

Bitdefender®

MDR

# Bitdefender Managed Detection & Response Service

**ZEITGEMÄSSE MDR-SERVICES FÜR UNTERNEHMEN UND ORGANISATIONEN JEDLICHER GRÖSSE**



Wir bieten rund um die Uhr erweiterten Schutz vor Angriffen und Abhilfe bei Cybervorfällen, so dass Sie sich damit nicht herumzuschlagen brauchen.

„Bitdefender MDR gibt mir die Sicherheit, dass unser gesamtes Netzwerk in Echtzeit überwacht wird, auch wenn weder ich noch sonst irgendein Mitarbeiter im Büro ist.“ IT-Leiter einer Erzdiözese

## Wir lösen Sicherheitsprobleme für Ihr Unternehmen

Fragen der Sicherheit werden für Unternehmen in aller Welt immer mehr zum Risikofaktor und rücken daher auch immer mehr in den Fokus. Die Cyberangriffe werden immer raffinierter und umgehen in zunehmendem Maße die herkömmlichen Schutzmaßnahmen. Deshalb müssen die Unternehmen ihre Sicherheitsstrategie und -ressourcen anpassen, um Sicherheitsverletzungen schnell und effektiv zu identifizieren und umgehend darauf reagieren zu können.

33 % der Sicherheitsverletzungen sind auf Social-Engineering-Angriffe wie Phishing zurückzuführen. Notebooks und Desktop-Computer waren Angriffsziele bei etwa 25 % der Sicherheitsverletzungen - DBIR-Bericht von Verizon, 2019

**Zu wenig SOC-Personal verfügbar:** Sicherheitsexperten sind knapp und teuer, sie sind nur schwer zu bekommen und zu halten. Bei einer kürzlich von Ponemon durchgeführten Umfrage gaben 60 Prozent der befragten Sicherheitsanalysten an, dass sie daran denken, das SOC zu verlassen, weil ihnen der Stress zu groß ist.

**Erkennung von komplexen Angriffen** Komplexe Angriffe sind nur schwer zu erkennen, weil sie Taktiken, Techniken und Verfahren einsetzen, die einzeln betrachtet auf normales Systemverhalten hindeuten. Die durchschnittlichen Kosten eines Cybervorfalles für Unternehmen sind in den letzten fünf Jahren um 72 Prozent auf 13 Millionen Dollar gestiegen. Dies geht aus dem 2019 erstellten Bericht "Cost of Cybercrime" von Accenture hervor.

**Zeitraubende Untersuchungen:** Sicherheitsanalysten haben einfach nicht die Zeit, jede einzelne Warnmeldung zu bewerten und zu validieren sowie Prioritäten für weitergehende Untersuchungen festzulegen. Bei den meisten Organisationen liegt die mittlere Reaktionszeit (MTTR) im Bereich von Monaten, während die Angreifer Daten innerhalb von Tagen manipulieren und herausschleusen.

**Zu viele Tools:** In vielen Unternehmen erfolgt die Sicherheitsverwaltung über mehrere Konsolen, die auf ganz unterschiedlichen Technologien basieren. Fast 40 Prozent der Befragten in der Ponemon-Studie gaben an, dass sie sich mit zu vielen Tools herumschlagen müssen. Und 71 Prozent benötigen einen höheren Automatisierungsgrad zur Verwaltung von Alarmmeldungen und zum Erfassen von Beweisen.

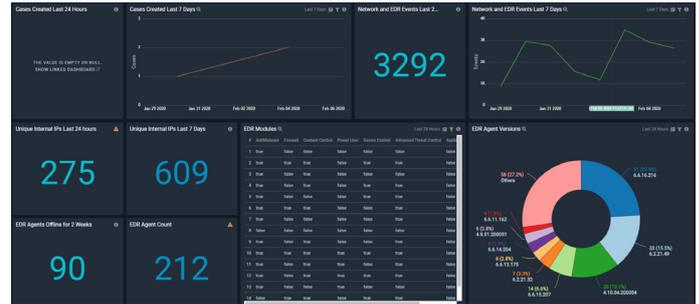
## Wie kann der Bitdefender MDR-Service hier Abhilfe schaffen?

Der von Bitdefender angebotene MDR-Service (Managed Detection and Response) bietet branchenweit führende Cybersicherheit für Endpunkte sowie Netzwerk- und Sicherheitsanalysen einschließlich Know-how zur Verfolgung von Bedrohungen. Für das Bitdefender-SOC arbeiten erstklassige Sicherheitsanalysten der US Air Force und Navy, der NSA und des britischen Geheimdienstes. Unsere aus dem Verteidigungsbereich entlehnte Methodik ermöglicht es uns, Angriffsindikatoren für neue und raffinierte Bedrohungen zu entwickeln und entsprechende Gegenmaßnahmen für unsere Kunden bereitzustellen.

**SOC-Personal auf Abruf:** Bitdefender stellt den Kunden ein SOC mit ausreichend Personal zur Verfügung, das effizient an die Größenentwicklung des Kunden angepasst werden kann. Dabei ist sichergestellt, dass unsere Sicherheitsexperten über die für die von ihnen betreuten Kundenumgebungen erforderliche Technologie und Ausbildung verfügen.

**Erkennung komplexer Angriffe:** Die Sicherheitsanalysten arbeiten rund um die Uhr daran, auf der Grundlage von kundenspezifischen Bedrohungsprofilen Erkenntnisse zu Bedrohungen zu sammeln und Mittel zu deren Bekämpfung zu finden. Sie erweitern diese Daten durch Host- und Netzwerk-gestützte Telemetriedaten sowie Sicherheitsanalysen, um komplexe und gezielte Angriffe aufzuspüren.

**Verbesserte Erkennung und schnelle Antwortzeiten:** Telemetrie und Alarmmeldungen in Echtzeit werden über mehrere Datenströme miteinander korreliert; gleichzeitig werden für jeden Kunden maßgeschneiderte Reaktionsmaßnahmen erarbeitet, die effektive Reaktionen ermöglichen, um die Auswirkungen eines Sicherheitsvorfalls auf das Unternehmen zu begrenzen.



**Verringerte Auswirkungen auf den Betrieb:** Der MDR-Service von Bitdefender verwaltet die Sicherheitstechnologie für Sie, sodass sich Ihr Team intensiver um strategische Geschäftsinitiativen kümmern kann. Dadurch können Sie unmittelbar Kosten sparen, denn Sie haben weniger Personalkosten und benötigen weniger Lizenzen für Tools. Echtzeit-Dashboards, Flash- und After-Action-Berichte liefern den Sicherheitsverantwortlichen den benötigten Kontext, monatliche Berichte leisten Beiträge für strategische Entscheidungen.

## Die Varianten des Bitdefender MDR-Service

Wir bieten zwei unterschiedliche MDR-Lösungen. Je nach lizenziertem MDR-Services-Paket sind weitere Zusatzmodule verfügbar.

	MDR Advanced	MDR Enterprise
AV der nächsten Generation (NGAV)	☑	☑
Automatisierte Bereinigung	☑	☑
Anwendungs- & Gerätesteuerung	☑	☑
Host-basierte Firewall- & Web-Überwachung	☑	☑
Endpoint Detection & Response (EDR)	☑	☑
Account Manager	☑	☑
Analyse des Faktor-Mensch-Risikos	☑	☑
Gezielte Verfolgung von Bedrohungen	☑	☑
Angepasste Reaktionen auf Vorfälle nach vordefinierter Strategie	☑	☑
Kundenspezifisches Bedrohungsmodell	☑	☑
Überwachung auf Registrierung von Phishing-Domains		☑
Überwachung auf unberechtigte Veröffentlichung von Code oder Kundendaten		☑
Darknet-Überwachung		☑
Einbindung der Tools des Kunden		☑
Überwachung unternehmenskritischer und risikobehafteter Angriffsziele		☑
<b>Add-Ons</b>		
Agentenloser Schutz von IoT-Geräten	☑	☑

Nähere Informationen finden Sie unter <https://www.bitdefender.com/MDR>

# WARUM BITDEFENDER?

## UNANGEFOCHTENER INNOVATIONSFÜHRER.

38 % der Cybersicherheitsanbieter weltweit haben mindestens eine Bitdefender-Technologie in ihre Produkte integriert. Wir sind in 150 Ländern vertreten.

## WELTWEIT ERSTER ANBIETER VON LÜCKENLOSER SICHERHEIT

Die erste Sicherheitslösung, die Härtung, Prävention, Erkennung und Reaktion für Endpunkt, Netzwerk und Cloud vereint.

## BESTBEWERTETE SICHERHEIT. VIELFACH BESTÄTIGT.



# Bitdefender

## IM ZEICHEN DES WOLFS

**Gründung** 2001 in Rumänien  
**Anzahl der Mitarbeiter** 1800+

**Hauptsitz**  
Unternehmenszentrale – Santa Clara, Kalifornien, USA  
Technologiezentrum – Bukarest, Rumänien

### NIEDERLASSUNGEN AUF DER GANZEN WELT

**USA & Kanada:** Ft. Lauderdale, Florida | Santa Clara, Kalifornien | San Antonio, Texas | Toronto, Kanada

**Europa:** Kopenhagen, DÄNEMARK | Paris, FRANKREICH | München, DEUTSCHLAND | Mailand, ITALIEN | Bukarest, Iasi, Cluj, Timisoara, RUMÄNIEN | Barcelona, SPANIEN | Dubai, VAE | London, GB | Den Haag, NIEDERLANDE

**Australien:** Sydney, Melbourne

Die Herausforderung des Fachgebietes Datensicherheit liegt darin, dass nur der klarste Blick, der schärfste Verstand und der tiefste Einblick gewinnen kann - Fehler sind keine Option. Unsere Aufgabe ist es, jedes Mal zu gewinnen, tausendmal aus 1.000 und 1 Million mal aus 1.000.000.

Und das tun wir. Wir sind der Leader in der Branche, jedem Hacker und Sicherheitsexperten um Schritte voraus. Der Scharfsinn unseres kollektiven Bewusstseins wird durch einen **helleuchtenden Drachen-Wolf** repräsentiert. Er steht Ihnen zur Seite und schützt Sie mit seiner aus unserer Ingenieurskunst hervorgegangenen Intuition vor allen Gefahren, die in den verborgenen Tiefen der digitalen Welt lauern.

Dieser Scharfsinn ist unsere Superkraft und bildet den Kern all unserer richtungsweisenden Produkte und Lösungen.