SOPHOS

Managed Detection and Response Buyer's Guide

Da Cyberbedrohungen sich ständig weiterentwickeln, greifen viele Unternehmen und Organisationen auf Managed Detection and Response (MDR) Services zurück. MDR-Experten überwachen Bedrohungen rund um die Uhr und ergreifen umgehend Maßnahmen, um moderne Angreifer zu stoppen.

Mittlerweile gibt es im Bereich MDR allerdings so viele verschiedene Anbieter, Tools und Bereitstellungsoptionen, dass es immer schwieriger wird, den richtigen MDR-Service-Partner für die eigenen spezifischen Sicherheitsanforderungen zu finden.

In diesem Guide erklären wir, welche Funktionen ein leistungsstarker MDR-Service bieten und welche Cybersecurity- und Geschäftsergebnisse er erzielen sollte. Mit diesen Erkenntnissen sind Sie bestens gerüstet, um die richtige Entscheidung für Ihr Unternehmen oder Ihre Organisation zu treffen.

Sophos-Whitepaper, März 2024

Wachsender Bedarf an Security Operations

Die jüngsten Veränderungen in der Bedrohungslandschaft stellen Cybersecurity-Teams vor immer größere Herausforderungen und lassen den Bedarf an gezielter Unterstützung bei der Bereitstellung von Security Operations in Unternehmen und Organisationen jeder Größe in die Höhe schnellen.

Die Entwicklung der Cyberkriminalität

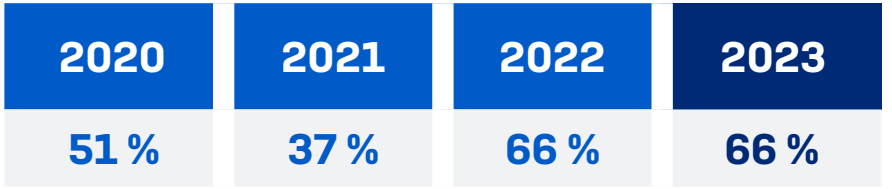
In den letzten Jahren hat sich die Cyberkriminalität zu einem regelrechten Wirtschaftszweig entwickelt: Bedrohungsakteure gehen zunehmend professionell vor, sind gut vernetzt und bieten sogar unterstützende Dienstleistungen an.

Genau wie seriöse Technologieunternehmen setzen auch Cyberkriminelle vermehrt auf ein „As-a-Service"-Modell. Dies erleichtert den Einstieg in die Cyberkriminalität und ermöglicht es Bedrohungsakteuren, immer schneller immer mehr Angriffe mit zunehmend schwerwiegenden Folgen auszuführen. Angreifer sind daher in der Lage, im großen Stil verschiedenste Arten von Angriffen durchzuführen.

Weitere Informationen erhalten Sie in unserem Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen.

Ransomware bleibt eine ständige Bedrohung

Zwei Drittel (66 %) der Unternehmen und Organisationen gaben an, dass sie im letzten Jahr Opfer eines Ransomware-Angriffs waren.



Wurde Ihr Unternehmen/Ihre Organisation im letzten Jahr von Ransomware getroffen?

Ja. Anzahl=3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020)

Während das im Jahr 2023 gemeldete Angriffsaufkommen im Vergleich zum Vorjahr stabil geblieben ist, befinden sich die Datenverschlüsselungsraten bei Ransomware-Angriffen auf dem höchsten Niveau seit vier Jahren. Bei mehr als drei Viertel der Angriffe (76 %) konnten Cyberkriminelle Daten verschlüsseln.

Lesen Sie unsere jährliche Ransomware-Studie, den Ransomware-Report, um mehr über die Häufigkeit, Kosten und Ursachen von Angriffen zu erfahren.

Remote-Ransomware ist eine rasant wachsende Bedrohung, die sich katastrophal auf betroffene Unternehmen und Organisationen auswirken kann. [1]Remote-Ransomware kommt bei rund 60 % der manuell gesteuerten Ransomware-Angriffe zum Einsatz. Bei dieser Angriffsform wird ein kompromittiertes Gerät zur Verschlüsselung von Daten auf anderen Geräten im selben Netzwerk zweckentfremdet.

Bei Remote-Ransomware macht ein einziges nicht verwaltetes oder unzureichend geschütztes Gerät das gesamte Netzwerk anfällig für Remote-Verschlüsselung, auch wenn auf allen anderen Geräten Next-Gen-Antivirus oder -Endpoint-Security läuft.

Technologie allein kann Angreifer nicht stoppen

23 %
waren im letzten Jahr Opfer eines aktiven Angriffs

30 %
zählten aktive Angriffe zu ihren Hauptsorgen in der Cybersecurity in 2023

Praktisch jedes Unternehmen und jede Organisation investiert in Technologien zur Minimierung von Cyberrisiken. Aber unabhängig von der Leistungsstärke dieser Abwehrmaßnahmen wird es unbeirrten Angreifern früher oder später gelingen, die Technologien zu überlisten.

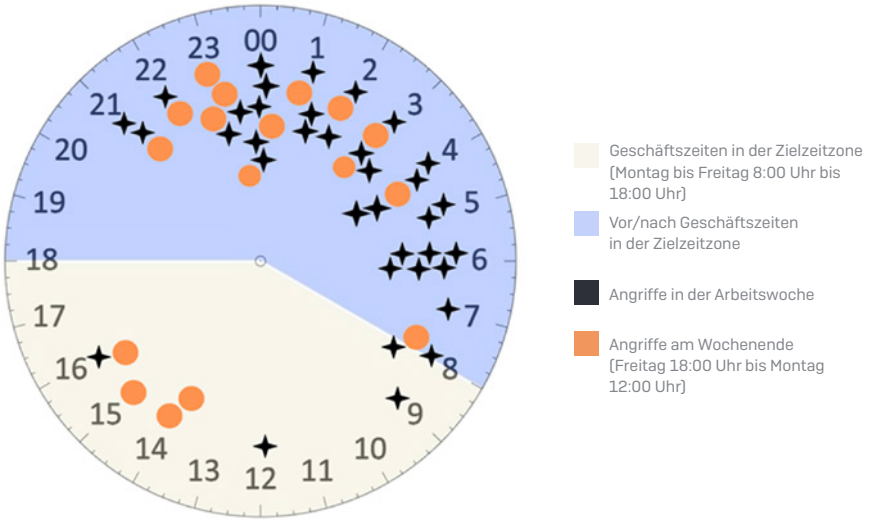
Aktive Angreifer sind versierte Cyberkriminelle, die häufig umfassende Software- und Netzwerkkenntnisse besitzen. Sie verschaffen sich Zugriff auf die Systeme eines Unternehmens, entziehen sich der Erkennung und passen ihre Techniken kontinuierlich an. Mit manuellem Hacking und KI-gestützten Methoden umgehen sie präventive Sicherheitskontrollen und führen den Angriff aus.

Diese Angriffe führen oft zu verheerenden Ransomware-Vorfällen und Datenschutzverletzungen und lassen sich nur sehr schwer stoppen. Zudem sind manuelle Angriffe mittlerweile weit verbreitet. So verzeichneten 23 % der kleinen und mittelgroßen Unternehmen und Organisationen im vergangenen Jahr einen Angriff durch einen aktiven Angreifer[2].

Diese versierten, hartnäckigen Bedrohungsakteure bedienen sich verschiedenster Angriffsmethoden und verfolgen dabei unter anderem folgende Ziele:

- **Ausnutzen von Sicherheitslücken** (gestohlene Zugangsdaten, ungepatchte Schwachstellen und Fehlkonfigurationen von Sicherheitstools), um die Abwehr zu überlisten und sich lateral im Netzwerk zu bewegen.
- **Zweckentfremden legitimer IT-Tools**, um keine Erkennungen auszulösen, z. B. PowerShell, PsExec und RDP.
- **Anpassen ihrer Angriffe in Echtzeit an Sicherheitskontrollen**, indem sie auf neue Techniken ausweichen (z. B. Remote-Ransomware), bis sie ihre Ziele erreichen.
- **Nachahmen autorisierter Benutzer und Ausnutzen von Sicherheitslücken**, um automatisierte Erkennungstechnologien zu überlisten, die nicht zwischen legitimen Benutzern und Angreifern unterscheiden können.
- **Durchführen mehrphasiger Angriffe**, vom Erstzugriff über laterale Bewegungen bis hin zu Erhöhungen der Berechtigungsstufe usw. Aufgrund der vielfältigen Ausprägungsformen mehrphasiger Angriffe ist es wichtig, Einblick in alle wichtigen Angriffsflächen zu haben, um einen Angriff schneller zu erkennen. Denn einzelne Technologien (Endpoint, Firewall, Identity usw.) bilden möglicherweise nur einen kleinen Teil des tatsächlichen Angriffsgeschehens ab.
- **Unternehmen und Organisationen aktiv ins Visier nehmen, wenn eine höhere Wahrscheinlichkeit besteht, unerkannt zu bleiben** – 91 % der Ransomware-Angriffe, die von Sophos Incident-Respondern behoben werden, beginnen außerhalb der regulären Geschäftszeiten in der Zeitzone des betroffenen Unternehmens (Montag bis Freitag vor 8:00 oder nach 18:00 Uhr)[3].

Zu welcher Tageszeit Ransomware-Angreifer zuschlagen[4]



Herausforderungen bei der Bereitstellung von Security Operations

Aufgrund des aktuellen Wandels von Geschäftsumgebungen wird die Situation immer komplexer: Benutzer arbeiten im Büro, mobil oder sind ständig unterwegs. Gleichzeitig können Unternehmensdaten lokal, in der Cloud und auf den Geräten von Remote-Mitarbeitern an verschiedensten Standorten gespeichert werden.

Angesichts dieser Komplexität ist es nicht überraschend, dass mehr als die Hälfte der Unternehmen und Organisationen (52 %) diese modernen Cyberbedrohungen nicht mehr selbst bewältigen können[5].

Zu den größten Herausforderungen von IT-Teams bei der Bereitstellung effektiver Security Operations gehören:

Mangel an Fachkenntnissen – 93 % der IT-Teams erachten Sicherheitsaufgaben als Herausforderung[6] und Fachkräfte sind nach wie vor Mangelware. Ohne die nötige Expertise können Mitarbeiter möglicherweise nicht feststellen, inwieweit eine Sicherheitswarnung einer Reaktion bedarf. Dies löst einen Dominoeffekt aus: Da die Analyse von Warnmeldungen mehr Zeit in Anspruch nimmt, haben die Teams weniger Kapazitäten, was wiederum das Risiko erhöht.

Keine 24/7-Abdeckung – für Unternehmen und Organisationen ist es schwierig, Warnmeldungen und verdächtige Aktivitäten außerhalb der normalen Geschäftszeiten (nachts, an Wochenenden oder Feiertagen) aktiv zu überwachen und entsprechend zu reagieren. Analysten müssen in der Lage sein, verdächtige Aktivitäten proaktiv zu erkennen, diese unmittelbar zu analysieren und darauf zu reagieren.

Reizüberflutung – 71 % der Unternehmen und Organisationen wissen nicht, welche Warnmeldungen sie analysieren sollen. Zu viele Warnhinweise von unterschiedlichen Systemen überfordern Benutzer, die die Signale/Meldungen oft nicht priorisieren können und so Indikatoren für einen Angriff möglicherweise nicht erkennen.

Nicht korrelierte Daten – Bedrohungssignale beschränken sich auf bestimmte Technologien. IT-Teams verfügen daher nicht über den notwendigen Überblick, um schnell auf Warnmeldungen oder Vorfälle reagieren zu können.

Mangelnde Integration – Sicherheitstools lassen sich nicht miteinander verbinden oder in die IT-Infrastruktur eines Unternehmens integrieren, was die Komplexität erhöht.

Manuelle Prozesse – IT-Teams verbringen viele Stunden damit, Ereignisse, Protokolle und Informationen miteinander zu korrelieren, um Geschehnisse nachzuvollziehen. Dadurch werden Angriffe nicht schnell genug erkannt und die Reaktion verzögert sich.

Reaktive Maßnahmen – Viele IT-Teams geraten ins Hintertreffen und reagieren auf Bedrohungen erst, nachdem bereits Schaden entstanden ist, statt sie früher in der Angriffskette zu stoppen.

Fokus auf Akutmaßnahmen – IT-Teams sind mit den täglichen Aufgaben zur Bedrohungsbekämpfung ausgelastet und können sich nicht auf langfristige Verbesserungen konzentrieren. Im Zuge fieberhafter Akutmaßnahmen haben IT-Teams oft nicht die Gelegenheit, den Ursachen von Vorfällen auf den Grund zu gehen und diese zu beheben.

Unternehmen setzen vermehrt auf MDR Services

Aufgrund dieser Bedrohungen und betrieblichen Herausforderungen ergänzen immer mehr Unternehmen und Organisationen ihre internen Cybersecurity-Ressourcen mit einem MDR-Service-Anbieter. Gartner® prognostiziert, dass 60 % der Unternehmen und Organisationen bis 2025 MDR-Service-Provider in Anspruch nehmen werden, gegenüber 30 % im Jahr 2023[7].

MDR-Grundlagen

MDR-Angebote sind 24/7 Fully-Managed Services, die durch ein Team von Sicherheitsexperten bereitgestellt werden. Diese sind auf das Erkennen und Bekämpfen von Cyberangriffen spezialisiert, gegen die reine Technologie-Lösungen machtlos sind. Im Idealfall bietet der MDR Service eine umfassende Incident Response und benachrichtigt Sie nicht nur über Bedrohungen, sondern ergreift auch Reaktionsmaßnahmen für Sie.

Durch Kombination von Expertenwissen mit leistungsstarken Schutztechnologien und künstlicher Intelligenz können Sicherheitsanalysten selbst hochkomplexe, manuell gesteuerte Angriffe erkennen, analysieren und darauf reagieren, Ransomware stoppen, Datenschutzverletzungen verhindern und Betriebsunterbrechungen vermeiden.

MDR sollte nicht mit EDR (Endpoint Detection and Response) oder XDR (Extended Detection and Response) verwechselt werden. Alle drei Lösungen unterstützen zwar Threat Hunting und EDR- und XDR-Tools ermöglichen den Sicherheitsanalysten von Unternehmen und Organisationen, nach potenziellen Bedrohungen zu suchen und diese zu analysieren. Doch nur bei MDR-Services umfasst das Leistungsangebot die Bedrohungssuche, -analyse und -beseitigung durch Analysten eines Sicherheitsanbieters, die diese Aufgaben im Auftrag von Unternehmen und Organisationen übernehmen.

Ein MDR-Service-Provider sollte auf jeden Fall Folgendes bieten:

- **24/7 Threat Monitoring** – ein Expertenteam überwacht Ihre Umgebung, um verdächtige Verhaltensweisen zu erkennen, die auf eine Kompromittierung oder eine Sicherheitsverletzung hindeuten könnten.
- **Von Experten geleitete Reaktionsmaßnahmen** – sofortige ferngesteuerte Gegenmaßnahmen sowie Analyse- und Eindämmungsaktivitäten, die über Warnmeldungen und Benachrichtigungen hinausgehen – ohne Einschränkungen hinsichtlich des Arbeits- und Zeitumfangs für den Erkennungs-, Analyse- und Reaktionsprozess.
- **Umfassende Transparenz** – ein vom Anbieter betriebener Technologiestack (entweder proprietär oder von ausgewählten Partnern kuratiert) wird verwendet, um Einblick in Endpoint-, Firewall-, Identity-, E-Mail-, Netzwerk-, Cloud-, Backup- und andere Sicherheitsdaten-Quellen zu erhalten.
- **Threat Hunting durch Bedrohungsexperten** – konzentriert sich auf die Suche nach Bedrohungen, die mit den derzeitigen Abwehr- oder Erkennungstechnologien nicht erkannt werden können.
- **Threat Intelligence** – Inhalte und Analysen zu Bedrohungen werden zum Erkennen neuartiger Bedrohungen eingesetzt (auch bekannt als „Detection Engineering“).
- **Optimierte Bedrohungserkennung** – spezialisierte MDR-Service-Provider erkennen mehr Cyberbedrohungen als reine Sicherheitstools.

Vorteile durch MDR: Bessere Cybersecurity- und Geschäftsergebnisse

Nachdem wir uns angeschaut haben, was ein MDR-Service auf funktionaler Ebene leisten sollte, möchten wir Ihnen einen umfassenden Überblick darüber verschaffen, wie Ihr Unternehmen von MDR profitieren kann und worauf Sie bei der Wahl eines geeigneten MDR-Anbieters achten sollten. MDR-Services sollten optimale Sicherheits- und Geschäftsergebnisse erzielen.

Stärkere Cyberabwehr und geringeres Cyberrisiko

Ein wesentlicher Vorteil von MDR-Services gegenüber internen Security-Operations-Programmen ist der bessere Schutz vor Ransomware und anderen komplexen Cyberbedrohungen. Dies wiederum minimiert das Cyberrisiko.

Mit MDR profitieren Sie von der umfassenden Erfahrung der Analysten des jeweiligen Anbieters. Im Gegensatz zu einzelnen Unternehmen müssen sich MDR-Anbieter fortlaufend mit verschiedensten Angriffen befassen. So verfügen sie über weitreichende Kenntnisse, die sich interne IT-Teams kaum aneignen können.

MDR-Teams untersuchen zudem täglich Vorfälle und reagieren permanent auf Bedrohungen, sodass sie über viel mehr Routine bei der Bedrohungssuche verfügen. So können sie in allen Phasen des Prozesses schneller und genauer reagieren – vom Erkennen wichtiger Signale bis hin zum Analysieren potenzieller Vorfälle und Beseitigen schädlicher Aktivitäten.

Die Arbeit in einem großen Team ermöglicht es Analysten zudem, ihr Wissen und ihre Kenntnisse auszutauschen, was wiederum ihre Reaktion beschleunigt. Erfahrene MDR-Teams stellen sogenannte „Runbooks" oder „Playbooks" (dokumentierte Prozesse und Protokolle) für jede Bedrohung oder jeden einzelnen Angreifer zusammen. Sobald im Zuge einer Analyse ein Angreifer identifiziert wird, beziehen sich Analysten direkt auf das Runbook und können sofort Gegenmaßnahmen ergreifen, anstatt während des Angriffs umfangreiche Untersuchungen anstellen zu müssen.

Ein weiterer Vorteil von MDR-Services besteht darin, dass sicherheitsrelevante Erkenntnisse auch auf andere Kunden angewendet werden können, die dem gleichen Zielprofil entsprechen. So lassen sich ähnliche Angriffe in dieser Kohorte verhindern. Sollten die Analysten verdächtige Signale erkennen, sind sie in der Lage, die Situation schnell zu untersuchen und die Bedrohung zu beseitigen, was der betroffenen Gruppe eine gemeinschaftliche Immunität verschafft

Mehr Effizienz in der IT

64 % der Unternehmen möchten, dass ihre IT-Abteilungen mehr Zeit für strategische Projekte statt für fieberhafte Akutmaßnahmen gegen Cyberangriffe aufwenden.[8] MDR Services sollten es Ihnen ermöglichen, dieses Ziel zu erreichen.

Threat Hunting ist zeitaufwändig und unvorhersehbar. IT-Experten, die mit mehreren Aufgaben und Prioritäten jonglieren, stoßen schnell an ihre Grenzen: 79 % der kleinen und mittelgroßen Unternehmen und Organisationen räumen ein, dass sie nicht in der Lage sind, alle Protokolle vollständig zu prüfen, um verdächtige Signale und Aktivitäten zu erkennen.

Angesichts der potenziellen Auswirkungen eines Angriffs müssen Ihre Teams jedoch sofort alles stehen und liegen lassen, wenn verdächtige Aktivitäten beobachtet werden, damit die Bedrohung analysiert und umgehend bekämpft werden kann. Die Dringlichkeit der Arbeit führt oft dazu, dass sich Teams nicht mehr auf strategisch wichtige Aufgaben konzentrieren können.

Die Zusammenarbeit mit einem MDR-Service ermöglicht Ihnen, IT-Kapazitäten freizusetzen, um geschäftskritische Projekte voranzutreiben.

Mehr Expertise – ohne mehr Personal

Ein weiterer Vorteil bei der Inanspruchnahme eines MDR-Service besteht darin, dass die Anwerbung spezialisierter Threat Hunter und Sicherheitsanalysten entfällt. Threat Hunting ist ein hochkomplexer Vorgang. Experten in diesem Bereich müssen über spezifisches Fachwissen und Nischenkompetenzen verfügen, was die Rekrutierung für viele Unternehmen und Organisationen zu einer schwierigen – wenn nicht sogar unlösbaren Aufgabe macht.

Cybersecurity Return on Investment (ROI) maximieren

Branchenführende MDR-Anbieter unterstützen Sie dabei, das Potenzial Ihrer bestehenden Sicherheitsinvestitionen optimal auszuschöpfen, indem sie Integrationen mit Ihren bereits vorhandenen Cybersecurity-Technologien ermöglichen. Dank dieses anbieterunabhängigen Ansatzes können Analysten auf Telemetriedaten Ihrer vorhandenen Technologien zurückgreifen, um die Transparenz über mehrere Sicherheitskontrollpunkte hinweg zu erhöhen und die Bedrohungserkennung, -analyse und -reaktion zu beschleunigen. Je mehr die Analysten sehen, desto schneller können sie reagieren.

Wenn Sie sich jedoch in einem früheren Stadium Ihrer Cybersecurity-Implementierung befinden, sollten Sie nach einem MDR-Anbieter suchen, der auch ein breites Portfolio von Sicherheitslösungen anbietet, die tief in die Erkennungs- und Reaktionswerkzeuge integriert sind. Denn die Zusammenarbeit mit einem einzigen Plattformanbieter bietet Ihnen erhebliche betriebliche und finanzielle Vorteile. Anstatt einen Anbieter für den Endpoint-Schutz und einen anderen für einen MDR-Service zu bezahlen, kann die Zusammenarbeit mit demselben Anbieter Ihre Lizenzkosten und den täglichen Verwaltungsaufwand reduzieren. Zudem erhalten Sie alle Dienstleistungen aus einer Hand.

Darüber hinaus erhöhen MDR-Services Ihren Schutz, wodurch Sie Ihr Risiko für kostspielige Datenschutzverletzungen oder Ransomware-Vorfälle und Bereinigungsmaßnahmen senken. Im Jahr 2023 betrugen die durchschnittlichen Kosten für die Behebung eines Ransomware-Angriffs ganze 1,82 Mio. US$[9]. Einen MDR-Service in Anspruch zu nehmen, ist daher eine sinnvolle Investition.

Cyberversicherungs-Schutz optimieren

Cyberversicherungs-Prämien sind in den letzten Jahren deutlich gestiegen und die Anwendung von Policen ist komplexer und zeitaufwändiger geworden. Versicherer fordern striktere Cyber-Kontrollmechanismen. So bestätigten 95 % der Unternehmen und Organisationen, die im letzten Jahr eine Versicherung abgeschlossen hatten, dass die Qualität ihrer Abwehrmaßnahmen direkten Einfluss auf ihren Versicherungsstatus hatte[10].

Die besten Versicherungskonditionen erzielen Sie, indem Sie Cyberrisiken minimieren. Durch die Investition in starke Abwehrmaßnahmen, einschließlich 24/7 Sicherheitsservices und branchenführender Detection and Response Tools, erhalten Sie bessere Konditionen bei Cyber-Versicherungen. Besserer Cyberschutz

1. erleichtert den Abschluss von Cyberversicherungen.
2. kann Prämien reduzieren und die Konditionen verbessern.
3. verringert die Wahrscheinlichkeit von Schadensfällen – und die daraus resultierenden höheren Prämien.
4. reduziert das Risiko, dass die Versicherung nicht zahlt.

Services, die die Erkennung und Reaktion optimieren und somit das Risiko eines Cybervorfalls minimieren, stehen bei Cyber-Versicherern besonders hoch im Kurs. Unternehmen und Organisationen, die MDR Services in Anspruch nehmen, gelten bei Versicherern häufig als Premium-Kunden, da sie das geringste Risiko darstellen.

Zentrale Überlegungen

Nachdem Sie jetzt eine genauere Vorstellung davon haben, welche Funktionen ein leistungsstarker MDR-Service bieten sollte, haben wir hier einige Aspekte aufgeführt, die Sie berücksichtigen sollten, bevor Sie potenzielle Anbieter in die engere Wahl ziehen.

1. **Was möchten Sie erreichen?**

   Wie definieren Sie Erfolg für Ihr Unternehmen/Ihre Organisation? Bei dieser Überlegung spielen auch Ihre aktuellen Herausforderungen und Beweggründe für die Nutzung eines MDR-Service eine wichtige Rolle.

2. **Wie möchten Sie mit dem MDR-Service zusammenarbeiten?**

   Betrachten Sie Ihre derzeitige IT-/Cybersecurity-Organisation und überlegen Sie, inwiefern Ihr aktuelles Team involviert werden soll und welche Aufgaben Sie dem MDR-Service übertragen möchten. Suchen Sie nach zusätzlichem Cyberschutz an Wochenenden, Feiertagen und nachts? Soll der MDR-Service Sie über Vorfälle benachrichtigen, damit Sie selbst reagieren können, oder wünschen Sie, dass der MDR-Service für Sie Reaktionsmaßnahmen ergreift?

3. **Welche Sicherheitslösungen nutzen Sie aktuell?**

   Machen Sie sich mit den IT- und Sicherheitstechnologien vertraut, die Sie bereits einsetzen, z. B. Endpoint-Schutz, Netzwerk-Firewalls, E-Mail-Gateways, Identity-Lösungen usw. Im Idealfall kann der MDR-Service Telemetriedaten dieser Produkte einbeziehen. So erhält das Team einen besseren Einblick in Ihre Umgebung und kann Bedrohungen schneller erkennen, analysieren und darauf reagieren

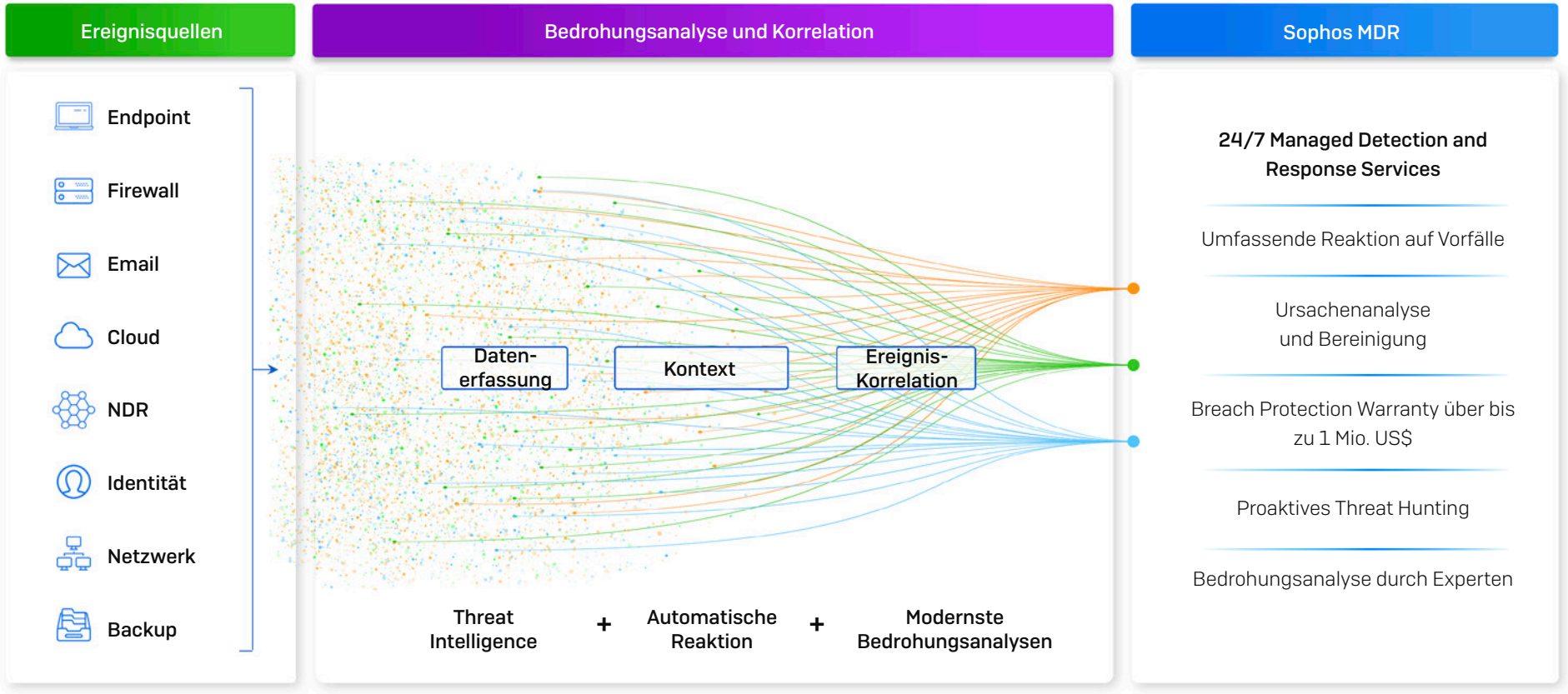
10 Fragen, die Sie bei der Auswahl eines MDR-Service beachten sollten

Nachdem Sie Ihre Anforderungen ermittelt haben, finden Sie hier einige Fragen, die Sie einem potenziellen Anbieter stellen sollten.

1. Welche nativen Sicherheitslösungen stellen Sie Ihren MDR-Analysten zur Verfügung (Endpoint Protection, E-Mail Security usw.)?
2. Kann der Service in meine bestehenden Cybersecurity-Lösungen von anderen Anbietern integriert werden?
3. Welchen Mehrwert bieten diese Integrationen Ihren MDR-Analysten?
4. Wie lange dauert es in der Regel, bis Ihr Team auf Bedrohungen reagiert?
5. Welche Reaktionsmaßnahmen kann Ihr Team für uns ergreifen und welche Aufgaben müssen wir intern übernehmen?
6. Kann der MDR-Service erweitert werden, wenn unser Unternehmen/unsere Organisation wächst?
7. Bieten Sie Ihre Supportleistungen in verschiedenen Abstufungen an? Bieten Sie angepasste Servicelevel an?
8. Was sagen Bestandskunden über Ihren Service?
9. Bieten Sie einen umfassenden Incident-Response-Service, bei dem aktive Bedrohungen gestoppt, eingedämmt und vollständig beseitigt werden? Sind diese Maßnahmen Teil Ihres Service oder werden sie separat in Rechnung gestellt?
10. Bieten Sie eine Breach Protection Warranty an?

Sophos Managed Detection and Response (MDR)

Sophos MDR ist ein vollständig verwalteter 24/7-Service, der von Experten bereitgestellt wird. Die hochspezialisierten Experten erkennen Cyberangriffe auf Ihre Computer, Server, Netzwerke, Cloud Workloads und E-Mail-Konten und ergreifen Reaktionsmaßnahmen. Mit Sophos MDR stoppen unsere Experten komplexe, manuell gesteuerte Angriffe und ergreifen Sofortmaßnahmen, um Bedrohungen zu beseitigen, bevor diese Ihre Geschäftsabläufe stören oder Ihre sensible Daten gefährden können.



MDR – maßgeschneidert für Sie

Sophos MDR ist der weltweit meist genutzte Managed Detection and Response Service. Er schützt Unternehmen und Organisationen in allen Branchen – von kleinen Unternehmen mit begrenzten IT-Ressourcen bis hin zu Großkonzernen mit eigenen Security-Operations-Teams. Die drei beliebtesten Response-Modelle von Sophos MDR sind:

- Sophos MDR verwaltet die Reaktion auf Bedrohungen für Sie.
- Sophos MDR arbeitet mit Ihrem internen Sicherheitsteam zusammen und koordiniert die Maßnahmen zur Bedrohungserkennung und -reaktion.
- Sophos MDR unterstützt und ergänzt Ihre interne IT-Security, meldet Vorfälle, die Maßnahmen erfordern, und liefert Informationen zu Bedrohungen sowie Empfehlungen zur Reaktion.

Dank unseres flexiblen Ansatzes kann Sophos die spezifischen Anforderungen Ihres Unternehmens bzw. Ihrer Organisation optimal erfüllen. Vom vollständig verwalteten 24/7-Service bis hin zur gezielten Ergänzung interner Security-Teams – wir bieten individuell auf Ihre Bedürfnisse zugeschnittene Service-Leistungen.

Rund um die Uhr aktiv – mit sieben globalen Security Operations Centern (SOCs)

Unser global aufgestelltes Team mit über 500 Threat Detection and Response-Experten ist auf sieben Security Operations Center (SOCs) verteilt: Diese befinden sich in den USA, Europa (UK/Irland und Deutschland), Asien und Australien.

Unsere Experten sind spezialisiert auf alle Bereiche rund um das Thema Cyberbedrohungen, darunter Malware, künstliche Intelligenz und Bedrohungsbereinigung. Damit verfügen sie über eine außerordentlich fundierte und breitgefächerte Expertise, die sich interne IT-Teams kaum aneignen können.

Branchenweit führende Analyse- und Reaktionszeiten

Dank der einzigartigen Kombination aus menschlicher Expertise, Technologie und Bedrohungserfahrung bereinigt Sophos MDR Bedrohungen in durchschnittlich nur 38 Minuten und sorgt so für effektiven Cyberschutz.

- Durchschnittliche Zeit bis zur Erkennung (Mean Time To Detect, MTTD): 1 Minute
- Durchschnittliche Zeit für die Analyse (Mean Time To Investigate, MTTI): 25 Minuten
- Durchschnittliche Zeit bis zur Reaktion (Mean Time To Respond, MTTR): 12 Minuten

Sophos Breach Protection Warranty

Sophos MDR ist der MDR-Service, dem branchenweit die meisten Unternehmen vertrauen. Mit der Sophos Breach Protection Warranty erhalten Kunden von Sophos MDR Complete die Gewissheit, dass sie im Schadensfall finanziell abgesichert sind.

Die Sophos Breach Protection Warranty ist ohne Aufpreis in unserer **Sophos MDR Complete** Subscription enthalten. Die Warranty deckt Kosten

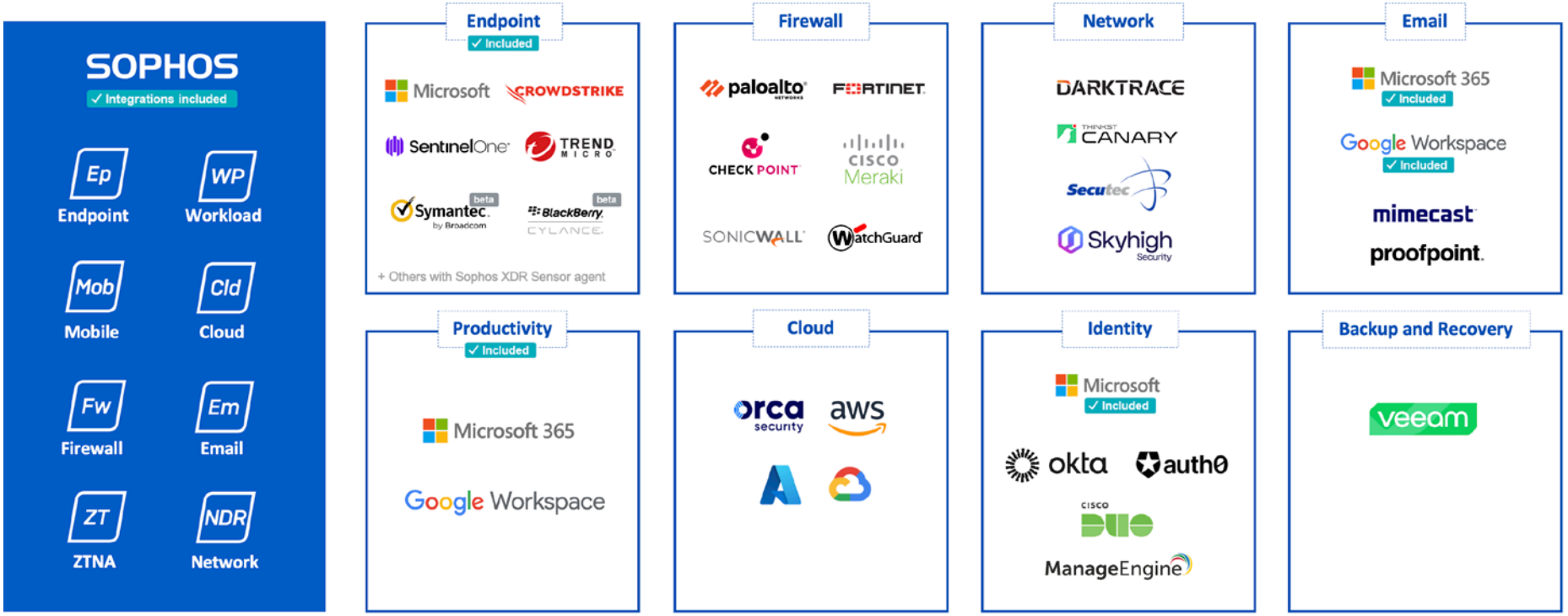
- bis zu 1 Mio. US$ für Reaktionsmaßnahmen.
- bis zu 100.000 US-Dollar Lösegeld (als Teil des Limits pro Gerät).
- bis zu 1.000 US-Dollar pro kompromittiertem System.
- Und sie deckt diverse Ausgaben ab, darunter Kosten für die Anzeige des Datenschutzverstoßes, PR-, Rechts- und Compliance-Kosten.

Die vollständigen Bedingungen finden Sie unter www.sophos.de/legal

Branchenführende Kompatibilität

Ganz gleich, ob Sie die Tools von Sophos, Ihre vorhandenen Technologien oder eine Kombination aus beidem verwenden möchten: Sophos MDR lässt sich in die gesamte vorhandene IT-Struktur integrieren, einschließlich nativer und Fremdanbieter-Integrationen mit Endpoint-, Netzwerk-, Cloud-, E-Mail- und Microsoft-365-Lösungen.

Unser anbieterunabhängiger Ansatz bietet unseren Analysten einen umfassenden Einblick in Ihre gesamte IT-Umgebung, was zu einer schnelleren Bedrohungserkennung, -analyse und -reaktion führt. Darüber hinaus erhöhen diese Integrationen den Return on Investment vorhandener Lösungen. Wir bieten u. a. folgende Integrationen an:



Die Lösungen Sophos Endpoint und Sophos Workload Protection sind in Sophos XDR und MDR enthalten. Für Integrationen anderer Sophos-Produkte ist eine Subscription der entsprechenden Lösung erforderlich.

Endpoint-, Microsoft- und Google-Workspace-Drittintegrationen sind in den Subscriptions von Sophos XDR und MDR ohne Aufpreis enthalten.

Integration Packs für andere Lösungen, die nicht von Sophos stammen, sind als Add-on Subscriptions für jede Integrationskategorie erhältlich. Die Lizenzierung erfolgt nach Gesamtzahl der Benutzer und Server.

Integrationen ab 8. Februar 2024. Eine aktuelle Liste erhalten Sie auf Anfrage bei Ihrem Sophos-Ansprechpartner.

Bessere Cybersecurity- und Geschäftsergebnisse mit Sophos MDR

Weiter oben in diesem Guide haben wir uns die Ergebnisse angeschaut, die jeder MDR-Service liefern sollte. Jetzt möchten wir darauf eingehen, wie Sophos MDR für bessere Cybersecurity- und Geschäftsergebnisse sorgt.

Cyberabwehr verstärken, Cyberrisiken minimieren

Sophos-Analysten verfügen über einen weitreichenden Erfahrungsschatz, den sich interne IT-Teams kaum aneignen können. Zudem sind sie routiniert im Umgang mit Threat-Hunting-Tools und der Auswertung von Telemetriedaten. So können sie in allen Phasen des Prozesses schnell und gezielt reagieren – vom Erkennen wichtiger Signale bis hin zum Analysieren potenzieller Vorfälle und Beseitigen schädlicher Aktivitäten.

Sophos MDR schützt mehr Unternehmen und Organisationen als alle anderen Anbieter. So erreichen wir eine gemeinschaftliche Immunität. Sicherheitsrelevante Erkenntnisse können auch auf andere Kunden angewendet werden, die dem gleichen Zielprofil entsprechen. Auf diese Weise kann Sophos ähnliche Angriffe in dieser Kohorte proaktiv verhindern.

★★★★★

„Die Pentester waren fassungslos, dass sie keine Eintrittspforte finden konnten. Ab da wussten wir, dass wir dem Service von Sophos voll vertrauen können."

University of South Queensland

★★★★★

„Mit Sophos MDR können wir viel schneller auf Bedrohungen reagieren."

Tata BlueScope Steel

★★★★★

„Wir werden in Echtzeit über alle Bedrohungen benachrichtigt."

Bardiani Valvole

Sicherheitsinvestitionen optimal nutzen

Mit Sophos MDR steigern Sie die Effizienz Ihrer Sicherheitstools und Ihres IT-Security-Teams. Die Bedrohungserkennung und -reaktion beansprucht IT-Kapazitäten stark. Sophos MDR schafft hier Abhilfe und setzt wertvolle IT-Ressourcen für strategische Aufgaben frei.

MDR-Kunden können unsere Security-Operations-Experten rund um die Uhr telefonisch erreichen und Reports zur Bedrohungsaktivität in der Sophos-Central-Plattform abrufen. So können sie schneller und genauer auf Warnmeldungen reagieren.

Sophos MDR verbessert Ihre Abwehr durch Einbindung von Telemetriedaten Ihrer vorhandenen Sicherheitstools. So wird die Transparenz erhöht, die Bedrohungserkennung -und reaktion beschleunigt und dabei Ihr Return on Investment vorhandener Lösungen gesteigert.

★★★★★

„Anstatt Zeit mit Analysen und manuellen Suchen in Bedrohungsdatenbanken usw. zu verbringen, habe ich mit dem MDR-Team von Sophos hochqualifizierte Experten an meiner Seite, die diese Warnmeldungen für mich rund um die Uhr im Auge behalten."

United Musculoskeletal Partners, USA

★★★★★

„Seit der Einführung von Sophos konnten wir im operativen Bereich erheblich Zeit einsparen. So haben unsere Teams wieder mehr Kapazitäten, um sich Aufgaben zu widmen, die den Studierenden zugutekommen und deren Zufriedenheit erhöhen."

London South Bank University

★★★★★

„Sophos MDR meldet, behebt und entfernt Bedrohungen schnell und zuverlässig. So haben wir mehr Zeit, uns auf wertschöpfende Aufgaben zu konzentrieren."

Tomago Aluminium

Von mehr Expertise profitieren – ohne mehr Personal

Bei Sophos bieten mehr als 500 erfahrene Analysten über 20.000 Kunden auf der ganzen Welt zuverlässige MDR-Services. Mit Sophos MDR können Unternehmen und Organisationen Ihre Security Operations ohne zusätzliches Personal aufstocken.

„Wir konnten unser Security-Team erweitern, ohne selbst zusätzliche Experten einstellen zu müssen."

Hammondcare, Australien

„Mit einem erfahrenen MDR-Team wie dem von Sophos erhalten Sie Unterstützung von Experten, die Meister ihres Fachs sind."

United Musculoskeletal Partners, USA

„Sophos MDR hat uns geholfen, dem rasanten Anstieg an immer komplexeren Bedrohungen Herr zu werden, ohne dass wir unser Sicherheitsteam erweitern mussten."

Tourism Finance Corporation of India Limited, Indien

„Sophos erspart uns die Kosten, bis zu fünf neue Mitarbeiter für diese Arbeit einzustellen."

AG Barr, UK

Cyberversicherungs-Schutz optimieren

Mit Sophos MDR erfüllen Unternehmen viele Kontrollmechanismen, die Versicherer an ihre besten Angebote knüpfen, z. B. 24/7 Detection and Response, Incident-Response-Pläne, Protokollierung und Monitoring, und mehr.

Kunden von Sophos MDR schildern uns, dass Versicherer ihnen bessere Konditionen beim Versicherungsschutz bieten, weil sie Cyberrisiken reduzieren. Darüber hinaus erkennen mehrere führende Versicherungsanbieter die Cyberrisiko-Senkung durch unseren Service an und bieten exklusive Prämienrabatte und automatische Versicherungsangebote für Kunden von Sophos MDR. Wenn Sie Fragen haben oder Unterstützung benötigen, hilft Ihnen Ihr Sophos-Partner gerne weiter.

„Durch unsere Zusammenarbeit mit Sophos for XDR und MDR konnten wir unsere Cyberversicherungs-Prämien senken, obwohl uns zu Beginn der Partnerschaft gesagt wurde, dass sich die Prämien verdoppeln würden. Das ist ein großer Erfolg, der einen echten Mehrwert darstellt. Sogar unser CFO bedankte sich für unseren Einsatz und MDR trug entscheidend dazu bei."

Bob Pellerin, CISO, The Fresh Market

Branchenweit führender MDR-Service

Sophos ist der weltweit führende MDR-Anbieter und schützt mehr Unternehmen als alle anderen Anbieter vor Ransomware, Sicherheitsvorfällen und anderen Bedrohungen, die Technologien allein nicht stoppen können. Sophos MDR sorgt für Schutz von Unternehmen und Organisationen aller Branchen weltweit und bietet beispiellose Expertise zu branchenspezifischen Cyberbedrohungen.

Gartner® Peer Insights™

Sophos ist die am besten und häufigsten bewertete MDR-Lösung bei Gartner® Peer Insights™ mit einer durchschnittlichen Bewertung von 4.8/5 (435 Bewertungen insgesamt [mehr als jeder andere Anbieter], Stand: 23. Januar 2024). 97 % der Kunden würden uns weiterempfehlen. Darüber hinaus wurde Sophos als einziger Anbieter in all diesen Kategorien zur Gartner Customers' Choice ernannt:

- Managed Detection and Response (MDR)
- Endpoint Protection Plattformen
- Netzwerk-Firewalls
- Mobile Threat Defense

Gartner® Magic Quadrant™ for Endpoint Protection Platforms

Sophos wurde 2023 zum 14. Mal in Folge im Gartner® Magic Quadrant™ for Endpoint Protection Platforms (EPP) als Leader eingestuft.

Der Report bietet Lesern eine umfassende Bewertung der branchenführenden Endpoint-Prevention-Lösungen und bewertet XDR- und MDR-Angebote. Die Stärke sowohl unserer XDR-Plattform als auch unseres MDR-Service trug dazu bei, dass wir bei dieser Bewertung weiterhin eine Leader-Position einnehmen.

Im IDC MarketScape 2024 in der Kategorie „Worldwide Modern Endpoint Security for Small and Midsize Businesses" ausgezeichnet

Bei diesen Bewertungen von IDC MarketScape wird untersucht, inwieweit die Endpoint-, EDR- und MDR-Lösungen unterschiedlicher Anbieter den Anforderungen von sowohl kleinen als auch mittelgroßen Unternehmen gerecht werden. Die Stärke unseres MDR-Services trug zu unserer führenden Position als Leader in beiden Bewertungen bei.

G2 Grid® Reports

Sophos ist Leader in den G2 Grid® Reports für Managed Detection and Response und Leader für MDR im G2 Grid für den Midmarket- und Enterprise-Sektor insgesamt. In den Winterreports 2024 von G2 wurde Sophos in mehreren Kategorien als Leader eingestuft, darunter XDR, EDR, Network Firewall und Endpoint Protection.

MITRE Engenuity ATT&CK Evaluations 2023

Sophos erzielte bei den MITRE Engenuity ATT&CK® Evaluations 2023, die sich explizit auf die Erkennung und Reaktion von Bedrohungen konzentrierten, Bestleistungen. Unsere XDR-Lösung Sophos XDR erkannte bei den Tests 99 % der Bedrohungsaktivitäten und meldete umfangreiche analytische Daten zu 98 % der Teilschritte in den Tests.

Ein wichtiges Ergebnis, da Sophos XDR unseren MDR-Service unterstützt.

Die Analysten von Sophos MDR nutzen unsere XDR-Funktionen, um die Bedrohungserkennung und -reaktion zu unterstützen und zu beschleunigen.

MITRE Engenuity ATT&CK Evaluation für Security Service Provider 2022

Sophos MDR erzielte in jeder Kategorie der ATT&CK® Evaluation for Security Services Providers 2022 Bestleistungen – der ersten ATT&CK Evaluation für Managed Services. Sophos konnte während der Bewertung mit einer außergewöhnlichen Leistung bei analytischen Erkennungen, bei der Teilschrittabdeckung, Alarmkonsolidierung und Expertenanalyse punkten.

Zusammenfassung

Da Angreifer ihr Verhalten und ihre Tools ständig an aktuelle Gegebenheiten anpassen und weiterentwickeln, wird MDR für immer mehr Unternehmen und Organisationen jeder Größe unverzichtbar. Die Zusammenarbeit mit einem bewährten MDR-Anbieter wie Sophos bietet zahlreiche Vorteile – ganz gleich, ob Sie Ihr Threat Hunting komplett auslagern oder Ihre internen Services ergänzen und verbessern möchten:

1. Sie verbessern Ihre Cyberabwehr.
2. Sie steigern Ihre IT-Effizienz.
3. Sie profitieren von mehr Expertise – ohne mehr Personal.
4. Sie steigern Ihren Cybersecurity ROI.
5. Sie optimieren Ihren Cyber-Versicherungsschutz.

Weitere Informationen zu Sophos MDR erhalten Sie bei Ihrem Sophos-Partner oder unter www.sophos.de/mdr

1 Microsoft Digital Defense Report 2023

2 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen – Sophos

3 So stoppen Sie aktive Angreifer: Neueste Erkenntnisse aus der Cybersecurity-Praxis – Sophos [nimmt Bezug auf Ransomware-Angriffe, weil sie die zuverlässigsten und objektivsten Indikatoren in der Analyse waren]

4 So stoppen Sie aktive Angreifer: Neueste Erkenntnisse aus der Cybersecurity-Praxis – Sophos

5 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen – Sophos

6 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen – Sophos

7 Gartner® Market Guide for Managed Detection and Response Services 2023

8 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen – Sophos

9 Ransomware-Report 2023 – Sophos

10 Sophos Guide zu Cyberversicherungen – Sophos

Mehr dazu, wie Unternehmen und Organisationen von Sophos MDR profitieren können, erfahren Sie unter sophos.de/mdr

2023-02-27 (WP-NP)

SOPHOS