LÖSUNGSBROSCHÜRE

Sophos + Microsoft

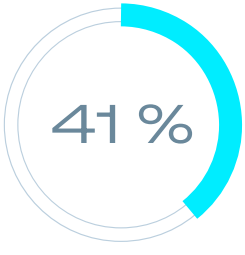
Gemeinsam stärker für bessere Sicherheit

Moderne Cyberbedrohungen verlangen nach intelligenterem, flexiblem Schutz für Ihre Microsoft-Infrastruktur. Verbessern Sie Ihren Schutz, reduzieren Sie Risiken und maximieren Sie die Rendite Ihrer Sicherheitsinvestitionen, indem Sie die branchenführenden Lösungen von Sophos mit Ihren vertrauten Microsoft-Tools kombinieren.

Microsoft-zentrierte Unternehmen und Organisationen stehen unter enormem Sicherheitsdruck

Bedrohungsakteure zielen zunehmend auf Identitäten ab, nutzen Lücken in isolierten Sicherheitslösungen aus und überfluten Teams mit Warnmeldungen. Business Email Compromise-Angriffe und Session Hijacking umgehen häufig die Multi-Faktor-Authentifizierung (MFA) und machen die Identität zu einem primären Bedrohungsvektor in Microsoft-Umgebungen. Unterdessen ermöglichen Remote-Ransomware-Verschlüsselung und manuelle Tastatureingaben Angreifern, Microsoft-Abwehrmechanismen zu überlisten. In Verbindung mit begrenzter interner Expertise führt dies zu gravierenden Lücken in der Transparenz und Reaktionsfähigkeit.

Schnellere Sicherheitsergebnisse



Prozentsatz der Sophos MDR-Bedrohungsfälle, die durch Microsoft-Telemetrie ausgelöst werden

Anzahl der Angriffe auf Microsoft-Umgebungen, die 2025 von Sophos MDR beseitigt wurden

Im Schnitt von Sophos MDR benötigte Zeit für die Reaktion auf Bedrohungen in Microsoft-Umgebungen

Vorteile

- **Microsoft-Investitionen maximieren:** Erweitern Sie den Nutzen Ihrer Microsoft-Tools durch mehr Transparenz, eine verbesserte Bedrohungserkennung und eine Experten-geführte Reaktion.
- **Schutz erhöhen:** Schließen Sie Sicherheitslücken in den Bereichen Identität, Endpoint, E-Mail und Netzwerk.
- **Sicherheitsergebnisse beschleunigen:** Die Sophos MDR-Analysten können Bedrohungen schnell für Sie beseitigen.
- **Betriebliche Komplexität reduzieren:** Vereinfachen Sie das Sicherheitsmanagement mit integrierter Intelligenz, einheitlichen Workflows und Expertenberatung, die Ihr Team entlastet.
- **Resilienz stärken:** Profitieren Sie von Schutz, der auf Telemetriedaten aus Hunderttausenden von Microsoft-Umgebungen basiert.

Gemeinsam stärker

Sophos stärkt die Sicherheit Ihrer Microsoft-Umgebung und erhöht ihren Nutzen – durch bessere Einblicke, schnellere Reaktion und fundierte Security- Expertise.

Schutz für jeden Microsoft-Plan: Egal ob Sie M365 Business Basic/Standard/Premium, E3 oder E5 nutzen – Sophos bietet Ihnen modernste Sicherheit, Erkennung und Reaktion.

Gemeinsam besser geschützt: Die Erkenntnisse aus der Verteidigung Hunderttausender Microsoft-Kunden fließen kontinuierlich in unseren Schutz ein und erhöhen somit die Sicherheit der gesamten Sophos Community.

Sicherheit für die gesamte Umgebung: Endpoint, E-Mail, Firewall, ITDR, MDR, Advisory Services – alles integriert in Microsoft, um Risiken zu reduzieren und aktive Bedrohungen zu stoppen.

Tiefgreifende, bidirektionale Integrationen: Sophos wertet umfangreiche Microsoft-Telemetriedaten aus, um das Verhalten von Angreifern zu ermitteln und direkt in Ihrer Microsoft 365-Umgebung Reaktionsmaßnahmen zu ergreifen.

Echte Ergebnisverantwortung – keine reine Weiterleitung von Warnmeldungen: Die Analysten von Sophos MDR benachrichtigen Sie nicht nur, sondern können direkt in Ihrem Microsoft-Mandanten Sofortmaßnahmen ergreifen.

Microsoft-zertifizierte Experten: Die Sophos MDR-Teams verfügen über Sicherheitsanalysten, die auf das Erkennen und Bekämpfen von Cyberangriffen mit maßgeschneiderten Microsoft Response Playbooks spezialisiert sind.

Wie Sophos Ihre Microsoft-Produktpalette optimiert

Sophos bietet ein komplettes Paket an Sicherheitsfunktionen, die nahtlos mit Ihren Microsoft-Tools zusammenarbeiten. Jede dieser Lösungen verleiht Ihrer umfassenden Microsoft-Strategie mehr Tiefe, Intelligenz und Resilienz. Von Endpoints und Identitäten bis hin zu E-Mails, Netzwerken und darüber hinaus bietet Sophos umfassenden Schutz, der die Lücken schließt, auf die Angreifer setzen.

Sophos MDR für Microsoft-Umgebungen

24/7 Managed Detection and Response, die proprietäre Erkennungsmethoden, Microsoft-Signale und Expertenanalysten kombiniert, um Bedrohungen schnell zu beseitigen. Ideal für Unternehmen und Organisationen mit Microsoft- oder gemischten Umgebungen, die ein Expertenteam benötigen, das die Verantwortung für ihre Cybersicherheit übernimmt und nicht nur Warnmeldungen verschickt.

- Nutzt Microsoft-Signale, um raffinierte Angriffe zu erkennen und abzuwehren, die mit Technologien allein nicht gestoppt werden können.
- Nutzt Telemetriedaten der Microsoft Graph Security and Management Activity APIs, um auch ohne E5-Lizenzierung einen hohen Mehrwert bei der Erkennung zu erzielen.
- Beinhaltet Integrationen sowohl mit Microsoft- als auch anderen Lösungen zum umfassenden Schutz Ihrer gesamten IT-Umgebung.
- Ergreift Reaktionsmaßnahmen schnell und direkt in Ihrer Microsoft-Umgebung, einschließlich Widerruf von Benutzersitzungen, Deaktivierung von Anmeldungen und Aussetzung schädlicher Posteingangsregeln.
- Kann mit Sophos Endpoint (im Lieferumfang enthalten) oder Microsoft Defender for Endpoint verwendet werden – Sie haben die Wahl.

Sophos MDR ist eine von Microsoft über die Microsoft Intelligent Security Association (MISA) verifizierte Lösung für kleine und mittlere Unternehmen (KMU), die eine umfassende Integration mit Microsoft Defender for Endpoint und Defender for Business gewährleistet und so stärkeren und schnelleren Schutz für Microsoft-Umgebungen bietet.

Sophos ITDR für Entra ID

Sophos Identity Threat Detection and Response (ITDR) scannt Entra ID kontinuierlich auf Fehlkonfigurationen und Sicherheitslücken, überwacht den Missbrauch von Zugangsdaten (einschließlich Funden im Darknet) und ermöglicht Analysten, in Entra ID Reaktionsmaßnahmen zu ergreifen, um Identitätsangriffe schnell einzudämmen. Sophos ITDR erweitert die nativen IAM-Funktionen von Entra ID um einzigartigen Bedrohungsschutz von Sophos.

Sophos Endpoint für besseren Ransomware-Schutz

Bei 70 %* der modernen, manuell gesteuerten Ransomware-Angriffe kommt Remote-Verschlüsselung zum Einsatz, um einer Erkennung durch Tools wie Microsoft Defender zu entgehen. Sophos Endpoint beinhaltet proprietäre CryptoGuard-Technologie, um lokale und Remote-Ransomware-Angriffe sofort zu stoppen. Die nutzerbasierte Lizenzierung bietet maximalen Mehrwert, wenn Teammitglieder über mehrere Geräte verfügen, darunter auch Endpoints mit älteren und nicht mehr unterstützten Windows-Betriebssystemen.

Sophos Email für Microsoft 365

In Kombination mit Exchange Online bietet Sophos Email effektiven Schutz vor Phishing- und Business Email Compromise-Angriffen sowie zusätzlich Benutzer-Awareness-Trainings und Phishing-Simulationen, ohne den E-Mail-Verkehr oder die Sicherheitsrichtlinien von Microsoft zu beeinträchtigen.

Sophos Firewall für Microsoft-Umgebungen

Die Sophos Firewall ist für Microsoft-Umgebungen optimiert und bietet flexible Hardware-, virtuelle und Cloud-Bereitstellungsoptionen (einschließlich Azure und Hyper-V), Entra ID-Integration für Zero-Trust-Remote-Zugriff und Azure Virtual WAN-Integration für SD-WAN-Overlay-Netzwerkbereitstellungen.

Taegis XDR mit Next-Gen SIEM für Microsoft E5 + Sentinel

Die optimale Lösung für Unternehmen, die eine Datenspeicherung auf SIEM-Niveau und übergreifende Erkennungsfunktionen mit vorhersehbaren Datenspeicher-Kosten benötigen. Taegis vereint Telemetriedaten von Microsoft und Nicht-Microsoft-Systemen, bietet eine nahtlose Integration mit Sentinel und vermeidet eine variable Abrechnung nach „Events per Second“.

Sophos Intelix für Microsoft Copilot

Sophos Intelix integriert die Threat Intelligence von Sophos X-Ops in Microsoft Security Copilot und Microsoft 365 Copilot und bietet so eine intelligentere Sicherheit, die sich nahtlos in Microsoft-Umgebungen einfügt. Durch diese Integrationen ist modernste Cyber Intelligence sofort dort verfügbar, wo Verteidiger, IT-Administratoren und Unternehmensanwender bereits operieren.

Die optimale Kombination aus Sophos und Microsoft

Stärkerer Schutz für Ihre Microsoft-Umgebung beginnt mit der Auswahl der richtigen Kombination aus Sophos-Funktionen und Microsoft-Technologien. Ganz gleich, ob Sie Ihren bestehenden Microsoft-Plan ausbauen oder eine bestimmte Sicherheitsherausforderung angehen möchten: Sophos zeigt Ihnen klare Strategien auf, um Ihren Schutz zu maximieren, den Betrieb zu vereinfachen und bessere Ergebnisse zu erzielen.

Abgestimmt auf Ihren Microsoft-Plan

Ermitteln Sie basierend auf Ihrer M365 Subscription die optimale Kombination von Sophos- und Microsoft-Funktionen. Jede Kombination ist darauf ausgelegt, die Transparenz zu erhöhen, die Bedrohungsreaktion zu verbessern und die Lücken zu schließen, auf die Angreifer setzen.

Für M365 Business Basic, Business Standard, O365 E1 und O365 E3

Unternehmen und Organisationen, die diese auf Produktivität ausgerichteten Microsoft-Pläne nutzen, benötigen oft leistungsfähigere Endpoint-, E-Mail- und Erkennungsfunktionen, um moderne Bedrohungen effektiv abzuwehren.

Empfohlene Ergänzungen von Sophos:

- **Sophos MDR** – bietet 24/7-Erkennung und eine Experten-geführte Reaktion mithilfe von Microsoft-Telemetrie.
- **Sophos Endpoint** – modernster Schutz, einschließlich leistungsstarkem Schutz vor Remote-Ransomware.
- **Sophos Email** – verbesserter Schutz vor Phishing und Business Email Compromise (BEC).

Für M365 Business Premium, M365 E3 und E5 mit Microsoft Defender-Lösungen

Diese Pläne werden zwar um integrierte Schutzmechanismen erweitert, doch benötigen Teams häufig stärkere Erkennungs- und Reaktionsfunktionen sowie leistungsfähigere Möglichkeiten zum Prüfen ihres Sicherheitsstatus.

Empfohlene Ergänzungen von Sophos:

- **Sophos MDR** mit Microsoft Defender for Endpoint (oder Wechsel zu Sophos Endpoint).
- **Sophos Advisory Services** –Sicherheitslücken mithilfe von Penetrationstests und Bewertungen erkennen.
- **Sophos Email Monitoring System** – mehrschichtige Transparenz und Erkennung ergänzend zu Microsoft 365-Email.
- **Taegis XDR mit Next-Gen SIEM** – übergreifende Erkennungsfunktionen bei vorhersehbaren Kosten für die verlängerte Datenaufbewahrung.

Abgestimmt auf Ihre Sicherheitsanforderungen

Identitätsbasierte Bedrohungen

Angreifer nehmen immer häufige Entra-IDs und Benutzeridentitäten ins Visier, um sich Zugang zu Ihrer Umgebung zu verschaffen.

Empfohlene Kombination:

- **Microsoft Entra ID + Sophos MDR**
  - Ergänzen Sie **Sophos ITDR** zur proaktiven Erkennung und Bekämpfung von Identitätsrisiken.

Remote-Ransomware

Bei 70 %* der modernen, manuell gesteuerten Ransomware-Angriffe kommt Remote-Verschlüsselung zum Einsatz, um einer Erkennung durch Tools wie Microsoft Defender zu entgehen.

Empfohlene Kombination:

- **Sophos Endpoint + Sophos MDR**
  - Oder **Microsoft Defender for Endpoint + Sophos MDR**, falls Defender bereits im Einsatz ist.

Business Email Compromise (BEC)

BEC-Angriffe basieren auf Identitätsdiebstahl, Manipulation von Posteingangsregeln und Techniken zur Umgehung der Multi-Faktor-Authentifizierung (MFA).

Empfohlene Kombination:

- **Microsoft 365 E-Mail + Sophos Email + Sophos MDR**

Sicherheitsstatus und Risikoreduzierung

Unternehmen und Organisationen, die ihre Resilienz stärken möchten, profitieren von proaktiven Sicherheitstests durch Sicherheitsexperten.

Empfohlene Kombination:

- **Sophos Advisory Services zur Aufdeckung von Schwachstellen**
  - Plus **Lösungen von Microsoft und Sophos** zum Bekämpfen der identifizierten Risiken.

Sophos bietet maßgeschneiderte Kombinationen an, die gezielt auf die in Microsoft-Umgebungen am häufigsten auftretenden Bedrohungen abgestimmt sind. Schließen Sie Sicherheitslücken in den Bereichen Identität, Endpoint, E-Mail und Netzwerk.

Kontaktieren Sie uns, um gemeinsam die passende Sicherheitsstrategie für Ihre Microsoft-Umgebung zu entwickeln. Unser Team unterstützt Sie dabei, die richtige Kombination aus Sophos- und Microsoft-Funktionen für Ihre M365 Subscription zu bestimmen – damit Sie den Nutzen Ihrer Microsoft-Investitionen voll ausschöpfen können.

Weitere Informationen: sophos.de/microsoft

* Microsoft Digital Defense Report 2024.

Sales DACH
Tel.: +49 611 5858-0
E-Mail: sales@sophos.de

2026-03-02 BR-DE (TA) CRE-4588