SOPHOS

E-BOOK

EDR, XDR, MDR

Wie unterscheiden sich diese Lösungen und welche ist die richtige für Ihr Unternehmen?

INHALT

EDR, XDR, MDR

Wie unterscheiden sich diese Lösungen und welche ist die richtige für Ihr Unternehmen?

IT- und Security-Verantwortliche stehen zunehmend unter Druck, die Cyber-Resilienz zu stärken, ohne dabei knappe Ressourcen oder Budgets zu überlasten. Gleichzeitig werden Cyberangriffe nicht nur häufiger, sondern auch immer komplexer. Daher sind kluge Investitionen in Erkennungs- und Reaktions-Funktionen wichtiger denn je.

Ganz gleich, ob Sie weltweit operieren oder ein kleineres Team leiten: Ihre Sicherheitsstrategie sollte auf das Risikoprofil und die operativen Rahmenbedingungen Ihres Unternehmens abgestimmt sein. Für viele Verantwortliche bedeutet dies auch, zu entscheiden, ob Erkennung und Reaktion intern gemanagt oder gemeinsam mit einem verlässlichen Partner erfolgen sollen.

Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) und Managed Detection and Response (MDR) bieten jeweils andere Vorteile. Die Herausforderung besteht darin, zu bestimmen, welche Lösung den größten Mehrwert für Ihr Unternehmen bringt. EDR und XDR sind Technologien, die Ihrem Team helfen, Bedrohungen schneller zu erkennen, zu analysieren und darauf zu reagieren. MDR ist ein Service, der 24/7-Monitoring und -Reaktion durch Experten bietet, in der Regel unter Einsatz von XDR und anderen Technologien.

Zu verstehen, wie sich diese Ansätze unterscheiden – und wie sie sich ergänzen können – ist der erste Schritt zu einer effektiven und zukunftsfähigen Sicherheitsstrategie.

Warum Erkennung und Reaktion so wichtig sind

Ein robuster Endpoint-Schutz bleibt eine entscheidende erste Verteidigungslinie. Doch immer öfter schaffen es Angreifer, diese Abwehr zu umgehen: Sie missbrauchen legitime Zugangsdaten, geben sich als vertrauenswürdige Nutzer aus und zweckentfremden native IT-Tools. Solche Angriffe erscheinen für ein einzelnes Präventions-Tool unter Umständen nicht bösartig und bleiben unentdeckt.

Erkennungs- und Reaktionsfunktionen wie EDR, XDR und MDR schließen diese wichtige Lücke. Die Lösungen ermöglichen es, Bedrohungen zu erkennen und zu beseitigen, die es durch die Abwehr schaffen, bevor sie sich zu schwerwiegenden Sicherheitsvorfällen entwickeln.

WAS IST EDR?

Endpoint Detection and Response (EDR) ist Teil einer ganzheitlichen Endpoint-Security-Strategie. EDR unterstützt Security-Teams dabei, Bedrohungen und Sicherheitsvorfälle auf Endgeräten wie Laptops, Desktop-Computern und Servern zu überwachen, zu erkennen und darauf zu reagieren.

Wichtigste Vorteile von EDR:

Echtzeit-Transparenz über Endpoint-Aktivitäten: EDR bietet umfassende Einsicht in Vorgänge wie Dateiausführungen, Prozessverhalten und laterale Bewegungen. Dadurch können Teams Bedrohungen schnell erkennen und stoppen, bevor sie sich ausbreiten.

Erkennung evasiver Bedrohungen durch Verhaltensindikatoren: EDR erkennt Anomalien im Verhalten von Prozessen und Systemen und deckt so Angriffe auf, die klassische Präventions-Tools oft übersehen.

Automatisierte Reaktionsmaßnahmen: EDR kann infizierte Endpoints automatisch isolieren oder schädliche Prozesse beenden. Dadurch wird die Verweildauer der Angreifer verkürzt und verhindert, dass sie weiteren Zugriff erlangen.

Auf unserer Webseite zu Sophos EDR erfahren Sie mehr dazu, wie Sophos EDR Ihre Endpoints und Server vor komplexen, manuell gesteuerten Angriffen schützen kann – im Büro, im Netzwerk oder in der Cloud.

WAS IST XDR?

Extended Detection and Response (XDR) bietet deutlich mehr Transparenz über Bedrohungen, denn XDR nutzt Daten aus dem gesamten Security-Ökosystem. Einbezogen werden neben Endpoints und Servern auch Firewalls, E-Mails, Cloud-Infrastrukturen, Identity-Systeme, Backup- und Recovery-Lösungen, Produktivitäts-Tools etc. XDR ermöglicht dadurch eine effektivere Korrelation verdächtiger Aktivitäten.

Während EDR sich auf die Endpoint-Ebene konzentriert, stellt XDR Zusammenhänge zwischen Daten aus allen Systemen her. So entsteht ein ganzheitliches Lagebild, das es einfacher macht, mehrstufige, multi-vektorielle Angriffe zu erkennen, die sonst eventuell übersehen werden.

Wichtigste Vorteile von XDR:

Korrelation von Signalen über mehrere Angriffsvektoren hinweg: Dies ermöglicht es, Muster zu erkennen und hochrelevante Warnmeldungen klar zu priorisieren. So wird die Flut irrelevanter Daten reduziert und komplexe, mehrere Systeme betreffende Bedrohungen rücken in den Fokus.

Schnellere, fundiertere Untersuchungen: Durch optimierte Analyse-Workflows können Teams schneller und souveräner reagieren. Analysten erhalten eine klare Sicht darauf, wie ein Angriff begonnen und sich ausgebreitet hat. So erhalten sie Erkenntnisse, wie sich ähnliche Vorfälle künftig verhindern lassen.

Effizientere Bereinigung: XDR unterstützt die Workflows zur Untersuchung und Reaktion mit KI-gestützten Tools. So werden eine schnellere Analyse und Bereinigung eines Vorfalls ermöglicht.

Auf unserer Webseite zu Sophos XDR erfahren Sie mehr dazu, wie Sophos XDR es Ihnen ermöglicht, verdächtige Aktivitäten in Ihrer gesamten Umgebung zu erkennen, zu analysieren und darauf zu reagieren.

WAS IST MDR?

Managed Detection and Response (MDR) ist ein serviceorientiertes Modell, das KI-gestützte Technologien mit der Expertise erfahrener Security-Analysten kombiniert. MDR bietet 24/7 Monitoring, Threat Hunting und Incident Response. Der Service eignet sich ideal für Unternehmen, die keine eigenen 24/7 Security Operations betreiben oder gewährleisten können, mit begrenzten Ressourcen oder wachsender Komplexität zu kämpfen haben.

MDR kann als vollständig ausgelagerte Lösung betrieben werden oder als co-managed Erweiterung des internen Security Teams. In beiden Fällen hilft MDR, die Verweildauer von Angreifern zu verkürzen und Vorfälle wie Ransomware zu stoppen, bevor sie eskalieren.

Wichtigste Vorteile von MDR:

Lückenloser 24/7-Schutz: Cyberangriffe halten sich nicht an Geschäftszeiten. 88 % der Ransomware-Angriffe erfolgen außerhalb der regulären Arbeitszeiten. MDR gewährleistet Schutz rund um die Uhr.

Zugriff auf erfahrene Security-Analysten: MDR-Teams arbeiten täglich mit realen Angriffsszenarien. Sie erkennen typische Muster und Taktiken von Angreifern, priorisieren Vorfälle und ergreifen sofort Maßnahmen, um weiterhin einen reibungslosen Geschäftsablauf zu gewährleisten.

Keine Alert Fatigue und weniger manuelle Triage: MDR filtert irrelevante Informationen heraus, sodass sich Ihr Team auf strategische Aufgaben konzentrieren kann, statt ständig Fehlalarme zu prüfen.

Schnelle Reaktion in kritischen Situationen: Bei kritischen Vorfällen wie Ransomware-Angriffen können MDR-Teams Bedrohungen erkennen und eindämmen, bevor interne Teams den Vorfall überhaupt bemerken. So werden Störungen verhindert und Risiken reduziert.

Auf unserer Webseite zu Sophos MDR erfahren Sie mehr dazu, wie Sophos MDR Ihr Team ergänzen und entlasten kann und gleichzeitig für mehr Sicherheit sorgt.

EDR, XDR, MDR: WANN WELCHE LÖSUNG PASST

Lösung	Sinnvoll in diesen Fällen:	Weniger geeignet in diesen Fällen:
EDR	• Sie benötigen eine robuste Endpoint Detection and Response. • Sie möchten Ihre Abwehrmaßnahmen über präventive Endpoint Protection hinaus erweitern. • Sie bauen eine mehrschichtige Verteidigung auf, die künftige XDR- oder MDR- Integrationen unterstützen soll	• Sie benötigen umfassendere Transparenz über Ihre gesamte Umgebung (Cloud, Identity, Netzwerk, Backup etc.). • Sie erwarten 24/7 Detection and Response ohne Outsourcing oder zusätzliches Personal.
XDR	• Sie benötigen einen zentralen Überblick über alle wichtigen Angriffsvektoren, einschließlich Endpoint, Firewalls, Netzwerk, Cloud, Identity, Backup und Produktivitätstools. • Sie möchten eine schnellere Korrelation von Bedrohungsdaten erreichen und irrelevante Warnmeldungen reduzieren. • Sie wollen den ROI Ihrer bestehenden und künftigen Security- und IT-Investitionen steigern.	• Sie überwachen nur Endpoints und Server. • Sie benötigen mehr praktische Unterstützung, als Ihr Team leisten kann. • Ihnen fehlen die internen Ressourcen, um eine XDR Plattform selbst zu managen.
MDR	• Sie benötigen eine von Experten geleitete 24/7 Threat Detection and Response. • Sie kämpfen mit Alert Fatigue, Fachkräftemangel oder Burnout. • Sie möchten einen proaktiven Partner, der Bedrohungen für Sie analysiert und beseitigt. • Sie möchten Ihre Position bei Cyberversicherungen verbessern (z. B. niedrigere Prämien, bessere Bedingungen).	• Sie verfügen bereits über ein voll funktionsfähiges internes SOC mit ausreichend hochqualifizierten Spezialisten, das verlässliche 24/7/365 Abdeckung bietet. • Sie sind noch nicht bereit, Teile Ihrer Detection- und Response-Prozesse auszulagern.

WEITERE ÜBERLEGUNGEN VOR DER ENTSCHEIDUNG

Bei der Auswahl zwischen EDR, XDR oder MDR gibt es zentrale Faktoren, die darüber entscheiden, welche Lösung am besten zu Ihrem Unternehmen passt – und welcher Partner dieses Leistungsversprechen tatsächlich einlösen kann.

Threat Intelligence ist entscheidend

Die Effektivität jeder Detection and Respone-Lösung steht und fällt mit der Qualität der zugrunde liegenden Bedrohungsdaten. Je umfassender, aktueller und kontextreicher die Daten sind, desto schneller lassen sich Bedrohungen erkennen und stoppen. Achten Sie darauf, dass potenzielle Anbieter transparent darlegen können, woher ihre Bedrohungsdaten stammen, wie umfassend diese Daten sind und wie häufig sie aktualisiert werden.

Service sollte mehr sein als ein Versprechen

Selbst die beste Technologie bleibt wirkungslos, wenn der zugehörige Service nicht zuverlässig ist. Ob Sie eine Lösung selbst betreiben oder auf einen Partner für Managed Services setzen – entscheidend ist, dass Sie im Bedarfsfall schnell und kompetent Hilfe erhalten. Klären Sie mit Anbietern: Wer reagiert im Ernstfall und wie schnell? Welche Leistungen sind enthalten? Wie erhalten Sie Unterstützung während eines aktiven Vorfalls?

Ermitteln Sie die tatsächlichen Kosten

Ein Lösungsansatz muss nicht zwingend teurer sein als ein anderer. Die Preise variieren stark, je nachdem, wie die jeweilige Lösung implementiert und betrieben wird. Überlegen Sie genau, was Sie wirklich benötigen: Berücksichtigen Sie vorhandene personelle Ressourcen und bestehende Investitionen. Auch die Kosten für benötigte interne Ressourcen vs. externe Ressourcen sind wichtig.

Detection-and Response-Lösungen – insbesondere MDR – können sich positiv auf Ihre Cyberversicherung auswirken. Viele Versicherer bewerten Unternehmen mit einer 24/7-Bedrohungsüberwachung und -abwehr mittlerweile günstiger, was zu niedrigeren Prämien oder besseren Versicherungsbedingungen führen kann.

Eine fundierte ROI-Analyse, die operative Einsparungen, Risikoreduzierung, Personalkosten und mögliche Vorteile bei der Cyberversicherung einbezieht, kann dabei helfen, die tatsächlichen Kosten und den Mehrwert der einzelnen Ansätze zu ermitteln.

FAZIT

1,53 Mio. US$

Durchschnittliche Kosten für die Wiederherstellung nach einem Ransomware-Angriff – ohne Berücksichtigung etwaiger Lösegeldzahlungen.*

40 %

der von Ransomware betroffenen Unternehmen geben an, dass fehlende Cybersecurity-Expertise zum Angriff beigetragen hat.*

Eine fundierte Entscheidung schafft langfristige Sicherheit.

Die Wahl der passenden Detection-and-Response-Strategie ist mehr als eine reine Technologie-Entscheidung. Sie legt den Grundstein dafür, Ihre Mitarbeitenden wirksam zu unterstützen, Ihre Geschäftsprozesse zu schützen und eine resiliente Cyberabwehr aufzubauen, die auch künftigen Herausforderungen standhält.

*Sophos Ransomware-Report

SOPHOS
DEFEAT CYBERATTACKS

WEITERE INFORMATIONEN ZU SOPHOS-LÖSUNGEN UND -SERVICES

Sophos unterstützt Sie dabei, Bedrohungen zuverlässig zu erkennen und effektiv darauf zu reagieren – und Ihre Sicherheitsstrategie kontinuierlich weiterzuentwickeln.

Sprechen Sie mit einem Sophos-Experten, um herauszufinden, welche Lösung am besten zu Ihren Anforderungen passt.