

Bitdefender[®] **ANTIVIRUS FOR MAC**



BENUTZERHANDBUCH





Bitdefender Antivirus for Mac **Benutzerhandbuch**

Veröffentlicht 2020.07.19

Copyright© 2020 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und die dazugehörige Dokumentation sind urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „ohne Mängelgewähr“ gegeben. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokument entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von Bitdefender erstellte oder von Bitdefender kontrollierte Webseiten und somit übernimmt Bitdefender auch keine Verantwortung für die Inhalte dieser Webseiten. Der Besuch der in diesem Dokument aufgelisteten Drittanbieter-Webseiten erfolgt damit auf eigene Gefahr. Bitdefender stellt diese Links der Einfachheit zur Verfügung. Dies bedeutet nicht, dass Bitdefender den Inhalt einer Website Dritter befürwortet oder Verantwortung dafür übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.



Inhaltsverzeichnis

Zur Verwendung dieses Handbuchs	v
1. Zielsetzung und Zielgruppe	v
2. Über dieses Handbuch	v
3. In diesem Handbuch verwendete Konventionen	v
3.1. Typografie	v
3.2. Hinweise	vi
4. Ihre Mithilfe	vii
1. Installation und Deinstallation	1
1.1. Systemanforderungen	1
1.2. Installation von Bitdefender Antivirus for Mac	1
1.2.1. Installationsvorgang	2
1.3. Bitdefender Antivirus for Mac entfernen	6
2. Erste Schritte	7
2.1. Über Bitdefender Antivirus for Mac	7
2.2. Öffnen Sie Bitdefender Antivirus for Mac	7
2.3. Das Hauptfenster	8
2.4. Dock-Symbol der App	9
2.5. Navigationsmenü	10
2.6. Dark Mode	10
3. Schutz gegen böartige Software	12
3.1. Empfohlene Vorgehensweisen	12
3.2. Ihren Mac scannen	13
3.3. Scan-Assistent	14
3.4. Quarantäne	15
3.5. Bitdefender-Schild (Echtzeitschutz)	16
3.6. Scan-Ausnahmen	16
3.7. Internet-Schutz	17
3.8. Anti-Tracker	19
3.8.1. Anti-Tracker-Benutzeroberfläche	20
3.8.2. Deaktivieren von Bitdefender Anti-Tracker	21
3.8.3. Erlauben von Tracking auf einer Website	21
3.9. Sichere Dateien	21
3.9.1. Anwendungszugriff	23
3.10. Time-Machine-Schutz	23
3.11. Alle beheben	24
3.12. Benachrichtigungen	25
3.13. Aktualisierung	26
3.13.1. Benutzergesteuertes Update	27
3.13.2. Updates über einen Proxy Server	27
3.13.3. Upgrade auf eine neue Version durchführen	27
3.13.4. Informationen zu Bitdefender Antivirus for Mac finden	28
4. VPN	29
4.1. Über VPN	29
4.2. Öffnen des VPN	29



4.3. Netzwerkkarte	30
4.4. Abonnements	32
5. Einstellungen konfigurieren	33
5.1. Zugriff auf Einstellungen	33
5.2. Schutzeinstellungen	33
5.3. Erweiterte Einstellungen	34
5.4. Sonderangebote	34
6. Bitdefender Central	35
6.1. Über Bitdefender Central	35
6.2. So können Sie Bitdefender Central aufrufen:	36
6.3. Zwei-Faktor-Authentifizierung	36
6.4. Hinzufügen vertrauenswürdiger Geräte	38
6.5. Aktivität	38
6.6. Meine Abonnements	39
6.6.1. Abonnement aktivieren	39
6.7. Meine Geräte	40
6.7.1. Persönliche Anpassungen	40
6.7.2. Fernzugriffsaktionen	41
7. Häufig gestellte Fragen	42
8. Hilfe erhalten	47
8.1. Support	47
8.1.1. Online-Ressourcen	47
8.1.2. Hilfe anfordern	49
8.2. Kontaktinformation	49
8.2.1. Internet-Adressen	49
8.2.2. Händler vor Ort	50
8.2.3. Bitdefender-Niederlassungen	50
Arten von böartige Software	52



Zur Verwendung dieses Handbuchs

1. Zielsetzung und Zielgruppe

Dieses Benutzerhandbuch ist für alle Macintosh-Benutzer vorgesehen, die sich für **Bitdefender Antivirus for Mac** als Sicherheitslösung für Ihre Computer entschieden haben. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen, die gewohnt sind unter Macintosh zu arbeiten.

Es wird erklärt, wie Sie Bitdefender Antivirus for Mac konfigurieren und einsetzen, um sich vor Bedrohungen und Schad-Software zu schützen, Sie erfahren, wie Sie alles aus Bitdefender herausholen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

2. Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

Erste Schritte (S. 7)

Beginnen Sie mit Bitdefender Antivirus for Mac und der Benutzeroberfläche.

Schutz gegen bösartige Software (S. 12)

Lernen Sie wie Sie Bitdefender Antivirus for Mac anwenden, um sich vor gefährlicher Software zu schützen.

Einstellungen konfigurieren (S. 33)

Lernen Sie mehr über die Bitdefender Antivirus for Mac Voreinstellungen.

Hilfe erhalten (S. 47)

Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

3. In diesem Handbuch verwendete Konventionen

3.1. Typografie

Um die Lesbarkeit zu fördern werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der nachfolgenden Tabelle.



Erscheinungsbild	Beschreibung
Syntaxbeispiele	Syntaxbeispiele werden in einer Schriftart mit fester Laufweite angegeben.
https://www.bitdefender.de	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
Zur Verwendung dieses Handbuchs (S. v)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Dateiname	Dateien und Verzeichnisse werden in einer Schriftart mit fester Laufweite angegeben.
Option	Alle Produktoptionen werden fett gedruckt dargestellt.
Stichwort	Wichtige Stichwörter oder Begriffe werden durch Fettdruck hervorgehoben.

3.2. Hinweise

Hierbei handelt es sich um Hinweise innerhalb des Textflusses, welche mit einer kleinen Grafik markiert sind. Es handelt sich um Informationen, die Sie in jedem Fall beachten sollten.



Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten in der Regel nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.



Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden wichtige Informationen zum jeweiligen Thema gegeben, die nicht übersprungen werden sollten.



Warnung

Diese kritische Information erfordert größtmögliche Aufmerksamkeit. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst kritische Thematik handelt.



4. Ihre Mithilfe

Wir laden Sie ein mit zu helfen unser Buch zu verbessern. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen. Bitte schreiben Sie uns bezüglich Fehler, die in diesem Buch finden oder auch bezüglich Dinge, die Ihrer Meinung nach verbessert werden könnten. Dies hilft uns Ihnen die beste mögliche Dokumentation zur Verfügung zu stellen.

Schicken Sie uns Ihre E-Mail an documentation@bitdefender.com. Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.



1. INSTALLATION UND DEINSTALLATION

Dieses Kapitel beinhaltet die folgenden Themen:

- *Systemanforderungen (S. 1)*
- *Installation von Bitdefender Antivirus for Mac (S. 1)*
- *Bitdefender Antivirus for Mac entfernen (S. 6)*

1.1. Systemanforderungen

Sie können Bitdefender Antivirus for Mac auf Macintosh-Computern mit OS X Yosemite (10.10) oder höher installieren.

Sie benötigen auf Ihrem Mac zudem mindestens 1 GB verfügbaren Speicherplatz auf der Festplatte.

Für die Registrierung und Updates von Bitdefender Antivirus for Mac ist eine aktive Internetverbindung notwendig.



Beachten Sie

Bitdefender Anti-Tracker und Bitdefender VPN können nur auf Systemen mit macOS 10.12 oder höher installiert werden.



So finden Sie heraus, welche macOS-Version und Hardware Sie nutzen

Klicken Sie in der linken oberen Bildschirmcke auf das Apple-Symbol und wählen Sie **Über diesen Mac**. Im sich öffnenden Fenster werden Ihre Betriebssystem-Version und andere nützliche Informationen eingeblendet. Klicken Sie auf **Systembericht**, um detaillierte Informationen zur Hardware zu erhalten.

1.2. Installation von Bitdefender Antivirus for Mac

Die Bitdefender Antivirus for Mac-App kann wie folgt über Ihr Bitdefender-Benutzerkonto installiert werden:

1. Als Administrator anmelden.
2. Gehen Sie zu: <https://central.bitdefender.com>.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.



4. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **SCHUTZ INSTALLIEREN**.
5. Wählen Sie eine der beiden verfügbaren Optionen:
 - **Dieses Gerät schützen**
 - a. Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
 - b. Speichern Sie die Installationsdatei.
 - **Andere Geräte schützen**
 - a. Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
 - b. Klicken Sie auf **DOWNLOAD-LINK SENDEN**.
 - c. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL VERSENDEN**.

Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.
 - d. Rufen Sie auf dem Gerät, auf dem Bitdefender installiert werden soll, das angegebene E-Mail-Konto auf und klicken Sie in der E-Mail auf die Download-Schaltfläche.
6. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.
7. Führen Sie die Installationsschritte durch.

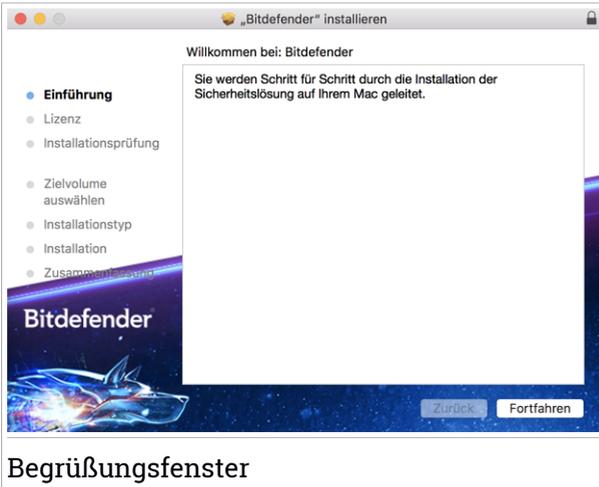
1.2.1. Installationsvorgang

Anleitung zur Installation von Bitdefender Antivirus for Mac:

1. Klicken Sie auf die heruntergeladene Datei. Der Installationsassistent wird geöffnet und führt Sie durch den Installationsvorgang.
2. Folgen Sie den Anweisungen des Installationsassistenten.



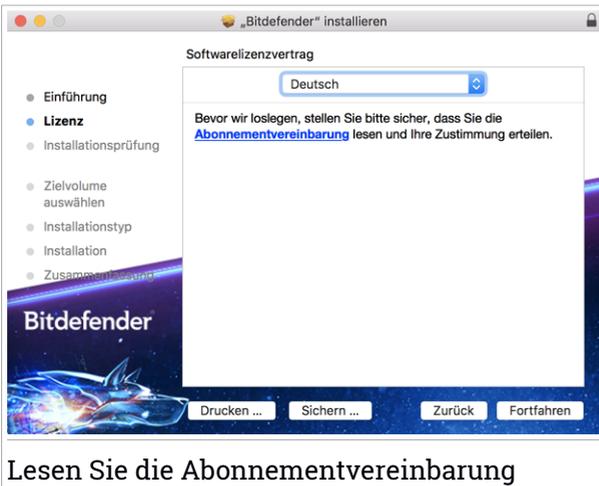
Schritt 1 - Willkommensfenster



Begrüßungsfenster

Klicken Sie auf **Fortfahren**.

Schritt 2 - Lesen Sie die Abonnementvereinbarung



Lesen Sie die Abonnementvereinbarung

Bevor Sie mit der Installation fortfahren, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment



Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Antivirus for Mac nutzen dürfen.

In diesem Fenster können Sie auch die Sprache auswählen, in der Sie das Produkt installieren möchten.

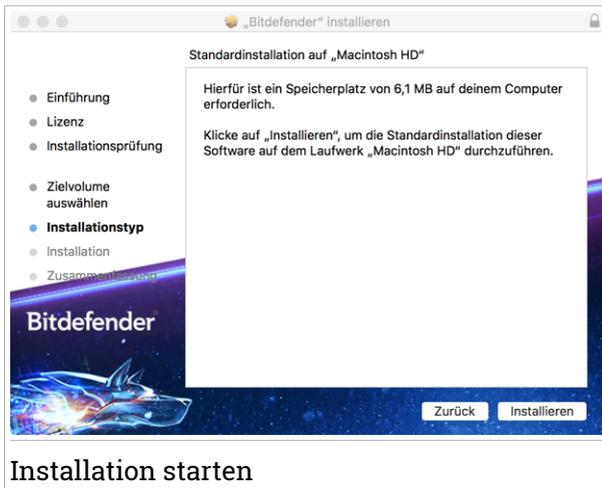
Klicken Sie auf **Weiter** und danach auf **Zustimmen**.



Wichtig

Falls Sie die Nutzungsbedingungen nicht akzeptieren möchten, klicken Sie auf **Weiter** und dann auf **Nicht zustimmen**. Der Installationsvorgang wird dann abgebrochen und der Installationsassistent geschlossen.

Schritt 3 - Installation starten



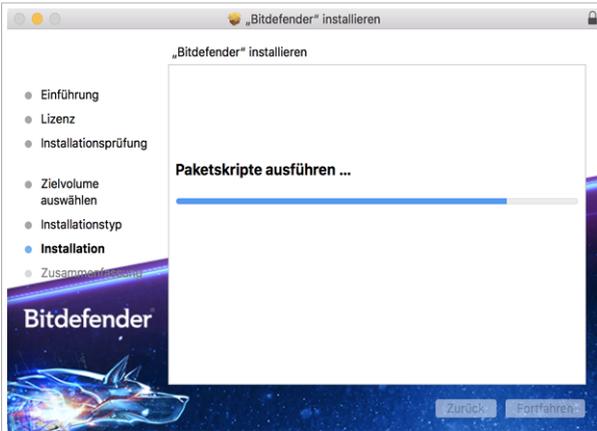
Installation starten

Bitdefender Antivirus for Mac wird installiert in Macintosh HD/Library/Bitdefender. Der Installationspfad kann nicht geändert werden.

Klicken Sie auf **Installieren**, um die Installation zu starten.



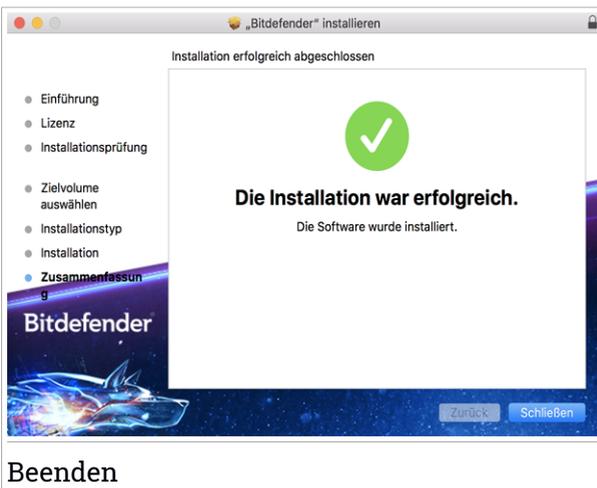
Schritt 4 - Bitdefender Antivirus for Mac installieren



Installation von Bitdefender Antivirus for Mac

Warten Sie, bis die Installation abgeschlossen ist und klicken Sie auf **Weiter**.

Schritt 5 - Fertigstellung



Beenden

Klicken Sie auf **Schließen**, um das Installationsfenster zu schließen. Damit ist der Installationsvorgang abgeschlossen.



Wichtig

- Wenn Sie Bitdefender Antivirus for Mac unter macOS High Sierra 10.13.0 oder einer neueren Version installieren, wird die Meldung **System-Erweiterung blockiert** angezeigt. Sie weist Sie darauf hin, dass die von Bitdefender signierten Erweiterungen blockiert wurden und manuell aktiviert werden müssen. Klicken Sie auf **Weiter**. Klicken Sie im daraufhin angezeigten Bitdefender Antivirus for Mac-Fenster auf den Link **Sicherheit & Privatsphäre**. Klicken Sie unten im Fenster auf **Erlauben** oder wählen Sie Bitdefender SRL aus der Liste aus und klicken Sie auf **OK**.
- Falls Sie Bitdefender Antivirus for Mac unter MacOS Mojave 10.14 oder einer neueren Version installieren, wird ein neues Fenster angezeigt, in dem Sie darauf hingewiesen werden, dass Sie die Berechtigungen **Bitdefender Vollzugriff auf die Festplatte erlauben** sowie **Erlauben, dass Bitdefender geladen wird** erteilen müssen. Befolgen Sie die Anleitung auf dem Bildschirm, um das Produkt ordnungsgemäß zu konfigurieren.

1.3. Bitdefender Antivirus for Mac entfernen

Bitdefender Antivirus for Mac ist eine komplexe Anwendung und kann nicht auf herkömmliche Weise deinstalliert werden, indem das Symbol für die Anwendung aus dem Verzeichnis Anwendungen in den Papierkorb gezogen wird.

Um Bitdefender Antivirus for Mac zu entfernen, gehen Sie folgendermaßen vor:

1. Öffnen Sie **Finder** und wählen Sie den Programme-Ordner.
2. Öffnen Sie den Bitdefender-Ordner und doppelklicken Sie nach auf Bitdefender-Deinstallationsprogramm.
3. Klicken Sie auf **Deinstallieren**, und warten Sie, bis der Vorgang abgeschlossen ist.
4. Klicken Sie zum Abschluss auf **Schließen**.



Wichtig

Ist ein Fehler aufgetreten, so können Sie die Kundenbetreuung von Bitdefender wie in [Support \(S. 47\)](#) beschrieben, kontaktieren.



2. ERSTE SCHRITTE

Dieses Kapitel beinhaltet die folgenden Themen:

- *Über Bitdefender Antivirus for Mac (S. 7)*
- *Öffnen Sie Bitdefender Antivirus for Mac (S. 7)*
- *Das Hauptfenster (S. 8)*
- *Dock-Symbol der App (S. 9)*
- *Navigationsmenü (S. 10)*
- *Dark Mode (S. 10)*

2.1. Über Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac ist ein leistungsstarker Virenschanner, der alle Arten von Schad-Software („Bedrohungen“) erkennen und entfernen kann:

- Ransomware
- Adware
- Viren
- Spyware
- Trojaner
- Keylogger
- Computerwürmer

Diese App erkennt und entfernt nicht nur Mac-spezifische, sondern auch Windows-spezifische Bedrohungen und verhindert so, dass Sie infizierte Dateien versehentlich an die PCs Ihrer Familie, Freunde und Kollegen weiterleiten.

2.2. Öffnen Sie Bitdefender Antivirus for Mac

Sie haben mehrere Möglichkeiten Bitdefender Antivirus for Mac zu öffnen.

- Klicken Sie im Launchpad auf das "Bitdefender Antivirus for Mac"-Symbol.
- Klicken Sie in der Menüleiste auf das Symbol  und wählen Sie **Hauptfenster öffnen**.
- Öffnen Sie ein Finder-Fenster, wählen Sie Anwendungen aus und doppelklicken Sie auf das Bitdefender Antivirus for Mac-Symbol.



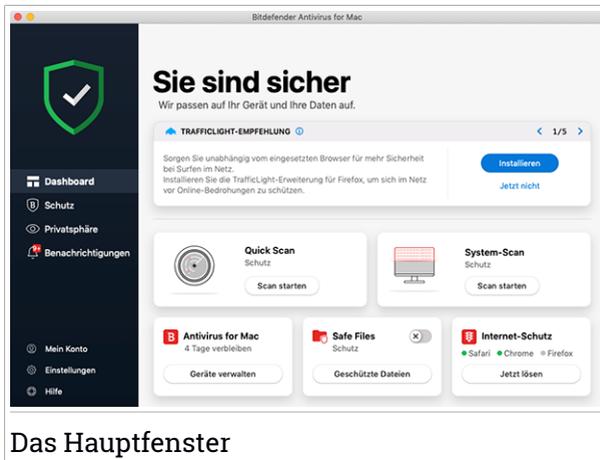
Wichtig

Wenn Sie Bitdefender Antivirus for Mac zum ersten Mal unter macOS Mojave 10.14 oder einer neueren Betriebssystemversion öffnen, wird eine Sicherheitsempfehlung angezeigt. Der Grund dafür ist, dass unsere Software bestimmte Berechtigungen benötigt, um Ihr System vollständig scannen zu können. Um diese Berechtigungen zu erteilen, müssen Sie als Administrator angemeldet sein. Gehen Sie dazu wie folgt vor:

1. Klicken Sie auf den Link **Systemeinstellungen**.
2. Klicken Sie auf das Symbol  und geben Sie dann Ihre Administratorzugangsdaten ein.
3. Ein neues Fenster wird geöffnet. Ziehen Sie die Datei **BDLDaemon** mit der Maus auf die Liste der zugelassenen Apps.

2.3. Das Hauptfenster

Bitdefender Antivirus for Mac entspricht den Bedürfnissen sowohl von Profis als auch von Beginners. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.



Das Hauptfenster

Oben links wird ein Assistent eingeblendet, der Sie durch die Elemente der Bitdefender-Oberfläche leitet und Ihnen bei der Konfiguration zur Seite steht. Klicken Sie auf die Spitze Klammer rechts, um dem Assistenten weiter zu folgen, oder **Einführung überspringen**, um den Assistenten zu schließen.



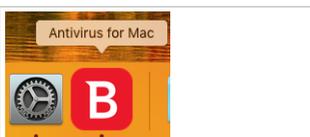
Die Statusleiste oben im Fenster informiert Sie mit eindeutigen Meldungen und Farbanzeigen über den Sicherheitsstatus des Systems. Liegen keine Warnungen in Bitdefender Antivirus for Mac vor, ist die Statusleiste grün. Wird ein Sicherheitsproblem gefunden, wechselt die Farbe der Statusleiste zu rot. Detaillierte Informationen zu Problemen und wie diese beseitigt werden können, finden Sie unter *Alle beheben* (S. 24).

Um einen wirksamen Betrieb und noch besseren Schutz bei Ihren verschiedenen Aktivitäten sicherzustellen, fungiert der **Bitdefender-Autopilot** als Ihr persönlicher Sicherheitsberater. Je nachdem, was Sie gerade machen - egal, ob Sie arbeiten oder gerade Online-Zahlungen durchführen - der Bitdefender-Autopilot liefert Ihnen kontextabhängige Empfehlungen, die sich an Ihrer Gerätenutzung und an Ihren Anforderungen orientieren. So lernen Sie alle Vorteile der Funktionen in Ihrer Bitdefender Antivirus for Mac-App kennen und können umfassend davon profitieren.

Über das Navigationsmenü auf der linken Seite können Sie auf die Bitdefender-Bereiche für die detaillierte Konfiguration und erweiterte Verwaltung (Reiter **Schutz** und **Privatsphäre**), Benachrichtigungen, Ihr **Bitdefender-Konto** und die **Einstellungen** zugreifen. Sie können uns zudem jederzeit kontaktieren (Reiter **Hilfe**), um Unterstützung zu erhalten, falls Sie Fragen haben oder etwas Unerwartetes auftritt.

2.4. Dock-Symbol der App

Das "Bitdefender Antivirus for Mac"-Symbol wird sofort nach Öffnen der Anwendung im Dock angezeigt. Über das Symbol im Dock können Sie Dateien und Ordner schnell und einfach auf Bedrohungen prüfen. Ziehen Sie die Datei oder den Ordner einfach per Drag und Drop auf das Symbol im Dock, um den Scan sofort zu starten.



Produktsymbol im Dock



2.5. Navigationsmenü

Auf der linken Seite der Bitdefender-Oberfläche finden Sie das Navigationsmenü mit Schnellzugriff auf alle Bitdefender-Funktionen, die Sie für den Umgang mit Ihrem Produkt benötigen. In diesem Bereich finden Sie die folgenden Reiter:

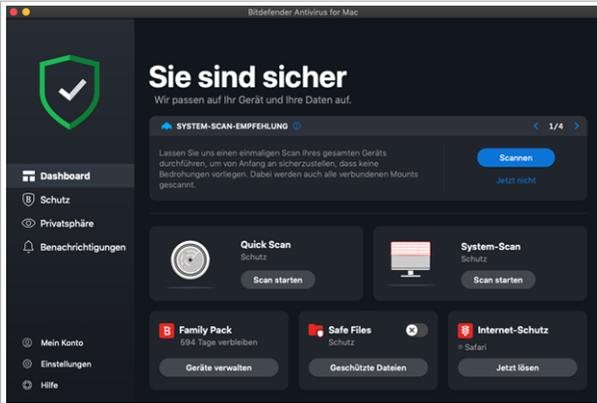
-  **Dashboard.** Von hier aus können Sie Sicherheitsprobleme schnell beheben, von Ihren Systemanforderungen und Nutzungsverhalten abgeleitete Empfehlungen anzeigen, Schnellaktionen ausführen und Ihr Bitdefender-Konto aufrufen, um die Geräte zu verwalten, die Sie Ihrem Bitdefender-Abonnement hinzugefügt haben.
-  **Schutz.** Von hier aus können Sie Virenschutz-Scans starten, Dateien zur Ausnahmeliste hinzufügen, Dateien und Anwendungen vor Ransomware-Angriffen schützen, Ihre Time Machine-Backups sichern und den Schutz beim Surfen im Internet konfigurieren.
-  **Benachrichtigungen.** Von hier aus können Sie die Bitdefender VPN-App öffnen und die Anti-Tracker-Erweiterung in Ihrem Browser installieren.
-  **Benachrichtigungen.** Von hier aus können Sie Details über die für gescannte Dateien ausgeführten Aktionen einsehen.
-  **Mein Konto.** Von hier aus können Sie Ihr Bitdefender-Benutzerkonto aufrufen, um Ihre Abonnements einzusehen und auf den von Ihnen verwalteten Geräten Sicherheitsaufgaben ausführen. Hier finden Sie auch Einzelheiten zu Ihrem Bitdefender-Benutzerkonto und dem aktuell verwendeten Abonnement.
-  **Einstellungen.** Von hier aus können Sie die Bitdefender-Einstellungen konfigurieren.
-  **Hilfe.** Wenn Sie Unterstützung beim Umgang mit Ihrem Bitdefender-Produkt benötigen, können Sie sich von hier aus an den technischen Support wenden. Von hier aus können Sie uns zudem Ihr Feedback schicken, um uns bei der Verbesserung des Produkts zu helfen.

2.6. Dark Mode

Um Ihre Augen bei Nachtarbeiten oder in einer lichtarmen Umgebung vor Blendung und Licht zu schützen, unterstützt Bitdefender Antivirus for Mac



den Dark Mode für Mojave 10.14 und höher. Die Farben der Benutzeroberfläche wurden so optimiert, dass Sie Ihren Mac verwenden können, ohne Ihre Augen anzustrengen. Die Bitdefender Antivirus for Mac-Benutzeroberfläche passt sich an die Darstellungseinstellungen Ihres Geräts an.



Dark Mode



3. SCHUTZ GEGEN BÖSARTIGE SOFTWARE

Dieses Kapitel beinhaltet die folgenden Themen:

- *Empfohlene Vorgehensweisen* (S. 12)
- *Ihren Mac scannen* (S. 13)
- *Scan-Assistent* (S. 14)
- *Quarantäne* (S. 15)
- *Bitdefender-Schild (Echtzeitschutz)* (S. 16)
- *Scan-Ausnahmen* (S. 16)
- *Internet-Schutz* (S. 17)
- *Anti-Tracker* (S. 19)
- *Sichere Dateien* (S. 21)
- *Time-Machine-Schutz* (S. 23)
- *Alle beheben* (S. 24)
- *Benachrichtigungen* (S. 25)
- *Aktualisierung* (S. 26)

3.1. Empfohlene Vorgehensweisen

Um Ihr System vor Bedrohungen zu schützen und eine versehentliche Infizierung anderer Systeme zu verhindern, sollten Sie folgende Empfehlungen beachten:

- Lassen Sie das **Bitdefender-Schild** aktiviert, damit Systemdateien automatisch von Bitdefender Antivirus for Mac gescannt werden können.
- Halten Sie Ihr Bitdefender Antivirus for Mac-Produkt mit den neusten Bedrohungsinformationen und Produktupdates immer aktuell.
- Überprüfen und beheben Sie die von Bitdefender Antivirus for Mac aufgelisteten Probleme regelmäßig. Detaillierte Informationen finden Sie im Kapitel *Alle beheben* (S. 24).
- Überprüfen Sie das detaillierte Ereignisprotokoll mit allen Bitdefender Antivirus for Mac-Aktivitäten auf Ihrem Computer. Alle Ereignisse, die sich auf Ihr System oder Ihre Daten auswirken, werden als neue Nachricht in



den Bereich Bitdefender-Benachrichtigungen aufgenommen. Weitere Details dazu finden Sie hier: *Benachrichtigungen (S. 25)*.

- Darüber hinaus sollten Sie folgende Empfehlungen berücksichtigen:
 - Sie sollten grundsätzlich alle Dateien scannen, die Sie von externen Speichern (z.B. USB-Sticks oder CDs) herunterladen, insbesondere wenn Ihnen die Quelle nicht bekannt ist.
 - Bei DMG-Dateien sollten diese zunächst gemountet und dann ihr Inhalt (die Dateien im gemounteten Volume/Image) gescannt werden.

Der einfachste Weg, eine Datei, Verzeichnis etc. zu scannen ist, diese per drag&drop in das Anwendungsfenster von Bitdefender Antivirus for Mac oder das Dock-Symbol zu ziehen.

Es sind keine weitere Konfigurationen oder Aktionen erforderlich. Sie können jedoch bei Bedarf Anpassungen an den Einstellungen vornehmen. Weitere Informationen finden Sie im Kapitel *Einstellungen konfigurieren (S. 33)*.

3.2. Ihren Mac scannen

Der **Bitdefender-Schild** überwacht alle installierten Anwendungen auf Aktionen, die auf Bedrohungen hindeuten, und verhindert, dass neue Bedrohungen auf Ihr System gelangen. Darüber hinaus können Sie Ihren Mac oder einzelne Dateien jederzeit nach Bedarf scannen.

Der einfachste Weg, eine Datei, Verzeichnis etc. zu scannen ist, diese per drag&drop in das Anwendungsfenster von Bitdefender Antivirus for Mac oder das Dock-Symbol zu ziehen. Der Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang.

Sie können einen Scan wie folgt starten:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Wechseln Sie zum Reiter **Virenschutz**.
3. Klicken Sie auf einen der drei Scan-Schaltflächen, um den gewünschten Scan zu starten.
 - **Quick Scan** - überprüft die sensibelsten Verzeichnisse Ihres Systems (beispielsweise die Verzeichnisse mit Dokumenten, Downloads, Mail-Downloads und temporären Dateien eines Benutzers) auf Bedrohungen.



- **System-Scan** - durchsucht das gesamte System eingehend nach möglichen Bedrohungen. Alle eingebundenen Dateisysteme werden ebenfalls gescannt.



Beachten Sie

Je nach Größe Ihrer Festplatte kann ein vollständiger System-Scan einige Zeit in Anspruch nehmen (bis zu einer Stunde und mehr). Um die Systemleistung nicht zu beeinträchtigen, sollte diese Aufgabe nicht zeitgleich mit anderen ressourcenintensiven (z.B. Videobearbeitung) Aufgaben ausgeführt werden.

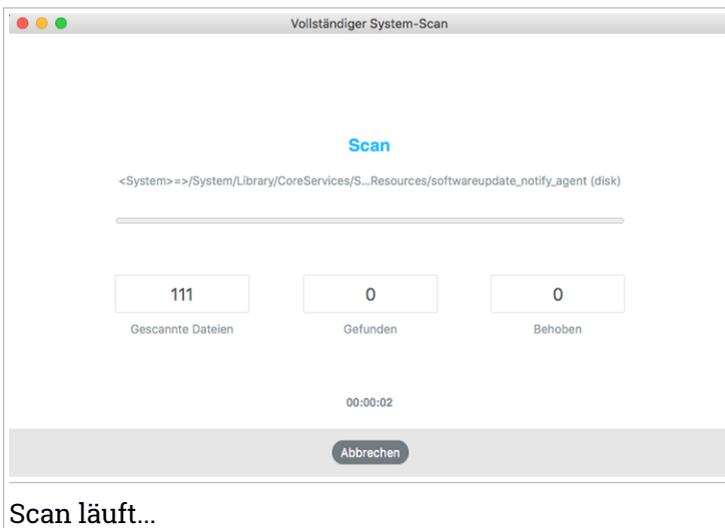
Falls gewünscht, können Sie bestimmte Laufwerke vom Scan ausschließen, indem Sie sie in im Fenster Schutz zur Liste der **Ausnahmen** hinzufügen.

- **Benutzerdefinierter Scan** - hiermit können einzelne Dateien, Verzeichnisse etc. auf Bedrohungen geprüft werden.

Sie können über das Dashboard auch einen System-Scan oder einen Quick Scan starten.

3.3. Scan-Assistent

Sobald Sie einen Scan starten, öffnet sich der Bitdefender Antivirus for Mac-Assistent.





Während eines Scans werden Informationen zu gefundenen und behobenen Bedrohungen in Echtzeit angezeigt.

Bitte warten Sie, bis Bitdefender Antivirus for Mac den Scan beendet hat.

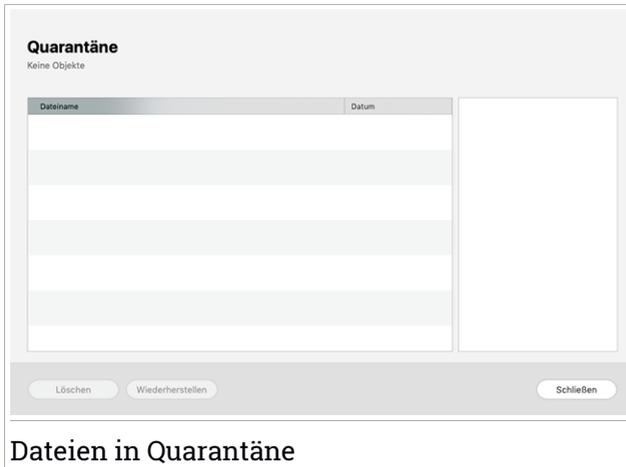


Beachten Sie

Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

3.4. Quarantäne

Mit Bitdefender Antivirus for Mac können infizierte oder verdächtige Dateien in einem sicheren Bereich, der Quarantäne, isoliert werden. Bedrohungen in Quarantäne können keinen Schaden anrichten, da sie dort nicht geöffnet oder ausgeführt werden können.



Der Bereich Quarantäne zeigt alle Dateien an, die sich zur Zeit im Quarantäne-Ordner befinden.

Um eine Datei aus der Quarantäne zu löschen, markieren Sie diese und klicken Sie dann auf **Löschen**. Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

So können Sie eine Liste mit allen zur Quarantäne hinzugefügten Objekten anzeigen:



1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Das Fenster **Virenschutz** wird geöffnet.
Klicken Sie im Bereich **Quarantäne** auf **Öffnen**.

3.5. Bitdefender-Schild (Echtzeitschutz)

Bitdefender bietet Ihnen Echtzeitschutz vor einer Vielzahl an Bedrohungen, indem es alle installierten Apps und ihre jeweiligen Updates sowie alle neuen und veränderten Dateien scannt.

So können Sie den Echtzeitschutz deaktivieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Deaktivieren Sie **Bitdefender-Schild** im Fenster **Schutz**.



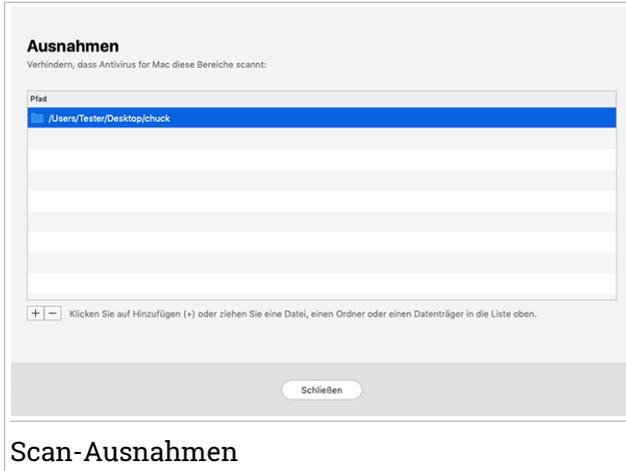
Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen den Echtzeitschutz so kurz wie möglich zu deaktivieren. Während der Echtzeitschutz deaktiviert ist, sind Sie nicht vor Bedrohungen geschützt.

3.6. Scan-Ausnahmen

Wenn Sie möchten, können Sie Bitdefender Antivirus for Mac so einstellen, dass spezielle Dateien, Ordner oder auch komplette Laufwerke, nicht gescannt werden. Zum Beispiel könnten Sie vom Scannen ausschließen:

- Dateien die fälschlicherweise als infiziert identifiziert wurden (bekannt als "false positives")
- Dateien die Scanfehler verursachen
- Backup-Laufwerke



Scan-Ausnahmen

In der Ausnahmeliste sind alle Pfade aufgeführt, die vom Scan ausgenommen wurden.

So können Sie die Ausnahmeliste aufrufen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Das Fenster **Virenschutz** wird geöffnet.
Klicken Sie im Bereich **Ausnahmen** auf **Öffnen**.

Es gibt zwei Wege um eine Scan-Ausnahme einzurichten:

- Ziehen Sie die gewünschte Datei, den Ordner oder das Laufwerk per Drag&Drop in die Ausnahmeliste.
- Klicken Sie auf das Pluszeichen (+) unterhalb der Ausnahmeliste. Wählen Sie danach die Datei, den Ordner oder das Laufwerk, das vom Scan ausgeschlossen werden soll.

Um eine Scan-Ausnahme zu entfernen, wählen Sie den entsprechenden Eintrag aus der Liste aus und klicken Sie auf das Minuszeichen (-) unterhalb der Ausnahmeliste.

3.7. Internet-Schutz

Bitdefender Antivirus for Mac verwendet die TrafficLight-Erweiterungen, um Ihnen ein sicheres Surfen im Web zu ermöglichen. Die



TrafficLight-Erweiterungen lesen, verarbeiten und filtern den gesamten Datenverkehr und blockieren dabei alle schädlichen Inhalte.

Die Erweiterungen lassen sich in die folgenden Browser integrieren: Mozilla Firefox, Google Chrome and Safari.

Aktivierung von Linkchecker-Erweiterungen

So können Sie die TrafficLight-Erweiterungen aktivieren:

1. Klicken Sie in der **Internet-Schutz**-Kachel im Dashboard auf **Jetzt lösen**.
2. Das Fenster **Internet-Schutz** wird geöffnet.

Der auf Ihrem System installierte Browser wird erkannt und angezeigt. Um die Linkchecker-Erweiterung zu installieren, klicken Sie auf **Erweiterung herunterladen**.

3. Sie werden umgeleitet auf:

<https://www.bitdefender.com/solutions/trafficlight.html>

4. Wählen Sie hier **Kostenloser Download**.
5. Folgen Sie den Anweisungen, um die Linkchecker-Erweiterung für Ihren Browser zu installieren.

Verwalten von Erweiterungseinstellungen

Ihnen steht eine große Auswahl an Funktionen zur Verfügung, die Sie vor allen möglichen Bedrohungen im Internet schützen. Sie können sie aufrufen, indem Sie auf das TrafficLight-Symbol neben Ihren Browser-Einstellungen und danach auf  **Einstellungen**-Schaltfläche klicken:

● Bitdefender-TrafficLight-Einstellungen

- Internet-Schutz - Verhindert, dass Sie Websites aufrufen, die zur Verbreitung von Malware sowie von Phishing- und Betrugsversuchen eingesetzt werden.
- Suchberater - Warnt Sie schon in Ihren Suchergebnissen vor gefährlichen Websites.

● Ausnahmen

Wenn Sie die Website, die Sie zu den Ausnahmen hinzufügen möchten, bereits aufgerufen haben, klicken Sie auf **Aktuelle Website zur Liste hinzufügen**.



Wenn Sie eine weitere Website hinzufügen möchten, geben Sie deren Adresse in das entsprechende Feld ein und klicken Sie auf .

Es wird keine Warnmeldung mehr angezeigt, auch wenn von den ausgenommenen Seiten eine Bedrohung ausgeht. Sie sollten dieser Liste nur Website hinzufügen, denen Sie uneingeschränkt vertrauen.

Seitenbewertung und Warnungen

Abhängig von der Linkchecker-Einstufung für die Webseite, die sie gerade besuchen, wird eines der folgenden Symbole in diesem Bereich eingeblendet:

-  Diese Seite ist sicher. Sie können mit Ihrer Arbeit fortfahren.
-  Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.
-  Sie sollten die Webseite umgehend verlassen, da diese Malware oder andere Bedrohungen enthält.

In Safari sind die TrafficLight-Symbole schwarz hinterlegt.

3.8. Anti-Tracker

Viele der von Ihnen aufgerufenen Websites verwenden Tracker, um Informationen über Ihr Surf-Verhalten zu sammeln, entweder um sie mit anderen Unternehmen zu teilen oder um Werbeanzeigen einzublenden, die für Sie relevanter sind. Website-Betreiber verwenden die hierdurch erzielten Einnahmen, um Ihnen kostenlose Inhalte anzubieten oder den eigenen Betrieb aufrechtzuerhalten. Das Sammeln dieser Informationen kann sich auch auf Ihre Surf-Geschwindigkeit auswirken und übermäßig Bandbreite in Anspruch nehmen.

Durch Aktivierung der Bitdefender Anti-Tracker-Erweiterung verhindern Sie dieses Tracking, so dass Ihre Daten während des Surfens im Netz privat bleiben. Darüber hinaus können Websites schneller geladen werden.

Die Bitdefender-Erweiterung ist mit den folgenden Web-Browsern kompatibel:

-  Google Chrome
-  Mozilla Firefox
-  Safari

Die von uns erkannten Tracker sind in die folgenden Kategorien unterteilt:



- **Werbung** - Dient der Analyse von Website-Verkehr, von Nutzerverhalten oder von Datenverkehrsmustern von Website-Besuchern.
- **Kundeninteraktion** - Dient der Messung der Benutzerinteraktion mit verschiedenen Eingabemöglichkeiten wie Chat oder Support.
- **Wesentlich** - Dient der Überwachung kritischer Webseiten-Funktionen.
- **Site Analytics** - Dient der Sammlung von Daten über die Nutzung von Webseiten.
- **Social Media** - Dient der Überwachung von Social-Media-Zielgruppen sowie der Aktivitäten und Nutzerbindung über verschiedene Social-Media-Plattformen.

Aktivieren von Bitdefender Anti-Tracker

So können Sie die Erweiterung Bitdefender Anti-Tracker in Ihrem Browser aktivieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Privatsphäre**.
2. Wechseln Sie zum Reiter **Anti-tracker**.
3. Klicken Sie neben dem Browser, für den Sie die Erweiterung aktivieren möchten, auf **Erweiterung aktivieren**.

3.8.1. Anti-Tracker-Benutzeroberfläche

Nach Aktivierung der Bitdefender Anti-Tracker-Erweiterung erscheint das -Symbol neben der Suchleiste in Ihrem Web-Browser. Jedes Mal, wenn Sie eine Website besuchen, ist auf dem Symbol ein Zähler zu sehen, der die Anzahl der erkannten und blockierten Tracker angibt. Um weitere Details zu den blockierten Trackern anzuzeigen, klicken Sie auf das Symbol, um die Benutzeroberfläche zu öffnen. Neben der Anzahl der blockierten Tracker können Sie die Ladezeit der Seite und die Kategorien, zu denen die erkannten Tracker gehören, einsehen. Um eine Liste der Websites anzuzeigen, auf denen Tracker zum Einsatz kommen, klicken Sie auf die gewünschte Kategorie.

Um Bitdefender davon abzuhalten, Tracker auf der aktuell von Ihnen besuchten Website zu blockieren, klicken Sie auf **Schutz für diese Website anhalten**. Diese Einstellung gilt nur, solange die Website geöffnet ist und wird beim Schließen der Website in den Ausgangszustand zurückgesetzt.



Um Trackern aus einer bestimmten Kategorie die Überwachung Ihrer Aktivität zu erlauben, klicken Sie auf die gewünschte Aktivität, und klicken Sie dann auf die entsprechende Schaltfläche. Klicken Sie erneut auf die gleiche Schaltfläche, falls Sie Ihre Meinung ändern.

3.8.2. Deaktivieren von Bitdefender Anti-Tracker

So können Sie die Erweiterung Bitdefender Anti-Tracker über Ihren Browser deaktivieren:

1. Öffnen Sie Ihren Internet-Browser.
2. Klicken Sie auf das -Symbol neben der Adressleiste in Ihrem Web-Browser.
3. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmcke.
4. Verwenden Sie zum Deaktivieren den entsprechenden Schalter.

Das Bitdefender-Symbol wird grau.

3.8.3. Erlauben von Tracking auf einer Website

Wenn Sie beim Besuch einer bestimmten Website das Tracking erlauben möchten, können Sie die entsprechende Adresse wie folgt zu den Ausnahmen hinzufügen:

1. Öffnen Sie Ihren Internet-Browser.
2. Klicken Sie neben der Suchleiste auf das -Symbol.
3. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmcke.
4. Wenn Sie die Website, die Sie zu den Ausnahmen hinzufügen möchten, bereits aufgerufen haben, klicken Sie auf **Aktuelle Website zur Liste hinzufügen**.

Wenn Sie eine weitere Website hinzufügen möchten, geben Sie deren Adresse in das entsprechende Feld ein und klicken Sie auf .

3.9. Sichere Dateien

Bei Ransomware handelt es sich um Schadsoftware, die anfällige Systeme infiziert und den Zugriff darauf sperrt. Von den Benutzern wird dann für die



Freigabe ihrer Daten ein Lösegeld erpresst. Diese Schadsoftware geht intelligent vor und zeigt Benutzern gefälschte Warnmeldungen an, um sie in Angst zu versetzen und sie dazu zu bringen, das geforderte Geld zu zahlen.

Durch den Einsatz neuester Technologien stellt Bitdefender die Integrität des System sicher. Kritische Systembereiche werden vor Ransomware-Angriffen geschützt, ohne dabei das System zu beeinträchtigen. Um zu verhindern, dass nicht vertrauenswürdige Anwendungen auf Ihre Dokumente, Fotos oder Videos zugreifen, bietet Ihnen Bitdefender Safe Files Ihnen die Möglichkeit, Ihre persönlichen Dateien zu beschützen und selbst festzulegen, welche Apps autorisiert sind, Änderungen an geschützten Dateien vorzunehmen.

So können Sie auch zu einem späteren Zeitpunkt weitere Dateien zur geschützten Umgebung hinzufügen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Wechseln Sie zum Reiter **Ransomware-Schutz**.
3. Klicken Sie im Bereich Sichere Dateien auf **Geschützte Dateien**.
4. Klicken Sie auf das Pluszeichen (+) unterhalb der Liste mit den geschützten Dateien. Wählen Sie danach die Datei, den Ordner oder das Laufwerk aus, das Sie vor dem Zugriff durch Ransomware schützen möchten.

Um Systembeeinträchtigungen zu vermeiden, sollten Sie nicht mehr als 30 Ordner hinzufügen oder mehrere Dateien in einem Ordner speichern.

Die Ordner Bilder, Dokumente, Desktop und Downloads werden standardmäßig vor Angriffen geschützt.



Beachten Sie

Benutzerdefinierte Ordner können nur für den aktuellen Benutzer geschützt werden. Externe Laufwerke sowie System- und Anwendungsdateien können der Schutzumgebung nicht hinzugefügt werden.

Sie werden informiert, sobald eine unbekannte Anwendung mit ungewöhnlichen Verhalten versucht, die von Ihnen hinzugefügten Dateien zu verändern. Klicken Sie auf **Zulassen** oder **Blockieren**, um sie zur Liste der **verwalteten Anwendungen** hinzuzufügen.



3.9.1. Anwendungszugriff

Anwendungen, die versuchen, geschützte Dateien zu verändern oder zu löschen, können als potenziell unsicher markiert und zur Liste der blockierten Anwendungen hinzugefügt werden. Falls eine solche Anwendung blockiert wurde und Sie sich sicher sind, dass ihr Verhalten normal ist, können Sie ihre Ausführung wie folgt zulassen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Wechseln Sie zum Reiter **Ransomware-Schutz**.
3. Klicken Sie im Bereich Sichere Dateien auf **Anwendungszugriff**.
4. Ändern Sie den Status neben der blockierten App auf Erlauben.

Ebenso können Sie den Status zugelassener Anwendungen auf blockiert setzen.

Nutzen Sie Drag&Drop oder klicken Sie auf das Pluszeichen (+), um weitere Apps zur Liste hinzuzufügen.

Anwendungszugriff

Hier werden alle Anwendungen angezeigt, die versucht haben, Ihre geschützten Dateien zu verändern.

Anwendung	Details	Aktion

Klicken Sie auf Hinzufügen (+), um neue Anwendungen zu verwalten.

Schließen

Sichere Dateien

3.10. Time-Machine-Schutz

Der Bitdefender-Time-Machine-Schutz bietet zusätzliche Sicherheit für Ihr Backup-Laufwerk und alle darauf gespeicherten Dateien, indem es den Zugriff durch externe Quellen verhindert. Werden Dateien in Ihrem



Time-Machine-Laufwerk von Ransomware verschlüsselt, können Sie sie auch ohne Lösegeldzahlung wiederherstellen.

Falls Sie Objekte aus einer Time-Machine-Sicherung wiederherstellen müssen, finden Sie die entsprechende Anleitung auf der Apple-Support-Seite.

Aktivierung und Deaktivierung des Time-Machine-Schutzes

So können Sie den Time-Machine-Schutz aktivieren oder deaktivieren:

1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Schutz**.
2. Wechseln Sie zum Reiter **Ransomware-Schutz**.
3. Aktivieren oder deaktivieren Sie den Schalter **Time-Machine-Schutz**.

3.11. Alle beheben

Bitdefender Antivirus for Mac spürt automatisch mögliche Probleme, die die Sicherheit Ihres Systems beeinflussen können, auf und informiert Sie. So können Sicherheitsrisiken einfach und frühzeitig behoben werden.

Beheben Sie die in Bitdefender Antivirus for Mac angezeigten Probleme, um schnell und einfach den optimalen Schutz für Ihr System und Ihre Daten sicherzustellen.

Zu den erkannten Problemen gehören:

- Das neueste Update der Bedrohungsinformationen wurde nicht von unserer Servern heruntergeladen.
- Auf Ihrem System wurden Bedrohungen gefunden, die das Produkt nicht automatisch beheben kann.
- Der Echtzeitschutz ist deaktiviert.

Um erkannte Probleme zu überprüfen und zu beheben:

1. Liegen keine Warnungen in Bitdefender vor, ist die Statusleiste grün. Wird ein Sicherheitsproblem gefunden, wechselt die Farbe der Statusleiste zu rot.
2. Überprüfen Sie die Beschreibung für weitere Informationen.
3. Wird ein Problem erkannt, können Sie mit einem Klick auf die entsprechende Schaltfläche Gegenmaßnahmen einleiten.



Fenster mit nicht beseitigten Bedrohungen

Die Liste der nicht behobenen Bedrohungen wird nach jedem System-Scan aktualisiert. Dies geschieht unabhängig davon, ob der Scan automatisch im Hintergrund durchgeführt oder von Ihnen angestoßen wurde.

Für nicht beseitigte Bedrohungen sind die folgenden Aktionen verfügbar:

- Manuelles Löschen. Mit dieser Aktion können Sie Infektionen manuell entfernen.
- **Zu den Ausnahmen hinzufügen**. Diese Aktion ist nicht für Bedrohungen verfügbar, die innerhalb von Archiven gefunden wurden.

3.12. Benachrichtigungen

Bitdefender führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer. Immer wenn etwas passiert, was die Sicherheit Ihres Systems oder Ihrer Daten betrifft, wird in den Bitdefender-Benachrichtigungen eine Nachricht erstellt, ähnlich einer neuen E-Mail in Ihrem Postfach.

Benachrichtigungen sind ein wichtiges Hilfsmittel für die Überwachung und Verwaltung Ihres Bitdefender-Schutzes. So können Sie z. B. überprüfen, ob ein Update erfolgreich durchgeführt wurde oder ob Bedrohungen oder Schwachstellen im System gefunden wurden. Zudem können Sie bei Bedarf weitere Aktionen ausführen oder die von Bitdefender ausgeführten Aktionen anpassen.



Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Benachrichtigungen**, um auf das Benachrichtigungsprotokoll zuzugreifen. Bei jedem kritischen Ereignis wird auf dem -Symbol ein Zähler eingeblendet.

Je nach Art und Schwere werden Benachrichtigungen sortiert nach:

- **Kritische** Ereignisse weisen auf kritische Probleme hin. Sie sollten sich umgehend darum kümmern.
- **Warnung** Diese Ereignisse weisen auf nicht-kritische Probleme hin. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
- **Information** Diese Ereignisse weisen auf erfolgreich ausgeführte Vorgänge hin.

Mit einem Klick auf den jeweiligen Reiter erhalten Sie weitere Informationen zu den Ereignissen. Mit einem einfachen Klick auf den Ereignisnamen werden die folgenden Kurzinfos angezeigt: Kurzbeschreibung, die von Bitdefender durchgeführte Aktion sowie Datum und Zeitpunkt des Ereignisses. Unter Umständen werden Ihnen Optionen zur weiteren Vorgehensweise angeboten.

Zur übersichtlicheren Verwaltung der protokollierten Ereignisse enthält das Benachrichtigungsfenster Optionen, mit denen Sie alle Ereignisse in einem Abschnitt löschen oder als gelesen markieren können.

3.13. Aktualisierung

Jeden Tag werden neue Bedrohungen entdeckt und identifiziert. Deshalb ist es so wichtig, Bitdefender Antivirus for Mac über Updates ständig auf dem neuesten Stand zu halten.

Die Aktualisierung der Bedrohungsinformationen wird „on the fly“ durchgeführt. Das bedeutet, dass die zu aktualisierenden Dateien schrittweise ersetzt werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System zu keiner Zeit gefährdet.

- Wenn Bitdefender Antivirus for Mac up-to-date ist, spürt die Software die neuesten Bedrohungen auf und säubert infizierte Dateien.
- Ist Bitdefender Antivirus for Mac nicht auf dem neuesten Stand, kann es die neuesten, von den Bitdefender-Laboren entdeckten Bedrohungen nicht erkennen und entfernen.



3.13.1. Benutzergesteuertes Update

Ein manuelles Update können Sie jederzeit durchführen.

Für regelmäßige Updates und Downloads ist eine aktive Internetverbindung nötig.

Führen Sie folgende Schritte für ein manuelles Update durch:

1. Klicken Sie auf die Schaltfläche **Aktionen** in der Menüleiste.
2. Wählen Sie **Update der Bedrohungsinformationen**.

Alternativ können Sie ein Update auch manuell anfordern, indem Sie CMD + U drücken.

Der Update-Fortschritt und die heruntergeladenen Dateien werden eingeblendet.

3.13.2. Updates über einen Proxy Server

Bitdefender Antivirus for Mac kann Updates über einen Proxy Server nur dann durchführen, wenn dafür keine Autorisierung notwendig ist. Sie müssen keine Programmeinstellungen konfigurieren.

Wenn Ihre Internetverbindung über einen Proxy-Server läuft, der eine Autorisierung verlangt, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um die neuesten Bedrohungsinformationen herunterladen zu können.

3.13.3. Upgrade auf eine neue Version durchführen

Von Zeit zu Zeit veröffentlichen wir Produkt-Updates, die neue Funktionen bringen oder bestimmte Aspekte der Software verbessern oder Probleme beheben. Bei diesen Updates kann es notwendig werden, das System neu zu starten, um die Installation neuer Dateien zu ermöglichen. Falls ein Update einen Neustart erforderlich macht, wird Bitdefender Antivirus for Mac standardmäßig bis zum Neustart des Systems die bereits vorhandenen Dateien nutzen. So beeinträchtigt der Aktualisierungsprozess den Benutzer nicht bei seiner Arbeit.

Ein Pop-up-Fenster fordert Sie auf das System neu zu starten, sobald das Update abgeschlossen wurde. Fall Sie diese Benachrichtigung verpassen, können Sie das System manuell neu starten oder in der Menüleiste auf **Für das Upgrade neu starten** klicken.



3.13.4. Informationen zu Bitdefender Antivirus for Mac finden

Informationen zur installierten Bitdefender Antivirus for Mac-Version finden Sie im Bereich **Info über**. Hier können Sie die Abonnementvereinbarung sowie die Datenschutzerklärung aufrufen und lesen sowie die Open-Source-Lizenzen anzeigen.

So rufen Sie das Fenster „Info über“ auf:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Über Antivirus for Mac**.



4. VPN

Dieses Kapitel beinhaltet die folgenden Themen:

- *Über VPN (S. 29)*
- *Öffnen des VPN (S. 29)*
- *Netzwerkkarte (S. 30)*
- *Abonnements (S. 32)*

4.1. Über VPN

Mit Bitdefender VPN schützen Sie Ihre Daten bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen, Einkaufszentren, Cafés oder Hotels. So vermeiden Sie unglückliche Situationen wie den Diebstahl Ihrer persönlichen Daten oder Versuche, Ihre Geräte-IP-Adresse für Hacker offenzulegen.

Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihre Daten werden professionell nach Bankenstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über spezielle Server weitergeleitet, was es nahezu unmöglich macht, Ihr Gerät neben den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit Bitdefender VPN im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.



Beachten Sie

In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Konsequenzen zu vermeiden, wird Ihnen bei der ersten Nutzung der Bitdefender-VPN-App eine Warnmeldung angezeigt. Durch die weitere Nutzung der App bestätigen Sie, dass Sie sich aller einschlägigen Rechtsvorschriften in Ihrem Land sowie der möglichen Risiken, denen Sie sich aussetzen, bewusst sind.

4.2. Öffnen des VPN

Sie haben drei Möglichkeiten zum Öffnen der Bitdefender VPN-App:

- Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Privatsphäre**.



Klicken Sie in der Kachel Bitdefender VPN auf **Öffnen**.

- Klicken Sie in der Menüleiste auf das -Symbol.
- Öffnen Sie im Ordner Anwendungen den Ordner Bitdefender und doppelklicken Sie danach auf das Bitdefender VPN-Symbol.

Beim ersten Öffnen der App werden Sie aufgefordert, Bitdefender das Hinzufügen von Konfigurationen zu erlauben. Indem Sie Bitdefender erlauben, Konfigurationen hinzuzufügen, stimmen Sie zu, dass alle Netzwerkaktivitäten Ihres Geräts gefiltert oder überwacht werden können, wenn Sie die VPN-App verwenden.



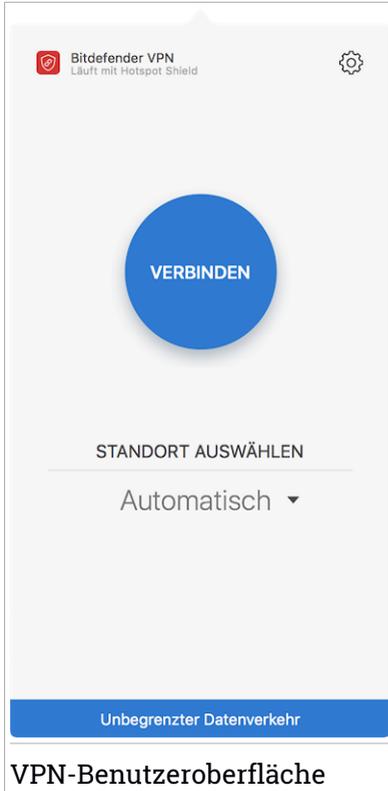
Beachten Sie

Die Bitdefender-VPN-App kann nur unter macOS Sierra (10.12.6), macOS High Sierra (10.13.6) oder macOS Mojave (ab 10.14) installiert werden.

4.3. Netzwerkkarte

In der VPN-Benutzeroberfläche wird der Status der App angezeigt, verbunden oder getrennt. Der Serverstandort wird für Anwender mit der kostenlosen Version von Bitdefender automatisch auf den geeignetsten Server festgelegt. Premium-Anwender können den Serverstandort selbst wählen, indem sie ihn aus der Liste **Virtueller Standort** auswählen. Weitere Einzelheiten zu den VPN-Abonnements finden Sie unter **Abonnements (S. 32)**.

Klicken Sie auf die Statusanzeige oben im Bild, um die Verbindung herzustellen oder zu trennen. Ein schwarzes Symbol in der Menüleiste zeigt an, dass eine Verbindung besteht. Ist das Symbol weiß, wurde die Verbindung getrennt.



Während die Verbindung besteht, wird die verstrichene Zeit unten in der Benutzeroberfläche angezeigt. Klicken Sie oben rechts auf das -Symbol, um auf weitere Optionen zuzugreifen.

- **Mein Konto** - Hier finden Sie Details zu Ihrem Bitdefender-Benutzerkonto und Ihrem VPN-Abonnement. Klicken Sie auf **Konto wechseln**, wenn Sie sich mit einem anderen Konto anmelden möchten.
- **Einstellungen** - Hier können Sie das Produktverhalten individuell anpassen:
 - Benachrichtigungen
 - Legen Sie fest, dass das VPN beim Systemstart ausgeführt wird
 - Produktberichte



- **Automatisch verbinden** - mit diese Funktion, die Sie im Reiter **Erweitert** finden, können Sie festlegen, dass Bitdefender VPN automatisch genutzt wird, wenn Sie auf ein ungesichertes oder öffentliches WLAN-Netzwerk zugreifen oder wenn eine Peer-to-Peer-Anwendung zur Dateifreigabe gestartet wird.
- **Support** - Sie werden auf die Support Center-Plattform weitergeleitet, wo Sie einen hilfreichen Artikel zur Nutzung der Bitdefender VPN lesen können.
- **Über** - Hier finden Sie Informationen zur installierten Version.
- **Beenden** - hiermit verlassen Sie die Anwendung.

4.4. Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Ihre Verbindung bei Bedarf abzusichern. Sie werden automatisch mit dem besten Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Mit einem Klick auf **Upgrade** können Sie über die Benutzeroberfläche jederzeit ein Upgrade auf Bitdefender Premium VPN durchführen.

Ein Bitdefender Premium-VPN-Abonnement läuft unabhängig von dem Bitdefender Antivirus for Mac-Abonnement, d. h. Sie können es über den gesamten Verfügbarkeitszeitraum hinweg nutzen, unabhängig von Status Ihres Sicherheitsabonnement. Wenn Ihr Bitdefender Premium-VPN-Abonnement abläuft, Ihr Bitdefender Antivirus for Mac-Abonnement aber weiterhin aktiv ist, kehren Sie zum kostenlosen Angebot zurück.

Bitdefender VPN ist ein plattformübergreifendes Produkt, das in Bitdefender-Produkten für Windows, macOS, Android und iOS verfügbar ist. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen, vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.



5. EINSTELLUNGEN KONFIGURIEREN

Dieses Kapitel beinhaltet die folgenden Themen:

- *Zugriff auf Einstellungen* (S. 33)
- *Schutzeinstellungen* (S. 33)
- *Erweiterte Einstellungen* (S. 34)
- *Sonderangebote* (S. 34)

5.1. Zugriff auf Einstellungen

Um das Einstellungen-Fenster von Bitdefender Antivirus for Mac zu öffnen:

1. Wählen Sie eine der folgenden Methoden:

- Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
- Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Einstellungen**.

5.2. Schutzeinstellungen

Über das Schutzeinstellungsfenster können Sie den gesamten Scan-Vorgang konfigurieren. Sie können die Aktionen, die bei infizierten oder verdächtigen Dateien vorgenommen werden sollen oder auch allgemeine Einstellungen konfigurieren.

- **Bitdefender-Schild.** Das Bitdefender-Schild bietet Ihnen Echtzeitschutz vor einer Vielzahl an Bedrohungen, indem es alle installierten Apps und ihre jeweiligen Updates sowie alle neuen und veränderten Dateien scannt. Wir empfehlen Ihnen, Bitdefender-Schild nicht zu deaktivieren. Sollte es dennoch einmal notwendig werden, sollten Sie den Zeitraum so kurz wie möglich halten. Während das Bitdefender-Schild deaktiviert ist, sind Sie nicht vor Bedrohungen geschützt.
- **Nur neue und geänderte Dateien.** Aktivieren Sie diese Option, wenn Bitdefender Antivirus for Mac nur Dateien prüfen soll, die vorher noch nicht geprüft wurden oder die seit dem letzten Scan modifiziert wurden.

Sie können festlegen, dass diese Einstellung für benutzerdefinierte und Drag-and-Drop-Scans nicht angewandt wird, indem Sie das entsprechende Kästchen deaktivieren.



- **Backup-Inhalte nicht scannen.** Markieren Sie dieses Kästchen, um Backup-Dateien vom Scan auszuschließen. Werden infizierte Dateien zu einem späteren Zeitpunkt wiederhergestellt, erkennt Bitdefender Antivirus for Mac diese automatisch und leitet geeignete Maßnahmen ein.

5.3. Erweiterte Einstellungen

Sie können eine übergeordnete Aktion auswählen, die für alle Probleme und verdächtige Objekte, die während eines Scan-Vorgangs gefunden werden, durchgeführt werden soll.

Vorgehen bei infizierten Objekten

Versuchen, zu desinfizieren oder in die Quarantäne zu verschieben - Wenn infizierte Dateien gefunden werden, versucht Bitdefender, sie zu desinfizieren (den Schadcode zu entfernen) oder sie in die Quarantäne zu verschieben.

Keine Aktion durchführen. - Es werden keine Aktionen für die gefundenen Dateien durchgeführt.

Vorgehen bei verdächtigen Objekten

Dateien in Quarantäne verschieben - Wenn verdächtige Dateien gefunden werden, verschiebt Bitdefender sie in die Quarantäne.

Keine Aktion durchführen. - Es werden keine Aktionen für die gefundenen Dateien durchgeführt.

5.4. Sonderangebote

Sind Sonderangebote verfügbar, wird das Bitdefender-Produkt Sie per Pop-up-Benachrichtigung darüber informieren. So können Sie von unseren Vorteilspreisen profitieren und Ihre Geräte länger schützen.

So können Sie Benachrichtigungen über Sonderangebote aktivieren oder deaktivieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Wechseln Sie zum Reiter **Sonstige**.
3. Aktivieren oder deaktivieren Sie den Schalter **Meine Angebote**.

Die Option **Meine Angebote** ist standardmäßig aktiviert.



6. BITDEFENDER CENTRAL

Dieses Kapitel beinhaltet die folgenden Themen:

- *Über Bitdefender Central* (S. 35)
- *Meine Abonnements* (S. 39)
- *Meine Geräte* (S. 40)

6.1. Über Bitdefender Central

Bitdefender Central stellt Ihnen eine Plattform zur Verfügung, über die Sie auf die Online-Funktionen und -Dienste des Produkts zugreifen und wichtige Aufgaben auf allen Geräten ausführen können, auf denen Bitdefender installiert ist. Über <https://central.bitdefender.com> können Sie sich mit jedem internetfähigen Computer oder Mobilgerät bei Ihrem Bitdefender-Konto anmelden. Alternativ können Sie auf Ihren Android- und iOS-Geräten auch die Bitdefender Central-App nutzen.

So können Sie die Bitdefender Central-App auf Ihren Geräten installieren:

- **Android** - Suchen Sie Bitdefender Central in Google Play, laden Sie die App herunter und installieren Sie sie. Folgen Sie den Anweisungen, um die Installation abzuschließen.
- **iOS** - Suchen Sie Bitdefender Central im App Store, laden Sie die App herunter und installieren Sie sie. Folgen Sie den Anweisungen, um die Installation abzuschließen.

Nachdem Sie sich angemeldet haben, stehen Ihnen die folgenden Optionen zur Verfügung:

- Laden Sie Bitdefender herunter und installieren Sie es auf Windows-, macOS-, iOS- und Android-Betriebssystemen. Die folgenden Produkte stehen zum Download bereit:
 - Bitdefender Antivirus for Mac
 - Die Bitdefender-Windows-Produktlinie
 - Bitdefender Mobile Security für Android
 - Bitdefender Mobile Security for iOS
- Ihre Bitdefender-Abonnements verwalten und verlängern.



- Neue Geräte zu Ihrem Netzwerk hinzufügen und diese Geräte aus der Ferne verwalten.

6.2. So können Sie Bitdefender Central aufrufen:

Bitdefender Central kann auf verschiedene Weise aufgerufen werden. Je nach durchzuführender Aufgabe stehen Ihnen die folgenden Optionen zur Verfügung:

- Über das Bitdefender Antivirus for Mac-Hauptfenster:
 1. Klicken Sie rechts unten in der Benutzeroberfläche auf den Link **Zum eigenen Konto**.
- Über Ihren Web-Browser:
 1. Öffnen Sie einen Web-Browser auf jedem beliebigen internetfähigen Gerät.
 2. Gehen Sie zu: <https://central.bitdefender.com>.
 3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Konto an.
- Über Ihr Android- oder iOS-Gerät:

Öffnen Sie die bei Ihnen installierte Bitdefender Central-App.



Beachten Sie

Hier finden Sie alle Optionen, die Ihnen über die Web-Oberfläche zur Verfügung gestellt werden.

6.3. Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung fügt Ihrem Bitdefender-Benutzerkonto eine weitere Sicherheitsebene hinzu, indem sie zusätzlich zu Ihren Anmeldeinformationen einen Authentifizierungscode anfordert. Auf diese Weise verhindern Sie unbefugten Zugriff auf Ihr Benutzerkonto und schützen sich vor Cyberangriffen wie Keylogger-, Brute-Force- oder Wörterbuchangriffen.

Aktivieren der Zwei-Faktor-Authentifizierung

Durch die Aktivierung der Zwei-Faktor-Authentifizierung wird Ihr Bitdefender-Benutzerkonto deutlich besser abgesichert. Sie müssen Ihre



Identität für jede Anmeldung über ein neues Gerät erneut bestätigen, so zum Beispiel wenn Sie eines der Bitdefender-Produkte installieren, Ihren Abonnementstatus einsehen oder per Fernzugriff Aufgaben auf Ihren Geräten ausführen.

So aktivieren Sie die Zwei-Faktor-Authentifizierung:

1. Rufen Sie **Bitdefender Central** auf.
2. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmcke.
3. Klicken Sie im Slide-Menü auf **Bitdefender-Konto**.
4. Wechseln Sie zum Reiter **Passwort und Sicherheit**.
5. Klicken Sie auf **ERSTE SCHRITTE**.

Wählen Sie eine der folgenden Methoden aus:

- **Authentifizierungsanwendung** - Verwenden Sie eine Authentifizierungsanwendung, um für jede Anmeldung bei Ihrem Bitdefender-Konto einen Code zu generieren.

Wenn Sie eine Authentifizierungs-App verwenden möchten, sich aber nicht sicher sind, welche App Sie verwenden sollen, können Sie sie aus einer Liste mit den von uns empfohlenen Authentifizierungs-Apps auswählen.

- a. Klicken Sie zunächst auf **AUTHENTIFIZIERUNGSANWENDUNG VERWENDEN**.
- b. Verwenden Sie zur Anmeldung auf einem Android- oder iOS-Gerät Ihr Gerät, um den QR-Code zu scannen.

Zur Anmeldung auf einem Laptop oder Computer können Sie den angezeigten Code manuell eingeben.

Klicken Sie auf **FORTFAHREN**.

- c. Geben Sie den von der App generierten bzw. den im vorherigen Schritt angezeigten Code ein, und klicken Sie dann auf **AKTIVIEREN**.

- **E-Mail** - Bei jeder Anmeldung an Ihrem Bitdefender-Konto wird ein Bestätigungscode an Ihre E-Mail-Adresse gesendet. Rufen Sie Ihre E-Mails ab und verwenden Sie den erhaltenen Code.

- a. Klicken Sie zunächst auf **E-MAIL VERWENDEN**.
- b. Rufen Sie Ihre E-Mails ab, und geben Sie den erhaltenen Code ein.



c. Klicken Sie auf **AKTIVIEREN**.

Gehen Sie folgendermaßen vor, wenn Sie die Zwei-Faktor-Authentifizierung nicht mehr nutzen möchten:

1. Klicken Sie auf **ZWEI-FAKTOR-AUTHENTIFIZIERUNG DEAKTIVIEREN**.
2. Sehen Sie in die App oder rufen Sie Ihre E-Mails ab, und geben Sie den erhaltenen Code ein.
3. Bestätigen Sie Ihre Auswahl.

6.4. Hinzufügen vertrauenswürdiger Geräte

Um sicherzustellen, dass nur Sie auf Ihr Bitdefender-Konto zugreifen können, fragen wir unter Umständen zunächst einen Sicherheitscode ab. Wenn Sie bei Anmeldungen über das gleiche Gerät diesen Schritt überspringen möchten, empfehlen wir, dass Sie ein vertrauenswürdiges Gerät festzulegen.

So können Sie Geräte als vertrauenswürdige Geräte festlegen:

1. Rufen Sie **Bitdefender Central** auf.
2. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmcke.
3. Klicken Sie im Slide-Menü auf **Bitdefender-Konto**.
4. Wechseln Sie zum Reiter **Passwort und Sicherheit**.
5. Klicken Sie auf **Vertrauenswürdige Geräte**.
6. Es wird eine Liste mit Geräten angezeigt, auf denen Bitdefender installiert ist. Klicken Sie auf das gewünschte Gerät.

Sie können beliebig viele Geräte hinzufügen, vorausgesetzt, dass Bitdefender auf ihnen installiert ist und Sie über ein gültiges Abonnement verfügen.

6.5. Aktivität

Im Bereich Aktivität können Sie Informationen zu den Geräten einsehen, auf denen Bitdefender installiert ist.

Im Fenster **Aktivität** können Sie auf die folgenden Kacheln zugreifen:

- **Meine Geräte**. Hier können Sie die Anzahl der verbundenen Geräte sowie deren Schutzstatus einsehen. Um Probleme auf den erkannten Geräten per Fernzugriff zu beheben, klicken Sie auf **Probleme beheben** und dann auf **SCANEN UND PROBLEME BEHEBEN**.



Um Details zu den erkannten Problemen anzuzeigen, klicken Sie auf **Probleme anzeigen**.

Von iOS-Geräten können keine Informationen zu erkannten Bedrohungen abgerufen werden.

- **Blockierte Bedrohungen.** Hier können Sie ein Diagramm mit einer Gesamtstatistik mit Informationen über die blockierten Bedrohungen der letzten 24 Stunden bzw. 7 Tage anzeigen. Die angezeigten Informationen werden abhängig von dem schädlichen Verhalten abgerufen, das bei den aufgerufenen Dateien, Anwendungen und URLs erkannt wurde.
- **Benutzer mit den meisten blockierten Bedrohungen.** Hier können Sie eine Übersicht mit den Anwendern anzeigen, bei denen die meisten Bedrohungen gefunden wurden.
- **Geräte mit den meisten blockierten Bedrohungen.** Hier können Sie eine Übersicht mit den Geräten anzeigen, auf denen die meisten Bedrohungen gefunden wurden.

6.6. Meine Abonnements

Über die Bitdefender Central-Plattform können Sie bequem die Abonnements für alle Ihre Geräte verwalten.

6.6.1. Abonnement aktivieren

Sie können Ihr Abonnement während des Installationsvorgangs mithilfe Ihres Bitdefender-Kontos aktivieren. Sobald die Aktivierung abgeschlossen ist, beginnt die Laufzeit des Abonnements.

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer Ihres Bitdefender-Abonnements um diesen Zeitraum verlängern.

So können Sie Ihr Abonnement mit einem Aktivierungscode aktivieren:

1. Rufen Sie **Bitdefender Central** auf.
2. Klicken Sie oben links im Fenster auf das -Symbol und öffnen Sie den Bereich **Meine Abonnements**.
3. Klicken Sie auf **AKTIVIERUNGSCODE** und geben Sie den Code in das entsprechende Feld ein.
4. Klicken Sie zum Fortfahren auf **AKTIVIEREN**.



Das Abonnement wurde aktiviert.

Informationen zur Installation des Produktes auf Ihren Geräten finden Sie im Abschnitt *Installation von Bitdefender Antivirus for Mac (S. 1)*.

6.7. Meine Geräte

Über Ihr Bitdefender-Benutzerkonto können Sie im Bereich **Meine Geräte** die Bitdefender-Produkte auf Ihren Geräten aus der Ferne installieren und verwalten, sofern die Geräte eingeschaltet und mit dem Internet verbunden sind. Auf den Gerätekacheln sind der Gerätename, der Sicherheitsstatus angegeben sowie die Information, ob Sicherheitsprobleme auf Ihren Geräten bestehen.

6.7.1. Persönliche Anpassungen

Sie können Gerätenamen vergeben, um die Geräte später leichter identifizieren zu können:

1. Rufen Sie **Bitdefender Central** auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol  in der rechten oberen Ecke.
4. Tippen Sie auf **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Gerätename** ein und klicken Sie dann auf **SPEICHERN**.

Sie können für jedes Ihrer Geräte zur einfacheren Verwaltung einen Besitzer anlegen und zuordnen:

1. Rufen Sie **Bitdefender Central** auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol  in der rechten oberen Ecke.
4. Wählen Sie **Profil**.
5. Klicken Sie auf **Besitzer hinzufügen** und füllen Sie dann die entsprechenden Felder aus. Passen Sie das Profil nach Bedarf an, indem Sie ein Foto



hinzufügen, einen Geburtstag auswählen und eine E-Mail-Adresse sowie eine Telefonnummer eingeben.

6. Klicken Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
7. Wählen Sie aus der **Gerätebesitzer**-Liste den gewünschten Besitzer aus und klicken Sie auf **ZUORDNEN**.

6.7.2. Fernzugriffsaktionen

So können Sie Bitdefender per Fernzugriff auf Ihren Geräten aktualisieren:

1. Rufen Sie **Bitdefender Central** auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol  in der rechten oberen Ecke.
4. Wählen Sie **Update**.

Klicken Sie auf eine Gerätekarte, um die folgenden Reiter anzuzeigen:

- **Dashboard**. In diesem Fenster können Sie Details zum ausgewählten Gerät anzeigen, den Schutzstatus sowie die Zahl der blockierten Bedrohungen der letzten sieben Tage einsehen. Der Sicherheitsstatus ist grün, wenn es keine Sicherheitsprobleme gibt, gelb, wenn es etwas gibt, was Ihre Aufmerksamkeit erfordert, und rot, wenn Ihr Gerät gefährdet ist. Gibt es Probleme, die sich auf Ihr Gerät auswirken, klicken Sie im oberen Statusbereich auf den Drop-down-File, um weitere Details anzuzeigen. Von hier aus können die Probleme, die Ihre Gerätesicherheit beeinträchtigen, manuell behoben werden.
- **Schutz**. Von diesem Fenster aus können Sie einen Quick Scan oder einen Vollständiger Scan auf Ihren Geräten durchführen. Klicken Sie auf **SCAN**, um den Vorgang zu starten. Sie können auch nachvollziehen, wann der letzte Scan auf dem Gerät durchgeführt wurde, und einen Bericht für den aktuellsten Scan abrufen, in dem die wichtigsten Informationen zusammengefasst werden. Details zu diesen beiden Scan-Arten finden Sie unter *Ihren Mac scannen (S. 13)*.



7. HÄUFIG GESTELLTE FRAGEN

Wie kann ich Bitdefender Antivirus for Mac testen, bevor ich ein Abonnement abschlieÙe?

Sie sind ein neuer Bitdefender-Kunde und möchten unser Produkt testen, bevor Sie es kaufen. Der Testzeitraum beträgt 30 Tage. Nach Ablauf dieser Frist können Sie das Produkt nur weiterverwenden, wenn Sie ein Bitdefender-Abonnement erwerben. Um Bitdefender Antivirus for Mac zu testen, müssen Sie:

1. Erstellen Sie ein Bitdefender-Konto wie folgt:
 - a. Gehen Sie zu: <https://central.bitdefender.com>.
 - b. Geben Sie die Daten in die entsprechenden Felder ein. Die hier eingetragenen Daten bleiben vertraulich.
 - c. Bevor Sie fortfahren können, müssen Sie zunächst den Nutzungsbedingungen zustimmen. Rufen Sie die Nutzungsbedingungen auf und lesen Sie sie aufmerksam durch, da Sie hier die Bedingungen zur Nutzung von Bitdefender finden.

Darüber hinaus können Sie auch die Datenschutzrichtlinie aufrufen und lesen.
 - d. Klicken Sie auf **KONTO ERSTELLEN**.
2. Laden Sie Bitdefender Antivirus for Mac wie folgt herunter:
 - a. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **SCHUTZ INSTALLIEREN**.
 - b. Wählen Sie eine der beiden verfügbaren Optionen:
 - **Dieses Gerät schützen**
 - i. Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
 - ii. Speichern Sie die Installationsdatei.
 - **Andere Geräte schützen**
 - i. Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.



- ii. Klicken Sie auf **DOWNLOAD-LINK SENDEN**.
- iii. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL VERSENDEN**.

Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.

- iv. Rufen Sie auf dem Gerät, auf dem Bitdefender installiert werden soll, das angegebene E-Mail-Konto auf und klicken Sie in der E-Mail auf die Download-Schaltfläche.

c. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.

Ich habe einen Aktivierungscode. Wie verlängere ich damit die Laufzeit meines Abonnements?

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer Ihres Bitdefender-Abonnements um diesen Zeitraum verlängern.

So können Sie Ihr Abonnement mit einem Aktivierungscode aktivieren:

1. Rufen Sie **Bitdefender Central** auf.
2. Klicken Sie oben links im Fenster auf das -Symbol und öffnen Sie den Bereich **Meine Abonnements**.
3. Klicken Sie auf **AKTIVIERUNGSCODE** und geben Sie den Code in das entsprechende Feld ein.
4. Klicken Sie zum Fortfahren auf **AKTIVIEREN**.

Die Erweiterung wird jetzt in Ihrem Bitdefender-Konto sowie im rechten unteren Bereich der Oberfläche Ihres installierten Bitdefender Antivirus for Mac-Produkts angezeigt.

Das Scan-Protokoll zeigt bisher noch nicht gelöste Probleme. Wie kann ich diese beheben?

Mögliche noch nicht gelöste Probleme im Scan-Protokoll sind zum Beispiel:

- Archive mit eingeschränktem Zugriff (xar, rar usw.)



Lösung: Finden Sie die Datei über die Option **Im Finder zeigen** und löschen Sie sie von Hand. Vergessen Sie dabei nicht, den Papierkorb zu leeren.

- Postfächer mit eingeschränktem Zugriff (Thunderbird usw.)

Lösung: Entfernen Sie den Eintrag mit der infizierten Datei mithilfe der Anwendung.

- Backup-Inhalte

Lösung: Aktivieren Sie in den Schutz-Einstellungen die Option **Backup-Inhalte nicht scannen** oder schließen Sie die gefundenen Dateien mit **Zu den Ausnahmen hinzufügen** vom Scan aus.

Werden infizierte Dateien zu einem späteren Zeitpunkt wiederhergestellt, erkennt Bitdefender Antivirus for Mac diese automatisch und leitet geeignete Maßnahmen ein.



Beachten Sie

Dateien mit beschränktem Zugriff sind Dateien, die Bitdefender Antivirus for Mac zwar öffnen, aber nicht bearbeiten kann.

Wo kann ich detaillierte Informationen zu den Produktaktivitäten einsehen?

Bitdefender führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere kritische Nachrichten über die eigenen Aktivitäten. Um auf diese Informationen zuzugreifen, klicken Sie im Navigationsmenü der Bitdefender-Oberfläche auf **Benachrichtigungen**.

Kann ich Bitdefender Antivirus for Mac über einen Proxy-Server aktualisieren?

Bitdefender Antivirus for Mac kann Updates über einen Proxy Server nur dann durchführen, wenn dafür keine Autorisierung notwendig ist. Sie müssen keine Programmeinstellungen konfigurieren.

Wenn Ihre Internetverbindung über einen Proxy-Server läuft, der eine Autorisierung verlangt, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um die neuesten Bedrohungsinformationen herunterladen zu können.

Wie kann ich Bitdefender Antivirus for Mac entfernen?

Um Bitdefender Antivirus for Mac zu entfernen, gehen Sie folgendermaßen vor:

1. Öffnen Sie **Finder** und wählen Sie den Programme-Ordner.



2. Öffnen Sie den Bitdefender-Ordner und doppelklicken Sie nach auf Bitdefender-Deinstallationsprogramm.
3. Klicken Sie auf **Deinstallieren**, und warten Sie, bis der Vorgang abgeschlossen ist.
4. Klicken Sie zum Abschluss auf **Schließen**.



Wichtig

Ist ein Fehler aufgetreten, so können Sie die Kundenbetreuung von Bitdefender wie in *Support (S. 47)* beschrieben, kontaktieren.

Wie entferne ich die Linkchecker-Erweiterungen aus meinem Browser?

- Um die Linkchecker-Erweiterungen aus Mozilla Firefox zu entfernen, gehen Sie folgendermaßen vor:
 1. Klicken Sie auf **Tools** und danach auf **Add-ons**.
 2. Klicken Sie in der Spalte links auf **Erweiterungen**.
 3. Wählen Sie die Erweiterung aus und klicken Sie auf **Entfernen**.
 4. Starten Sie den Browser neu, um den Entfernungsvorgang abzuschließen.
- Um die Linkchecker-Erweiterungen aus Google Chrome zu entfernen, gehen Sie folgendermaßen vor:
 1. Klicken Sie am oberen rechten Bildschirmrand auf **Mehr** .
 2. Wählen Sie im Bereich **Weitere Tools** den Eintrag **Erweiterungen** aus.
 3. Klicken Sie neben der Erweiterung, die Sie entfernen möchten, auf **... entfernen** .
 4. Klicken Sie auf **Entfernen**, um den Entfernungsvorgang zu bestätigen.
- Um Bitdefender TrafficLight aus Safari zu entfernen, gehen Sie folgendermaßen vor:
 1. Rufen Sie die **Einstellungen** auf oder drücken Sie **Befehl-Komma(,)**.
 2. Wählen Sie den Menüpunkt **Erweiterungen**.

Eine Liste mit allen installierten Erweiterungen wird angezeigt.



3. Wählen Sie die Erweiterung Bitdefender TrafficLight aus, und klicken Sie dann auf **Deinstallieren**.
4. Klicken Sie erneut auf **Deinstallieren**, um den Deinstallationsvorgang zu bestätigen.

Wann sollte ich Bitdefender VPN nutzen?

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um sicherzustellen, dass Sie beim Surfen im Netz jederzeit geschützt sind, empfehlen wir den Einsatz von Bitdefender VPN, wenn Sie:

- Verbindungen zu öffentlichen WLAN-Netzwerken herstellen möchten
- auf Inhalte zugreifen möchten, die regionalen Zugangsbeschränkungen unterliegen, egal ob Sie zuhause oder im Ausland sind
- Ihre persönlichen Daten vor Zugriff schützen möchten (Benutzernamen, Passwörter, Kreditkartendaten etc.)
- Ihre IP-Adresse verbergen möchten

Wirkt sich Bitdefender VPN auf die Akkulaufzeit meines Gerätes aus?

Bitdefender VPN wurde eigens entwickelt, um Ihre persönlichen Daten zu schützen, Ihre IP-Adresse bei Verbindungen mit ungesicherten WLAN-Netzwerken zu verbergen und Ihnen den Zugriff auf Inhalte mit länderspezifischen Zugangsbeschränkungen zu ermöglichen. Um Ihren Akku zu entlasten, empfehlen wir, das VPN nur bei Bedarf zu nutzen und die Verbindung danach wieder zu trennen.

Wird meine Internetverbindung langsamer, wenn ich eine Verbindung mit Bitdefender VPN herstelle?

Bitdefender VPN ist auf einen ressourcenschonenden Betrieb beim Surfen im Netz ausgelegt. Ihre Internetverbindung bzw. die Entfernung zu Server, mit dem Sie eine Verbindung hergestellt haben, können sich jedoch negativ auf die Verbindungsgeschwindigkeit auswirken. Wenn es nicht unbedingt notwendig ist, dass Sie sich von Ihrem Standort aus mit einem weit entfernten Server verbinden (z. B. von Deutschland aus nach China), sollten Sie in solchen Fällen Bitdefender VPN erlauben, automatisch eine Verbindung mit dem nächstgelegenen Server herzustellen bzw. einen Server zu finden, der näher an Ihrem Standort liegt.



8. HILFE ERHALTEN

Dieses Kapitel beinhaltet die folgenden Themen:

- *Support* (S. 47)
- *Kontaktinformation* (S. 49)

8.1. Support

Bitdefender hat es sich zur Aufgabe gemacht, seinen Kunden beispiellos schnellen und sorgfältigen Support zu bieten. Sollten Sie mit Ihrem Bitdefender-Produkt Probleme haben oder es hat sich eine Frage ergeben, so stehen Ihnen verschiedene Online-Quellen zur Verfügung, wo Sie schnell eine Antwort oder Lösung finden können. Sie können auch das Kundenbetreuungs-Team von Bitdefender kontaktieren. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

8.1.1. Online-Ressourcen

Für die Lösung Ihres Problems und Fragen im Zusammenhang mit Bitdefender stehen Ihnen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:
<https://www.bitdefender.de/support/consumer.html>
- Bitdefender-Support-Forum:
<http://forum.bitdefender.com>
- Das Computer-Sicherheitsportal HOTforSecurity:
<http://www.hotforsecurity.com>

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

Bitdefender-Support-Center

Das Bitdefender-Support-Center ist eine Online-Sammlung von Informationen zu Ihren Bitdefender-Produkten. Hier sind in einem unkomplizierten Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams



gespeichert. Hinzu kommen Artikel zur Gefahrenprävention, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Das Bitdefender-Support-Center ist öffentlich zugänglich und frei durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. Alle berechtigten Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Support-Center wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Das Bitdefender-Support-Center steht Ihnen jederzeit unter der folgenden Adresse zur Verfügung: <https://www.bitdefender.de/support/consumer.html>.

Bitdefender-Support-Forum

Das Bitdefender-Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, schnelle Hilfe zu erhalten oder anderen Hilfestellung zu geben. Hier können Sie Ihre Probleme und Fragen rund um Ihr Bitdefender-Produkt posten.

Support-Techniker von Bitdefender überwachen neue Einträge in das Forum, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter <http://forum.bitdefender.com>. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Für den Zugriff auf den Bereich Konsumgüter klicken Sie bitte auf **Schutz für Privatanwender**.

Das Portal HOTforSecurity

Das Portal HOTforSecurity ist ein großer Fundus an Informationen rund um Computer-Sicherheit. Hier erfahren Sie mehr über die verschiedenen Bedrohungen, denen Ihr Computer während einer bestehenden Internetverbindung ausgesetzt ist (Malware, Phishing, Spams, Cyber-Kriminelle). Ein nützliches Wörterbuch hilft Ihnen, die unbekanntenen Computersicherheits-Fachausdrücke zu verstehen.



Ständig werden neue Artikel zu den neuesten Threats, aktuellen Sicherheitstrends und anderen Informationen zur Computersicherheits-Branche eingestellt, damit Sie up-to-date bleiben.

Die Adresse von HOTforSecurity ist <http://www.hotforsecurity.com>.

8.1.2. Hilfe anfordern

Nutzen Sie das Online-Support-Center, um Unterstützung anzufordern:

1. Gehen Sie zu <https://www.bitdefender.de/support/consumer.html>.
2. Durchsuchen Sie das Support-Center nach Artikeln, die eine Lösung für Ihr Problem enthalten könnten.
3. Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.
4. Sollten Sie keine entsprechende Lösung finden können, klicken Sie unten im Fenster auf **Kontakt**.
5. Im Kontaktformular können Sie ein E-Mail-Support-Ticket eröffnen oder auf weitere Kontaktoptionen zugreifen.

8.2. Kontaktinformation

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. BITDEFENDER hat sich seit 2001 einen herausragenden Ruf erarbeitet, indem es seine Kommunikation immer besser gemacht hat, um die Erwartungen unserer Kunden und Partner noch zu übertreffen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

8.2.1. Internet-Adressen

Vertrieb: vertrieb@bitdefender.de

Support-Center: <https://www.bitdefender.de/support/consumer.html>

Dokumentation: documentation@bitdefender.com

Händler vor Ort: <https://www.bitdefender.de/partners/>

Partnerprogramm: partners@bitdefender.com

Medienkontakt: pr@bitdefender.com

Karriere: jobs@bitdefender.com

Bedrohungseinsendungen: virus_submission@bitdefender.com

Spam-Einsendungen: spam_submission@bitdefender.com

Missbrauch melden: abuse@bitdefender.com



Website: <https://www.bitdefender.de>

8.2.2. Händler vor Ort

Bitdefender-Händler stehen für vertriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung.

So finden Sie einen Bitdefender-Händler in Ihrem Land:

1. Gehen Sie zu <https://www.bitdefender.de/partners/>.
2. Öffnen Sie die **Partner-Suche**.
3. Die Kontaktinformationen zum örtlichen Bitdefender Distributor sollten automatisch eingeblendet werden. Sollte dies nicht der Fall sein, so wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
4. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren. Bitte schreiben Sie uns Ihre E-Mail in Englisch, damit wir Ihnen umgehend helfen können.

8.2.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

U.S.A

Bitdefender, LLC

6301 NW 5th Way, Suite 4300

Fort Lauderdale, Florida 33309

Telefon (Geschäftsstelle&Vertrieb): 1-954-776-6262

Vertrieb: sales@bitdefender.com

Technischer Support: <https://www.bitdefender.com/support/consumer.html>

Web: <https://www.bitdefender.com>

Vereinigte Arabische Emirate

Dubai Internet City

Building 17, Office # 160

Dubai, UAE

Telefon Vertrieb: 00971-4-4588935 / 00971-4-4589186



Vertrieb EMail: mena-sales@bitdefender.com

Technischer Support: <https://www.bitdefender.com/support/consumer.html>

Website: <https://www.bitdefender.com>

Deutschland

Bitdefender GmbH

TechnoPark Schwerte

Lohbachstrasse 12

D - 58239 Schwerte

Geschäftsstelle: +49 2304 9 45 - 162

Fax: +49 2304 9 45 - 169

Vertrieb: vertrieb@bitdefender.de

Technischer Support: <https://www.bitdefender.de/support/consumer.html>

Web: <https://www.bitdefender.de>

Spanien

Bitdefender España, S.L.U.

C/Bailén, 7, 3-D

08010 Barcelona

Fax: +34 93 217 91 28

Telefon: +34 902 19 07 65

Vertrieb: comercial@bitdefender.es

Technischer Support: <https://www.bitdefender.es/support/consumer.html>

Website: <https://www.bitdefender.es>

Rumänien

BITDEFENDER SRL

Orhideea Towers, 15A Orhideelor Street, Sector 6

Bucharest

Fax: +40 21 2641799

Telefon Vertrieb: +40 21 2063470

Vertrieb EMail: sales@bitdefender.ro

Technischer Support: <https://www.bitdefender.ro/support/consumer.html>

Website: <https://www.bitdefender.ro>



Arten von böartige Software

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Bedrohung

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Bedrohungen können sich auch selbst vervielfältigen. Alle Computerbedrohungen wurden von Menschen programmiert. Eine einfache Bedrohung, die sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar eine solch einfache Bedrohung kann gefährlich sein, da sie im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Bedrohungen, die sich über Netzwerke hinweg selbst weiterversenden und Sicherheitssysteme umgehen.

Brute-Force-Angriff

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem in schneller Abfolge häufige Passwortkombinationen durchprobiert werden.

Keylogger

Ein Keylogger ist eine Anwendung, die alle Ihre Tastenanschläge aufzeichnet.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von



Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Polymorpher Virus

Eine Bedrohung, die ihre Form mit jeder Datei, die sie infiziert, ändert. Da diese Bedrohungen kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Ransomware

Bei Ransomware handelt es sich um schädliche Programme, die anfällige Systeme für den Benutzer sperren und für deren Freigabe Lösegeld erpressen. CryptoLocker, CryptoWall und TeslaWall sind nur einige Beispiele für Ransomware, die es auf Benutzercomputer abgesehen haben.

Die Infektion kann sich durch das Aufrufen einer Spam-Nachricht, das Herunterladen eines E-Mail-Anhangs oder die Installation von Anwendungen ausbreiten, ohne dass der Benutzer es überhaupt bemerkt. Ransomware-Hacker nehmen herkömmliche Benutzer und Unternehmen ins Visier.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.



Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einer Bedrohung durch ein trojanisches Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Trojaner

Ein böses Programm, das sich als eine legitime Anwendung ausgibt. Anders als Schad-Software und Würmer vervielfältigen sich Trojaner nicht selbst, können aber dennoch großen Schaden anrichten. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Bedrohungen zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.



Wörterbuchangriff

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem alle möglichen Wörter aus einem Wörterbuch als potenzielle Passwörter eingegeben werden. Dieselbe Methode wird auch verwendet um Schlüssel für verschlüsselte Nachrichten oder Dokumente zu erraten. Wörterbuchangriffe funktionieren, weil viele Benutzer kurze, leicht zu erratende Wörter als Passwörter benutzen.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.