SOLUTION BRIEF

NUR ONLINE VERFÜGBAR

Bitdefender

Sicherheit

Bitdefender + Microsoft Office 365 E3 Plattformübergreifende Sicherheitslösung

www.bitdefender.de

Contents

Das Problem im Überblick

Zahlreiche kleinere und mittelgroße Unternehmen kennen dieses Problem[1]. Sie haben Office 365 abonniert, sind in hohem Maße den Gefahren ausgesetzt, die sich durch die Nutzung von E-Mail, Internet und Cloud-Diensten ergeben können, und müssen als Ergänzung zu den Angeboten von Microsoft eine geeignete Cybersicherheitslösung finden, mit der die Sicherheit und Produktivität von Tausenden von Benutzern gewährleistet ist.

Die Umgebung umfasst einen Mix aus Windows-, Mac- und Linux-Endpunkten und -Servern sowie eine Cloud- und Virtualisierungsinfrastruktur, wobei der Schwerpunkt in den kommenden Jahren wahrscheinlich noch stärker auf den Komponenten virtueller Rechenzentren liegen wird.

Typisches Kundenprofil

- Kleiner oder mittelgroßes Unternehmen mit mehr als 5.000 Benutzern oder Endpunkten
- Handelsunternehmen, Universitäten, primäre oder sekundäre Bildungseinrichtung, staatliche oder kommunale Verwaltung
- Abonnement für Microsoft Office 365 vorhanden
- Betreibt eine gemischte Umgebung aus PCs, Mac- und Linux-Computern
- Einige Cloud- und Virtualisierungsressourcen sind bereits vorhanden, sollen aber ausgebaut werden
- Verfügt über ein mittleres bis großes IT-Sicherheitsteam, aber kein Security Operations Center (SOC)

Es wurde zwar ein Sicherheitsteam mit geeigneter Personalstärke und ausreichendem Cyberwissen aufgebaut, aber ohne ein eigenes Security Operations Center (SOC) müssen diese Fachleute immer sofort zur Stelle sein und disziplinübergreifend agieren. Dabei dürfen sie keine Zeit mit Doppelarbeit oder dem nutzlosen Sammeln unterschiedlicher Informationen von mehreren Standorten vergeuden.

Schließlich wissen sie, dass sie – unabhängig davon, ob sie kürzlich mit einem Sicherheitsvorfall zu tun hatten oder nicht – Gefahr laufen, in der Flut der täglichen Alarme unterzugehen. Oder sie suchen einfach nach Sicherheitslösungen, die das Angebot von Microsoft ergänzen, denn sie wissen, dass sie mehr als nur Windows-PCs und die Komponenten von Microsoft Office zu schützen haben.

Problembeschreibung / Folgen

Die Herausforderung besteht darin, angesichts von Agentenüberlastung, Alarmmüdigkeit, Qualifikationsdefiziten und anhaltenden Problemen bei der Bindung des Personals für die Cybersicherheit den Überblick über die Alarme zu behalten und die Aktivitäten im Kampf gegen die Cyberkriminalität von einer zentralen Stelle aus zu verwalten. Als Dauerproblem erweist sich die sofortige Versorgung der Systeme – einschließlich Nicht-Microsoft-Komponenten – mit Sicherheits-Patches, sobald diese jeweils verfügbar sind, und die Anforderung, einen Überblick über die oft heterogenen Plattformen mit ihren Endpunkt-, Rechenzentrums- und Cloud-Komponenten zu behalten.

Wenn Sie mit der Bedrohungslandschaft nicht Schritt halten können, besteht die Gefahr, dass Warnmeldungen ungeprüft bleiben oder dass keine Reaktion darauf erfolgt, dass Systeme unnötig lange gefährdet bleiben, und dass das Benutzerverhalten unbemerkt weitere Risiken schafft.

„Jede Änderung ist unbestreitbar eine Bedrohung für die Cybersicherheit, ebenso wie der Umstand, nicht darauf vorbereitet zu sein. Es steht viel auf dem Spiel: die Kundenbindung und das Vertrauen – ganz zu schweigen vom Geschäftsergebnis.“
Liviu Arsene, Global Cybersecurity Researcher bei Bitdefender

1 Per Gartner, SMB organizations have less than $50 million in annual revenue; Midsize enterprises < $1 billion.

Bestehende Alternativen

Microsoft präsentiert ein Sicherheitspaket mit dem Namen Enterprise 5 (E5), das die komplette ATP-Funktionalität (Advanced Threat Protection) des Unternehmens beinhaltet. Es handelt sich dabei um ein vollwertiges Lösungspaket, das sich zwar gut für ein SOC-Teams eignet, aber für viele kleinere und mittelgroße Unternehmen, die keinen Zugriff auf ein SOC haben, zu komplex ist. E5 erfordert eine zusätzliche Infrastruktur, erweiterte Fachkenntnisse und die Verfügbarkeit von Ressourcen für die Implementierung und Wartung. Mittlerweile gibt es von Microsoft das E3-Paket mit „abgespeckten" Sicherheitsfunktionen, die sich auf die Bekämpfung von Viren (AV) und den Schutz vor Datenverlust (DLP) beschränken.

Zentrale Fragen

Bei unseren Beratungen zu plattformübergreifenden Endpunkt-Sicherheitslösungen stellen wir den Security Managern und Verantwortlichen für die Geschäftsergebnisse mehrere Fragen, mit denen wir ihr gesamtes Umfeld untersuchen und die potenziellen Schwachstellen ermitteln:

- Benötigen Sie eine nahtlose, plattformübergreifende Sicherheitslösung für Windows-, MacOS- und Linux-Systeme?
- Sind Sie in der Lage, heterogene virtualisierte und Cloud-Umgebungen, einschließlich öffentlicher Clouds, abzusichern?
- Schränkt die Lizenzverwaltung für mehrere Tools die Produktivität Ihres Sicherheitsteams ein?
- Wie gut sind Ihre Sicherheitsfachleute auf die Handhabung einer komplexen Sicherheitslösung vorbereitet?
- Benötigen Sie Einsicht in riskantes Benutzerverhalten, Anwendungsschwachstellen oder die Fehlkonfiguration von Endpunkten?
- Haben Sie Bedenken, dass Ihre Sicherheitslösung negative Auswirkungen auf die Leistung Ihrer Systeme haben könnte?
- Verfügen Sie über ein Budget für zusätzliche Mitarbeiter und Hardware zur Unterstützung neuer Sicherheitslösungen?

Bitdefender + Microsoft Office 365 E3 Plattformübergreifende Sicherheitslösung

Die Lösungen **GravityZone Elite** und **GravityZone Ultra** von Bitdefender lassen sich mit **Microsoft Office 365 E3** kombinieren, um den Kunden umfassende Sicherheit sowohl für Office 365 als auch für nicht von Microsoft stammende Technologien unter Windows, MacOS und Linux zu bieten. Diese Lösung deckt von traditionellem Endpunktschutz bis hin zu Rechenzentrums-, Cloud- und Virtualisierungsplattformen alles ab. Im Vergleich zu Microsoft Office 365 E5 bieten Bitdefender + Microsoft E3 eine überlegene Lösung speziell für SMBs und mittelgroße Firmen, die keinen Zugriff auf ein SOC haben.

Warum: Die Lösung zeichnet sich durch überlegene Sicherheitseffizienz, vereinfachte Bereitstellung, unkomplizierte Verwaltung, geringere Betriebsbelastung und geringere Kosten aus

Wie: Lösung mit lediglich einem Agenten und einer Verwaltungskonsole, 100 % Cloud-basiert, vereinfachte Lizenzierung und MDR (Managed Detection and Response) über denselben Agenten

Was: Unkomplizierter Endpunktschutz mit EDR-, Windows-, Mac- und Linux-Abdeckung, skalierbare Multi-Cloud- und Virtualisierungsunterstützung, die auch AWS und Relaisstationen sowie virtuelle Sicherheits-Appliances umfasst.

Die wichtigsten Unterschiede zu Microsoft E5

- Integration in virtuellen Nicht-Microsoft-Umgebungen auf AWS-, VMware-, Citrix- oder Nutanix-Plattformen
- Minimale Anzahl von Lizenzen für die Technologie zur Vermeidung komplizierter Lizenz- und Abonnement-Modelle
- Unterstützung mehrerer Betriebssysteme wie z. B. ältere Windows-Versionen sowie mehrere Linux-Distributionen und MacOS-Geräte
- Patch Management zur automatischen Einspielung der neuesten Patches für Windows- und Drittanbieteranwendungen
- Komplexe mehrstufige Bedrohungsanalyse im Netzwerk mit Netzwerksensor, ICAP-Sensor für Speicherserver, Abwehr von Netzwerkangriffen am Endpunkt und/oder Analyse der Sicherheit des Netzwerkverkehrs

Die wichtigsten Vorteile für kleinere und mittelgroße Unternehmen

Virenschutz der nächsten Generation plus EDR: E3 NGAV plus Bitdefender EDR (Endpoint Detection and Response), Anwendungs- und Geräteüberwachung sowie Web-Überwachung und Host-basierte Firewall sorgen für eine optimale Allround-Prävention.

Integration von virtuellen und Cloud-Workloads: Bitdefender 2019, von Forrester Wave™ als Marktführer im Bereich Sicherheit von Cloud-Workloads ausgezeichnet, kann zusammen mit MSFT E3 in alle wichtigen virtualisierten und Cloud-Umgebungsplattformen integriert werden.

Automatische Untersuchung und Bereinigung: Sie können automatisierte Sicherheits-Workflows vereinfachen, relevante Sicherheitsereignisse schnell herausfiltern und umgehend darauf reagieren. Bitdefender bietet Ihnen zusätzliche Überwachungs- und Berichtsfunktionen für komplexe Bedrohungen.

Analyse des „Faktor-Mensch"- und Endpunkt-Risikos: Schwachstellen in der Sicherheit, die sich aus menschlichen Fehlern oder Systemfehlkonfigurationen ergeben, werden durch den Einsatz der Zero-Trust-Schutztechnologie schnell beseitigt.

Technische Vorteile und Unterscheidungsmerkmale

Testergebnisse im Vergleich

Die folgenden Zahlen und Diagramme zeigen die von Bitdefender und Microsoft in unabhängigen Tests von Drittanbietern erzielten Ergebnisse.

Die Testergebnisse zeigen, dass Bitdefender im Vergleich zu Microsoft bei möglichst geringen Leistungseinbußen einen erstklassigen Schutz bietet. Darüber hinaus sind unsere komplexen heuristischen Modelle, die mit maschinellem Lernen arbeiten, gut trainiert und erzeugen weniger Fehlalarme als die Microsoft-Lösung.

Schutz vor Malware-Infektionen (wie Viren, Würmer oder Trojaner)	Anzahl der Testergebnisse mit 100 % im Jahr 2020	
	Bitdefender	Microsoft
Schutz vor Zero-Day-Malware-Angriffen einschließlich Internet- und E-Mail-Bedrohungen (Tests unter Realbedingungen)	8/8	5/8
Erkennung weit verbreiteter und vorherrschender Malware, die innerhalb der letzten 4 Wochen entdeckt wurde (die AV-TEST-Referenzgruppe)	8/8	8/8

Abb. 1: Kumulierte Testergebnisse von AV-Test, Januar bis August 2020

Abb. 2 und 3 zeigen die Ergebnisse der Leistungstests von AV-Comparatives. Bei der Microsoft-Lösung sind die Auswirkungen auf die Systemressourcen deutlich größer. Bitdefender verfügt über einen schlanken Agenten mit einer einzigen Konsole, der schwerpunktmäßig erstklassigen Endpunktschutz bietet, ohne die Produktivität des Unternehmens zu beeinträchtigen.

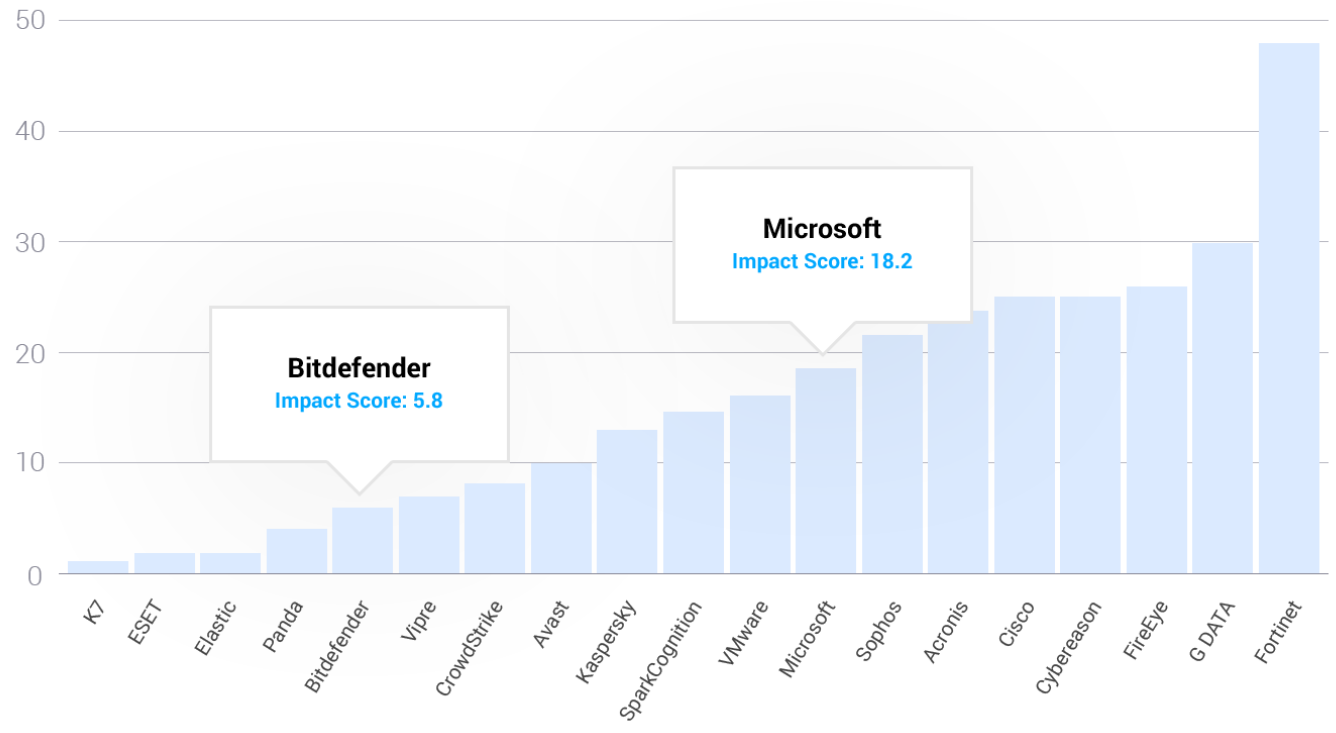

Abb. 2: AV-Comparatives – Bewertung der Auswirkungen auf die Leistung (Juni 2020)

Anbieter	Kopieren von Dateien		Archivieren/ Archivierung aufheben	Installation/ Deinstallation von Anwendungen	Starten von Anwendungen		Herunterladen von Dateien	Besuchen von Websites
	Erster Durchgang	Folgender Durchgang			Erster Durchgang	Folgender Durchgang		
Bitdefender	2/3	2/3	3/3	3/3	2/3	3/3	3/3	3/3
Microsoft	1/3	1/3	3/3	2/3	3/3	3/3	3/3	3/3

Abb. 3: AV-Comparatives – Leistungstests (Juni 2020)

Sicherheitstest unter realistischen Bedingungen	Business Security Test 2020		Business Security Test 2019		Business Security Test 2019		Business Security Test 2019			
	März-Juni		August-November		März-Juni		August-November		März-Juni	
Fehlalarme	Bitdefender 2	Microsoft 8	Bitdefender 25	Microsoft 54	Bitdefender 6	Microsoft 24	Bitdefender 1	Microsoft 83	Bitdefender 2	Microsoft 11

Abb. 4: AV-Comparatives – Fehlalarm-Test unter realen Bedingungen (2018-2020)

Neben der verbesserten Systemleistung zeichnet sich die Lösung von Bitdefender dadurch aus, dass sie im Vergleich zu Microsoft deutlich weniger Fehlalarme erzeugt. Die Effizienztests aus Abb. 4 zeigen, dass Microsoft zusammengenommen viermal so viele Fehlalarme auslöst wie Bitdefender. Dies bedeutet, dass die Fachleute aus der IT-Sicherheit viel Zeit damit verbringen müssen, irrelevante Ereignisse durchzugehen, bevor sie auf eine tatsächliche Bedrohung innerhalb der Organisation stoßen.

Architektur der Sicherheitsmanagement-Lösung

Microsoft bietet Lösungen an, die mithilfe von mehreren Konsolen verwaltet werden müssen. Obwohl Microsoft E5 über Lösungen mit vielen Sicherheitsfunktionen verfügt, ist die Kombination aus Microsoft E3 und Bitdefender hinsichtlich des Schutzes vor komplexen Bedrohungen leistungsfähiger als die Standalone-Lösung E5.

Die Sicherheitslösungen von Bitdefender werden über eine einzige, zentrale Stelle verwaltet, die Zugriff auf die allgemeine Sicherheitslage, globale Sicherheitsbedrohungen sowie die Steuerung aller Sicherheitsmodule zum Schutz virtueller oder physischer Desktops, Server und mobiler Geräte bietet.

Schutz von virtuellen und Cloud-Workloads

Das Erkennen und Verhindern von Sicherheitsverletzungen in virtuellen digitalen Arbeitsbereichen und hybriden Cloud-Umgebungen kann sich schwierig gestalten, wenn veraltete Antiviren- und Anti-Malware-Scanning-Tools eingesetzt werden. Microsoft E3 und Bitdefender ergänzen sich ideal, wenn es darum geht, leistungszentrierte Sicherheit und Schutz über hybride Clouds hinweg bereitzustellen. Microsoft E5 unterstützt keine Integration mit den externen Virtualisierungsplattformen, die nicht von Microsoft stammen.

Bitdefender bietet Integration mit VMware, Citrix, Nutanix, AWS, Microsoft Azure sowie Sicherheitsplattformen wie NSX-V oder NSX-T.

Netzwerk-Sicherheit

Die Lösungen von Microsoft verfügen über keine Funktion, mit der die Endpunktkommunikation zur Durchführung einer Sicherheitsprüfung abgefangen werden kann. Sie bieten keinen Schutz vor Bedrohungen, die Netzwerkschwächen ausnutzen.

Bitdefender stellt eine virtuelle Appliance für Netzwerksicherheit zur Verfügung, die die Kunden auf Netzwerkebene schützt. XDR führt eine verhaltensbasierte Analyse der Netzwerk-Metadaten durch, um die Angreifer daran zu hindern, den Perimeterschutz zu umgehen und Endpunkte anzugreifen. Darüber hinaus nutzt das Bitdefender-Modul Network Attack Defense auf Host-Ebene eine proaktive Technologie, die speziell zur Erkennung von Netzwerkangriffen dient, die versuchen, über spezifische Techniken, wie z. B. Brute-Force-Angriffe, Netzwerk-Exploits, Passwortdiebstahl, Drive-by-Download-Infektionsvektoren, Bots und Trojaner Zugriff auf Endpunkte zu erlangen.

E-Mail-Sicherheit

Microsoft bietet zwar erweiterte E-Mail-Sicherheitsfunktionen für Office 365 und lokale Exchange-Mailserver, aber keine Sicherheit für E-Mail-Clients, die auf Google Gmail oder Linux basieren.

Neben dem speziellen Schutz, den Bitdefender für Exchange-Server bereitstellt, umfasst GravityZone auch E-Mail-Sicherheit für Google Gmail- und Linux-E-Mail-Clients.

Patch-Management

Microsoft E5 bietet über die Software On-Prem System Center Configuration Manager ein Patch-Management für Anwendungen, bei denen es sich um reine Microsoft-Produkte handelt.

Bitdefender bietet ein integriertes Patch-Management-Modul, das die Prüfung und Verwaltung von Patches sowohl für Windows- als auch für Fremdanwendungen ermöglicht.

Sichtbarkeit der Risiken

Risiken ergeben sich typischerweise aus Fehlkonfigurationen der Endpunkte, unzureichenden Netzwerkperimeterschutz und menschlichen Fehlern. Die Microsoft E3-Lösung weist keine Funktionen zur Risikominimierung auf.

Durch die integrierte Risikoanalyse von Bitdefender erhalten Sie umfassende Transparenz auf Endpunkt-, Netzwerk- und Mitarbeiterebene. Die Mitarbeiter der IT-Sicherheit können Sicherheitslücken schnell schließen und verhindern, dass Cyberkriminelle Schwachpunkt ausnutzen.

Lizenzierung

Microsoft nutzt ein äußerst komplexes Lizenz- und Subskriptionsmodell, das Betriebssystem, Zugriff auf Clients, Lizenzen für Sicherheitslösungen und ein Service-Abonnement für Azure umfasst. Die Lizenz-Bundles sind volumen- und betriebssystemspezifisch konzipiert. Somit stehen mehrere Sicherheitsfunktionen bei bestimmten Lizenzen und/oder Windows-Editionen nicht zur Verfügung.

Bitdefender bietet ein einfacheres Lizenzmodell einschließlich Bundles, eine Lizenzierung à la Carte und Add-Ons für spezielle Funktionen. Bei Bitdefender sind die Sicherheitsfunktionen nicht auf bestimmte Betriebssystem-Editionen oder -Versionen beschränkt.

Auswahl einer passenden Kundenlösung

Mittelgroße Unternehmen suchen in der Regel nach einer zentral verwalteten Lösung, um mit der Flut der von mehreren Tools generierten Sicherheitsereignisse fertig zu werden. Sie legen Wert auf kostengünstige Lösungen mit geringen Beeinträchtigungen der IT-Leistung, die den Personalaufwand gering halten und Ereignisse so korrelieren, dass verdächtige Verhaltensmuster bereits vor einem Angriff erkannt werden.

Über die Erkennung hinaus wünschen sich diese Kunden eine Lösung, die genug Flexibilität bietet, um das maschinelle Lernen mit zusätzlichen Erkenntnissen anzureichern, die gegen komplexe Bedrohungen eingesetzt werden kann. Sie verstehen den Wert von Analysen, die Transparenz auf Endpunkt-, Netzwerk- und Mitarbeiterebene bieten, um das gesamte Risikoprofil des Unternehmens quantitativ zu erfassen.

Schließlich benötigen diese Kunden eine integrierte Lösung, mit der Risiken frühzeitig erkannt und Schwachstellen und Systemfehlkonfigurationen schnell behoben werden können. Durch die weit in die Tiefe gehenden integrierten Funktionen, gepaart mit modernsten Technologien für maschinelles Lernen, die die neuesten Erkenntnisse über Bedrohungen liefern, erfüllt Bitdefender GravityZone plus Microsoft E3 die Anforderungen von kleineren und mittelgroßen Unternehmen viel besser als Microsoft E5.

Der Endpunktsicherheitsanbieter mit den meisten Auszeichnungen

Bitdefender belegt in unabhängigen Tests und Bewertungen durch Dritte stets Spitzenplätze:

- Platz 1 und Editors' Choice von PC Mag in der Kategorie „Best Hosted Endpoint Protection and Security Software for 2020"
- Platz 1 und Editors' Choice von PC Mag in der Kategorie „Best Mac Antivirus Protection for 2020"
- Sieger im Wave-Report von Forrester im Bereich Cloud-Workload Security im 4. Quartal 2019
- „Der wichtigste EDR-Anbieter, den Sie nicht in Betracht gezogen haben, dies aber hätten tun sollen" – Forrester Research
- 100% Erkennung bei realistischen Bedrohungen, AV-Test (Januar bis August 2020)

Kostenloser Produkttest – Überzeugen Sie sich selbst

Bitdefender GravityZone Elite, Ultra und Ultra-Plus bieten als Ergänzung zu Microsoft E3 skalierbare Sicherheit.

- Nutzen Sie unser einzigartiges, zeitlich begrenztes Angebot, und testen Sie GravityZone 90 Tage lang in der Vollversion.
- Dienstleister können eine kostenlose Test-Vollversion der mandantenfähigen Lösung Cloud Security for MSP erhalten.

Weitere Informationen erhalten Sie bei uns!

Wenn Sie weitere Informationen benötigen, kontaktieren Sie uns, damit wir eine ausführliche Produktdemonstration vereinbaren können, bei denen wir Ihnen die Vorteile von Bitdefender GravityZone zeigen und Ihnen erläutern, wie Sie dieses Produkt zusammen mit Microsoft Office 365 E3 zur Absicherung Ihres Unternehmens einsetzen können.

Bitdefender ist der Technologieanbieter der Wahl: Weltweit verwenden 38 % der Dienstleister im Bereich Cybersicherheit eine oder mehrere Bitdefender-Technologien und bestätigen damit unsere Produktqualität und die hohe Erkennungsgenauigkeit. Wir legen Wert darauf, Technologien im eigenen Haus zu entwickeln und über 50 % unserer Belegschaft in Forschung und Entwicklung zu beschäftigen.

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

TECHNOLOGIEPARTNERSCHAFT

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-SolutionBrief-BUS365-WEB.USE_ONLY-creat4945-de_DE
11/19/20November 10, 2020 9:29 pm11/19/20