WHITEPAPER

WEB USE &
GERMAN MARKET ONLY

Bitdefender®

Sicherheit

# Managed Detection and Response

## MIT PROFESSIONELLER UNTERSTÜTZUNG AKTUELLE SICHERHEITSHERAUSFORDERUNGEN MEISTERN

www.bitdefender.com

# Inhalt

Management Summary ..... 3

Wozu Detection and Response? ..... 3

Detection and Response selbst betreiben? ..... 4

Herausforderungen einer eigenen Abwehr ..... 6

Die Alternative: MDR ..... 7

Mit MDR den Hackern einen Schritt voraus ..... 8

# Management Summary

Detection and Response wendet Schaden ab, wenn ein Einbruch in IT-Systeme erfolgreich stattgefunden hat. Einschlägige Lösungen, insbesondere Endpoint Detection and Response (EDR), bieten hier teilautomatisierte Abwehrmechanismen. Aber der umfassende Schutz rund um die Uhr gegen komplexe Attacken verlangt nach geeignetem Personal mit seltenen Qualifikationen, das seinen Preis hat.
Diese Ressourcen für eine eigene Abwehr kann ein Unternehmen einsparen, indem es auf Managed Detection and Response (MDR) setzt. Dann übernimmt ein Dienstleister mit seinem eigenen SOC (Security Operations Center) für einen Pauschalbetrag die Überwachung aller Systeme, wertet Alarmmeldungen aus, reagiert auf Vorkommnisse und erstattet regelmäßig Bericht. Die unternehmenseigene IT-Abteilung kann sich auf strategische Themen konzentrieren, weil für ihre Sicherheit auf dem höchsten professionellen Niveau gesorgt ist.

# Wozu Detection and Response?

Mittlerweile weiß es jeder und niemand verheimlicht es: Absolute Sicherheit kann es auch in der IT nicht geben. Vorbeugende Maßnahmen, wie Endpoint Protection, Patch Management und Firewalling, sind sehr erfolgreich darin, Malware und Hacks in der „Pre-Breach"-Phase oder „On Execution" zu erkennen und zu blocken. Aber ein Bruchteil der Angriffe – meist komplexe, neuartige Attacken hochprofessioneller Organisationen – hat Erfolg und kann in die IT eindringen.

Jeder kennt die Geschichte von Troja: Die Einwohner der Stadt zogen das von den Griechen scheinbar zurückgelassene Holzpferd in ihre Stadt und die Leichtgläubigkeit der Bürger eröffnete eine Sicherheitslücke, die von den Angreifern zum Eindringen ausgenutzt wurde.

Doch zunächst entstand noch kein Schaden. Erst als es in der Nacht den im Rumpf versteckten griechischen Kämpfern gelang, unbeobachtet die Stadttore von innen für ihre Mitkämpfer zu öffnen, besiegelte dies die Niederlage der Belagerten: Auf den Exploit der Sicherheitslücke folgte das Nachladen und Installieren einer schädlichen menschlichen „Payload". Sie führte dazu, dass die Angreifer die Kontrolle übernahmen.

**„Wir bieten das, was Kunden für eine umfassende IT-Sicherheit benötigen. Derzeit ist dies das Know-How und das qualifizierte Personal, um Bedrohungen abzuwehren und zu minimieren."**
Michael Gisevius,
Sales DACH bei Bitdefender

# Grenzschutz

Vereinfacht entspricht herkömmliche IT-Security einer Grenzbefestigung. Sie bietet keinen Schutz mehr, sobald diese erste Verteidigungslinie durchbrochen ist. Dann müssen andere Tools und Dienste greifen, die wie eine Polizeistreife oder ein Spezialkommando die grenznahen Bereiche durchforsten und gefährdete Bereiche genauestens überwachen. Beim Schutz des „Hinterlandes" reicht aber reine Technologie –

Ausrüstung, Videoüberwachung, Alarmanlagen oder forensische Laborausstattung – nicht aus: Menschen müssen diese Tools nutzen, Spuren sammeln, Informationen interpretieren, ihre Erfahrung einsetzen und letztlich Maßnahmen zur Gefahrenabwehr einleiten.

Eine umfassende Cyber-Sicherheit besteht dementsprechend aus vorbeugenden Pre-Breach-Instrumenten, dem On-Execution-Schutz aber auch der Abwehr eines erfolgreichen Einbruchs (Post Breach). Die Hilfsmittel und Tools für diese letzte Phase werden unter dem Etikett „Detection and Response" (Erkennung und Abwehr) zusammengefasst. Sie sollen Angriffe, die nicht zu verhindern sind, so eindämmen und Angriffsketten so unterbrechen, dass ein Schaden ausbleibt oder minimal bleibt. Ebenso werden Auswirkungen mutmaßlicher Angriffe beseitigt und eventuell vorhandene Schadsoftware beseitigt. Endpoint Detection and Response (EDR) ist die tragende Säule dieser Strategie. EDR-Tools verfolgen ständig und automatisch die Aktivitäten auf allen Endpunkten eines Unternehmens und alarmieren IT- und Sicherheitsteams über Auffälligkeiten und verdächtige Ereignisse.

# Detection and Response selbst betreiben?

Die Notwendigkeit für Detection and Response ist offenkundig: Über die Hälfte der deutschen Unternehmen (54 Prozent) sind zwischen 2017 und 2019 erfolgreich gehackt worden (Bitdefender-Studie „Hacked Off", Oktober 2019). Darüber hinaus hielten es laut derselben Studie über ein Viertel der IT-Security-Profis (26 Prozent) für wahrscheinlich, dass insgeheim derzeit ein solcher Angriff läuft, ohne dass ihr Unternehmen davon weiß . Komplexe Angriffe sind nur schwer zu erkennen, weil sie Taktiken, Techniken und Verfahren einsetzen, die – für sich betrachtet – ein scheinbar normales Systemverhalten abbilden. Doch gerade diese Angriffe können ein Unternehmen teuer zu stehen kommen: Die durchschnittlichen Kosten eines Cybervorfalls sind in den letzten fünf Jahren um 72 Prozent auf dreizehn Millionen Dollar gestiegen (Accenture, „Cost of Cybercrime", 2019).

Doch es gibt auch gute Nachrichten: Denn Endpoint Detection and Response ist nicht mehr länger nur für wenige große Firmen in Reichweite. Vor wenigen Jahren war EDR noch Unternehmen vorbehalten, die erhebliche Summen in das Produkt und dessen Betreuung investieren konnten. Laut einer Ponemon-Studie aus dem Jahr 2018 nutzten sogar von diesen Großunternehmen im Durchschnitt nur 46 Prozent die Funktionen ihres EDR aktiv, da EDR zu komplex war und zu viel Vorwissen erforderte (Ponemon, „State of Endpoint Security & Risk", 2018). Neuere Lösungen haben mittlerweile EDR auch kleineren Unternehmen zugänglich gemacht. Die Analysten von Forrester sprechen von einer „Demokratisierung" dieses Abwehransatzes.

Dafür ausschlaggebende Faktoren sind die gesunkenen Anschaffungskosten, die Integration in Endpoint-Protection-Plattformen sowie Behavioral Monitoring und Machine Learning. Dies hat die Reaktionsmaßnahmen stärker automatisiert und die Zahl der Fehlalarme erheblich reduziert. Ein Unternehmen benötigt im Ergebnis weniger Personal für den Betrieb eines EDR und die Kosten sinken.

Dennoch sind Menschen weiterhin notwendig. Und so bleibt ein Security Operations Center (SOC) oder ein vergleichbares Abwehrteam eine notwendige Vorbedingung, um Eindringlinge im Netzwerk auszubremsen. Als wichtigsten Mehrwert eines SOCs sehen deutsche Befragte Network Security Monitoring in Echtzeit, eine Threat-Intelligence-Analyse sowie Prävention und Penetrationstests (siehe Grafik).

# Was genau ist ein SOC?

Zunächst handelt es sich bei einem SOC um ein Team im Unternehmen mit der einzigen Aufgabe, die eigene IT zu schützen. Die unabhängige Organisationseinheit agiert abgetrennt von anderen IT-Teams wie der Administration oder der Entwicklung. Im SOC fließen die sicherheitsrelevanten Informationen aller IT-Ressourcen zentral zusammen, zum Beispiel von Endpoint Protection, Firewall, IDS/IPS, EDR und NTA (Network Traffic Analytics). Ebenso hat das SOC Zugriff auf alle Logs. Zentrales Tool, das die Sicherheitsvorfälle aggregiert, die notwendigen Tickets erstellt und verwaltet, ist häufig ein Security Information and Event Management (SIEM).

Im Ernstfall eines großangelegten Angriffs kommt es entscheidend auf Schnelligkeit und Kommunikation an. Dafür sorgen die Experten an ihren Arbeitsplätzen, die als Einsatzleitstelle fungieren. Im SOC-Raum verfolgen die Mitarbeiter an mehreren Bildschirmen pro Arbeitsplatz und zusätzlichen Großbildschirmen aktuelle Sicherheitswarnungen und bekommen neu entdeckte IT- Schwachstellen angezeigt. Ausstattung und Abläufe sind darauf ausgerichtet, große Datenmengen zu verarbeiten und im Ernstfall blitzschnell reagieren zu können. Je nach Bedrohung wird die Durchführung von Analyse und Abwehr aufgeteilt:

**Tier-1-Analysten** übernehmen die Echtzeitüberwachung. Sie erhalten über das SIEM Alarmmeldungen als Tickets und führen standardisierte Abwehrmaßnahmen durch. Auf diese Weise überprüfen sie zahlreiche Vorfälle und verwenden dabei meist nur wenige Minuten pro Ticket.

**Tier-2-Analysten** sind erfahrenere und höher qualifizierte Sicherheitsingenieure. Sie analysieren die Vorfälle, die auf Tier-1-Ebene nicht vollständig gelöst werden können oder schwerwiegend und zeitintensiv sind. Dazu fragen sie auch gegebenenfalls weitere Datenquellen an oder sprechen mit weiteren IT-Verantwortlichen, etwa den Zuständigen für Firewalls oder Desktop-PCs. Zudem kümmern sie sich darum, die Wirkungen eines erfolgreichen Hacks zu minimieren.

**Tier-3-Analysten** oder **Threat Hunters** werden hinzugezogen, sobald Tier-2-Experten einen Vorfall eskalieren. In erster Linie ist ihre Rolle jedoch eine proaktive: Sie suchen vorbeugend durch Penetrationstests nach Lücken in der Sicherheitsarchitektur eines Unternehmens, insbesondere wenn neue Threats oder Schwachstellen durch die Alerts der Sicherheitsanbieter bekannt werden. Zudem kommen sie bei Advanced Persistent Threats (APTs) ins Spiel, um komplexe Attacken einzudämmen. Ebenso untersuchen sie Datenlecks mit den Mitteln der Computerforensik. Dies sind Fälle, deren Bearbeitung Wochen oder Monate beanspruchen kann.

Eine eigene Rolle neben den Security-Analysten spielen **Plattformingenieure** oder **Content-Autoren**. Sie werten den Input der Analysten aus, um IT-Systeme mit optimierten Regeln und Prozessen kontinuierlich zu härten. Zudem entwickeln sie Konfigurationen, die genau auf das eigene Unternehmen und seine Bedürfnisse abgestimmt sind – etwa auf die Tätigkeiten und Funktionen, die von bestimmten Ländern oder Standorten aus getätigt werden dürfen. Zugleich optimieren sie das Patch-Management. Diese Aufgabe kann nicht den Security-Analysten überlassen werden. Denn diese sollen ja die Kontrollinstanz bleiben, die in den stetig verbesserten Konfigurationen nach Fehlern und Schwachstellen sucht.

Zum Team gehört außerdem noch mindestens ein **Manager**. Er hat zwei Funktionen: Einerseits leitet er das SOC-Team an und koordiniert es. Seine vielleicht wichtigste Aufgabe liegt jedoch darin, die detaillierten, technisch

komplexen Informationen und Ergebnisse der Arbeit für das Top-Management aufzubereiten und dieses regelmäßig zu informieren. So setzt er die nötigen Impulse, um das Unternehmen dauerhaft sicher aufzustellen. Der Manager ist zudem Ansprechpartner für Anfragen rund um Compliance für den Datenschutzbeauftragten oder die Aufsichtsbehörden.

Selbst ein kleineres SOC-Team braucht mindestens acht Mitarbeiter, um einen 24/7-Service gewährleisten zu können.

# Herausforderungen einer eigenen Abwehr

Von vornherein müssen also Unternehmen hohe Investitionen einplanen, um ein vollwertiges SOC zu unterhalten. Viele Unternehmen kämpfen zudem mit erheblichen **Schwierigkeiten** beim Betrieb. So sind sie bei der Sicherheitsverwaltung oft auf mehrere Konsolen angewiesen, die auf ganz unterschiedlichen Technologien basieren. Fast 40 Prozent der Befragten einer Ponemon-Studie gaben an, dass sie sich mit **zu vielen Tools** herumschlagen müssen. Und 71 Prozent wünschen sich einen höheren Automatisierungsgrad, um Alarmmeldungen verwalten oder digitale Beweismittel erfassen zu können. Darüber hinaus fehlen den vorhandenen Sicherheitsanalysten häufig die Kapazitäten für **zeitraubende Untersuchungen** und die Bewertung und Validierung jeder einzelnen Warnmeldung. So ist es oft allein schon angesichts der Masse an Alarmen unmöglich, auch nur die Prioritäten für weitergehende Untersuchungen systematisch festzulegen.

### EDR oder MDR?

**Leitfragen für Unternehmen**

- Haben Sie alle Produkte, die Sie brauchen, um komplexe Angriffe zu entdecken?
- Finden Sie ausreichend qualifiziertes Personal für IT-Sicherheit?
- Schafft es Ihr IT-Personal, allen kritischen Alarmmeldungen innerhalb einer Stunde nachzugehen?
- Findet Ihr IT-Personal Zeit zur Härtung der IT-Umgebung und für strategische Initiativen?
- Konnten Sie in allen Vorfällen, in denen Sie eine Cyberattacke vermutet haben, den Vorgang vollständig nachvollziehen?
- Können Sie dem Top-Management alle gewünschten Daten und Informationen zum Stand der IT-Sicherheit und bestehender Risiken geben?

Je mehr dieser Fragen Sie mit „Nein“ beantworten, desto eher ist MDR die passende Lösung für Ihr Unternehmen.

# Unterbesetzung

Die größte Herausforderung aber ist der **Personalmangel**. Sicherheitsexperten sind rar, teuer und daher nur schwer zu finden oder zu halten. Im Jahr 2019 waren in Deutschland laut Bitkom 124.000 Stellen für IT-Experten offen. Obendrein gehören Security-Experten mit einem Jahresgehalt von durchschnittlich über 75.000 Euro zu den teuersten IT-Mitarbeitern. Erschwerend kommt hinzu, dass nicht jeder dieser Experten sich auf Dauer den hohen Stressfaktoren im SOC aussetzen will: Nach Ansicht der Befragten einer Bitdefender-Studie ist Mangel an Budget und Fachpersonal so belastend, dass 13 Prozent der deutschen IT-Security-Fachleute bereits erwogen haben, ihren Job zu wechseln (Bitdefender, Studie „Hacked Off“, Oktober 2019).

Die Konsequenz: Bei den meisten Organisationen liegt die **mittlere Reaktionszeit (MTTR)** auf APTs im Bereich von Monaten, während die Angreifer Daten innerhalb von Tagen manipulieren und herausschleusen. Organisationen, die über leistungsfähige EDR-Tools verfügen, aber nicht über ausreichend Spezialisten, verpassen es, das Potenzial dieser Sicherheitstools zu erschließen. Und sie riskieren, dass vermeidbare Sicherheitsvorfälle einen Rufschaden oder Datenverlust verursachen.

# Die Alternative: MDR

Abhilfe ist möglich: Da SOCs ohnehin unabhängig agieren müssen, sind sie nicht notwendigerweise innerhalb eines Unternehmens angesiedelt, sondern können zu Dienstleistern für IT-Security ausgelagert werden. Laut der „Hacked Off"-Umfrage von Bitdefender, an der sich über 500 deutsche IT-Mitarbeiter beteiligt haben, verfügen 68 Prozent der deutschen Organisationen über ein SOC: Davon betreiben es 62 Prozent intern, 38 Prozent extern.

# Vom Anbieter oder vom Dienstleister

SOC und MDR als Dienstleistung werden von lokalen IT-Beratungen, Systemhäusern und von den Herstellern von Security-Produkten angeboten. Auch Managed Security Service Provider (MSSPs), welche die IT-Sicherheitsinfrastruktur für ihre Kunden betreiben, beziehen MDR oft als Dienst von großen Cyber-Security-Herstellern und bieten dies ihren Kunden als Zusatzservice an.

**„Bitdefender MDR gibt mir die Sicherheit, dass unser gesamtes Netzwerk in Echtzeit überwacht wird, auch wenn weder ich noch sonst irgendwelche Mitarbeiter im Büro sind."**
Der IT-Leiter einer Erzdiözese.

Für externe Sicherheitszentren spricht, dass sie dauerhaft das nötige Personal rekrutieren und Synergien zwischen ihren Auftraggebern erzielen können. Die Dienstleister können eine hocheffiziente technische Infrastruktur für Detection and Response aufbauen, bleiben bei technologischen Fortschritten auf dem neuesten Stand und verfügen durch ihre Telemetrie-Netzwerke über besonders gute Kontextdaten.

**MDR-Angebote bewerten**

**Leitfragen für Unternehmen**

- Steht hinter dem MDR-Service ein Security Operations Center mit 24x7-Service und -Telefonsupport?
- Gibt es für jedes Kundenunternehmen einen verantwortlichen Ansprechpartner?
- Nutzt der Anbieter führende und bewährte Produkte für Detection and Response?
- Kann der Anbieter physische, virtuelle und Cloud-Assets gleichermaßen überwachen?
- Enthält der MDR-Service auch vorbeugende Elemente wie Threat Intelligence, Härtung und Threat Hunting?
- Enthält der MDR-Service auch strategische Elemente wie Reporting und Beratung für das Top-Management?
- Kann der Anbieter auf der Basis definierter Prozesse selbst Abwehrmaßnahmen ergreifen?
- Hat der Anbieter jederzeit neue und neuartige Bedrohungen im Blick?
- Verfügt der Service über eine ausreichend hohe Zahl and Tier-2- und Tier-3-Bedrohungsanalysten?

Mit Managed Detection and Response (MDR) lagern Unternehmen sowohl die nötigen Tools und Produkte als auch deren Betrieb an die verschiedenen Betreiber von Security-Operation-Zentren aus. Für einen Pauschalbetrag pro Monat und Endpunkt erhalten sie so ganzjährig und rund um die Uhr eine professionelle Überwachung. Dabei kommen bewährte und aufeinander abgestimmte Sicherheitstechnologien zum Einsatz.

Große MDR-Dienste vereinen Cybersicherheit für Endpunkte aller Systeme mit der Analyse von Netzwerken und Risiken. So erkennen sie zuverlässig Bedrohungen und bieten Dienstleistungen wie Threat Hunting sowie proaktiven Recherche im Darknet nach gestohlenen Daten oder Angriffsplänen mit Bezug auf das Kundenunternehmen. Der Service enthält Echtzeit-Dashboards und regelmäßige Berichte für Sicherheitsverantwortliche und Geschäftsleitung. Je nach Budget stehen verschiedene modulare Pakete zur Auswahl.

# Mit MDR den Hackern einen Schritt voraus

IT-Sicherheit ist kein Zustand, sondern eine Handlung. Die Vorstellung, sich Sicherheit als Produkt zu kaufen, ist spätestens mit den komplexen, mehrstufigen Angriffsszenarien der Gegenwart überholt. Man kann sich aber Sicherheit als permanente Dienstleistung mieten, um sich gegen diese neue Bedrohungslandschaft zu wappnen.

## Mehrwehrt für Sicherheit

MDR zeichnet sich vor allem durch folgende Faktoren aus:

- **SOC-Personal an Bord:** MDR-Anbieter stellen den Kunden ein SOC mit ausreichenden Personalressourcen zur Verfügung. Sie stellen sicher, dass Sicherheitsexperten über die Technologie und das Know-How verfügen, um die jeweilige Umgebung zu betreuen.
- **Erkennung komplexer Angriffe:** Die Sicherheitsanalysten arbeiten rund um die Uhr daran, auf der Grundlage von kundenspezifischen Bedrohungsprofilen alle Erkenntnisse zu Bedrohungen zu sammeln und diese zu bekämpfen. Sie erweitern diese Informationen durch Host- und Netzwerk-gestützte Telemetriedaten sowie Sicherheitsanalysen, um auch komplexe und gezielte Angriffe aufzuspüren.
- **Verbesserte Erkennung und schnelle Antwortzeiten:** Telemetrie und Alarmmeldungen in Echtzeit werden über mehrere Datenströme miteinander korreliert. Gleichzeitig erarbeiten die Abwehrzentren für jeden Kunden einschlägige Reaktionsmaßnahmen, die effektive Reaktionen ermöglichen. So begrenzen sie die Auswirkungen eines Sicherheitsvorfalls auf das Unternehmen.
- **Entlastung des Unternehmens:** MDR verwaltet die Sicherheitstechnologie für die Kunden, so dass sich das interne IT-Team intensiver um strategische Geschäftsinitiativen kümmern kann. Die Betriebe haben weniger Personalkosten und müssen sich nicht um Kauf, Lizenzierung oder Pflege des Tool-Stacks sorgen.

MDR stellt der organisierten Cyberkriminalität einen mindestens ebenso gut organisierten Gegenspieler entgegen. Durch EDR-Tools, Automatisierungsmöglichkeiten, konsequente Bündelung des IT-Security-Know-hows und externe persönliche Expertise bleiben Unternehmen und Organisationen den Angreifern auf Dauer überlegen und können dafür sorgen, dass selbst anspruchsvolle Attacken folgenlos bleiben.

### Bitdefender MDR

Managed Detection and Response (MDR) von Bitdefender bietet die umfassenden Dienstleistungen des Bitdefender-eigenen Security Operations Center (SOC). Das 24x7-Serviceangebot umfasst Bitdefender GravityZone Ultra und Network Traffic Analytics (NTA), sowie zusätzliche Visualisierungs- und Management-Toolsets. Das SOC führt proaktive Cyber-Sicherheitsoperationen und Threat Hunting durch, die von hochqualifizierten Analysten mit tiefem interdisziplinärem Cybersicherheitswissen geleitet werden.

Bitdefender Managed Detection and Response ist in drei Stufen verfügbar:

### Bitdefender MDR-Optionen

| | MDR Core | 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 | | | ✓ |
| Add-Ons | | | |
| Agentenloser Schutz von IoT-Geräten | | ✓ | ✓ |

Weitere Informationen unter www.bitdefender.com/mdr .

# Kontakt

Wünschen Sie Informationen zu den Unternehmenslösungen von Bitdefender?

Kontaktieren Sie uns unter

sales_dach@bitdefender.de

# Über Bitdefender

Bitdefender ist ein weltweit führender Anbieter von Cybersicherheitslösungen schützt über 500 Millionen Systeme in mehr als 150 Ländern. Seit der Gründung im Jahr 2001 sorgen Innovationen des Unternehmens regelmäßig für ausgezeichnete Sicherheitsprodukte und intelligenten Schutz für Geräte, Netzwerke und Cloud-Dienste von Privatkunden und moderner Unternehmen. Als Zulieferer erster Wahl befindet sich Bitdefender-Technologie in 38 Prozent der weltweit eingesetzten Sicherheitslösungen und genießt Vertrauen und Anerkennung bei Branchenexperten, Herstellern und Kunden gleichermaßen.www.bitdefender.de

# Warum Bitdefender

## Stolz im Dienste unserer Kunden

Bitdefender bietet Lösungen und Services für kleine und mittlere Unternehmen sowie Dienstleister und Firmen im Bereich Technologieintegration. Wir sind stolz auf das Vertrauen, das uns Unternehmen wie **Mentor, Honeywell, Yamaha, Speedway, Esurance oder Safe Systems** entgegenbringen.

*Sieger im ersten Forrester Wave™-Report zur Sicherheit von Cloud-Workloads*
*Bewertung „empfehlenswert" beim NSS Labs AEP Group Test von NSS Labs*
*Zwei Jahre in Folge Auszeichnung zum SC Media Industry Innovator für die Hypervisor Introspection*
*Bewertung als „Representative Vendor of Cloud-Workload Protection Platforms" durch Gartner®*

## Ein Wort an unsere mehr als 20.000 Partner weltweit

Als exklusiver Channel-Anbieter verdankt Bitdefender seinen Erfolg auch seinem Netzwerk aus Wiederverkäufern und Vertriebspartnern.

*Vier Jahre in Folge 5-Sterne-Partner von CRN Aufnahme in die „Security 100 List" von CRN*
*Zwei Jahre in Folge Cloud-Partner von CRN*
*Mehr MSP-Lösungen als jeder andere Sicherheitsanbieter*
*3 Bitdefender-Partnerprogramme, damit alle unsere Partner – Wiederverkäufer, Dienstleister und Hybridpartner – im Rahmen ihrer eigenen Spezialisierung sich vorrangig dem Vertrieb von Bitdefender-Lösungen widmen können*

## Vertrauenswürdige Sicherheitsinstitution

Bitdefender ist stolz auf seine Partnerschaften mit namhaften Virtualisierungsanbietern und den Beitrag, den wir gemeinsam mit **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS und Pivotal zur Entwicklung sicherer Ökosysteme leisten.**
Bitdefender ist zudem in enger Zusammenarbeit mit dem FBI und Europol aktiv an der Bekämpfung der internationalen Cyberkriminalität beteiligt und unterstützt Initiativen wie NoMoreRansom und TechAccord. So konnte Bitdefender z. B. zur Abschaltung des Online-Schwarzmarktes Hansa beitragen. 2019 wurde Bitdefender darüber hinaus von MITRE als CVE Numbering Authority autorisiert.

**ANERKANNT VON FÜHRENDEN ANALYSTEN UND UNABHÄNGIGEN PRÜFORGANISATIONEN**

CRN AV-TEST AV Comparatives Gartner 451 Research FORRESTER IDC GLOBAL

**TECHNOLOGIEPARTNERSCHAFTEN**

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX

Bitdefender

**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

## IM ZEICHEN DES WOLFS

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 **hellleuchtenden Drachen-Wolf** repräsentiert. Er steht Ihnen zur Seite und schützt Sie mit seiner aus unserer Ingenieurskunst hervorgegangen 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.

Bitdefender-Whitepaper-MDR-NoLocalization-cres5047-A4-de_DE
12/10/20.january 21, 2021 5:23 pm01/21/21