LÖSUNGSBROSCHÜRE

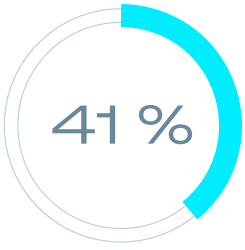
Taegis MDR + Microsoft E5 und Sentinel

Gemeinsam stärker für bessere Sicherheit

Unternehmen mit umfangreichen Microsoft-Investitionen in E5-Lizenzen, die Defender-Suite und Sentinel erreichen häufig einen Reifegrad, bei dem zwar eine hohe Transparenz vorhanden ist, operative Kapazitäten und Resilienz jedoch weiterhin Lücken aufweisen. Taegis MDR bietet eine ergänzende, Sicherheitsanbieter-unabhängige Erkennung und Reaktion, die den Betrieb vereinheitlicht, die Sicherheitsergebnisse in der Praxis verbessert und den strategischen Wert von Sentinel erhält, ohne die Komplexität oder das Kostenrisiko zu erhöhen.

Microsoft-zentrierte Unternehmen und Organisationen stehen unter enormem Sicherheitsdruck

Microsoft-zentrierte Unternehmen und Organisationen stehen unter enormem Druck, da identitätsbasierte Angriffe, KI-gestützte Bedrohungen und Cloud-Sprawl genau die Systeme betreffen, auf die sie für E-Mails, Zusammenarbeit, Identity und Infrastrukturen angewiesen sind. Bedrohungsakteure zielen zunehmend auf Identitäten ab, nutzen Lücken in isolierten oder falsch konfigurierten Sicherheitslösungen aus und überfordern Teams mit einer Flut von Informationen und Warnmeldungen. Darüber hinaus können der Mangel an Sicherheitsdaten von anderen Tools als Microsoft sowie der Spagat zwischen lückenloser Sicherheitstransparenz und beschränktem Budget dazu führen, dass Angriffe zu spät erkannt oder in einigen Fällen sogar völlig übersehen werden.



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

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

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

Vorteile

- **Maximieren Sie Ihre Microsoft-Investition** durch mehr Transparenz, eine verbesserte Bedrohungserkennung und eine Experten-geführte Reaktion.
- **Schützen Sie Microsoft- und Hybridumgebungen** mit einem konsistenten Betriebsmodell, das mit aktuellen und zukünftigen Sicherheitstools kompatibel ist.
- **Profitieren Sie von vorhersehbaren Datenspeicher-Kosten** durch die großflächige Vereinheitlichung von Microsoft- und Nicht-Microsoft-Telemetriedaten.
- **Erhöhen Sie Ihren Schutz** durch Schließen von Sicherheitslücken in den Bereichen Identität, Endpoint, E-Mail und Netzwerk.
- **Schützen Sie Microsoft- und Hybridumgebungen ganzheitlich** mit einem konsistenten Betriebsmodell – unabhängig von Ihren aktuellen und zukünftigen Sicherheitstools.

Gemeinsam stärker

Taegis MDR optimiert Ihre Abwehrmaßnahmen und hilft Ihnen, das Sicherheitspotenzial Ihrer Microsoft E5-Lizenzen besser auszuschöpfen. Gemeinsam mit Microsoft-Technologie implementiert Taegis MDR einen adaptiven Sicherheitsstatus, der sich kontinuierlich verbessert und von Grund auf resilient ist.

Architektonische Resilienz
Die Abhängigkeit von einem einzigen Anbieter birgt ein korreliertes Risiko. Taegis MDR bietet eine unabhängige Erkennung und Reaktion und sorgt so für Redundanz und Resilienz bei anbieterweiten Vorfällen.

Das passende Werkzeug für jede Aufgabe
Sentinel liefert bei Microsoft-nativer Korrelation, Azure-Umgebungen und Compliance Reporting ausgezeichnete Ergebnisse. Taegis MDR bietet eine übergreifende Erkennung und Reaktion sowie einheitliche Betriebsabläufe.

Ergebnisverantwortung
Die Analysten von Taegis MDR benachrichtigen Sie nicht nur, sondern können mit Ihrer vorherigen Zustimmung auch direkt in Ihrem Microsoft-Mandanten Sofortmaßnahmen ergreifen.

Keine SIEM-Kostenbeschränkungen
Taegis MDR ermöglicht eine breitangelegte Erfassung von Telemetriedaten ohne Kostenkompromisse, da nur hochwertige Signale an Sentinel zur Speicherung, Analyse, Governance und Compliance gesendet werden, ohne das Budget zu überschreiten.

Zukunftssicheres SOC
Egal, ob Sie Ihre Microsoft-Implementierung ausweiten oder weiter auf ein hybrides Konzept setzen möchten: Taegis MDR stabilisiert den SOC-Betrieb und vermeidet kostspielige Plattformwechsel.

Microsoft-zertifizierte Experten
Sicherheitsanalysten, die auf das Erkennen und Bekämpfen von Cyberangriffen mit maßgeschneiderten Microsoft Response Playbooks spezialisiert sind.

Wie Taegis MDR Ihre Microsoft-Produktpalette optimiert

Taegis MDR bietet eine umfassende Palette an Sicherheitsfunktionen, die Ihre bestehenden Microsoft-Investitionen ergänzen und Ihre allgemeine Microsoft-Strategie um operative Kapazitäten und Resilienz erweitern.

Taegis MDR mit NextGen SIEM für Microsoft E5 + Sentinel

24/7 Managed Detection and Response, die proprietäre Erkennungen, Microsoft-Signale und jahrzehntelange Erfahrung in der Servicebereitstellung mit einer offenen Plattform kombiniert, um messbare Sicherheitsergebnisse zu erzielen. Ganz gleich, ob Sie Taegis MDR vollständig managen lassen oder gemeinsam mit Ihren eigenen Security-Analysten einsetzen: Die Lösung stärkt Ihr Sicherheitsniveau und sorgt für eine besonders leistungsfähige Erkennung und Reaktion – mit vorhersehbarer, kosteneffizienter Datenspeicherung von Microsoft- und Nicht-Microsoft-Telemetrie.

- Unabhängige Erkennungs- und Reaktionsschicht, die Microsoft-Telemetrie nutzt und das Risiko einer Abhängigkeit von einem einzelnen Anbieter/einer einzelnen Plattform reduziert.
- Umfassende Telemetrie-Erfassung von Microsoft- und Nicht-Microsoft-Technologielösungen zum umfassenden Schutz Ihrer gesamten IT-Umgebung.
- Funktioniert parallel zu Sentinel und bietet vorhersehbare Kosten und flexible Skalierbarkeit, optimiert Hunting- und Triage-Workflows und arbeitet mit Sentinel-Tuning-Partnern zusammen.
- Nutzt Microsoft-Signale, um raffinierte Angriffe zu erkennen und abzuwehren.
- Taegis MDR Enhanced behandelt Sentinel-Vorfälle über einen einheitlichen Workflow, sodass Analysten problemlos zu Sentinel wechseln können, um Daten anzureichern oder zu validieren.
- Offene Plattform, die Sie wahlweise mit Microsoft Defender for Endpoint, Sophos Endpoint (im Lieferumfang enthalten) oder einer beliebigen anderen Endpoint-Protection-Lösung nutzen können.

Taegis MDR kann Daten von den folgenden Microsoft-Produkten erfassen:

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft 365 Defender
- Microsoft Entra ID Protection
- Microsoft Purview Data Loss Prevention
- Microsoft Purview Insider Risk Management
- Microsoft Azure Activity Log
- Microsoft Azure Application Gateway
- Microsoft Azure Event Hubs
- Microsoft Azure Firewall
- Microsoft Azure Front Door
- Microsoft Azure Network Watcher Flow Logs
- Microsoft Azure Storage Account

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 ist in Taegis MDR enthalten und nativ integriert. Als offene Plattform ermöglicht Taegis MDR Unternehmen und Organisationen, ihre bestehende Endpoint-Protection-Lösung zu nutzen oder für besseren Schutz optional auf Sophos Endpoint upzugraden.

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.

Ergänzende Sophos-Lösungen für Microsoft-Umgebungen

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 Identitäten bis hin zu E-Mails, Netzwerken und darüber hinaus bietet Sophos umfassenden Schutz, der die Lücken schließt, auf die Angreifer setzen.

Sophos Identity Threat Detection and Response (ITDR) für Entra ID

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 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.

Sophos Intelix für Microsoft Copilot

Sophos Intelix integriert die Threat Intelligence von Sophos XOps in Microsoft Security Copilot und Microsoft 365 Copilot und bietet so 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.

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.

Optimal abgestimmt auf Ihre Sicherheitsanforderungen

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 noch heute, um gemeinsam mit uns die optimale Sicherheitsstrategie für Ihre Microsoft-Umgebung zu erarbeiten. Unser Team hilft Ihnen dabei, die optimale Kombination aus Sophos- und Microsoft-Funktionen für Ihre M365 Subscription zu finden, damit Sie das Potenzial Ihrer Microsoft-Investitionen voll ausschöpfen können.

Weitere Informationen: sophos.de/microsoft

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

2026-03-02 BR-DE) CRE-4736