

Kundenleitfaden für ein **optimiertes** Sicherheits-Level

Kluge Investitionen
in Schutz auf EDR-
Niveau und was
Ihr Unternehmen
davon hat



Zusammenfassung

Jahrelang konnten sich SMBs und mittlere Großunternehmen darauf verlassen, dass ihre Endpoint Protection-Plattformen (EPP) sie gegen die überwiegende Mehrzahl von Commodity-Bedrohungen schützt. Da sich Cyberkriminelle jedoch zunehmend neue, unbekannte und versteckte Bedrohungen zunutze machen, die EPPs umgehen können, müssen Abwehrmaßnahmen mithilfe von EDR- (Endpoint Detection and Response) und/oder MDR-Lösungen (Managed Detection and Response) optimiert werden.

Im vorliegenden Kundenleitfaden wird beschrieben, wie Sie in nur 8 einfachen Schritten den optimalen Schutz auf EDR-Niveau für Unternehmen sicherstellen. Am besten beginnen Sie mit einer Bestandsaufnahme Ihres bestehenden Endpoint-Schutzes, um gravierende Schwachstellen aufzudecken. Darüber hinaus muss die Zielausrichtung klar sein, damit Sie genau den Schutz bekommen, der Ihren Anforderungen gerecht wird. Dazu dienen unsere Anwendungsfälle. Und Sie sollten sich sowohl EDR als auch MDR als Lösung für die Ausweitung Ihres Sicherheits-Portfolios ansehen, um auf dieser Grundlage eine Liste mit den wesentlichen Funktionen zu erstellen, die sie von potentiellen Anbietern benötigen.

Nachdem Sie sich diesen Leitfadens durchgelesen haben, werden Sie ein klares Bild davon bekommen, wie und warum Sie Ihre Abwehrmechanismen ausbauen sollten. Sie werden die Vorteile der verfügbaren Lösungen kennen und erfahren, wie Sie eine optimale Sicherheitslösung einrichten, die nicht nur den Anforderungen Ihres Unternehmens, sondern auch den Fachkenntnissen Ihres IT-Sicherheitsteams entspricht.

Warum sollten Sie Ihren Schutz verbessern – und warum gerade jetzt?



Fortschrittliche Cybersicherheitslösungen wie Endpoint Detection and Response (EDR) sind eines der am stärksten diskutierten Themen auf dem Markt – und das aus gutem Grund. Vor allem, wenn Sie ein kleines bis mittelständisches Unternehmen (SMB) oder ein mittleres Großunternehmen sind.

Warum sind gerade diese Segmente betroffen? Die Veränderungen in der Cybersicherheitslandschaft bedeuten, dass sich Angreifer heute auf Organisationen jeglicher Größe, Branche und Bereitschaft konzentrieren. Gerade größere SMBs und mittlere Großunternehmen stehen im Fokus von hochentwickelten, versteckten Bedrohungen, die bislang nur auf Großkonzerne abzielten.

**Optimieren Sie
Schlüsselressourcen
und konzentrieren Sie
sich voll und ganz auf
Ihre Cybersicherheit,
statt Ihre Zeit mit
False Positives und
Warnhinweisen zu
vergeuden**

Als Reaktion darauf haben IT-Sicherheitsteams ihre vorhandenen Endpoint Protection-Plattformen (EPP) durch EDR- und/oder MDR-Lösungen (Managed Detection and Response) ergänzt, um Sicherheitsvorfälle zu erkennen und zu untersuchen, eine Bedrohung am Endpoint einzudämmen sowie automatische Abwehrmaßnahmen einzuleiten und/oder eine Anleitung zur Beseitigung zu erhalten.

Leider verursacht der Einsatz dieser Lösungen manchmal genauso viele Probleme, wie er löst – so werden Sicherheitsteams auf Unmengen von Bedrohungen aufmerksam gemacht, die zwar verdächtig sind und untersucht werden müssen, sich letztendlich aber als harmlos herausstellen. Für IT-Teams im eigenen Haus mit begrenzter Sicherheitsexpertise oder Zeit, um diese Warnhinweise abzuarbeiten, kann das schnell zum Problem werden.

Eine ideale Lösung ergänzt den Endpoint-Schutz durch Sicherheit auf EDR-Niveau und senkt die EDR-Arbeitslast spürbar. Denn je mehr Bedrohungen frühzeitig erkannt werden, desto weniger Aufwand entsteht für die Sicherheitsteams. Das wiederum bedeutet, dass IT-Sicherheitsteams Schlüsselressourcen optimieren und sich voll und ganz auf die Cybersicherheit konzentrieren kann, statt ihre Zeit mit False Positives und Warnhinweisen im Übermaß zu vergeuden.

Welches sind jetzt aber die Veränderungen in der Bedrohungslandschaft, die einen fortschrittlicheren Schutz erforderlich machen? Und inwiefern variieren diese für verschiedene Arten von Unternehmen? Und wie können Sie diesen Bedrohungen mit einer Lösung begegnen, die zum einen am besten zu Ihrem Unternehmen, der Größe und dem Know-how Ihres IT-Teams passt und zum anderen der Art von Cyberangriffen, denen Sie möglicherweise ausgesetzt sind?

Der vorliegende Kundenleitfaden soll diese Fragen anhand der folgenden Themenstränge beantworten:

- Weshalb die vorhandene Endpoint Security keinen ausreichenden Schutz gegen die neue Bedrohungen gewährleistet.
- Wie Sie die sich entwickelnden Sicherheitsanforderungen bewerten.
- Wie Sie herausfinden, welcher Schutz für Ihre Anforderungen am besten ist – sowohl im Hinblick auf die Bedrohungen, denen Sie zunehmend ausgesetzt sind, als auch auf das Security Know-how Ihres IT-Teams.
- Was tun, wenn Ihre Zeit, die Anzahl der Mitarbeiter und/oder die interne Expertise begrenzt sind.
- Wie die neuesten Lösungen in die wachsende Security -Landschaft passen.

Weshalb die vorhandene Endpoint Security keinen ausreichenden Schutz gegen neue Bedrohungen gewährleistet

Wenn es um die Verbesserung der Endpoint Security geht, ist es leicht anzunehmen, es gehe nur darum, eine EDR-Lösung zu finden sowie zu implementieren, die für das eigene Unternehmen geeignet erscheint. Aber genauso wie es nicht ratsam wäre, ein neues Stockwerk auf ein Gebäude zu setzen, ohne vorher das Fundament zu prüfen, sollte Ihr erster Schritt darin bestehen, die vorhandene EPP-Plattform genauestens unter die Lupe zu nehmen.

So schlägt IDC¹ beispielsweise Folgendes vor:

Lassen Sie sich gar nicht erst ein auf eine minderwertige oder schwache EPP-Plattform, die die Leistungsfähigkeit der gesamten Endpoint-Lösung mindert¹. Ein Unternehmen sollte nicht eine schwache EPP mit EDR (und viel Aufwand für Sicherheitsanalysten) ausgleichen müssen.

- Bevor Sie Überlegungen zu EDR anstellen, empfiehlt IDC zunächst einen Blick auf die bestehende EPP-Lösung zu werfen. Eine EPP sollte den Endpoint-Schutz als unabhängige Lösung gewährleisten.
- Lassen Sie sich gar nicht erst ein auf eine minderwertige oder schwache EPP-Plattform, die die Leistungsfähigkeit der gesamten Endpoint-Lösung mindert. Ein Unternehmen sollte nicht eine schwache EPP mit EDR (und viel Aufwand für Sicherheitsanalysten) ausgleichen müssen.

Die EPP spielt eine entscheidende Rolle beim Schutz des Unternehmens vor einer Vielzahl von Bedrohungen und sollte die Arbeitslast der IT-Sicherheitsteams minimieren. Wenn aber versteckte Bedrohungen im Spiel sind, brauchen Sie noch mehr.

Um die von der neuen Bedrohungslandschaft ausgehenden Risiken einzudämmen, müssen Sie zunächst die Effektivität Ihres bestehenden Endpoint-Schutzes überprüfen und mögliche Schwachstellen in Ihrer Abwehr ausräumen.

Warum Sie eventuell gar nicht so gut geschützt sind, wie Sie denken

Auch wenn Sie vielleicht meinen, Ihr Unternehmen sei gut geschützt: Schätzungen zufolge gab es allein in der ersten Jahreshälfte 2019 nahezu **4 000** Datenschutzverletzungen², bei denen die Daten von mehr als vier Milliarden Nutzern gefährdet waren.

Diese alarmierende Zahl wird in dem jährlichen Bericht von Kaspersky, in dem wir die Ergebnisse unserer globalen Umfrage zu globalen IT-Sicherheitsrisiken vorstellen, zitiert. Im Rahmen der Studie wurden nahezu 5 000 SMBs und Großunternehmen in 23 Ländern befragt. Daraus resultierten einige beunruhigende Ergebnisse. Zum Beispiel:

55 %

der Unternehmen sind „absolut sicher“, dass ihr Netzwerk nicht gehackt wurde, obwohl 38 % das Gefühl haben, dass sie keinen ausreichenden Überblick über die Bedrohungen haben mit denen Ihr Unternehmen konfrontiert wird.

12 %

der Unternehmen haben Angst vor einer Malware-Infektion, was einen der kostspieligsten Sicherheitsvorfall für Sie bedeuten würde.

51 %

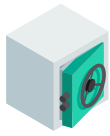
der Großunternehmen und 47 % der SMBs stimmen zu, dass es Ihnen immer schwerer fällt, zwischen einem generischen und einem gezielten Sicherheitsangriff zu unterscheiden.

66 %

der SMBs sowie der Großunternehmen planen, Ihre Investitionen in IT-Fachkräfte im Jahr 2020 zu erhöhen, trotz des gravierenden weltweiten Fachkräftemangels – vor allem im Bereich der Cybersicherheit.

¹ IDC, Doc Nr. US45794219 – Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, 01/2020
² <https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report>

Was diese Zahlen belegen, ist eine gefährliche Diskrepanz zwischen der Wahrnehmung der Cyberbedrohungslandschaft durch die Unternehmen, den Arten von Angriffen, die die größten potentiellen Risiken (einschließlich finanzieller Art) darstellen, und der eigenen Bereitschaft und Fähigkeit, diese abzuwehren.



Für Unternehmen ist eine Malware-Infektion auf firmeneigenen Geräten, die Form der Datenschutzverletzung mit den größten finanziellen Auswirkungen, die allein 2019 Unternehmen **2,73 Millionen US-Dollar** gekostet haben. Und das, obwohl sich nur 12 % der Unternehmen in Bezug auf eine mögliche Malware-Infektion „sehr besorgt“ zeigen.



Auch SMBs ignorieren diese Form des Angriffs, welche mit extrem hohen Kosten verbunden sind. Die bislang teuerste Datenschutzverletzung, bezogen auf kleinere Unternehmen, betrug **162.000 US-Dollar** und bestand in erfolgreichen Angriffen gegen extern gehostete IT-Infrastrukturen. Trotzdem stufen SMBs dies lediglich als fünftwichtigste Maßnahme ein und machten sich eher Sorgen um Fragen des Datenschutzes, wie den Verlust physischer Geräte oder Datenverluste durch einen gezielten Angriff.



SMBs und Großunternehmen können immer weniger zwischen allgemeinen und gezielten Sicherheitsangriffen unterscheiden, so dass sie den potentiellen Schaden der Vorfälle nur schwer erkennen oder einschätzen können. Dies ist ein möglicher Grund, weshalb sie immer anfälliger sowohl für moderate als auch hochentwickelte Malware-Bedrohungen werden.

Der Bericht schließt mit den Worten: „Es ist wichtig, dass Unternehmen weiter investieren und ihre IT-Sicherheitsprozesse überdenken, um bei der wachsenden Zahl von Cyberangriffen stets die Nase vorn zu behalten und die entstandenen finanziellen Verluste zu begrenzen.“ Das können sie aber nur erreichen, wenn sie gezielt die tatsächlichen Bedrohungen angehen, denen sie zunehmend ausgesetzt sind – d. h. indem Sie in Schutz auf EDR-Niveau investieren, um sich gegen versteckte Bedrohungen zu schützen.

Schritt 1: Überprüfen des vorhandenen Endpoint-Schutzes



Bei so vielen fortschrittlichen Cybersicherheitslösungen auf dem Markt gerät die wesentliche Rolle, die Ihr Endpoint-Schutz spielt, manchmal aus dem Blickfeld. Warum sind Endpoints so wichtig? Endpoints sind nicht nur die gängigsten Eintrittspunkte in eine Unternehmensinfrastruktur und das Hauptziel von Cyberkriminellen, sondern auch eine wichtige Quelle für die Daten, die in einer effektiven Untersuchung komplexer Vorfälle erforderlich sind.

Daher sollte jede Organisation eine EPP-Plattform wählen, die automatisierten Schutz gegen eine Vielzahl von potentiellen Commodity-Bedrohungen, aber auch gegen dateilose Bedrohungen und Ransomware bietet.

Ein solches Setup erfordert relativ wenige Fachkenntnisse oder Sicherheitsexperten und wird damit den Anforderungen von SMBs oder kleinen Großunternehmen gerecht. Sie verfügen über kein dediziertes Sicherheitsteam oder lediglich über ein sehr geringes Maß an Know-how im Bereich der Cybersicherheit.

Für größere mittelständische Unternehmen sowie Großunternehmen bildet dieses Setup eine wichtige Grundlage. Denn durch das automatische Abarbeiten von kleineren Bedrohungen gibt die Lösung Sicherheitsteams den Freiraum, sich auf fortschrittliche Abwehrmaßnahmen zu konzentrieren.

Folgende Punkte müssen Sie ebenfalls bedenken, wenn Sie Ihre EPP dahingehend prüfen, ob sie wirklich den Funktionsumfang bietet, den Sie benötigen:

Wie effektiv ist die Lösung?

Wie viele Fehlalarme erhalten Sie?

Bietet sie effektive Funktionen zur Reduzierung der Angriffsfläche wie Web-, Programm- und Gerätekontrollen?

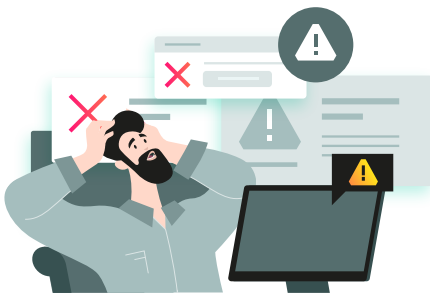
Ermöglicht sie die Automatisierung von Routineaufgaben?

Ist sie benutzerfreundlich und minimiert die Kosten und den Aufwand für Ihr IT-Team?

Bietet sie Unterstützung bei kritischen Aufgaben wie Schwachstellenanalysen und Patch Management?



Schritt 2: Aufspüren von Schwachstellen im vorhandenen Endpoint-Schutz



Die EPP-Plattform schützt Sie zwar vor einer Vielzahl von Commodity-Bedrohungen, trotzdem brauchen Sie aber auch wirksame Abwehrmaßnahmen gegen neue, unbekannte und versteckte Bedrohungen, die Ihre EPP umgehen.

Einen Cyberangriff umzusetzen, wird für Cyberkriminelle immer kostengünstiger, wodurch immer mehr Organisationen ins Visier geraten. Neben der zunehmenden Häufigkeit werden derartige Angriffe auch immer raffinierter, da die Kriminellen verschiedene Techniken kombinieren, ausprobieren und anwenden, um die Endpoint Security geschickt zu umgehen.

Die Notwendigkeit diese Bedrohungen zu kontrollieren, rückt im Zuge der Veränderungen in der Arbeitswelt, wie dem zunehmendem mobilen Arbeiten, immer mehr in den Fokus.

Erste alarmierende Anzeichen deuten darauf hin, dass die traditionelle EPP dringend ausgebaut werden muss:

Kaufen Sie nur die Funktionen, die Sie auch wirklich brauchen, statt Unmengen von Funktionen, die Sie gar nicht haben möchten

- Bereits jetzt vermag Ihre EPP eine wachsende Zahl von neuen, unbekannten und versteckten Bedrohungen nicht mehr zu stoppen.
- Es fehlt Ihnen an Transparenz, um zu sehen, was auf Ihren Endpoints vor sich geht. Dazu gehört, dass sie nicht in der Lage sind, Ursachenanalysen, Untersuchungen und Abwehrreaktionen in Echtzeit durchzuführen – oder dies mit den standardmäßigen Betriebssystem-Tools manuell und auf den jeweiligen Fall bezogen machen müssen, was langsam, komplex und fehleranfällig ist.
- Sie verfügen nicht über die erforderlichen Fachkenntnisse oder Kapazitäten im Bereich IT-Sicherheit, um mit immer raffinierteren Bedrohungen umzugehen.
- Sie sind besorgt aufgrund der drohenden Geldstrafen oder der möglichen Rufschädigung für Ihr Unternehmen als Folge eines größeren Sicherheitsvorfalls.

Um eine effektive Lösung zur Abwehr dieser Bedrohungen zu finden, müssen Sie bestimmte Faktoren Ihres Unternehmens berücksichtigen. Dazu zählt die Größe, das Unternehmensprofil, das Sicherheitslevel, vorhandene Ressourcen sowie das Know-how und vor allem die Kompetenzen in puncto Sicherheit (bzw. den „Reifegrad“) Ihres IT-Sicherheitsteams oder Ihrer IT.

Außerdem brauchen Sie eine Lösung, die alle benötigten Funktionen optimal einsetzt, damit Sie nicht für eine große Anzahl von Funktionen bezahlen, die Sie gar nicht haben möchten, für die Sie aber IT-Sicherheitsexperten einstellen müssen, um sie bedienen zu können.

Schritt 3: Klare Zielsetzung

Laut Gartner³ bieten EDR-Tools technischen Fachleuten im Sicherheits- und Risikomanagement eine Methode, die Antworten auf die beiden wesentlichen Fragen zur Sicherheit ihrer Umgebung liefert:

- Was ist hier passiert?
- Was passiert gerade jetzt?

Viele Organisationen verfügen nur über begrenztes Fachwissen (oder kleine IT-Sicherheitsabteilungen und keine Pläne, diese zu vergrößern), müssen aber trotzdem wissen, was in ihrer Infrastruktur vor sich geht, und müssen auf versteckte Bedrohungen reagieren, bevor diese Schaden anrichten.

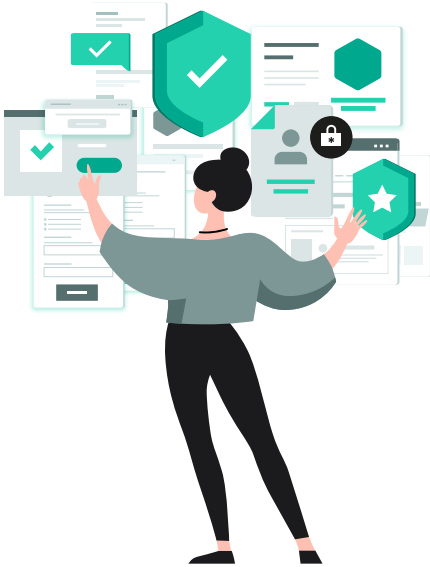
Mit passenden EDR-Funktionen zusätzlich zu einer EPP lässt sich eine sehr effektive Abwehr gegen hochentwickelte und versteckte Bedrohungen aufbauen. Ein solches System sollte IT-Sicherheitsexperten Informationen und Einblicke für eine effektive Untersuchung liefern, aber auch alle erforderlichen Tools enthalten, um Ursachenanalysen durchzuführen, eigene Gefährdungsindikatoren (IoCs) zu erstellen, IoCs zu importieren und sämtliche Endpunkte nach IoCs zu durchforsten. Darüber hinaus sollten es automatisierte und/oder schnelle, präzise Abwehrmechanismen per Mausklick ermöglichen, Dateien in Quarantäne zu setzen, den Host zu isolieren, Prozesse anzuhalten, Objekte zu löschen etc.

Schritt 4. Die Schutzlösung finden, die Ihren Anforderungen am ehesten gerecht wird

In vielen Unternehmen fehlt häufig ein Mitarbeiter, der speziell für die IT-Sicherheit zuständig ist. Einige sind eventuell gerade erst dabei, eine IT-Sicherheitsabteilung aufzubauen. Andere wiederum verfügen bereits über ein gut aufgestelltes und qualifiziertes IT-Sicherheitsteam. Die Qualität des in diesen Organisationen vorhandenen Fachwissens in Bezug auf die Bedrohungsabwehr fällt daher sehr unterschiedlich aus. Ebenso wie die Zeit, die sie zur Bearbeitung dieser Aufgabe aufwenden können.

Um diesen wechselnden Bedingungen gerecht zu werden, müssen Organisationen ohne spezielles IT-Sicherheitspersonal in erster Linie auf Automation als strategisches Tool gegen die neuesten versteckten Bedrohungen setzen.

Dafür müssen sie Ihre EPP-Plattform mit zusätzlichen EDR-Tools ergänzen, die vor diesen Bedrohungen schützen und gleichzeitig einen angemessenen Automatisierungsgrad (komplett oder teilweise) aufweisen.



³ Gartner – Solution Comparison for Endpoint Detection and Response Technologies and Solutions – 01/2020

Tools, die so einfach und benutzerfreundlich wie möglich gehalten sind, sparen Zeit und verhindern Frust

Anstatt in eine übermäßig komplexe EDR-Lösung zu investieren, mit der sie möglicherweise fachlich und zeitlich überfordert sind, verfügen sie mit Managed Detection and Response (MDR) über Funktionen wie 24/7 Sicherheitsüberwachung durch Branchenexperten, automatisiertes und Managed Threat Hunting sowie geführte und Remote-Abwehrszenarien. Die Bereitstellung kann dann entweder über einen Anbieter, einen Managed Service Provider (MSP) oder einen Managed Security Service Provider (MSSP) erfolgen.

Eine dritte Möglichkeit besteht darin, EDR und MDR zu kombinieren. Viele Unternehmen verfügen nicht über das erforderliche Fachwissen für das Threat Hunting. Daher ist die Auslagerung dieser Aufgabe kombiniert mit passenden Detection and Response-Funktionen oft die beste Lösung. Diese Herangehensweise ist vor allem für Unternehmen geeignet, die ein eigenes Cybersicherheitsteam aufbauen möchten, gleichzeitig aber nicht über genügend Ressourcen, (Mitarbeiter und/oder Kompetenzen) verfügen, um Erkennungs- und Abwehrsysteme auf Expertenniveau aufrechtzuerhalten.

Ganz gleich, welches Szenario auf Sie am ehesten zutrifft, Sie brauchen Tools, die so einfach und benutzerfreundlich wie möglich gehalten sind. Denn nur so sparen Sie Zeit und verhindern unnötigen Frust. Um Alarmermüdung zu vermeiden, brauchen Sie außerdem eine Lösung, die einen Großteil der potentiellen Bedrohungen automatisch abarbeitet.

Schritt 5: Schauen Sie sich unsere Anwendungsfälle an

Um herauszufinden, welche Schutzlösung Ihrem Bedarf entspricht, müssen Sie vorab klare Anforderungen definieren. Dafür müssen Sie sich darüber im Klaren sein, welche kritischen Aspekte von der Lösung abgedeckt und dauerhaft gewährleistet sein müssen, d. h. welche Anwendungsfälle und welche Ergebnisse Sie erwarten.

Wenn Sie beispielsweise einen Warnhinweis erhalten, sollten EDR und/oder MDR in der Lage sein, Antworten auf die folgenden Kernfragen zu geben:

In welchem Kontext tritt die Warnung auf?

Welche Maßnahmen wurden aufgrund der Warnung bereits eingeleitet?

Ist die erkannte Bedrohung noch immer aktiv?

Sind weitere Hosts von dem Angriff betroffen?

Welchem Pfad ist der Angriff gefolgt?

Was ist die Kernursache der Bedrohung?



Außerdem sollte die Lösung einen Einblick in das komplette Ausmaß der Bedrohung geben. Zum Beispiel:

Wenn das Risiko einer globalen Bedrohung steigt, möchte Ihr Management-Team mit Sicherheit die Gewissheit haben, dass Sie aktuell nicht Ziel eines Angriffs sind. Um derlei Bedenken zu beseitigen, müssen Sie in der Lage sein, Gefährdungsindikatoren (IoC) aufzuspüren und das System zu scannen.

Wenn eine Aufsichtsbehörde Sie auffordert, Ihre Systeme auf bestimmte IoCs zu prüfen, müssen Sie IoCs aus vertrauenswürdigen Quellen importieren und regelmäßig Scans durchführen, um Anzeichen eines Angriffs zu erkennen.

Wenn Sie einen Warnhinweis gründlich untersucht und auf der Grundlage der erkannten Bedrohung einen IoC generiert haben, sollten Sie nicht mehr derjenige sein, der das gesamte Netzwerk absuchen muss, um herauszufinden, ob noch andere Hosts betroffen sind. Vielmehr sollte das automatisch für Sie erledigt werden.

Gegen Bedrohungen, die sich extrem schnell ausbreiten, sollten Sie außerdem folgende Maßnahmen umgehend einleiten können:

- Eindämmung der Bedrohung, indem der Host isoliert, die Datei in Quarantäne gesetzt oder Dateien während der Untersuchung an der Ausführung gehindert werden
- Automatisierte, Endpoint-übergreifende Abwehr auf Basis von IoC-Scans – damit Sie auf versteckte Bedrohungen reagieren können, sobald diese entdeckt werden
- Und wenn Sie MDR verwenden: Geführte oder Remote-Abwehrszenarien.

Folgende Ergebnisse sollten Sie daher von Ihrer Lösung erwarten können:

- Schutz vor immer häufiger auftretenden und immer destruktiveren, versteckten Bedrohungen
- Zeit- und Ressourcenersparnis dank einem einfachen, automatisierten Tool
- Überblick über das komplette Ausmaß an versteckten Bedrohungen im gesamten Netzwerk
- Klärung der Bedrohungsursache und wie sie zustande gekommen ist
- Abwendung weiteren Schadens durch schnelle automatisierte Gegenmaßnahmen



Was tun, wenn Ihre Zeit und/oder interne Security Expertise begrenzt sind?

Angenommen, Ihr Know-how im Bereich der IT-Sicherheit ist begrenzt oder Ihr Sicherheitsteam ist klein und besteht nur aus ein oder zwei Mitarbeitern. Nehmen wir weiter an, dass Sie vor der Entscheidung stehen, ob Sie Ihre EPP mit EDR und/oder MDR erweitern sollen. Welche Vorteile bieten die Lösungen und welche ist die Richtige für Sie?

Schritt 6: EDR und MDR im Detail ansehen

Wenn Sie einen eher praktischen Ansatz bevorzugen (und Ihr IT-Team über ausreichende Kompetenzen in Sachen IT-Sicherheit verfügt), können Sie mit EDR Geschäftsunterbrechungen verhindern und Schaden abwenden, indem es die Risiken beseitigt, die von neuen, unbekannten und versteckten Bedrohungen ausgehen. Außerdem verschafft es Ihrem Sicherheitspersonal den für die Untersuchung von Bedrohungen, die Ursachenanalyse und die Abwehr erforderlichen Einblick.

Damit lässt sich die Kosteneffizienz steigern, weil Ihr Sicherheitsteam effektiver arbeiten kann, ohne zwischen unterschiedlichen Tools und Konsolen hin- und herwechseln zu müssen. So können auch Kapazitäten durch die Automatisierung einer Vielzahl von Prozessen optimal eingesetzt werden. Gleichzeitig lassen sich Bedrohungen zuverlässig überwachen, Abwehrmaßnahmen einleiten und Angriffe wirksam verhindern.

Wenn Sie Ihre interne IT-Sicherheitskapazität durch Auslagerung von wichtigen Erkennungs- und Abwehraufgaben verbessern möchten, dann bietet Ihnen MDR 24/7 fortschrittlichen Schutz vor Bedrohungen, die ansonsten automatisierte Sicherheitsbarrieren umgehen können. So können Sie dem Fachkräftemangel in der Cybersicherheit entgegenwirken und genießen ohne immens hohe Kosten alle Vorteile eines Security Operations Centers (SOC), das 24/7 für Sie im Einsatz ist.



Mit MDR können sich Ihre firmeninternen Ressourcen gezielt auf die kritischen Aufgaben konzentrieren, bei denen der Eingriff Ihres IT-Sicherheitsteams auch wirklich erforderlich ist. Fortschrittliche, lernfähige Systeme sorgen gleichzeitig für eine deutliche Erhöhung des Durchsatzes der Analysten und verringern die Mean-time-to-Respond. Neben diesen Kostensenkungen und Effizienzsteigerungen bietet MDR eine kontinuierliche Sicherheitsüberwachung durch Branchenexperten sowie automatisiertes und Managed Threat Hunting. Dazu gehört die Analyse von komplexen Bedrohungen abseits von Malware sowie von gefährlichen, schwer vorhersagbaren Bedrohungen über seriöse Betriebssystem-Tools.

Mit einer Kombination aus EDR und MDR können Sie dagegen die Funktionen auf EDR-Niveau an Ihre speziellen Bedürfnisse anpassen, indem Sie zum Beispiel Threat Hunting auslagern (weil das Know-how dafür nicht vorhanden ist), während Sie die Erkennungs- und Abwehrfunktionen intern implementieren.

Und was gibt es darüber hinaus?

Nachdem Sie Ihre Wahl bezüglich EDR und/oder MDR getroffen haben, möchten Sie vermutlich wissen, wie die verschiedenen verfügbaren Lösungen vom Markt beurteilt werden. Bei der Wahl eines so wichtigen Produkts wie einer Cybersecurity-Lösung sollten Bewertungen von unabhängigen Experten und anderen Nutzern eine weitaus größere Rolle spielen als die Werbeversprechen der Anbieter. Deshalb sollten Sie zum Beispiel:



Welche persönlichen Erfahrungen haben Sie mit anderen Produkten desselben Anbieters gemacht?

Was sagen die Kollegen innerhalb Ihrer Branche?

Welche denken die Kunden des Anbieters?

Zu welchem Ergebnis kommen unabhängige Tests und Bewertungen?

Was sagen Analysten über den Anbieter und seine Produkte?

Schritt 7: Die breitere Sicherheitslandschaft mit in Betracht ziehen

In vielen Unternehmen müssen EPP-, EDR- und/oder MDR-Lösungen in ein viel breiteres Sicherheits-Framework integriert werden und in dessen Rahmen funktionieren.

Neben diesen Lösungen können Sie z. B. von Folgendem profitieren:

Automatisierte Sandbox: Bietet Ihren Endpoints ein höheres Maß an Sicherheit, indem Bedrohungen aufgedeckt werden, die gegenüber der Endpoint-Sicherheit inaktiv bleiben und erst in Erscheinung treten, wenn der Host Schwächen zeigt. Daher müssen sie in einer kontrollierten, isolierten Umgebung analysiert werden.

Threat Intelligence: Hilft bei Problemen wie Cyberbedrohungen in verdächtigen Dateien, URLs, IPs und Domänen, damit Sie Bedrohungen schneller und gründlicher untersuchen können.

Schulungen zum Sicherheitsbewusstsein für Ihre Mitarbeiter, um das Sicherheitsbewusstsein zu schärfen und eine Verhaltensänderung zu erreichen – vor allem in Bezug auf die Cybervorfälle, die auf menschliches Versagen zurückzuführen sind.



Darüber hinaus sollten Sie sich überlegen, wie Ihre Lösung verwaltet werden soll – zum Beispiel über eine einheitliche, Cloud-basierte und zentrale Konsole, die für alle verschiedenen Komponenten einschließlich einer Möglichkeit zur lokalen, Online- oder Air Gap-Verwaltung fungiert.

Schritt 8: Fragen Sie Ihren Anbieter, ob er all dies bietet:

Die einzelnen EDR- und MDR-Lösungen unterschiedlicher Anbieter variieren (teilweise stark) in Bezug auf den Funktionsumfang. Eine umfassende Lösung sollte idealerweise Folgendes zu bieten haben.



- Schnelle und problemlose Bereitstellung
- Einfach und intuitiv zu bedienende Tools, ohne langwierige Einarbeitung oder Nachschulung
- Eine einheitliche Verwaltungskonsole, damit Sie alle Ihre Cybersicherheitstools von einem zentralen Punkt aus konfigurieren und direkt von dort auf Vorfälle reagieren können
- Zugeschnitten auf Ihre speziellen Anforderungen auch in Bezug auf die Bereitstellungsoption: Cloud, Hybrid oder Air Gap
- Transparenz der Bedrohung
- Ursachenanalyse einschließlich Visualisierung und detaillierter Darstellung im Sinne einer schnelleren und bequemeren Analyse
- IoC-Import, -Generierung und -Scan
- Schnelle und vorzugsweise automatisierte Abwehroptionen
- Anleitung mit Abwehrszenarien
- Automatisiertes Threat Hunting mit Unterstützung der Experten des Anbieters/MS(S)P
- Stark integrierte Funktionen sowohl für Endpoint-Schutz als auch für Endpoint Detection and Response
- Sandbox-Funktion
- Integrierter Schutz vor dateilosen Bedrohungen
- Anti-Exploit-Technologie
- Ransomware-Schutz
- Vulnerability und Patch Management-Funktion
- Programm-, Internet- und Gerätekontrolle sowie weitere Methoden zur Systemhärtung
- Hohe Leistung, um Beeinträchtigungen von Nutzern oder Netzwerk zu verhindern
- Effektiver technischer Support in Ihrer Sprache

Vorteile von Kaspersky Optimum Security

In unabhängigen Tests zeigt Kaspersky immer wieder ein höheres Schutzniveau im Vergleich zu anderen Anbietern.

Zum dritten Mal in Folge wurden wir 2019 von Gartner Peer Insights zur Customers' Choice für Endpoint Protection-Plattformen⁴ und zum 7. Mal zum am häufigsten getesteten und ausgezeichneten Anbieter gewählt.

Im Jahr 2020 gehörten wir außerdem zu einem von sechs Anbietern weltweit, die die Auszeichnung Gartner Peer Insights Customers' Choice for Endpoint Detection and Response-Lösungen⁵ erhielten, wobei wir im Bereich Service und Support von allen Anbietern die höchste Bewertung erzielten.

Weitere Auszeichnungen:

- AA-Produktbewertung im Gruppentest für NSS Labs Advanced Endpoint Protection (AEP) 2020.
- Höchstmöglicher Wert beim Schutz gegen hochentwickelte Cyberbedrohungen im Enhanced Real-World Test von AV-Comparatives.
- Jährlich vergebene Auszeichnung von SE Labs als Best Enterprise Endpoint 2020.

Kaspersky Optimum Security schützt Ihr Unternehmen vor neuen, unbekannten und versteckten Bedrohungen, ohne Ressourcen übermäßig zu belasten. Damit lässt sich im Handumdrehen eine effektive Lösung zur Bedrohungsprävention, -erkennung und -abwehr umsetzen, welche automatisiertes Threat Hunting beinhaltet sowie Sicherheitsüberwachung durch Kaspersky-Experten, die Ihnen 24/7 beratend und mit Remote-Abwehrszenarien zur Seite stehen.

Und wenn Sie eine EPP-, EDR- und MDR-Lösung suchen, die von einer Cloud-Konsole aus verwaltet wird und neben einer Sandbox, einem Threat Intelligence-Portal auch Schulungen zum Sicherheitsbewusstsein bietet, dann finden Sie in Kaspersky Optimum Security eine umfassende, einheitliche Schutzlösung für alle Ihre Endpunkte mit automatischer Prävention, Detection and Response, Managed Protection und Schulungen zur Cybersicherheit.

Fortschrittlicher Schutz vor Bedrohungen

- Fortschrittliche Präventions- und Erkennungsmechanismen (maschinelles Lernen, Verhaltensanalyse, Sandbox, automatisiertes Threat Hunting mit Angriffsindikatoren (IoA)) maximieren den Schutz vor gefährlichen, versteckten Bedrohungen – auf der Grundlage eines starken EPP-Schutzes vor Commodity-Bedrohungen mit Kaspersky Endpoint Security for Business
- Die höhere Transparenz der Bedrohungen sorgt für mehr Informationen in Bezug auf eben diese, während Sie mithilfe von Ursachenanalysen und Visualisierungstools jede einzelne Bedrohung schnell und effizient untersuchen und ihren Ursprung ermitteln können.
- Die automatisierte Threat Hunting-Funktion mit der 24/7 Überwachung ermöglicht Experten das frühzeitige und effektive Erkennen von Bedrohungen, sodass diese abgewehrt werden.
- Schnelle, Endpoint-übergreifende und automatisierte Abwehroptionen per Mausklick sowie IoC-Scans in der gesamten Infrastruktur unterstützen Sie dabei, umgehend auf Bedrohungen zu reagieren, die sich extrem schnell ausbreiten.
- Guided und Remote Response bietet Ihren Sicherheitsteams Expertenanalysen und Abwehrmaßnahmen gegen neue, unbekannte und versteckte Bedrohungen.
- Risiken durch den menschlichen Faktor sowie Social Engineering lassen sich mindern, indem das Bewusstsein für Cyberbedrohungen und die von Cyberkriminellen angewandten Techniken gestärkt wird und Mitarbeiter lernen, wie sie Angriffe grundsätzlich vermeiden können.

Schneller, skalierbarer Komplettschutz

- Funktioniert auf Workstations, Laptops und Servern, physischen und virtuellen Maschinen, in Public Clouds und Containern.
- Mit dieser konsolidierten, mehrstufigen Endpoint-Sicherheitslösung lassen sich Vorfälle priorisieren sowie die Erkennung und Untersuchung von Bedrohungen dank Threat Intelligence über ein komfortables Webportal beschleunigen.
- Bekämpft bekannte und neu entstehende Bedrohungen mit branchenführenden und bewährten Technologien für die Abwehr von Ransomware, Exploits, dateilosen und anderen Malware-Angriffen.

⁴ Gartner Peer Insights, Voice of the Customer: Endpoint Protection Platforms, 10. Dezember 2019

⁵ Gartner Peer Insights, Voice of the Customer: Endpoint Detection and Response Solutions, 1. Mai 2020

Minimaler Bedarf an zusätzlichem Personal oder Fachwissen

- Einfache Analyse- und Abwehrmechanismen innerhalb einer zentralen, Cloud-basierten Konsole sorgen dafür, dass Sicherheitsmitarbeiter weniger Zeit und Mühe für die Untersuchung und Beseitigung aufwenden müssen.
- Dank der einheitlichen Konsole können die wesentlichen Sicherheitsprogramme von Kaspersky zentral verwaltet werden. Cybersicherheitstools können von einem zentralen Punkt aus konfiguriert werden. So kann der Nutzer direkt von dort auf Vorfälle reagieren. Darüber hinaus erfüllen Sie die spezifischen Anforderungen jeder erdenklichen Bereitstellungsoption, wie lokale, Cloud-, Hybrid- oder Air Gap-Umgebungen.
- Die 24/7 Sicherheitsüberwachung sorgt für umfassenden Schutz, selbst in Organisationen, denen es an IT-Sicherheitspersonal mangelt.

Gründe, um in Kaspersky Optimum Security zu investieren

Mit **Kaspersky Optimum Security** minimieren wir das Risiko eines versteckten Angriffs und schaffen eine Situation, in der Sie Ihrer Endpoint-Sicherheit wieder vertrauen können. Statt Unsicherheit, was in Ihrer Umgebung vor sich geht, erhalten Sie Transparenz und Kontrolle über alle Ihre Endpoints, wo auch immer sie sich befinden. Und statt Sicherheitsupdates aufgrund der damit verbundenen Komplexität abzulehnen, genießen Sie die Sicherheit einer vereinfachten und konsolidierten Lösung, mit der Sie Ihre Ressourcen optimieren können.

Weitere Informationen, wie Sie an den fortschrittlichen Schutz kommen, den Ihr Unternehmen benötigt und gleichzeitig den Bedarf an zusätzlichen Ressourcen minimieren, finden Sie hier: go.kaspersky.com/de_optimum.

Neues über Cyberbedrohungen: de.securelist.com
IT Security News: www.kaspersky.de/blog
Threat Intelligence-Portal:
opentip.kaspersky.de
Technologien im Überblick: www.kaspersky.com/TechnoWiki
Preise und Auszeichnungen: media.kaspersky.com/en/awards
Interaktives Portfolio-Tool: kaspersky.com/int_portfolio

www.kaspersky.de