defense solution**
  - Entra ID is primarily an Identity and Access Management (IAM) tool, not a defense tool.
  - It provides identity and group management, RBAC controls, privileged access management, and conditional access policies.
- **Identity is a major attack vector**
  - 90% of organizations experienced at least one identity-related breach in the last year. *Source: 2024 Trends in Securing Digital Identities*
  - 79% of data breaches are identity related. *Source: Identity Defined Security Alliance*
- **Entra ID itself has the potential to be a security gap**
  - 95% of Microsoft Entra ID environments have critical misconfigurations. *Source: Sophos Incident Response team research*
- **Entra ID integration enables SSO with Sophos tools for friction-free access**

SOPHOS

Sophos solutions to complement Microsoft Entra ID

Microsoft Entra ID
Entra ID purchased standalone or as part of a bundle

Available with:

Entra ID P1 and Entra ID P2 available as standalone subscriptions
Entra ID P1 included in M365 E3 and M365 Business Premium
Entra ID P2 included in M365 E5

Sophos MDR

A 24/7 cybersecurity service that hunts for, detects and neutralizes advanced cyber threats.

Securing Microsoft environments

- **Uses threat telemetry from Entra ID** and other Microsoft solutions to detect advanced, human-led attacks that tools alone cannot stop.
- Sophos analysts can **execute Microsoft response actions** to neutralize attacks directly within the customer's Microsoft 365 environment.
- Sophos' **proprietary detection rules based on Microsoft events** accelerate threat response.

Licenses to sell

- Sophos MDR Essentials (with Sophos Endpoint (included) or Microsoft Defender)
- Sophos MDR Complete (with Sophos Endpoint)

Sophos ITDR

Detects and responds to identity threats that bypass traditional identity security controls.

Securing Microsoft environments

- **Scans Microsoft Entra ID environments** to rapidly identify misconfigurations and identity-based security gaps
- Scans the dark web to **find compromised credentials** before they can be exploited.
- When used with Sophos MDR, Sophos analysts can **take response actions in Entra ID** to neutralize identity threats.

Licenses to sell

Sophos ITDR requires Sophos MDR or Sophos XDR

- Sophos MDR + Sophos ITDR
- Sophos XDR + Sophos ITDR

Sophos Firewall

Next-gen firewall available as a hardware, software or virtual appliance.

Securing Microsoft environments

- **Entra ID single sign-on (SSO) integration** enables users to use their corporate network credentials for remote access VPN, eliminating friction.
- **Full next-gen firewall** optimized for the modern encrypted internet, offering industry-leading price per protected Mbps and comprehensive protection.

Licenses to sell

Requires software subscription and FW appliance

- Sophos Firewall XGS series appliance (hardware, software, virtual)
- Sophos Firewall Xtream protection subscription

SOPHOS

Why use Sophos solutions alongside Microsoft security tools

Microsoft security tools
Microsoft Defender solutions, inc. for Endpoint, Cloud Apps, and Identity.

Security plans include:
Defender for Endpoint P1/P2
M365 Business Premium
Microsoft 365 E3
Microsoft 365 E5

- **Reduce cyber risk**
  - Stop threats that technology alone (including Microsoft tools) cannot stop.
  - Elevate email security with a second layer of defense alongside Microsoft.
  - Identify gaps in your wider security posture for proactive mitigation.
- **Maximize technology investments**
  - Leverage two-way integrations to harness telemetry from your Microsoft solutions to detect and stop advanced threats.
- **Expand and accelerate your team**
  - Gain the expertise of Microsoft Certified Security Operations Analysts and their custom threat response playbooks for Microsoft environments.
  - Many organizations lack the in-house expertise to use Microsoft's multiproduct technology to investigate and respond to hundreds or thousands of alerts every day.

SOPHOS

Sophos solutions to complement Microsoft security tools

Microsoft security tools
Microsoft Defender solutions, inc. for Endpoint, Cloud Apps, and Identity.

Recommended plan alignment:

DEFENDER FOR ENDPOINT P1/P2	M365 BUSINESS PREMIUM	M365 E3	M365 E5

Sophos MDR

A 24/7 cybersecurity service that hunts for, detects and neutralizes advanced cyber threats.

Securing Microsoft environments

- **Uses threat telemetry from Microsoft solutions**, including Microsoft Defender, to detect advanced, human-led attacks that tools alone cannot stop.
- Sophos analysts can **execute Microsoft response actions** to neutralize attacks directly within the customer's Microsoft 365 environment.
- Sophos' **proprietary detection rules based on Microsoft events** accelerate threat response.

Licenses to sell

- Sophos MDR Essentials (with Microsoft Defender)

Sophos Advisory Services

Proactive testing and assessment services that identifies weak spots in your security posture.

Securing Microsoft environments

- **Evaluates Microsoft and non-Microsoft controls and policies** through a variety of security testing and assessment services.
- Delivered by the award-winning Sophos Red Team — world-class security experts with **deep knowledge of Microsoft environments**
- Use findings from the assessments to **identify additional Sophos and Microsoft solutions** required to address security gaps found.

Licenses to sell

- Sophos Advisory Services portfolio
- Follow-up additional Sophos / Microsoft solutions

Sophos Email Monitoring (EMS)

Detects threats that other email security solutions miss and enhances email solution efficacy.

Securing Microsoft environments

- **Seamlessly deploys on top of Microsoft Exchange Online**, adding an extra layer of threat identification without disrupting email flow or security policies.
- **Extends Exchange Online email security**, using 20+ Sophos proprietary AI/ML models to identify elusive phishing attempts, BEC attacks, and more.
- Significantly enhancing email security posture **without replacing existing Microsoft investments.**

Licenses to sell

- Sophos EMS
  (Note: For non-Sophos Email customers only)

SOPHOS

Sophos and Microsoft solutions to address customers’ security needs

SOPHOS

Stopping identity threats with Sophos and Microsoft

NEED

Identity-based threats, where adversaries impersonate legitimate users to compromise an organization, are on the rise. 79% of data breaches are identity-related.

RECOMMENDED IDENTITY THREAT SOLUTIONS

- **MS Entra ID + Sophos MDR**
- **MS Entra ID + Sophos MDR + Sophos ITDR**

MS Entra ID provides **Identity and Access Management** (IAM), enabling identity and group management, RBAC controls, privileged access management, and conditional access policies.

Sophos MDR uses threat telemetry from Entra ID and other Microsoft solutions to **detect advanced, human-led attacks** that tools alone cannot stop. Analysts can **neutralize attacks** directly within the Microsoft 365 environment.

Sophos ITDR scans Entra ID environments to rapidly **identify Entra ID misconfigurations** and identity-based security gaps. Sophos MDR analysts can **take response actions in Entra ID** to neutralize identity threats.

CASE STUDY

UK retail organization with 1,000+ stores and 9,000+ staff

- An employee receives a phishing email pretending to be from a known supplier.
- They click, enabling the attacker to capture the employee's credentials and session token.
- Sophos MDR's automated and AI-powered tools detect a suspicious login.
- A Sophos MDR analyst reviews Entra ID sign-in logs and confirms adversary activity.
- Sophos MDR works with the customer to remediate the attack and recommends additional risk reduction activities.
- Outcome: Threat neutralized. No impact to the business.

SOPHOS

Stopping ransomware with Sophos and Microsoft

NEED

- In 2025, the average cost to remediate a ransomware attack was $1.53 million**.
- 70% of successful ransomware attacks in Microsoft environments used remote encryption*.

RECOMMENDED RANSOMWARE DEFENSE SOLUTIONS

- **Sophos Endpoint + Sophos MDR**
- **MS Defender + Sophos MDR** (if MS Defender is already deployed)

Sophos MDR integrates with Sophos, Microsoft and third-party solutions to detect and neutralize human-led ransomware attacks that tools alone cannot stop – executing a broad range of remediation actions in Microsoft environments.

Sophos Endpoint advanced AI-powered endpoint security includes CryptoGuard universal ransomware protection, which identifies and rolls back all forms of ransomware, including remote encryption.

MS Defender provides advanced, AI-powered security for businesses (Defender for Business, Defender for Endpoint) to stop sophisticated threats like ransomware.

CASE STUDY

MSP-managed customer running Sophos Endpoint + Sophos MDR

- Ransomware actor accessed the company's network by exploiting 3 unpatched vulnerabilities in the MSP's RMM tool (SimpleHelp).
- The attacker tried to disable Sophos Endpoint multiple times but was unsuccessful.
- The Sophos MDR team swiftly detected using threat telemetry from Sophos Endpoint.
- Sophos MDR neutralized the attack, using Sophos Endpoint's Application Control as part of the remediation process.
- No data extracted. No devices encrypted.
- An MSP client that was not running Sophos had 42GB data extracted and a ransom demanded.

** Microsoft 2024 Digital Defense report* *** The State of Ransomware 2025, Sophos*

SOPHOS

Reducing cyber risk with Sophos and Microsoft

NEED | You can't fix security gaps if you don't know they exist. By proactively testing their cyber defense with penetration testing and security assessments, organizations can identify and address security weaknesses before attackers exploit them.

RECOMMENDED RISK REDUCTION SOLUTIONS

- **Sophos Advisory Services**
- Followed by **Sophos, Microsoft, and partner-led services**

Sophos Advisory Services – Uncovers potential weak spots in defenses and provides recommendations to fortify resilience, informed by leading threat intelligence and delivered by security experts.

Sophos products and services, Microsoft tools, and partner-led services – Address security gaps identified by the assessment.

EXAMPLE SCENARIOS

IDENTIFIED ISSUE	FOLLOW-ON SOLUTION
Weak credential management	• **MS Entra ID** to manage credentials • **Sophos MDR** to identify identity-based attacks • **Sophos ITDR** to identify credential abuse
Weak vulnerability management	• **Sophos Managed Risk** (requires Sophos MDR) to identify and prioritize unpatched vulnerabilities (term only)
Users susceptible to phishing	▪ **Sophos Email** for phishing simulations and user awareness training ▪ **Partner program delivery**, including phishing simulations, training and reporting.
Difficulty detecting attacks	▪ **Sophos MDR** provides 24/7 threat detection and response

SOPHOS

Stopping BEC with Sophos and Microsoft

NEED | AI and automation have made it easier for attackers to execute sophisticated Business Email Compromise (BEC) scams where they impersonate senior leaders to trick employees into giving them money or sensitive information.

RECOMMENDED BEC DEFENSE SOLUTIONS

- **Microsoft 365 Email + Sophos Email**
- **MS Entra ID**
- **Sophos MDR**

Sophos Email natively integrates with Exchange Online and Microsoft 365 Email. It automatically identifies high-profile targets for protection against malware-free impersonation and BEC attacks. Multiple layers of defense, including natural language processing (NLP) identify and block BEC attacks.

Microsoft Entra ID provides authentication and authorization, inc. SSO, MFA and Conditional Access to resources, making it harder for attackers to exploit compromised credentials.

Sophos MDR takes telemetry from customers' email security solutions and combines it with wider Sophos, Microsoft and third-party telemetry to detect and stop Business Email Compromise attacks.

CASE STUDY

Sophos MDR customer

- An attacker sends a phishing email to an employee.
- Using the Evilginx tool, they obtain their user's username, password and authorization tokens which they use to circumvent the MFA.
- With access to the user's email account, the attacker creates an email forwarding rule.
- Impersonating the user, the attacker asks the admin to validate their IP address, which gives them access to a Microsoft Dev Box in Azure.
- Sophos MDR detects the creation of a suspicious inbox rule and additional indicators of compromise.
- Sophos MDR isolates the compromised host, suspends the attack, and guides the customer to reset the credentials of the compromised user.

SOPHOS

Sample pricing to address common security needs

SOPHOS

Sample pricing (MRR per user)

STOPPING IDENTITY ATTACKS

Option 1

Microsoft Business Standard	$12.50
Microsoft Entra ID P1	$6.00
Sophos MDR Essentials (inc. Sophos Endpoint)	$6.27
Sophos ITDR	$3.62
TOTAL	**$28.39**

Option 2

Microsoft Business Premium (inc. MS Defender for O365 and Entra ID P1)	$22.00
Sophos MDR Essentials	$6.27
Sophos ITDR	$3.62
TOTAL	**$31.89**

STOPPING RANSOMWARE ATTACKS

Option 1

Microsoft Business Basic	$6.00
Sophos MDR Essentials (inc. Sophos Endpoint)	$6.27
TOTAL	**$12.27**

Option 2

Microsoft Business Premium (inc. MS Defender for Endpoints)	$22.00
Sophos MDR Essentials	$6.27
TOTAL	**$28.27**

STOPPING BEC ATTACKS

Option 1

Microsoft Business Basic (inc. MS 365 Email)	$6.00
Sophos Email	$1.93
Microsoft Entra ID P1	$6.00
Sophos MDR Essentials	$6.27
TOTAL	**$20.20**

Option 2

Microsoft Business Premium (inc. MS Defender for O365 and Entra ID P1)	$22.00
Sophos MDR Essentials	$6.27
TOTAL	**$28.27**

Sample pricing for illustrative purposes only. *Based on Microsoft pricing provided by a Sophos distributor and Sophos MSP pricing based on 100-499 users in the U.S. in January 2026. Actual Sophos and Microsoft pricing must be sourced from your distributor.*

SOPHOS

Supporting enterprise customers with next-gen SIEM needs

SOPHOS

Taegis MDR with Next-Gen SIEM to complement E5 Plans

Taegis MDR is an enterprise-grade 24/7 managed service from Sophos that protects against current and emerging threats and includes a powerful Next-Gen SIEM with generous, predictable, and cost-effective data retention.

Integrates seamlessly with Microsoft and other sources to provide threat prevention, detection, risk mitigation and response.

Extracts maximum security value from E5 plans by integrating with Azure, Defender Suite, O365, and other Microsoft technologies.

Includes 365 days of generous data retention as standard, with extended log retention for up to five rolling years at fixed additional costs.

Provides superior threat intelligence powered by telemetry from Sophos' 600,000+ customers and Sophos X-Ops expertise.

Lower cyber risk - fast

Taegis MDR detects and stops advanced attacks 24/7, combining deep human expertise with AI-accelerated threat detection and response.

With quick deployment, no need to "rip and replace" existing tools, and expert guidance at every point, you can start reducing cyber risk fast.

Predictable all-in data costs

Endpoint-based pricing with 1 year of data storage included across unlimited log sources, plus the option to upgrade to up to 5 years' storage.

No variable billing tied to events per second (EPS), volume or consumption, which is common in traditional SIEM models.

Increase cybersecurity RoI

Get more benefit from your existing and future security tool investments by using them to help detect threats.

Get Microsoft Defender for Endpoint telemetry directly within the Taegis platform, streamlining security operations.

SOPHOS

Taegis MDR: Predictable all-in data costs

Taegis is an ideal solution for organizations looking for a cost-effective, predictable data storage solution.

- **Endpoint-based pricing** with 1 year of data storage included across unlimited log sources, plus the option to upgrade to up to 5 years' storage.
- **No variable billing** tied to events per second (EPS), volume or consumption, which is common in traditional SIEM models.

CUSTOMER CASE STUDY

Customer profile: UK university with data storage needs for compliance

Challenge: Real-world Sentinel consumption costs ended up being almost 5 times higher than predicted.

- Predicted cost: £55,462
- Actual cost: £233,681

Saving with Taegis: 85% reduction in annual running costs.

- 1-year Sentinel cost: £264,832
- 1-year Taegis cost: £39,050

SOPHOS

Why use Taegis XDR/MDR alongside Microsoft Sentinel

Taegis + Microsoft Sentinel is resilient by design, predictable on cost, and operationally integrated. It enables you to reduce risk by diversifying your SecOps control plane while scaling coverage without being constrained by SIEM ingestion economics.

- **Architectural resilience (reduced single-vendor control-plane risk)**
  Taegis provides an independent detection/response plane, adding redundancy, reducing risk.

- **Maximize E5 ROI without being constrained by SIEM economics**
  Coverage decisions shouldn't be "how many logs can we afford?". With Taegis you can onboard broadly, prove outcomes fast, then selectively forward high-value signals/incidents into Sentinel for governance and retention.

- **Clear division of labor with (each tool doing what it's best at)**
  - Sentinel: Microsoft-native correlation, Azure-heavy use cases, compliance, SIEM governance/reporting.
  - Taegis: cross-stack detection + response, unified operations, faster onboarding across heterogeneous environments.

- **Two-way integration = unified operations**
  - Sentinel incidents → cases/workflows handled through Taegis MDR
  - Taegis MDR hunting/findings → pivot/validate/enrich in Sentinel where needed

- **Future-proofing without re-platforming risk**
  Whether you stay mixed vendor, consolidate into Defender, or evolve your tooling, the unified MDR operating model remains stable and open.

SOPHOS

Competitive

How Sophos stacks against other vendors

	Sophos	Huntress	Blackpoint Cyber	CrowdStrike	SentinelOne	Arctic Wolf
Platform integrates with Microsoft APIs	Yes	Yes	Yes	Yes	Yes	Yes
MDR service supports Microsoft Defender Endpoint	Yes	Yes	Yes	No	No	Yes
MDR service includes first-party endpoint security	Yes	No	No	Yes	Yes	Optional
Microsoft Verified SMB Solution	Yes	Yes	Yes	No	No	No
Threat intelligence agent for Microsoft Copilot	Yes	No	No	No	No	No
Full XDR security operations platform	Yes	No	Yes	Yes	Yes	No
Available identity threat detection and response (ITDR) for Entra ID	Yes	Partial	No	Yes	Yes	No
Available email protection solution that supports MS365	Yes	No	No	No	No	No
Available firewall that supports Entra ID authentication	Yes	No	No	No	No	No
Available advisory services, such as penetration testing	Yes	No	No	Yes	Yes	No

Sophos Confidential; For internal and partner use only

SOPHOS
DEFEAT CYBERATTACKS