

# So gelingt auch mit schlanken Teams zuverlässige Sicherheit



Alle Rechte vorbehalten. © 2025 Bitdefender. Alle hier genannten Marken, Handelsnamen und Produkte sind Eigentum ihrer jeweiligen Inhaber. Die in diesem Dokument enthaltenen Informationen sind vertraulich und nur für den Gebrauch durch den vorgesehenen Empfänger bestimmt.

Sie dürfen dieses Dokument nicht ohne vorherige Genehmigung durch Bitdefender veröffentlichen oder weiterverbreiten.

Die meisten Cybersicherheitsberichte beginnen mit Warnungen vor neuen Bedrohungen, doch für kleine Teams liegt die eigentliche Herausforderung woanders. Sie kennen die alarmierenden Statistiken, wie beispielsweise die [55 Milliarden](#) US-Dollar, die im letzten Jahrzehnt durch Business Email Compromise (BEC) verloren gingen, den Anstieg der BEC-Vorfälle um 66 % oder das Auftreten von Ransomware in 44 % der Sicherheitsverletzungen (ein Anstieg von 37 % im Vergleich zum Vorjahr)<sup>2,1</sup>.

Diese Zahlen sind zwar hilfreich zur Aufklärung von Vorständen und Führungskräften, aber für IT- und Sicherheitsverantwortliche sind sie nichts Neues, denn sie wissen, dass diese Bedrohungen seit Jahren zunehmen. Neu ist jedoch die zunehmende digitale Präsenz von Unternehmen und die damit einhergehend wachsende Angriffsfläche.

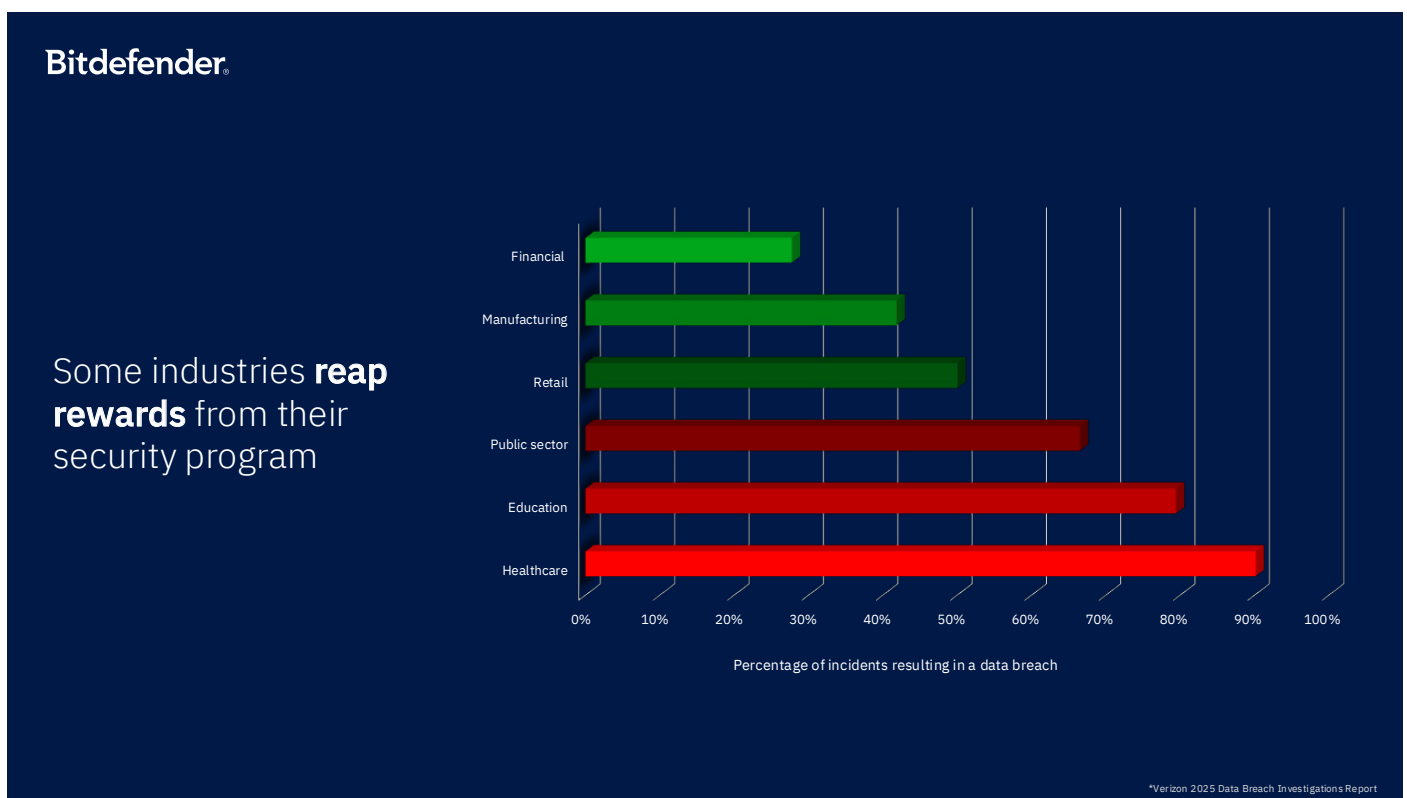
Wenn Sie keinen vollständigen Überblick über Ihre internen und externen Assets haben, einschließlich Ihrer Schatten-IT, Cloud-Apps und Daten, die in KI-Tools fließen, können Sie sicher sein, dass Angreifer Schwachstellen finden werden, die sie ausnutzen können. Ihre Mitarbeiter und Ihre Lieferkette sind ebenfalls Teil Ihrer Angriffsfläche und wenn Sie diese nicht im Blick haben, kann dies erhebliche blinde Flecken verursachen.

Laut dem Verizon-Bericht „Data Breach Investigations Report 2025“ sind 60 % der Sicherheitsverletzungen auf menschliche Fehler und 30 % auf das Verschulden Dritter zurückzuführen<sup>2</sup>. Eine Studie von Bitdefender zeigt zudem einen besorgniserregenden Trend: In 84 % der Sicherheitsvorfälle kapern Angreifer legitime, bereits auf Geräten installierte Tools. Diese Tools sind keine zu behebenden Sicherheitslücken, sondern sie sind für den legitimen Gebrauch bestimmt. Daher stellt die Erkennung dieser missbräuchlichen Nutzung eine erhebliche Herausforderung dar.

Weitere Untersuchungen von Verizon zeigen, dass Unternehmen durchschnittlich 32 Tage für die Behebung von Sicherheitslücken an Perimetergeräten benötigen<sup>2</sup>, wodurch diese viel zu lange angreifbar sind. Dies verdeutlicht die Folgen einer mangelnden Sichtbarkeit, da Schwachstellen, die nicht schnell erkannt werden, auch nicht schnell behoben werden können. Die eigentliche Herausforderung besteht darin, die notwendige Transparenz zu erlangen, um das Zeitfenster für Sicherheitslücken zu verkürzen – selbst mit begrenzten Ressourcen und einem kleinen Team.

## Wer hat die passende Sicherheitsstrategie?

Der Anteil der Sicherheitsvorfälle, die zu tatsächlichen Datensicherheitsverletzungen führen, variiert stark zwischen den Branchen und spiegelt Unterschiede bei den Sicherheitsinvestitionen und dem Reifegrad der Sicherheitsprogramme wider.



Finanzinstitute, die streng reguliert sind und in der Regel über beträchtliche Sicherheitsbudgets verfügen, weisen die niedrigsten Raten von Sicherheitsverletzungen auf, gefolgt vom verarbeitenden Gewerbe. Dies lässt darauf schließen, dass strukturierte Sicherheitsprogramme und spezialisierte Ressourcen die Wahrscheinlichkeit, dass sich Vorfälle zu Sicherheitsverletzungen ausweiten, deutlich verringern können. Am anderen Ende des Spektrums haben Branchen, die stark auf öffentliche Mittel angewiesen sind, darunter der öffentliche Sektor, das Bildungswesen und das Gesundheitswesen, deutlich größere Schwierigkeiten.

Betrachtet man dieselben Daten unter Berücksichtigung der Unternehmensgröße, erweisen sich größere Unternehmen als klare Gewinner. Fast 20 % weniger Unternehmen mit über 1.000 Mitarbeitern waren von einer Sicherheitsverletzung betroffen als Unternehmen mit weniger als 1.000 Mitarbeitern<sup>2</sup>.

Die wichtigste Erkenntnis daraus ist, dass Unternehmen, die der Cybersicherheit durch Richtlinien, Technologie und Mitarbeiterschulungen Priorität einräumen und in sie investieren, beim Auftreten von Sicherheitsvorfällen deutlich besser abschneiden. Umgekehrt sind diejenigen mit begrenzten Ressourcen oder weniger ausgereiften Programmen weitaus anfälliger, und Sicherheitsvorfälle können sich viel eher zu schwerwiegenden Sicherheitsverletzungen ausweiten.

## Die Frage ist: Was genau machen diese Unternehmen richtig, und wie können Sie das Gleiche tun?

### Absicherung Ihres Unternehmens während des gesamten Angriffslebenszyklus

Unternehmen, die das Thema Sicherheit richtig angehen, verfügen über ausgereifte Programme, die auf Risikomanagement- und Compliance-Frameworks basieren, und sie implementieren Sicherheit über den gesamten Angriffslebenszyklus hinweg.



Hier eine kurze Übersicht über die einzelnen Phasen und warum sie so wichtig sind:

### 1. Prävention

Die erste Phase ist die Prävention, bei der es darum geht, einen vollständigen Überblick über die Angriffsfläche zu gewinnen, Risiken zu identifizieren und Schwachstellen zu bewerten. Dann wissen Sie, was Sie verteidigen, und das hilft Ihnen, Ihr Risiko gegenüber potenziellen Bedrohungen proaktiv zu verringern.

### 2. Schutz

Hierfür setzen Teams automatisierte Tools ein, um Angriffe zu stoppen oder zu blockieren, bevor sie ausgeführt werden können, wodurch die Wahrscheinlichkeit einer Kompromittierung minimiert wird.

### 3. Erkennung

Unternehmen sind sich bewusst, dass kein System völlig undurchdringlich ist und investieren daher in Technologien, die Angriffe, die Präventivmaßnahmen umgehen, schnell erkennen und so potenziellen Schaden begrenzen können.

### 4. Reaktion auf Sicherheitsvorfälle

Wenn es zu Sicherheitsvorfällen kommt, verfügen leistungsstarke Unternehmen über Fähigkeiten, die Bedrohungen schnell einzudämmen, den Hergang zu untersuchen, sich von etwaigen Auswirkungen zu erholen und Abhilfemaßnahmen zu ergreifen, um ein erneutes Auftreten zu verhindern.

Geschwindigkeit ist bei der Erkennung und Reaktion von entscheidender Bedeutung. Sicherheitsteams überwachen Kennzahlen wie die durchschnittliche Erkennungszeit (MTTD), die durchschnittliche Eindämmungszeit (MTTC) und die durchschnittliche Reaktionszeit (MTTR), um die Sicherheitsmaßnahmen kontinuierlich zu verbessern.



## Darum ist proaktive Prävention der Schlüssel zum Erfolg

Die zentrale Erkenntnis hierbei ist, dass eine hervorragende proaktive Prävention ein Schlüsselfaktor ist, um die Wahrscheinlichkeit zu verringern, dass ein Sicherheitsvorfall zu einer Sicherheitsverletzung führt.

Durch ein effektives Management des gesamten Angriffslebenszyklus, von Prävention und Schutz bis hin zu Erkennung und Reaktion, verbessern die effektivsten Unternehmen ihre Widerstandsfähigkeit dramatisch und senken die Raten von Sicherheitsverletzungen selbst dann, wenn Angriffe stattfinden.

Für Sicherheitsverantwortliche wirft dies eine wichtige Frage auf: Messen sie die SecOps-Performance anhand dieser Kennzahlen und haben sie Einblick in jede Phase des Angriffslebenszyklus? Dieses Verständnis kann Lücken im Programm aufdecken und Möglichkeiten zur Stärkung der Abwehrmechanismen dort aufzeigen, wo es am wichtigsten ist.

# Tool-Wildwuchs erzeugt Komplexität

Die zunehmende Komplexität der verwendeten Tools stellt eine der größten Herausforderungen für die moderne Cybersicherheit dar, da sie die Kosten in die Höhe treibt und die Komplexität erhöht. Laut einer Studie von IBM<sup>3</sup>. Um das Ausmaß des Problems zu verdeutlichen: 52 % der Sicherheitsexperten sehen die Komplexität als größtes Hindernis für einen effektiven Betrieb<sup>3</sup>.

## Zu den gängigsten Kategorien von Sicherheitstools gehören:

- ▶ Tools zur Verwaltung der Angriffsfläche, die verschiedene Assets überwachen.
- ▶ Schutztools, wie z. B. Endpoint-, E-Mail-, Web- und Netzwerksicherheit.
- ▶ Erkennungstechnologien, die an allen Eintrittspunkten und für alle Assets eingesetzt werden.
- ▶ Sicherheitsvorfall- und Ereignis-Management-Plattformen, die versuchen, die Warnmeldungen der anderen Tools zu interpretieren.
- ▶ Reaktions- und Wiederherstellungs-Tools, die dabei helfen, Angriffe einzudämmen, zu analysieren und zu beheben.

Unternehmen setzen diesen komplexen Mix an Tools ein, um jede Phase eines Angriffs abzudecken, wobei jedes Tool einem bestimmten Zweck dient. Leider führt die schiere Anzahl der Tools auch zu operativen Reibungsverlusten, treibt die Kosten in die Höhe und erfordert hochspezialisiertes SecOps-Know-how, das teuer ist und dessen Rekrutierung und Bindung eine Herausforderung darstellen kann. Am wichtigsten ist jedoch, dass jedes dieser Tools die Angriffsfläche vergrößert und die Wahrscheinlichkeit von Fehlkonfigurationen erhöht, die Angreifer ausnutzen können.

Diese Ergebnisse verdeutlichen, wie wichtig es ist, die vorhandenen Tools nach Möglichkeit zu konsolidieren und zu optimieren. Die Vereinfachung einer komplexen Sicherheitsumgebung reduziert Ihr operatives Risiko und macht Ihre Abwehrmaßnahmen effektiver, während gleichzeitig Ihre Kosten im Laufe der Zeit sinken.

# So kann der Plattformansatz den Tool-Wildwuchs eindämmen

Die ideale Lösung zur Reduzierung des Tool-Wildwuchses und der Komplexität ist eine einheitliche Cybersicherheitsplattform. Theoretisch würde diese Plattform mehrere Sicherheitsfunktionen in einer einzigen, integrierten Umgebung zusammenführen. Dies würde Prävention, Schutz, Erkennung und Reaktion über den gesamten Angriffslebenszyklus hinweg optimieren, die operative Komplexität verringern und die Kosten senken.

Leider hat der Gedanke, alles zu integrieren, seine Grenzen. Kein Unternehmen kann (und sollte) jedes Tool und jeden Prozess zwanghaft auf einer einzigen Plattform konsolidieren. Große Unternehmen mit großen Budgets und umfangreichen SecOps-Teams arbeiten oft mit einer Vielzahl spezialisierter Tools und können die Komplexität bewältigen. Für sie war die Einführung neuer Lösungen selten ein Problem, da sie über das Personal und die Expertise verfügen, um mehrere Lösungen zu verwalten, selbst wenn dies zu Ineffizienzen und zusätzlichen Angriffsflächen führt.

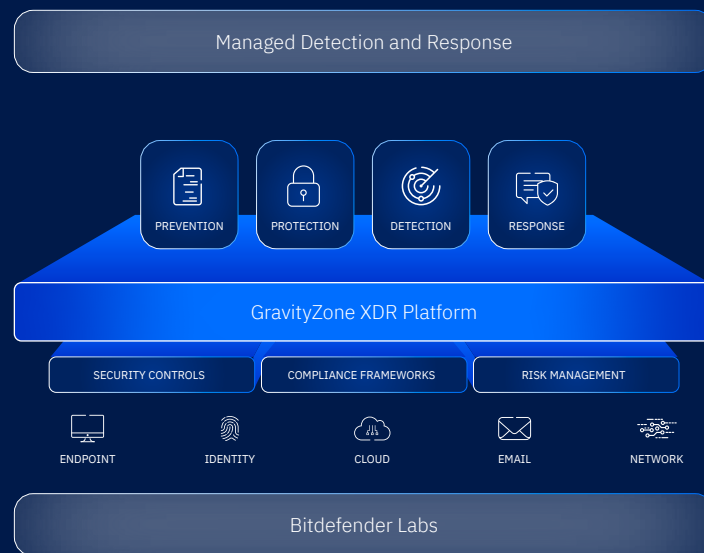
Der Plattformansatz erweist sich insbesondere für mittelständische Unternehmen mit kleinen IT- und Sicherheitsteams als wertvoll. In diesen Unternehmen birgt die unkontrollierte Ausbreitung von Tools ein erhebliches Risiko, da Fehlkonfigurationen, verzögerte Reaktionen und Lücken in der Abdeckung schnell zu schwerwiegenden Sicherheitsvorfällen eskalieren können. Die richtige Plattform bündelt wesentliche Funktionen, eliminiert redundante Tools und zentralisiert das Management. Sie ermöglicht kleineren Teams, im gleichen Umfang und mit der gleichen Effizienz wie größere Sicherheitsteams zu arbeiten.

Die Reduzierung der Komplexität und die Integration von Kernfunktionen sind die Stärken einer einheitlichen Plattform. Sie ermöglicht mittelständischen Unternehmen, ihr Geschäft umfassend abzusichern, ohne auf große Expertenteams angewiesen zu sein. Sie bietet Transparenz über den gesamten Angriffslebenszyklus hinweg, automatisiert kritische Funktionen und vereinfacht sowohl die Erkennung als auch die Reaktion.

Auch wenn sie keine Universallösung ist, kann eine sorgfältig ausgewählte Plattform für Unternehmen, die mit zu vielen Tools und zu wenigen Ressourcen zu kämpfen haben, ein potenziell chaotisches Sicherheitsumfeld in ein optimiertes, effektives und überschaubares Programm verwandeln. Kurz gesagt bietet sie Schutz der Enterprise-Klasse bei weitaus geringerer Komplexität.

# GravityZone bietet Schutz ohne Komplexität

Bitdefender hat GravityZone entwickelt, um die oben genannten Herausforderungen zu bewältigen, die durch die Vielzahl an Tools, die operative Komplexität und die steigenden Kosten für Cybersicherheit entstehen. Es vereint die Vorteile spezialisierter Tools, jedoch ohne den damit verbundenen Aufwand und die Notwendigkeit eines großen Teams von Sicherheitsexperten.



Bei der Konzeption von GravityZone wurden von Grund auf drei Kernziele verfolgt:

## 1. Umfassender Schutz über den gesamten Lebenszyklus einer Bedrohung oder eines Angriffs hinweg

GravityZone wurde entwickelt, um Ihnen die gesamte Sicherheit zu bieten, die Sie während des gesamten Angriffslebenszyklus benötigen, und deckt Prävention, Schutz, Erkennung und Reaktion ab. Ein solcher Schutz gewährleistet, dass sich Unternehmen in jeder Phase gegen Angriffe verteidigen können, wodurch die Wahrscheinlichkeit von Sicherheitsverletzungen selbst dann verringert wird, wenn es doch zu Sicherheitsvorfällen kommt.

## 2. Vereinfachte Sicherheitsabläufe

Durch die Vereinfachung von Sicherheitsabläufen dank GravityZone können Teams ihre Ziele effizient erreichen und gleichzeitig das Risiko minimieren. Die Zusammenführung wichtiger Funktionen in einer einzigen, integrierten Umgebung reduziert die Komplexität, die Kosten und den operativen Aufwand, die typischerweise mit der Verwaltung mehrerer Insellösungen verbunden sind.

## 3. Es basiert auf bewährten und vertrauenswürdigen Sicherheitstechnologien

Die Grundlage der Plattform sind die Bitdefender Labs. Bitdefender Labs, das auf über 16 Jahren KI-Innovation basiert, analysiert täglich über 500.000 neue Bedrohungsvarianten und bietet so einen umfassenden Präventions- und Schutz-Stack, der es Unternehmen mit kleinen Teams ermöglicht, Cybersicherheit von Anfang bis Ende effektiv umzusetzen.

Die Sicherheitstechnologien von Bitdefender werden immer wieder in Hunderten von unabhängigen Tests validiert. Zu den wichtigsten Erfolgen zählen eine Reaktionsquote von 99,3 % bei Bedrohungen, perfekte Ergebnisse bei Ausdauer- und Transparenz-Tests, 100 % Transparenz der Angriffskette und der höchste Anteil (93 %) an aussagekräftigen Berichten bei gleichzeitig geringster Anzahl versendeter Benachrichtigungen.



# So verbessert GravityZone die Sicherheit während des gesamten Angriffslebenszyklus

GravityZone unterstützt kleine IT- und Sicherheitsteams dabei, Risiken zu reduzieren und effizienter über den gesamten Angriffslebenszyklus hinweg zu arbeiten, indem Prävention, Schutz, Erkennung und Reaktion in einer einzigen Plattform vereint werden.

## Prävention

GravityZone stärkt Risikominderungsstrategien durch die Bereitstellung kontinuierlicher Sichtbarkeit auf der gesamten Angriffsfläche. Es identifiziert Schwachstellen, Fehlkonfigurationen, riskante Verhaltensweisen und wertvolle Ziele und ermöglicht es Unternehmen, Abhilfemaßnahmen nach Schweregrad und potenziellen Auswirkungen zu priorisieren.

**Im Test zeigte Proactive Hardening and Attack Surface Reduction (PHASR) von Bitdefender seine Wirksamkeit, da bestimmte Angriffsarten um 95 % reduziert werden konnten.**

Die Plattform ist darauf ausgelegt, Compliance-Bemühungen zu stärken, da sie Assets regulatorischen Frameworks zuordnet, Compliance-Bewertungen generiert, Lücken identifiziert und umsetzbare Empfehlungen bietet. Die automatisierte Berichtserstellung belegt den ROI von Risikomanagementprogrammen und liefert Nachweise für Audits, wodurch die Führungsebene konkrete Beweise für Verbesserungen der Sicherheitslage erhält.

## Schutz

Mit den mehrschichtigen Schutztechnologien von GravityZone können Unternehmen Bedrohungen automatisch über alle Assets und Angriffspunkte hinweg blockieren. Wenn Angreifern das Eindringen so schwer wie möglich gemacht wird, verringert sich die Wahrscheinlichkeit eines Sicherheitsvorfalls und der Aufwand für die Reaktion auf Sicherheitsvorfälle.

**Unabhängige Tests bestätigen die hohe Wirksamkeit und Genauigkeit von GravityZone bei minimalen falsch positiven Ergebnissen. Ein Kunde von Bitdefender berichtete sogar von einem Rückgang der Anzahl von Sicherheitsvorfällen im Zusammenhang mit Endgeräten um 80 bis 90 Prozent.**

Der Schutz bildet die zweite Verteidigungslinie, die die Wahrscheinlichkeit von Sicherheitsverletzungen minimiert und es den Sicherheitsteams ermöglicht, sich auf Aufgaben mit höherer Priorität zu konzentrieren, während gleichzeitig eine umfassende Schutzabdeckung in Ihrem Unternehmen gewährleistet wird.



## Erkennung

Sollte es Angreifern gelingen, Ihre proaktiven Maßnahmen zu umgehen, hilft Ihnen GravityZone dabei, dies schnell zu erkennen, indem Warnmeldungen über alle Bedrohungsvektoren und Assets hinweg korreliert werden. Es erkennt anomales Verhalten, laterale Bewegungen und Missbrauch von Anmeldeinformationen sowohl auf verwalteten als auch auf nicht verwalteten Geräten.

Es ist darauf ausgelegt, eine schnelle Reaktion und Eindämmung zu ermöglichen, indem Signale und Warnmeldungen priorisiert und korreliert sowie Sicherheitsvorfälle in einem für Menschen lesbaren Format dargestellt werden. Die kontextbezogene Sichtbarkeit von wertvollen und gefährdeten Assets verbessert die Entscheidungsfindung, während die automatisierte Analyse von Angriffspfaden die Untersuchungs- und Lösungszeit verkürzt.

**Ein Bitdefender-Kunde gab an, dass er mit GravityZone seinen Zeitaufwand für die Untersuchung und Behebung von Sicherheitsvorfällen um 50 % reduzieren konnte.**

Dieser ganzheitliche Ansatz ermöglicht es Ihrem Unternehmen, Bedrohungen frühzeitig zu erkennen und schnell zu reagieren, wodurch Schäden und Störungen begrenzt werden.

## Antwort

Sicherheitsteams müssen in der Lage sein, Angriffe schnell einzudämmen, zu untersuchen und zu beheben. GravityZone ermöglicht es, mit einem einzigen Klick Endpoints zu isolieren, schädliche Prozesse zu beenden und Systeme wiederherzustellen. Darüber hinaus bietet es eine nachträgliche Analyse des Vorfalls, um Erkenntnisse über die Ursachen zu gewinnen und Angriffspfade zu identifizieren, was Maßnahmen zur Verhinderung eines erneuten Auftretens unterstützt. Gleichzeitig wird durch umfassende Berichte die Einhaltung der Meldepflichten gegenüber Aufsichtsbehörden unterstützt und eine transparente Kommunikation mit Interessengruppen gewährleistet.

Durch die Kombination von schneller Eindämmung und detaillierten forensischen Erkenntnissen werden Ausfallzeiten, finanzielle Auswirkungen und Reputationsrisiken minimiert, sodass Ihre Teams die Geschäftskontinuität auch während Zwischenfällen aufrechterhalten können.



## Managed Detection & Response

Managed Detection and Response (MDR) kann Ihnen helfen, Ressourcen- und Expertenengpässe zu überwinden, indem es Ihnen rund um die Uhr SecOps-Support bietet. Sie können entweder Ihr bestehendes IT-Sicherheitspersonal ergänzen oder die Sicherheitsaufgaben vollständig an die Experten von Bitdefender auslagern, um den Bedarf an Rekrutierung und Schulung zu reduzieren.



Bitdefender wird im MDR Market Guide von Gartner erwähnt und hat auf deren Peer Insights-Bewertungsseite eine durchschnittliche Bewertung von 4,8/5.

Der MDR-Service von Bitdefender geht über reine Warnmeldungen hinaus – das Team reagiert aktiv auf Angriffe und dämmt diese in Ihrem Namen ein und bietet gleichzeitig fachkundige Beratung zur Weiterbildung Ihrer internen Teams. Dies umfasst maßgeschneiderte Empfehlungen, Unterstützung beim Threat-Hunting und strategische Einblicke, die Ihrem Unternehmen helfen, den sich ständig weiterentwickelnden Bedrohungen einen Schritt voraus zu sein.

MDR versetzt Ihr kleines IT- und Sicherheitsteam in die Lage, ein ähnliches Sicherheitsniveau wie Ihre Mitbewerber und Konkurrenten zu erreichen, und gibt Ihnen mehr Vertrauen in die kontinuierliche Überwachung Ihrer Umgebung.

Ein Bitdefender-Kunde sagte, für den Aufbau eines eigenen SOC hätte er ansonsten das Fünffache zahlen müssen, während ein anderer sagte, der Service von Bitdefender habe ihm 40 % der Betriebskosten eingespart.

## Bitdefender-Labore

Die Produkte und Dienstleistungen von Bitdefender basieren auf innovativen Sicherheitstechnologien, die vom Bitdefender Labs-Team entwickelt und betreut werden. Sie bilden die Grundlage der GravityZone-Plattform und werden von über 200 Technologieanbietern und Dienstleistern in deren Produkten lizenziert und eingesetzt.

Die Leistungsfähigkeit und Effektivität der Technologien werden regelmäßig von unabhängigen Dritten nachgewiesen, und Bitdefender erhält bei der Teilnahme an bisher über 450 veröffentlichten Evaluierungen durchweg hohe Bewertungen.

Fast die Hälfte der Mitarbeiter von Bitdefender arbeitet im Bereich Forschung und Entwicklung. Innovationen werden durch die Zusammenarbeit mit der Wissenschaft vorangetrieben, um zukunftsweisende Themen wie neuronale Netze, Quantencomputing und Deepfakes zu erforschen. Das Team hat zudem einen sehr guten Kontakt zu den Strafverfolgungsbehörden und unterhält 32 Partnerschaften mit Behörden weltweit, darunter Europol, Eurojust und Interpol.

Durch diese Validierung können wir sicherstellen, dass GravityZone für Bitdefender-Kunden weiterhin eine führende Rolle bei der Bedrohungsabwehr, dem Schutz, der Erkennung und der Reaktion auf Bedrohungen einnimmt.

## Den Schutz der Enterprise-Klasse trotz kleinem Team erreichen

GravityZone wurde speziell entwickelt, um umfassende Sicherheit der Enterprise-Klasse zu bieten und gleichzeitig den Betrieb für kleine IT-Teams zu optimieren.

**Zusammenfassend lassen sich die fünf wichtigsten Ergebnisse, die Unternehmen durch die Einführung von GravityZone erzielen, wie folgt darstellen:**

### 1. Nachweisliche Reduzierung des Risikos im gesamten Lebenszyklus eines Cyberangriffs

GravityZone bietet umfassende Prävention, Schutz, Erkennung und Reaktion. Die Sicherheitskompetenz von Bitdefender wird durch die Tatsache bestätigt, dass seine Produkte und Dienstleistungen in über 20 aktuellen Analystenberichten von Gartner, Forrester und IDC Erwähnung finden.

### 2. Bringen Sie Ihre Produkte schneller auf den Markt

Die schnelle und einfache Implementierung ermöglicht eine sofortige Visualisierung der Risiken, sodass Sie Maßnahmen zur Abhilfe und Minderung entsprechend priorisieren können. Die Plattform erhält bei Gartner Peer Insights eine sehr hohe Bewertung hinsichtlich Integration und Implementierung (4,6/5).

### 3. Steigerung der Effizienz und Produktivität kleiner IT- und Sicherheitsteams

GravityZone zeichnet sich durch eine einzige, intuitive Benutzeroberfläche mit umfangreichen Automatisierungsfunktionen aus. Dadurch können IT-Mitarbeiter Cybersicherheitsaufgaben schnell erledigen, während fortgeschrittene Funktionen für Spezialisten ebenfalls verfügbar sind. Ein Kunde berichtete auf Peer Insights von einer 70%igen Reduzierung des Zeitaufwands für die tägliche Sicherheitsadministration seit dem Wechsel zu Bitdefender.

### 4. Senken der Gesamtbetriebskosten (TCO)

Die Konsolidierung von Tools und optimierte Abläufe verringern die Abhängigkeit von großen Teams mit teuren Sicherheitsexperten. Ein Kunde berichtete von einem ROI von 120 %, ein anderer gab an, die Betriebskosten um 50 % gesenkt zu haben, ohne dabei an Effektivität einzubüßen.

### 5. Investieren Sie in Sicherheit, die mit Ihrem Unternehmen wächst

Flexible modulare Lizenzierung und kontinuierliche F&E-Updates sorgen dafür, dass sich die Plattform parallel zu neuen Bedrohungen weiterentwickelt. Das bedeutet auch, dass Sie im Zuge der Weiterentwicklung Ihres Unternehmens immer mehr Funktionen hinzufügen können.

Diese Ergebnisse zeigen, wie GravityZone die Sicherheitslage Ihres Unternehmens im gesamten Angriffslebenszyklus verbessert. Sie beziffern außerdem den messbaren ROI und die Reduzierung der Betriebskosten.

[Besuchen Sie unsere Website](#), um herauszufinden, wie GravityZone Ihnen dabei helfen kann, Komplexität zu beseitigen und Risiken durch eine auf Ihr Unternehmen optimierte Sicherheit zu reduzieren, die bei unabhängigen Bewertungen regelmäßig Spitzenleistungen erzielt.

#### Referenzen

- 1 [FBI IC3-Mitteilung I-091124-PSA, 11. September 2024](#)
- 2 [Verizon 2025 Data Breach Investigations Report](#)
- 3 [IBM Institute for Business Value: Capturing the cybersecurity dividend](#)

Als führender Anbieter von Cybersecurity-Lösungen bietet Bitdefender hochwertige Lösungen bei der Prävention, Erkennung und Beseitigung von Bedrohungen. Millionen von Verbrauchern, Unternehmen und staatlichen Organisationen vertrauen auf das Expertenwissen von Bitdefender, wenn es um die Bekämpfung von Cybergefahren, den Schutz von Daten, digitale Identitäten und Privatsphäre und den Aufbau von Cyberresilienz geht. Bitdefenders umfangreiche Investitionen in Forschung und Entwicklung zahlen sich aus: So entdecken die Bitdefender Labs Hunderte neue Bedrohungen pro Minute und prüfen mehrere Milliarden Bedrohungsabfragen pro Tag. Bitdefender zeichnet für zahlreiche bahnbrechende Innovationen im Malware-Schutz, der IoT-Sicherheit, bei Verhaltensanalysen und künstlicher Intelligenz verantwortlich, und die daraus resultierenden Technologien werden von über 200 der bekanntesten Tech-Unternehmen aus aller Welt eingesetzt. Bitdefender wurde 2001 gegründet, betreut Kunden in über 170 Ländern und ist weltweit mit Niederlassungen vertreten.

Stand: September 2025

Weitere Informationen finden Sie unter <https://www.bitdefender.de>.

#### Romania HQ

Orhideea Towers  
15A Orhideelor Road,  
6th District,  
Bukarest 060071

T: +40 21 4412452

#### US HQ

111 W. Houston Street,  
Suite 2105 Frost Tower  
Building  
San Antonio, Texas  
78205, USA