plusserver

Endpoint-Security-Lösungen im Fokus

Wie Sie Cyberbedrohungen erkennen und eindämmen, bevor Schaden entsteht

Whitepaper

Inhalt

Executive Summary

Die digitale Landschaft verändert sich rasant – und mit ihr wachsen die Gefahren, die auf Unternehmen lauern. Cyberbedrohungen sind heute raffinierter, schneller und weitreichender als je zuvor. Angriffe zielen zunehmend auf Endgeräte ab und lassen sich durch konventionelle Sicherheitslösungen oft erst erkennen, wenn der Schaden bereits angerichtet ist. Klassische Abwehrmechanismen wie einfache Virenscanner stoßen an ihre Grenzen. Die Folge? Betriebsunterbrechungen, hohe finanzielle Verluste sowie Reputationsschäden.

Hier setzt eine Endpoint-Detection-and-Response-Lösung (EDR) an. EDR agiert als „Frühwarnsystem“ für Ihre Endgeräte – sei es der Laptop Ihrer Führungskräfte, das Tablet Ihrer Außendienstmitarbeitenden oder die Desktop-PCs in der Verwaltung. Im Gegensatz zu traditionellen Schutzmechanismen kann die Lösung Bedrohungen nicht nur erkennen, sondern meist sogar in Echtzeit auf auffällige Aktivitäten reagieren. So werden Angriffe gestoppt, bevor sie sich in Ihrem Netzwerk ausbreiten können.

Warum ist das gerade jetzt so entscheidend? Cyberkriminelle entwickeln – auch gestützt durch künstliche Intelligenz (KI) – immer neue Methoden, um bestehende Sicherheitsbarrieren zu umgehen. Dies zeigt auch der neuste Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI). Phishing-Angriffe, Ransomware und Advanced Persistent Threats (APTs) richten sich gezielt gegen Schwachstellen in Unternehmensnetzwerken oder nutzen die mangelnde Aufmerksakeit der Mitarbeitenden aus. Ohne EDR-Lösung kann es passieren, dass Unternehmen ungeschützt in diese Fallen tappen. Um mit den Entwicklungen der Cyberkriminalität Schritt zu halten, benötigen sie eine Sicherheitsstrategie, die proaktiv agiert, anstatt nur auf Vorfälle zu reagieren.

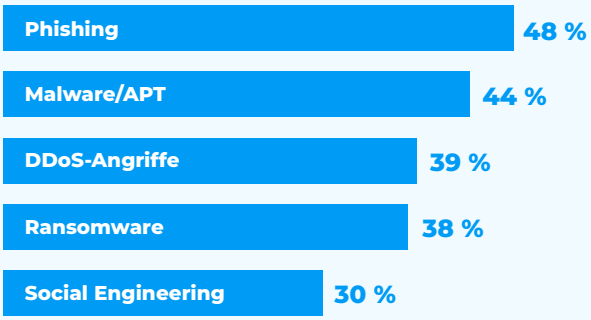
Dieses Whitepaper gibt Ihnen einen umfassenden Einblick in die Welt der EDR-Lösungen. Sie erfahren, wie sich EDR von anderen Sicherheitsansätzen unterscheidet und warum es ein integraler Baustein einer umfassenden IT-Sicherheitsstrategie sein sollte.

Die aktuelle Bedrohungslage für Unternehmen: Warum Endpoints besonders im Visier sind

Endpoints, also die Endpunkte eines Unternehmensnetzwerks, sind besonders beliebt bei Cyberkriminellen, da sie eine Vielzahl an Angriffsmöglichkeiten bieten. Die Arbeitswelt hat sich spätestens seit der Pandemie stark verändert. Mitarbeitende verbinden sich von verschiedenen Standorten aus mit dem Firmennetzwerk – oft auch über private Geräte oder unsichere WLAN-Verbindungen. Dadurch entstehen zahlreiche potenzielle Schwachstellen, die Angreifende ausnutzen können. Zudem sind Mitarbeitende und deren Endgeräte typische Einfallspunkte für Social Engineering/Phishing sowie jegliche Art von Ransomware, Malware, Viren und Trojanern.

Ein einziger kompromittierter Endpoint kann dazu führen, dass sich ein Angriff ungehindert im gesamten Netzwerk ausbreitet. Ein wirksamer Schutz der Endgeräte ist daher nicht nur eine Frage der IT-Sicherheit, sondern der gesamten Unternehmenssicherheit.

Top 5 der Cyberattacken



Die häufigsten Arten von Cyberangriffen.
Quelle: NIS2 Readiness in deutschen Unternehmen, techconsult GmbH im Auftrag von Plusnet, 2024

Endpoint Detection and Response (EDR) einfach erklärt

EDR ist eine Sicherheitslösung, die Endgeräte – also Computer, Laptops, Smartphones und Tablets – kontinuierlich überwacht und analysiert, um verdächtige Aktivitäten sofort zu erkennen und darauf zu reagieren. Dabei kann der Schutz auch die gesamte IT-Infrastruktur eines Unternehmens inkl. Servern im Rechenzentrum oder in der Cloud umfassen (man spricht dann auch von XDR, s. unten). Im Gegensatz zu herkömmlichen Virenscannern, die nur auf bereits bekannte Bedrohungen reagieren können, bietet EDR eine proaktive, intelligente Verteidigung gegen bekannte und unbekannte Angriffe.

Kontinuierliche Überwachung

EDR überwacht die Aktivitäten auf allen Endgeräten in Echtzeit. Dadurch können selbst kleinste Anomalien – wie ungewöhnliche Datenübertragungen, Prozesse oder Login-Versuche – sofort erkannt werden.

Bedrohungserkennung

Mithilfe von Verhaltensanalysen, maschinellem Lernen und künstlicher Intelligenz kann ein EDR auch bisher unbekannte Bedrohungen und neuartige Angriffe identifizieren, für die es noch keine spezifischen Signaturen gibt.

Schnelle Reaktionsmöglichkeiten

Sobald eine Bedrohung erkannt wird, kann ein EDR sofort Maßnahmen ergreifen. Dies kann das Stoppen eines schädlichen Prozesses, die Quarantäne einer Datei oder die Isolierung des betroffenen Geräts sein, um die Ausbreitung der Bedrohung zu verhindern.

Automatisierte und manuelle Analyse

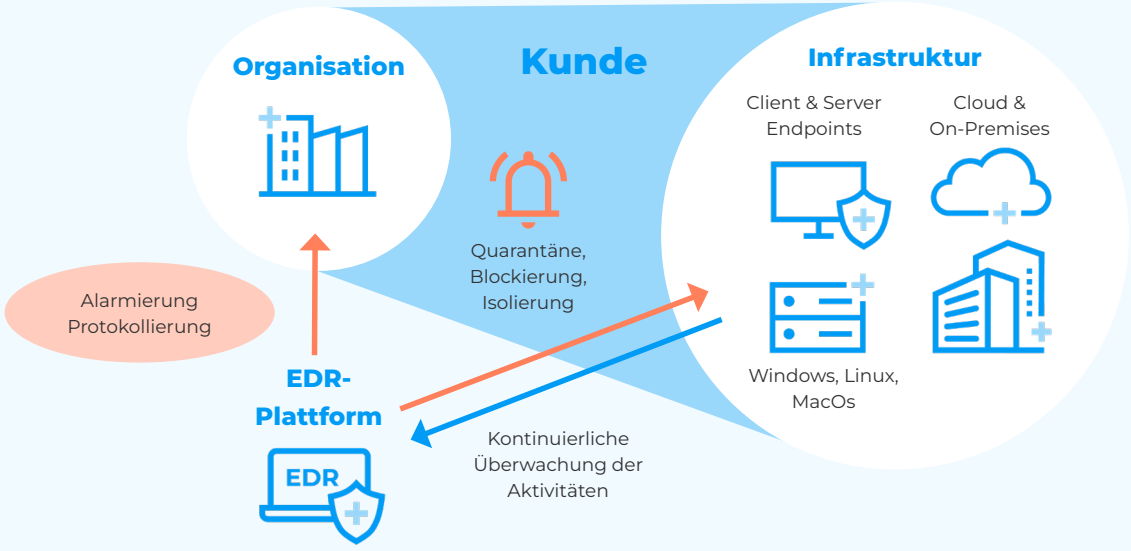
EDR-Lösungen bieten nicht nur automatisierte Schutzmechanismen, sondern ermöglichen auch die manuelle Untersuchung von Vorfällen. So können IT-Sicherheitsteams anhand der Details eines Angriffs die Ursache ermitteln.

Incident-Reporting und -Protokollierung

Durch die Protokollierung aller Vorfälle und Aktivitäten können Unternehmen nachvollziehen, wie der Angriff ablief, welche Geräte betroffen waren und welche Maßnahmen ergriffen wurden.

Die wichtigsten Eigenschaften von EDR im Überblick

Man kann sich EDR als eine Art „Alarmanlage“ für Endgeräte vorstellen. Diese bleibt rund um die Uhr wachsam, analysiert kontinuierlich, was auf den Geräten geschieht, und löst Alarm aus, sobald sie eine potenzielle Gefahr erkennt. Doch im Gegensatz zu einer klassischen Alarmanlage kann eine EDR-Lösung auch sofort eingreifen, um die Bedrohung zu neutralisieren – sei es durch Quarantäne der betroffenen Dateien, Blockierung schädlicher Prozesse oder sogar durch die Isolation des betroffenen Geräts vom Netzwerk.



Funktionsweise einer EDR/XDR-Plattform

EDR im Vergleich mit anderen Sicherheitslösungen

Neben EDR gibt es eine Reihe weiterer, teilweise recht ähnlicher Security-Lösungen auf dem Markt. Nutzen Sie den folgenden Überblick als Entscheidungshilfe und bewerten Sie, welchen Leistungsumfang und welches Service-Level Sie für Ihr Unternehmen benötigen.

EDR vs. Virenscanner

Virenscanner:
Reaktiv, erkennt nur bekannte Bedrohungen.
EDR:
Proaktiv, erkennt bekannte und unbekannte Bedrohungen, reagiert sofort.

Ein Virenscanner agiert wie ein „Türsteher“, der bekannte Bedrohungen am Eingang abfängt. Er arbeitet hauptsächlich mit Signaturdatenbanken, um bekannte Schadsoftware zu identifizieren und zu blockieren. Das Problem dabei ist, dass diese Lösungen oft keine Chance gegen neue, unbekannte Bedrohungen haben, da sie auf ein Update der Signaturdatenbank angewiesen sind.

Im Gegensatz dazu ist EDR ein „Bodyguard“, der Ihr System kontinuierlich überwacht und auch unbekannte Verhaltensmuster erkennen kann. Das bedeutet: Während der Virenscanner nur auf bekannte Bedrohungen reagiert, erkennt und stoppt EDR auch völlig neue Angriffe, indem es untypische Aktivitäten in Echtzeit analysiert und darauf reagiert. Dadurch schützt EDR auch dann, wenn die Bedrohung noch nie zuvor aufgetreten ist.

EDR vs. Managed Detection and Response (MDR)

MDR:
Externer Service inklusive menschlicher Experten.
EDR:
Interne Technologie zur Erkennung und Reaktion auf Bedrohungen.

MDR ist ein „Managed Service“, bei dem ein externes Team von Sicherheitsexpert:innen die Überwachung und Reaktion auf Bedrohungen übernimmt. Es ist ideal für Unternehmen, die nicht über ausreichend interne Ressourcen verfügen, um rund um die Uhr auf Sicherheitsvorfälle zu reagieren.
Der Unterschied zu EDR besteht darin, dass MDR nicht im eigenen Unternehmen implementiert, sondern als Service von einem Drittanbieter bereitgestellt wird. MDR nutzt oft EDR-Technologie als Teil seiner Dienstleistungen, ergänzt diese jedoch durch menschliche Expertise, um Bedrohungen zu erkennen, zu bewerten und zu beseitigen.


Ein ähnliches Angebot ist „EDR as a Service“, bei dem Anbieter die EDR-Plattform für ihre Kunden in einer Cloud betreiben und sich vollständig um deren Verfügbarkeit kümmern. In Kombination mit einem Security Operations Center (s. unten) entspricht EDR as a Service im Wesentlichen dem Leistungsumfang eines MDR.

EDR vs. Extended Detection and Response (XDR)

XDR:
Erweiterte Lösung, die mehrere Sicherheitsebenen (Endpunkte, Netzwerk, Cloud) integriert.
EDR:
Speziell auf Endgeräte fokussiert.

XDR erweitert das Konzept von EDR über Endgeräte hinaus und integriert zusätzliche Datenquellen wie Netzwerk-, E-Mail- und Cloud-Überwachung. Man kann sich XDR als ein „EDR auf Steroiden“ vorstellen, das nicht nur die Endgeräte schützt, sondern auch das gesamte Unternehmensnetzwerk im Blick hat.
Während EDR sich hauptsächlich auf die Endgeräte konzentriert, bietet XDR eine umfassendere Perspektive auf die gesamte IT-Umgebung und verbessert dadurch die Erkennungs- und Reaktionsmöglichkeiten.


Achten Sie bei der Auswahl Ihrer Lösung darauf, welchen Leistungsumfang der Anbieter angibt. Es werden aufgrund der größeren Bekanntheit des Namens auch EDR-Plattformen angeboten, die eigentlich dem XDR-Konzept entsprechen.

EDR vs. Managed Extended Detection and Response (MXDR)

MXDR:
Extern verwaltetes XDR mit menschlicher Expertise.
EDR:
Internes System, das sich auf Endgeräte beschränkt.

MXDR ist analog zu MDR die „Outsourcing-Version“ von XDR, bei der ein externer Dienstleister die Technologie betreibt und verwaltet. Unternehmen, die nicht über die internen Ressourcen verfügen, um eine umfassende XDR-Lösung zu betreiben, können mit MXDR auf professionelle Expertise zurückgreifen.


Aufgrund des weniger bekannten Akronyms empfiehlt sich auch hier ein Blick auf den tatsächlichen Umfang der Leistung, da Angebote gern als EDR beworben werden.

EDR vs. Security Orchestration, Automation and Response (SOAR)

SOAR:
Automatisierung und Orchestrierung von Sicherheitsmaßnahmen.
EDR:
Fokus auf Endgeräteüberwachung und Reaktion.

SOAR ist ein Tool, das verschiedene Sicherheitssysteme und -prozesse miteinander verknüpft, um die Reaktion auf Sicherheitsvorfälle zu automatisieren und zu beschleunigen. Somit stellt EDR die „Augen und Ohren“ eines Systems dar und SOAR fungiert als „Gehirn“, das alle Informationen sammelt, analysiert und Aktionen koordiniert.
Während SOAR also das gesamte Ökosystem von Sicherheitstools integriert und orchestriert, konzentriert sich EDR hauptsächlich auf die Erkennung und Reaktion auf Bedrohungen an Endgeräten.

EDR vs. Security Information and Event Management (SIEM)

SIEM:
Sammlung und Analyse von Daten, überwiegend passiv.
EDR:
Aktive Erkennung und Reaktion auf Endgeräten.

SIEM ist ein System zur Sammlung, Überwachung und Analyse von Sicherheitsereignissen in einer Organisation. Es sammelt Daten von verschiedenen Quellen, erkennt durch Analysen Muster und Trends, die auf gefährliche Aktivitäten schließen lassen und erstellt Berichte, die Unternehmen dabei helfen, potenzielle Bedrohungen zu erkennen sowie zu reagieren.

Allerdings ist SIEM in erster Linie eine passive Lösung, die auf das Erkennen und Melden von Vorfällen ausgelegt ist.
Im Gegensatz dazu handelt EDR aktiv und kann auf Bedrohungen reagieren, anstatt nur darüber zu berichten. Viele Unternehmen kombinieren SIEM und EDR, um ein vollständiges Bild der Sicherheitslage zu erhalten und gleichzeitig schnelle Reaktionsmöglichkeiten zu haben.

EDR vs. Security Operations Center (SOC)

SOC: Team aus Expert:innen, das mit verschiedenen Technologien arbeitet.
EDR: Technologisches System, das von einem SOC verwendet wird.

Beim SOC handelt es sich nicht um ein Tool, sondern um eine Abteilung oder einen Service. In einem Security Operations Center arbeitet ein Team von Sicherheitsexpert:innen zusammen und überwacht rund um die Uhr die Sicherheitslage eines Unternehmens. Dazu werden verschiedene Datenquellen zusammengeführt, wozu in der Regel auch ein EDR gehört. Das oben erwähnte SIEM ist dann die Standardlösung für die Sammlung und Aufbereitung der gemeldeten Ereignisse.

Wie ein EDR kann auch ein SOC als Managed Service bzw. „as a Service“ genutzt werden. Auf diese Weise müssen Unternehmen den Dienst nicht selbst aufbauen und betreiben, sondern greifen auf zentrale Expertise bei einem Anbieter zurück. Bundles aus EDR und SOC as a Service sind somit eine gute Lösung für Unternehmen, die ein begrenztes Security-Budget haben.

Zusammenfassung der Unterschiede

Lösung	Fokus	Vorteil	Nutzung
Virenscanner	Erkennung bekannter Schadsoftware	Basisschutz	Internes Tool
EDR	Endgeräteüberwachung und Reaktion	Erkennung und Reaktion in Echtzeit	Internes Tool
MDR	Externe Bedrohungserkennung	Externe Expertenüberwachung	Externer Service
XDR	Endgeräte, Netzwerk, Cloud	Umfassender Schutz	Internes Tool
MXDR	Extern verwaltetes XDR	Rundum-Service inklusive Expertise	Externer Service
SOAR	Automatisierung von Sicherheitsprozessen	Beschleunigte Reaktion	Internes Tool
SIEM	Analyse und Reporting	Übersicht über Sicherheitslage	Internes oder externes Tool
SOC	Rund-um-die-Uhr-Überwachung	Menschliche Expertise	Internes Team/ Externer Service

Argumentationshilfe für Sicherheitsverantwortliche: Welche Vorteile bietet eine EDR-Lösung für Unternehmen?

Vor der Anschaffung und Implementierung eines neuen Tools wird meist auch die Frage nach dem wirtschaftlichen Nutzen gestellt. In der folgenden Übersicht finden Sie daher wichtige Argumente für die Anschaffung einer Endpoint-Detection-and-Response-Lösung.

Proaktive Erkennung und Abwehr von Bedrohungen)

Der vielleicht größte Vorteil von EDR liegt in seiner Fähigkeit, Bedrohungen zu erkennen, bevor sie Schaden anrichten. Durch die kontinuierliche Überwachung der Endgeräte kann EDR ungewöhnliche Aktivitäten in Echtzeit aufspüren und sofort Gegenmaßnahmen einleiten.

Beispiel: Angenommen, ein Mitarbeitender wird Opfer eines Phishing-Angriffs, da er oder sie einen schädlichen Anhang öffnet. Eine traditionelle Sicherheitslösung würde hier möglicherweise zu spät reagieren. EDR hingegen erkennt das ungewöhnliche Verhalten des Anhangs (z. B. die sofortige Verschlüsselung von Dateien) und kann diesen Prozess blockieren, bevor Daten unwiederbringlich verloren gehen.

Ihr Nutzen: Durch diese proaktive Abwehr können finanzielle Schäden, Datenverlust und Produktionsausfälle erheblich reduziert werden.

Kosteneinsparungen und Effizienzsteigerung

Durch die Automatisierung der Bedrohungserkennung und -abwehr entlastet EDR die internen IT-Sicherheitsteams und ermöglicht es ihnen, sich auf strategischere Aufgaben zu konzentrieren, anstatt ständig auf Vorfälle reagieren zu müssen.

Beispiel: Ein mittelständisches Unternehmen kann durch den Einsatz von EDR mehrere Stunden Arbeitszeit pro Woche einsparen, die sonst für die manuelle Analyse von Vorfällen aufgewendet werden müsste.

Ihr Nutzen: EDR hilft, Ressourcen effizienter einzusetzen, was wiederum zu Kosteneinsparungen führt. Gleichzeitig wird das Risiko teurer Sicherheitsvorfälle reduziert.

Transparenz und Übersicht

Eine der Stärken von EDR liegt in seiner Fähigkeit, detaillierte Einblicke in die Aktivitäten auf den Endgeräten zu bieten. IT-Teams erhalten nicht nur Informationen über aktuelle Bedrohungen, sondern können auch rückblickend analysieren, wie ein Angriff erfolgte und welche Schwachstellen ausgenutzt wurden.

Beispiel: Nach einem erfolgreichen Angriff kann das EDR-System ein vollständiges Protokoll darüber liefern, welche Aktionen der Angreifer durchgeführt hat, welche Schwachstellen er ausnutzte und wie er in das System eingedrungen ist.

Ihr Nutzen: Diese Transparenz ermöglicht es Unternehmen, gezielte Maßnahmen zur Verbesserung ihrer Sicherheitsstrategie zu ergreifen und zukünftige Angriffe zu verhindern.

Einhaltung von Compliance- und Datenschutzanforderungen

In vielen Branchen ist die Einhaltung von Datenschutzvorschriften und Sicherheitsstandards gesetzlich vorgeschrieben. EDR kann dabei helfen, die Anforderungen von Regelwerken wie der DSGVO, NIS2 oder branchenspezifischen Sicherheitsstandards zu erfüllen, indem es umfassende Protokolle und Berichte bereitstellt.

Beispiel: Ein EDR-System kann automatisch protokollieren, wann und wie auf sensible Daten zugegriffen wurde und welche Maßnahmen ergriffen wurden, um potenzielle Verstöße zu verhindern.

Ihr Nutzen: Ein Nachweis über effektive Sicherheitsmaßnahmen hilft dabei, Strafen und Reputationsschäden durch Compliance-Verstöße zu vermeiden.

Sicherheit bei Remote-Arbeit und BYOD (Bring Your Own Device)

Mit dem zunehmenden Trend zur Remote-Arbeit und der Nutzung privater Geräte im Arbeitskontext sind Unternehmen mit einer größeren Angriffsfläche konfrontiert. EDR-Lösungen bieten Schutz über alle Endgeräte hinweg, unabhängig davon, ob sie sich im Unternehmensnetzwerk oder außerhalb befinden.

Beispiel: Ein Mitarbeitender arbeitet von zu Hause aus und lädt unwissentlich eine schädliche Datei herunter. Dank EDR wird diese Bedrohung erkannt und isoliert, bevor sie das Unternehmensnetzwerk erreicht.

Ihr Nutzen: Ein einheitlicher Schutz für alle Geräte reduziert die Risiken, die durch Remote-Arbeit entstehen, und sorgt dafür, dass sensible Daten auch außerhalb des Firmengeländes sicher bleiben.

EDR-Vorteile im Überblick

Vorteil	Nutzen für das Unternehmen
Proaktive Erkennung und Abwehr	Datenverlust und finanzielle Schäden lassen sich verhindern oder reduzieren
Kosteneinsparungen und Effizienzsteigerung	Kann IT-Teams entlasten und Betriebskosten reduzieren, insbesondere als Outsourcing-Lösung
Transparenz und Übersicht	Erleichtert Analyse und Prävention von Angriffen
Einhaltung von Compliance-Anforderungen	Trägt zum Schutz vor Strafen und Reputationsverlust bei
Schutz bei Remote-Arbeit und BYOD	Sichert den Zugriff auf Unternehmensdaten von überall ab

How to: EDR in bestehende Sicherheitsstrukturen integrieren

Die Implementierung einer Detection-and-Response-Lösung in eine bereits bestehende IT-Sicherheitsarchitektur kann auf den ersten Blick komplex erscheinen. Doch wenn dieser Prozess richtig angegangen wird, lässt sich EDR effektiv in vorhandene Strukturen einbetten und ergänzt das bestehende Sicherheits system optimal.

Analyse der bestehenden Sicherheitsarchitektur

Der erste Schritt für eine erfolgreiche EDR-Integration ist eine gründliche Analyse Ihrer aktuellen IT-Sicherheitslandschaft. Welche Tools und Lösungen sind bereits im Einsatz? Wie kommunizieren diese miteinander, und wo gibt es mögliche Lücken?

EDR als Teil des gesamten Sicherheitskonzepts integrieren

EDR sollte nicht isoliert betrachtet werden. Stattdessen fügt es sich als wichtiger Baustein in Ihr gesamtes Sicherheitskonzept ein. Es liefert detaillierte Einblicke in Endgeräteaktivitäten, die dann mit Informationen aus anderen Sicherheitslösungen wie Firewall, Antivirus oder SIEM kombiniert werden.

Konfigurieren Sie daher die EDR-Lösung so, dass sie Daten mit Ihrem SIEM-System austauscht und relevante Informationen in ein zentrales Dashboard überträgt. Dadurch können Sicherheitsverantwortliche alle Bedrohungsindikatoren an einem Ort überwachen und analysieren.

Interoperabilität mit vorhandenen Sicherheitstools sicherstellen

Viele moderne EDR-Lösungen bieten vorgefertigte Integrationen für gängige Sicherheitsanwendungen. Das Zusammenspiel mit Tools wie Firewalls, Antivirus-Programmen, Vulnerability-Management-Systemen oder Threat-Intelligence-Plattformen ist entscheidend, um umfassenden Schutz zu gewährleisten.

Setzen Sie auf offene APIs bei EDR-Lösungen, um die Kommunikation mit Ihren bestehenden Tools zu ermöglichen. Durch diese Schnittstellen können Bedrohungsdaten und Sicherheitsvorfälle automatisch zwischen den Systemen ausgetauscht werden, was zu einem deutlich effizienteren Betrieb führt.

Schrittweise Implementierung in Ihre Infrastruktur

Um die Komplexität der EDR-Integration zu minimieren, empfiehlt sich ein schrittweises Vorgehen. Starten Sie mit einer kleineren Gruppe von Endgeräten und erweitern Sie die Implementierung sukzessive, sobald die ersten positiven Ergebnisse sichtbar sind.
Beginnen Sie mit einem Pilotprojekt, bei dem die EDR-Lösung auf kritischen Systemen getestet wird. Nutzen Sie die gewonnenen Erfahrungen, um das Deployment schrittweise auf die gesamte IT-Infrastruktur auszuweiten. Dadurch lassen sich potenzielle Herausforderungen frühzeitig erkennen und anpassen.

Auf Automatisierung achten

Ein entscheidender Vorteil der EDR-Integration ist die Möglichkeit, Sicherheitsprozesse zu automatisieren. Dies bedeutet, dass bestimmte Reaktionen auf erkannte Bedrohungen direkt durch die EDR-Lösung ausgelöst werden, ohne dass manuelle Eingriffe erforderlich sind.

Legen Sie Regeln und automatisierte Reaktionen fest, etwa das Blockieren einer verdächtigen IP-Adresse oder die Isolierung eines infizierten Geräts, sobald ein Angriff erkannt wird. So wird die Reaktionszeit deutlich verkürzt.

Schulung und Sensibilisierung der Mitarbeitenden

Eine erfolgreiche EDR-Integration ist mehr als eine technische Aufgabe. Mitarbeitende müssen verstehen, wie die EDR-Lösung funktioniert und wie sie zur allgemeinen Sicherheitsstrategie beiträgt. Die Einführung neuer Technologien kann nur dann erfolgreich sein, wenn das Personal entsprechend geschult wird. Hierzu können beispielsweise Onboardings der EDR-Anbieter in Anspruch genommen werden. Zusätzliche generelle Awareness-Trainings tragen dazu bei, eine Sicherheitskultur im gesamten Unternehmen zu etablieren.

EDR als Teil einer Zero-Trust-Strategie

Die Integration von EDR in bestehende Sicherheitsstrukturen lässt sich ideal mit einer Zero-Trust-Strategie kombinieren, bei der grundsätzlich kein Netzwerkverkehr als sicher angesehen wird. EDR unterstützt diese Strategie, indem es kontinuierlich alle Aktivitäten auf Endgeräten überwacht und auch innerhalb des eigenen Netzwerks Bedrohungen erkennt.

Kombinieren Sie EDR mit einer Multi-Faktor-Authentifizierung (MFA) und Netzwerksegmentierung im Unternehmen, um sicherzustellen, dass selbst bei einem erfolgreichen Angriff nur begrenzter Schaden entstehen kann. EDR überwacht dabei verdächtiges Verhalten auf den Endgeräten, während andere Sicherheitsmaßnahmen zusätzliche Schutzschichten bieten.

Pro-Tipp: EDR in ein SOC integrieren

Ein Security Operations Center bildet das Herzstück moderner IT-Sicherheit in Unternehmen. Es ist der zentrale Knotenpunkt, an dem alle sicherheitsrelevanten Informationen zusammenlaufen, analysiert und bewertet werden. Die Integration einer Endpoint Detection and Response in ein SOC schafft eine leistungsstarke Symbiose, da EDR detaillierte Einblicke in Endgeräteaktivitäten bietet, die das SOC dann für die proaktive Bedrohungsabwehr nutzen kann.

Verknüpfung von EDR-Daten mit dem SOC

Die Einbindung ist jedoch nicht immer einfach. Eine der ersten Herausforderungen bei der Integration von EDR in ein SOC besteht darin, sicherzustellen, dass die von der EDR-Lösung gesammelten Daten effizient und vollständig im SOC ankommen. Schließlich liefert EDR jede Menge Daten – von Anomalien im Benutzerverhalten bis hin zu verdächtigen Prozessen auf Endgeräten. Für ein erfolgreiches Zusammenspiel müssen diese Daten nahtlos in die zentralen Überwachungs- und Analysesysteme des SOC einfließen.

Stellen Sie sicher, dass Ihre EDR-Lösung mit dem SIEM-System Ihres SOC kompatibel ist. Die Integration sollte automatisiert erfolgen, sodass relevante Daten in Echtzeit ins SOC gelangen. Dies ermöglicht es Ihren Analyst:innen, Anomalien frühzeitig zu erkennen und direkt darauf zu reagieren.

Automatisierte Reaktionen auf Bedrohungen

Ein großer Vorteil der EDR-SOC-Integration ist die Möglichkeit, automatisierte Reaktionen auf Bedrohungen einzuleiten. Nutzen Sie Playbooks und automatisierte Workflows, um definierte Reaktionen auf bestimmte Bedrohungsszenarien festzulegen. Durch diese Automatisierung kann Ihr SOC-Team schneller reagieren und den potenziellen Schaden eines Angriffs erheblich reduzieren. Beispielsweise können Sie bei einem Ransomware-Versuch sofortige Isolationsmaßnahmen für betroffene Geräte aktivieren.

Kontinuierliche Bedrohungsanalyse und -jagd

Eine EDR-Lösung sollte nicht nur reaktiv genutzt, sondern auch aktiv in die kontinuierliche „Bedrohungsjagd" (Threat Hunting) eingebunden werden. Ein SOC kann mit den bereitgestellten Daten gezielt nach Anomalien und potenziellen Angriffen suchen, bevor diese Schaden anrichten.

Schulen Sie Ihre SOC-Analyst:innen in der aktiven Nutzung der EDR-Daten für Threat Hunting. Dies bedeutet, dass sie proaktiv nach verdächtigen Aktivitäten suchen, etwa nach ungewöhnlichen Datenübertragungen oder auffälligem Verhalten von Endgeräten.

Gemeinsame Nutzung von Bedrohungsinformationen

Ein großer Vorteil eines EDR-SOC-Setups ist die Möglichkeit, Bedrohungsinformationen effektiv zu teilen (Threat Intelligence). Erkenntnisse aus EDR-Analysen können im SOC mit anderen Sicherheitsquellen verknüpft werden, um ein umfassendes Bild der Bedrohungslage zu erhalten.

Integrieren Sie dazu eine Threat-Intelligence-Plattform, die Daten aus der EDR-Lösung in Echtzeit mit Bedrohungsinformationen aus anderen Quellen kombiniert. Dies ermöglicht ein tieferes Verständnis der aktuellen Bedrohungslage und hilft dem SOC-Team, besser informierte Entscheidungen zu treffen.

Integration von Incident-Response-Plänen

Ein SOC sollte stets vorbereitet sein, wenn es zu einem Sicherheitsvorfall kommt. Eine EDR-Lösung kann hierbei als wertvolles Instrument dienen, um Vorfälle schneller zu erkennen und darauf zu reagieren. Die Integration von EDR-Daten in die Incident-Response-Pläne des SOC hilft, eine klare Strategie zu entwickeln, um schnell auf Bedrohungen reagieren zu können.

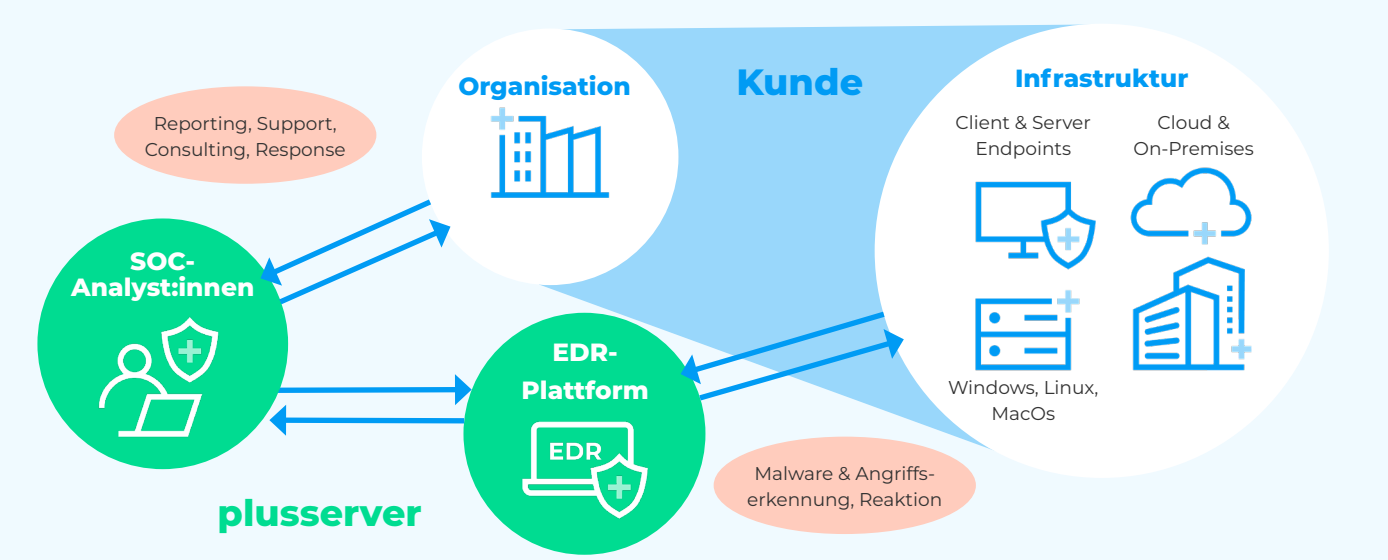
Stellen Sie sicher, dass der Ablaufplan im Falle eines Angriffs klar ist: Wer ist verantwortlich? Welche Maßnahmen werden ergriffen? Welche Daten werden benötigt? Eine gute Vorbereitung minimiert den potenziellen Schaden und beschleunigt die Wiederherstellung des normalen Betriebs.

Kontinuierliches Monitoring und Optimierung

Sowohl EDR-Lösungen als auch SOCs sind nicht statisch – sie müssen sich ständig an neue Bedrohungen und Technologien anpassen. Daher ist es wichtig, die Integration kontinuierlich zu überwachen und zu optimieren.

Führen Sie regelmäßige Reviews der EDR-SOC-Integration durch und passen Sie diese an neue Bedrohungsszenarien oder Geschäftsanforderungen an. Nutzen Sie Metriken wie Reaktionszeiten, Anzahl der identifizierten Bedrohungen und erfolgreiche Abwehrmaßnahmen, um die Effektivität der Integration zu bewerten.

EDR-Betrieb mit SOC



Die Kombination mit einem SOC erweitert den Leistungsumfang der EDR-Plattform und schafft einen Mehrwert für Unternehmen

Erfolgsbeispiele: Wie EDR den Unterschied macht

Die folgenden Fallstudien basieren auf den Erfahrungen aus typischen Kundenszenarien. Sie zeigen auf, wie EDR mit SOC-Integration in der Praxis einen erheblichen Mehrwert bietet und Sicherheitslücken effektiv schließt. Unternehmen profitieren von einer deutlich verbesserten Sichtbarkeit, Reaktionsgeschwindigkeit und Sicherheit ihrer Endpunkte, was letztendlich das Vertrauen in die IT-Sicherheit und den Schutz sensibler Daten erhöht.

Produktionsunternehmen schützt sich vor gezielten Angriffen

Unternehmensprofil:
Ein mittelständisches Produktionsunternehmen mit rund 500 Mitarbeitenden, verteilt auf mehrere Standorte. Bisher nutzte das Unternehmen nur herkömmliche Antivirus- und Firewall-Lösungen. In den letzten Monaten stieg jedoch die Anzahl der gezielten Phishing-Angriffe auf die Mitarbeitenden erheblich an, was zu einem erhöhten Risiko von Ransomware-Infektionen führte.

Herausforderung:
Die bisher eingesetzten Sicherheitstools konnten keine ausreichende Transparenz über Endgeräteaktivitäten bieten, und es gab keine Möglichkeit, ungewöhnliche Verhaltensmuster zu erkennen. Zudem fehlte es dem internen IT-Team an Kapazitäten, um Sicherheitsvorfälle rund um die Uhr zu überwachen.

Lösung:
Das Unternehmen entschied sich für die Implementierung einer EDR-Lösung, kombiniert mit der Integration in ein Managed SOC. Die EDR-Lösung ermöglichte es, sämtliche Endpunkte kontinuierlich zu überwachen, verdächtige Aktivitäten zu erkennen und im Fall einer Bedrohung automatisch zu reagieren.

Ergebnisse:
+ Innerhalb der ersten sechs Monate erkannte die EDR-Lösung 12 potenziell schädliche Angriffe, die von herkömmlichen Sicherheitstools nicht erfasst worden wären.
+ Der SOC-Dienst reagierte in Echtzeit auf Vorfälle, isolierte infizierte Geräte automatisch und verhinderte so eine Ausbreitung innerhalb des Netzwerks.
+ Das Unternehmen konnte die Anzahl der erfolgreichen Phishing-Angriffe um 80 Prozent reduzieren.

Finanzdienstleister reduziert Reaktionszeit bei Sicherheitsvorfällen

Unternehmensprofil:
Ein Finanzdienstleister mit rund 200 Mitarbeitenden, der eine hohe Anzahl sensibler Kundendaten verarbeitet. Die IT-Infrastruktur bestand aus einer Mischung aus internen Servern und Cloud-basierten Anwendungen. Die bestehende Sicherheitslösung war reaktiv und konnte nur begrenzt auf neue Bedrohungen reagieren.

Herausforderung:
Das Unternehmen sah sich einer zunehmenden Zahl von Cyberangriffen, insbesondere durch Ransomware und Phishing, ausgesetzt. Herkömmliche Sicherheitslösungen reichten nicht aus, um diese Bedrohungen effektiv zu erkennen und zu stoppen. Zudem war die Einhaltung branchenspezifischer Regularien (DORA, Digital Operational Resilience Act) von zentraler Bedeutung, um die betriebliche Resilienz zu gewährleisten.

Lösung:
Durch die Implementierung einer EDR-Lösung mit SOC-Integration realisierte das Unternehmen erstmals eine Echtzeit-Überwachung aller Endpunkte. Zusätzlich setzte der Finanzdienstleister auf Vulnerability-Management, um regelmäßig Schwachstellen zu identifizieren. Diese Kombination ermöglichte sowohl die proaktive Erkennung und Reaktion auf Bedrohungen als auch eine nachhaltige Beseitigung von Sicherheitslücken in der IT-Infrastruktur.

Ergebnisse:
+ Die durchschnittliche Reaktionszeit auf Sicherheitsvorfälle reduzierte sich von 48 Stunden auf weniger als 1 Stunde.
+ Kritische Schwachstellen konnten identifiziert und geschlossen werden.
+ Die Security-Maßnahmen tragen zur Einhaltung der DORA-Compliance bei.

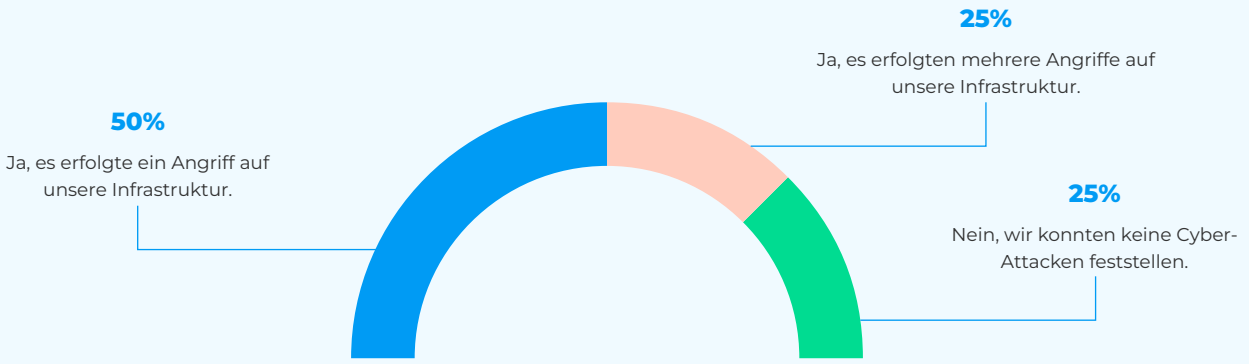
Fazit und nächste Schritte (+Checkliste)

In einer zunehmend digitalen Welt, in der Cyberbedrohungen immer ausgefeilter und zielgerichteter werden, ist der Schutz der Endpoints ein entscheidender Faktor für die Sicherheit eines Unternehmens. Wie wir in diesem Whitepaper gezeigt haben, bietet eine Detection-and-Response-Lösung in ihren unterschiedlichen Ausprägungen (EDR, XDR etc.) eine weitreichende und proaktive Möglichkeit, Angriffe frühzeitig zu erkennen, darauf zu reagieren und sie effektiv zu bekämpfen.

Die Stärke von EDR liegt dabei in seiner Fähigkeit, nicht nur bekannte Bedrohungen zu blockieren, sondern auch komplexe, noch unbekannte Angriffe aufzudecken – eine Herausforderung, die traditionelle Sicherheitslösungen oftmals nicht bewältigen können. Durch die Integration in ein Security Operations Center lässt sich der Nutzen einer EDR-Lösung sogar noch steigern: So wird eine lückenlose Überwachung rund um die Uhr sichergestellt und Vorfälle können in Echtzeit analysiert und behandelt werden.

Warum sollten Sie jetzt handeln?

Cyberkriminelle ruhen nicht und jedes Unternehmen ist potenziell im Visier – unabhängig von Größe oder Branche. Die Frage ist nicht mehr, ob, sondern wann ein Angriff versucht wird. Unternehmen, die proaktiv handeln und ihre IT-Sicherheitsinfrastruktur durch eine EDR-Lösung ergänzen, verschaffen sich einen entscheidenden Wettbewerbsvorteil: Sie minimieren das Risiko kostspieliger Ausfallzeiten, schützen sensible Daten und stärken das Vertrauen von Kunden und Partnern.



Drei von vier Unternehmen geben an, innerhalb eines Jahres mindestens einmal Opfer eines Cyberangriffs gewesen zu sein.
Quelle: NIS2 Readiness in deutschen Unternehmen, techconsult GmbH im Auftrag von Plusnet, 2024

Basis: 200 Unternehmen

Checkliste: Nächste Schritte auf Ihrem Weg zur EDR-Implementierung:

+ **Interne Bedarfsanalyse:** Überlegen Sie, welche spezifischen Anforderungen Ihr Unternehmen an eine EDR-Lösung stellt und welche Sicherheitsziele Sie erreichen möchten.
+ **Integration in bestehende Strukturen:** Überprüfen Sie, wie sich eine EDR-Lösung optimal in Ihre aktuelle IT-Landschaft integrieren lässt. EDR kann seine Vorteile noch besser ausspielen, wenn es mit anderen Sicherheitslösungen, zum Beispiel SIEM oder SOC, zusammenarbeitet.
+ **Pilotphase:** Implementieren Sie die EDR-Lösung zunächst in einem kleinen Bereich Ihres Unternehmens, um die Effektivität zu testen und Erfahrungen zu sammeln.
+ **Schulung der Mitarbeitenden:** Stellen Sie sicher, dass Ihr Team die Funktionsweise der EDR-Lösung versteht und weiß, wie es mit potenziellen Bedrohungen umgehen soll.

Wir unterstützen Sie Schritt für Schritt

Die EDR-Implementierung ist kein Einmalprojekt, sondern erfordert kontinuierliche Anpassungen. Ein zuverlässiger Partner, der auf Cybersicherheit spezialisiert ist, kann Sie bei der Einrichtung, Wartung und Optimierung Ihrer Lösung unterstützen. Für ein unverbindliches Beratungsgesprächzu Ihrem EDR mit SOC-Integration „as a Service“ stehen wir Ihnen gerne zur Verfügung.

› Jetzt Beratung anfragen