Endpoint Security

Alles über die Endpoint Security (Antivirus) Lösung der TU Braunschweig: Bitdefender

- Bitdefender: "Sie sind gefährdet!" Guide
- Bitdefender unter Windows
  - Installation (Windows)
  - Mögliche Fehlercodes (Windows)
  - Deinstallation (Windows)
- Bitdefender unter macOS
  - Installation (macOS)
  - Mögliche Fehlercodes (macOS)
  - Deinstallation (macOS)
- Bitdefender unter Linux
  - Installation (Linux)
  - Starten eines manuellen Scans (Linux)
  - Anzeigen der Quarantäne (Linux)
  - Mögliche Fehlercodes (Linux)
  - Deinstallation (Linux)

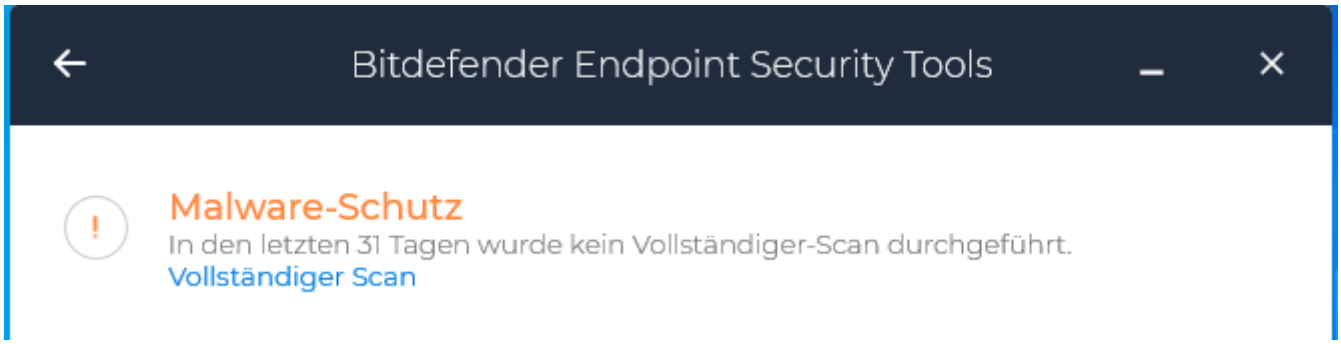
Bitdefender: "Sie sind gefährdet!" Guide



Bitdefender warnt oft mit der Meldung "Sie sind gefährdet" zu unterschiedlichsten Problemen und Fehlern.
Um hier Klarheit zu schaffen, ob das Gerät wirklich gefährdet ist oder nicht finden Sie hier ein paar Informationen.
Sollte Ihnen trotzdem unklar sein, warum Sie eine Meldung bekommen, schreiben Sie bitte ein Ticket an den IT-Service-Desk.

Probleme und Meldungen:

- "**Malware-Schutz**: In den letzten 31 Tagen wurde kein Vollständiger-Scan durchgeführt."



Diese Meldung lässt sich einfach beheben, in dem Sie "Vollständiger Scan" anklicken und den Scan durchführen lassen.
Hinweis: Ein vollständiger Scan kann einiges an Ressourcen Ihres Gerätes in Anspruch nehmen und dieses evtl. langsamer machen.

- "**Update**: Das Produkt ist nicht auf dem neusten Stand"

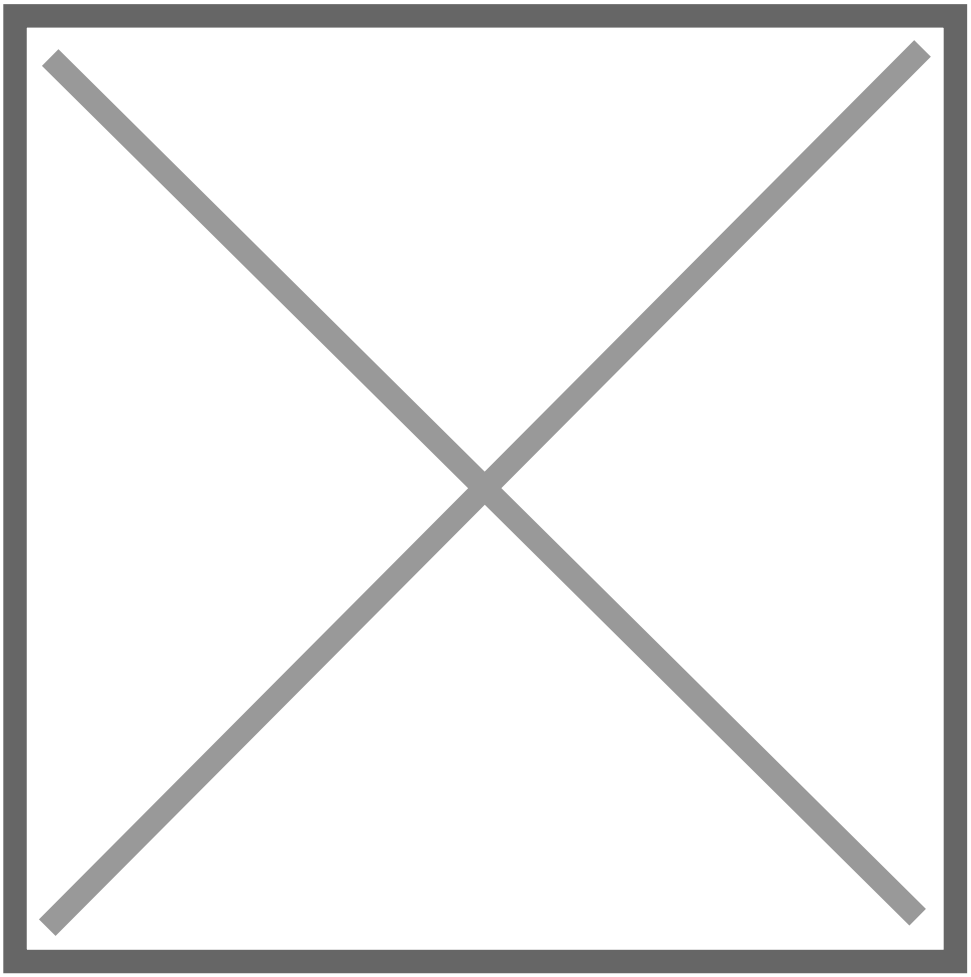


Aktualisieren Sie Bitdefender über das Hauptfenster -> Radar-Icon (rechts) -> Überprüfen auf Updates (unten)

- "Es besteht keine Verbindung zum Vorfall-Server"

Zur Zeit besteht keine Verbindung zum Bitdefender-Server. Bitte überprüfen Sie Ihre Verbindung zum Netzwerk der
TU Braunschweig.

- Bitdefender blockiert Webseite



Sollten Sie auf einer **HTTP-Webseite** einen Nutzernamen und ein Passwort eingegeben haben, wurden Sie von Bitdefender blockiert, da diese **ohne HTTPS-Verschlüsslung unsicher übertragen** werden würden.

- Kodierte Fehlermeldungen

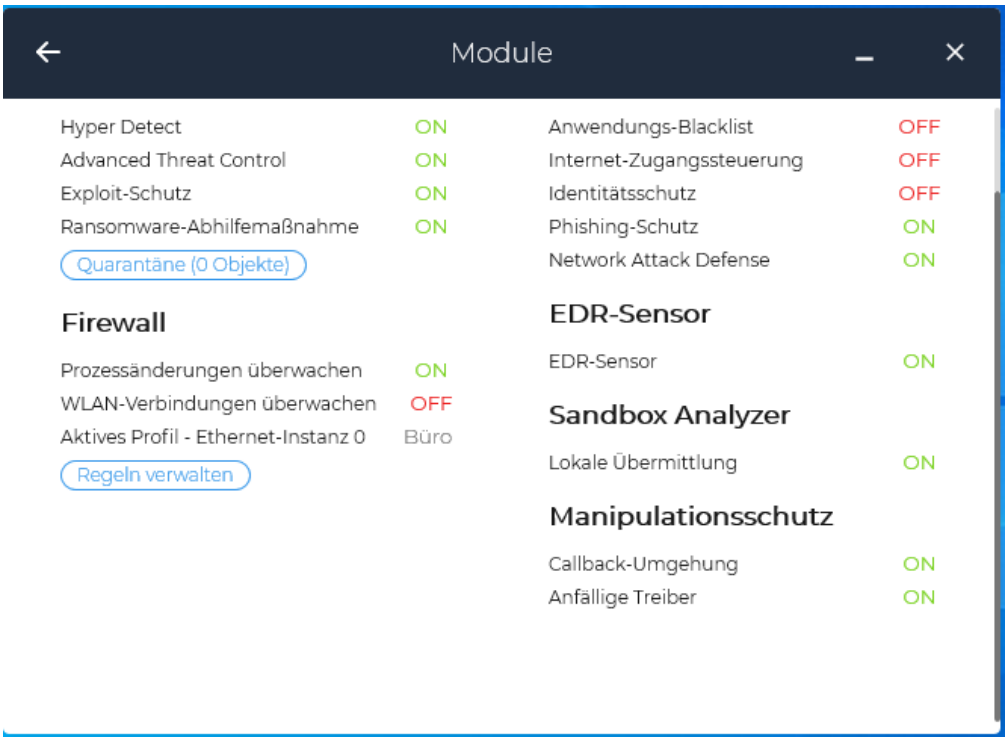
Es ist möglich, dass während der Installation und auch während des Betriebs Fehler in Bitdefender angezeigt werden. Entsprechend sind hier die häufigsten Fehlercodes als Hilfestellung aufgelistet.

Code	Kategorie	Fehler	Lösungsmöglichkeiten
-1002	Updates	Die Adresse des Bitdefender-Servers konnte nicht aufgelöst werden.	Überprüfen Sie Ihre Netzwerk- und DNS-Einstellungen und die Verbindung zu goku.rz.tu-bs.de.

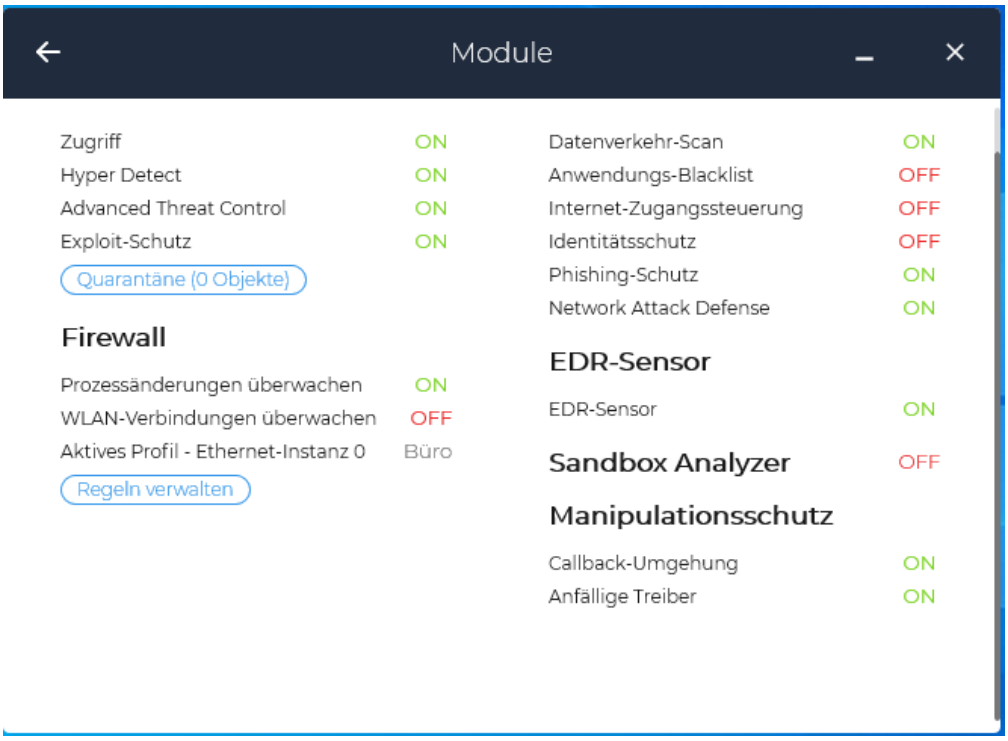
-1011	Updates	Time out beim Erreichen des Update Servers.	Überprüfen Sie Ihre Netzwerk-Einstellungen bzgl. der Verbindung zu goku.rz.tu-bs.de und ob der Port 7074 in Ihrer Firewall geöffnet wurde.
-1018	Updates	Fehler beim Herunterladen der Update Dateien.	Überprüfen Sie Ihre Netzwerk-Einstellungen bzgl. der Verbindung zu goku.rz.tu-bs.de und ob der Port 7074 in Ihrer Firewall geöffnet wurde. Falls eine Verbindung besteht und Sie diesen Fehler trotzdem bekommen, schreiben Sie bitte ein Ticket an den IT-Service-Desk.
-2011	Updates	Ein Update-Vorgang ist fehlgeschlagen. Bitte versuchen Sie es später noch einmal.	Überprüfen Sie Ihre Netzwerk-Einstellungen bzgl. der Verbindung zu goku.rz.tu-bs.de und ob der Port 7074 in Ihrer Firewall geöffnet wurde. Falls eine Verbindung besteht und Sie diesen Fehler trotzdem bekommen, schreiben Sie bitte ein Ticket an den IT-Service-Desk.

Bitdefender Module:

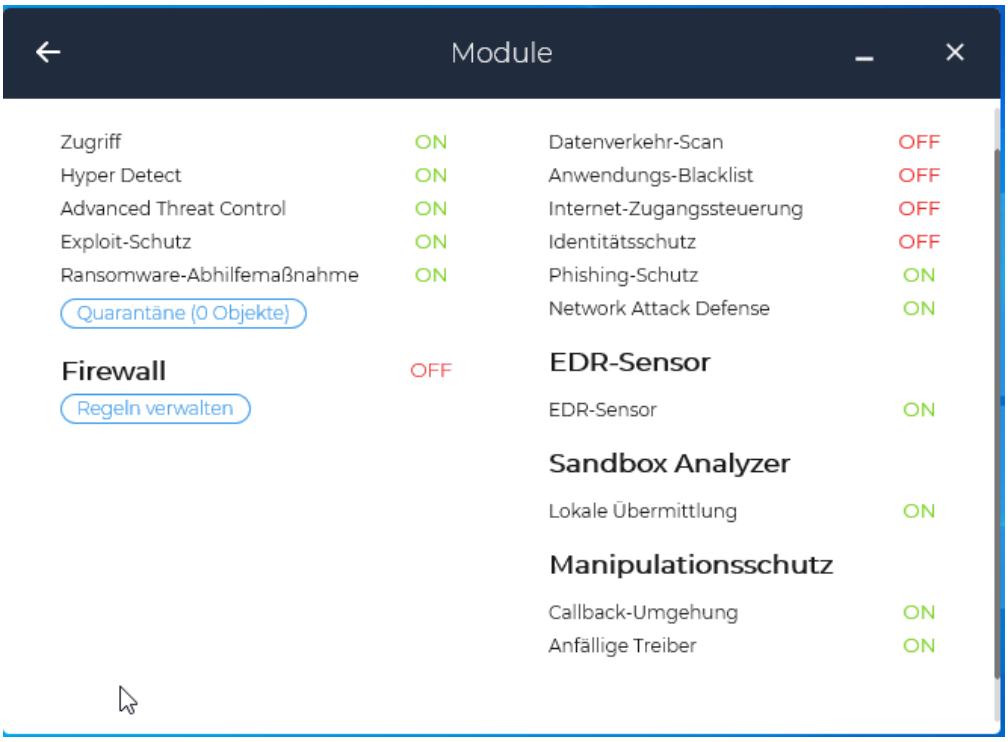
Im Folgenden können Sie die aktivierten / deaktivierten Module Ihrer Bitdefender Installation mit den hier gezeigten Bildern vergleichen. Beachten Sie dabei, dass nicht alle Module unter jedem Betriebssystem verfügbar sind und dass es für Windows **drei unterschiedliche Pakete** für Mitarbeiter, Studenten und Server gibt.
Installationen unter Windows:
Bitdefender Module unter Windows: Mitarbeiter Paket



Bitdefender Module unter Windows: Studenten Paket

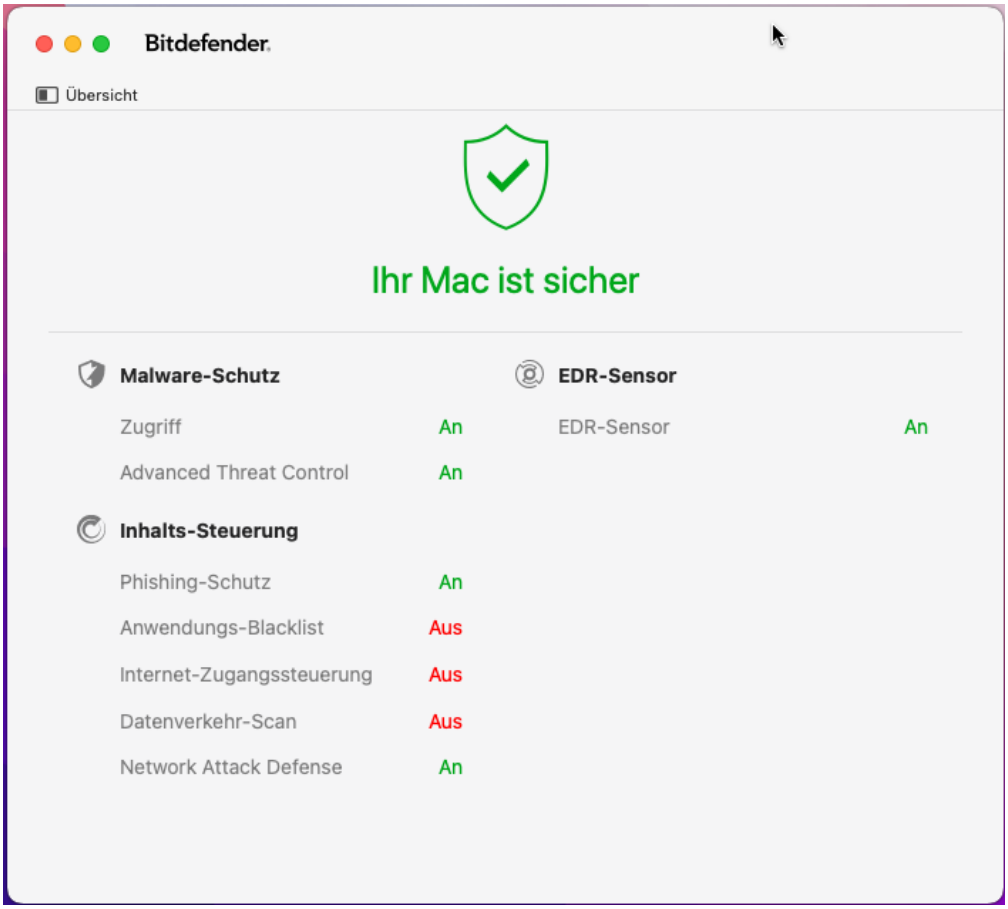


Bitdefender Module unter Windows: Server Paket

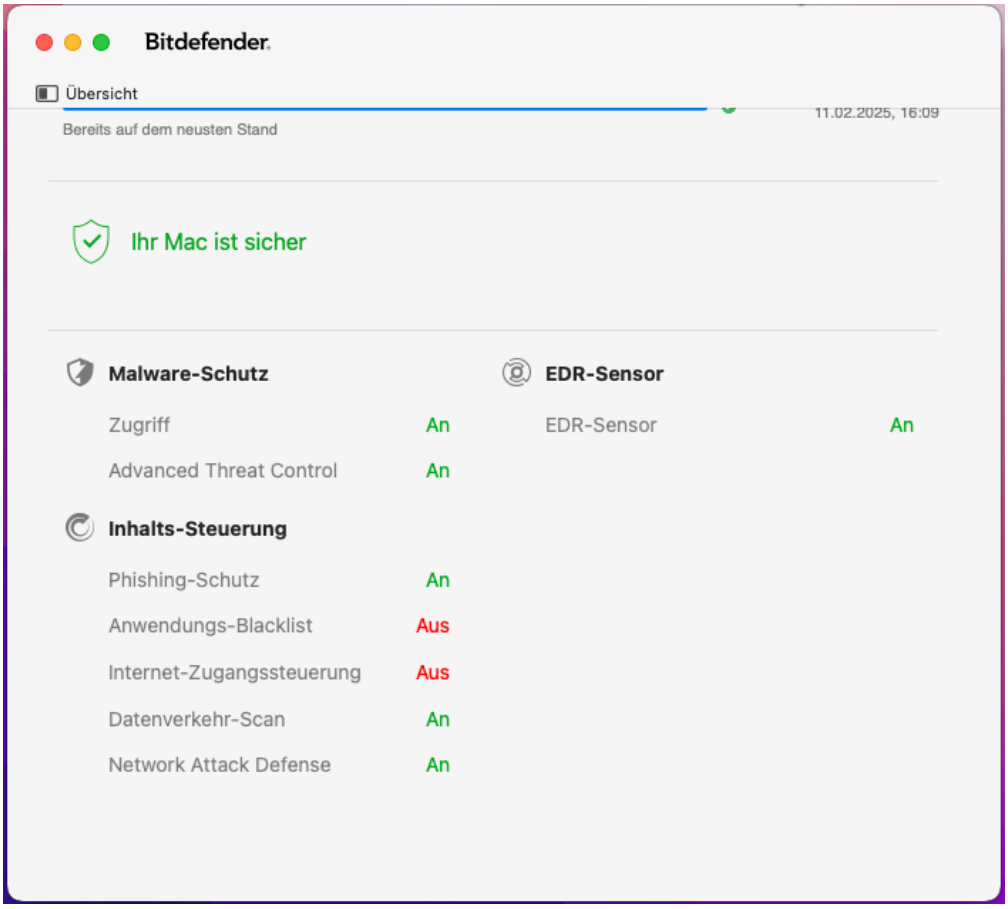


Hinweis: Das Firewall-Modul funktioniert grundsätzlich nur unter Client Windows Versionen (alle Windows 10 / 11 Versionen), aber nicht unter Windows Server. Dies ist von Bitdefender so gebaut.

Installationen unter MacOS:
Bitdfender Module unter MacOS: Mitarbeiter Paket



Bitdefender Module unter MacOS: Studenten Paket



Bitdefender unter Windows

Installation, Deinstallation und mögliche Fehler für Bitdefender unter Windows.

Installation (Windows)

Auf der Download-Seite des Gauß-IT-Zentrums befindet sich ein vorkonfiguriertes Installationspaket für Bitdefender Endpoint Security für Windows zum Herunterladen. Bitdefender Endpoint Security löst Sophos Endpoint Security als Nachfolger ab. Es ist geeignet für alle Windows-Versionen ab Windows 7 mit Service Pack 1. Insbesondere gilt das natürlich für Windows 8, 8.1, 10 und Windows 11. Die Installation erfolgt in deutscher Sprache, sie lässt sich aber problemlos anpassen.

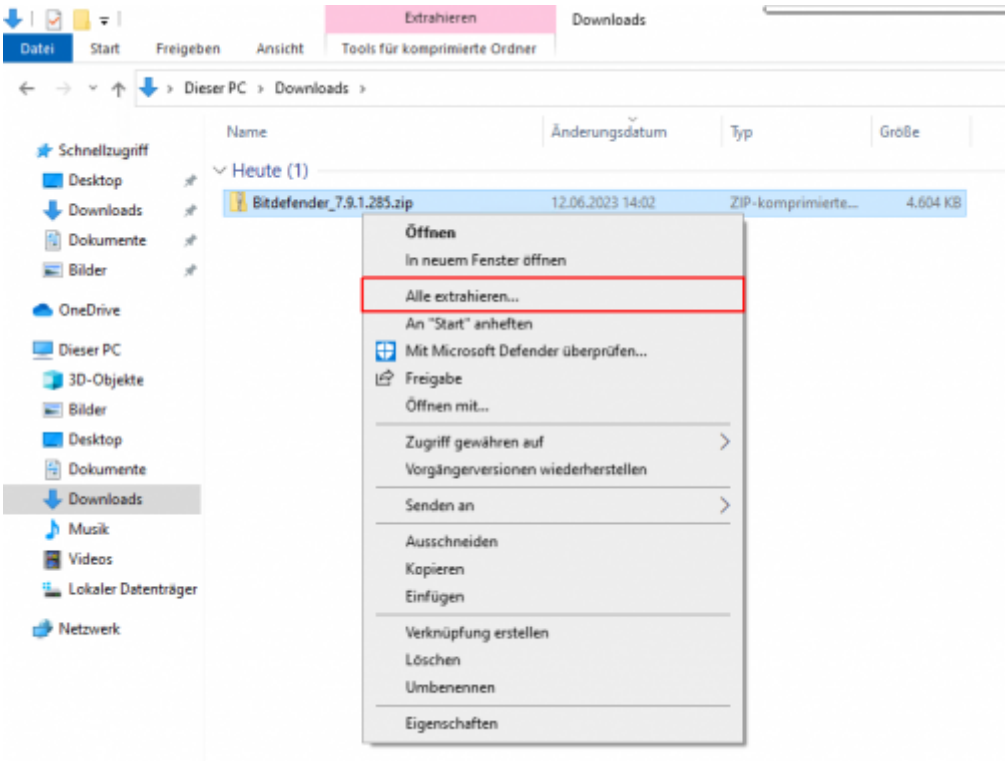
Diese Installationsanleitung ist gleichermaßen auf Windows Server anwendbar.
Das Serverpaket kann auf allen Windows Server Versionen ab Windows Server 2008 R2 installiert werden, einschließlich der Core Versionen ohne grafische Oberfläche.

> **Für die Installation muss sich Ihr System im Netzwerk der TU Braunschweig befinden.**
> Während der Installation von Bitdefender Endpoint Security wird Sophos Endpoint Security, sowie andere Virenscanner, automatisch deinstalliert. Diese müssen im Vorfeld nicht manuell deinstalliert werden.
> Die Installation dauert einige Minuten und wird im Hintergrund ausgeführt.
> Nach der Installation sollte das System neu gestartet werden.
> Starten Sie danach einen vollständigen Viren-Scan des Systems mit Bitdefender Endpoint Security.
>
> Diese Installationsanleitung gilt nicht für vom Gauß-IT-Zentrum verwaltete Geräte.

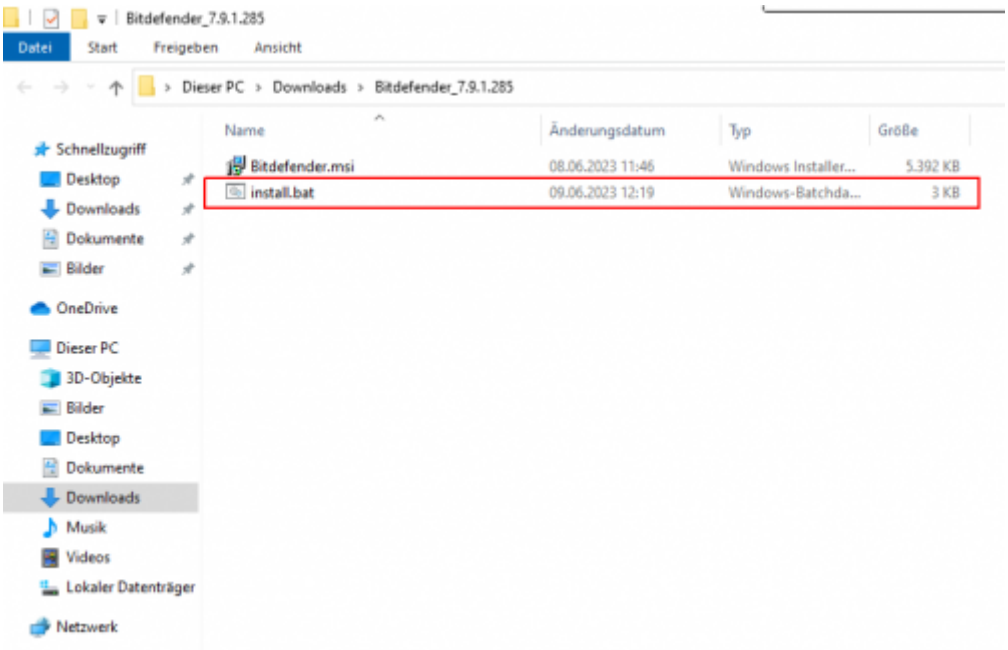
Rufen Sie mit Ihrem Internet-Browser https://www.tu-braunschweig.de/it/software auf und melden Sie sich unter **[Schnellzugriff]** an. Dann navigieren Sie unten zum Punkt **Virenscanner**. Klicken Sie auf **[Virenscanner]**. Laden Sie das Zip-Archiv bei **Windows** herunter und entpacken Sie dieses. Gehen Sie dann in den Ordner **Bitdefender_windows** und starten Sie die Installation mit einem Doppelklick auf das Installationsskript **install.bat**. Für die Installation benötigen Sie Administratorrechte.

Installation

Entpacken Sie das heruntergeladene Zip-Archiv über das Kontextmenü (Rechtsklick → „Alle extrahieren“):



Gehen Sie dann in den neuen Ordner und führen Sie das Installationsskript **install.bat** mit einem Doppelklick aus:

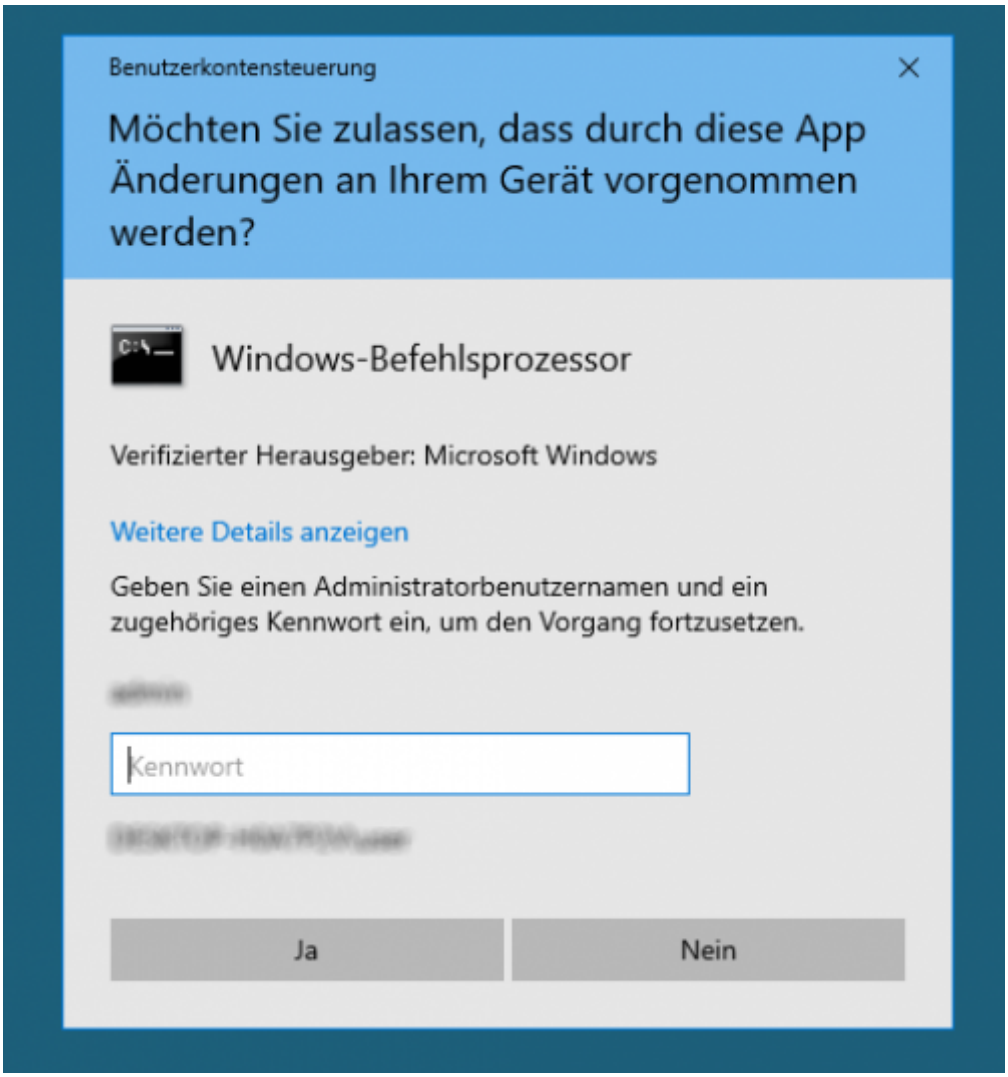


Gegebenenfalls müssen Sie die Ausführung bestätigen, indem Sie auf **[Weiteren Informationen]** und dann auf **[Trotzdem ausführen]** klicken:





Bestätigen Sie die Installation mit der Eingabe einer Administratorkennung:

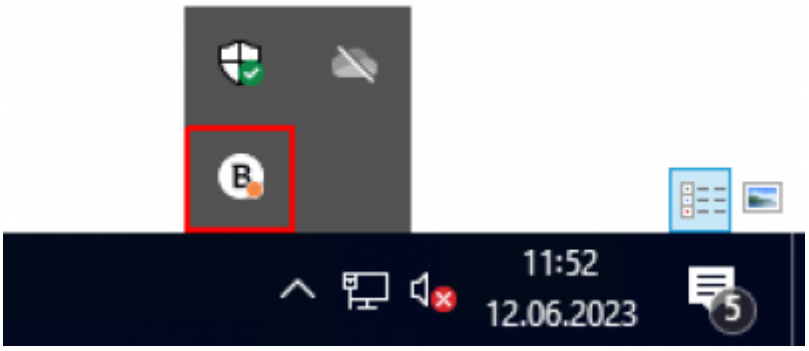


Nachdem das Fenster verschwunden ist, warten Sie einige Minuten, bis die Installation abgeschlossen und Bitdefender in der Taskleiste unter den ausgeblendeten Symbolen zu finden ist. Wenn Bitdefender dort nach zehn Minuten nicht zu finden ist, starten Sie das System neu.

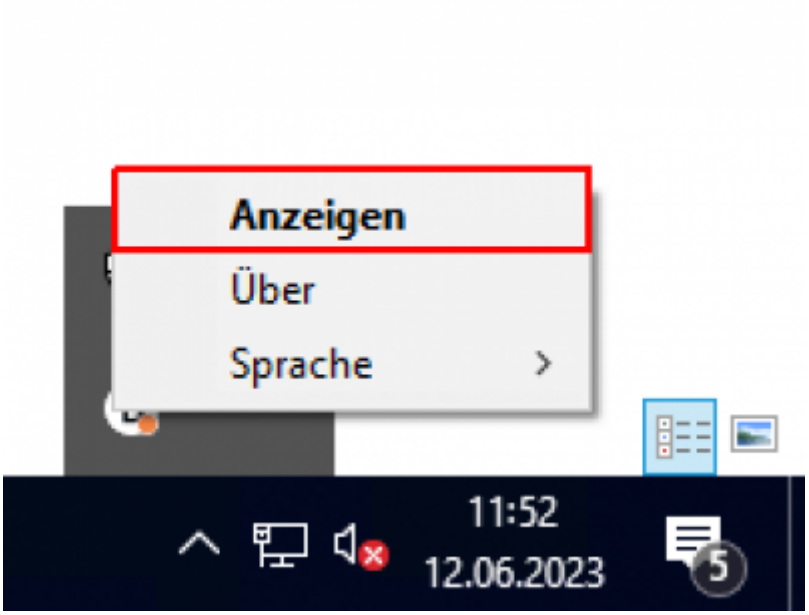
Inbetriebnahme

Hier finden Sie die Steuerung zu Bitdefender:



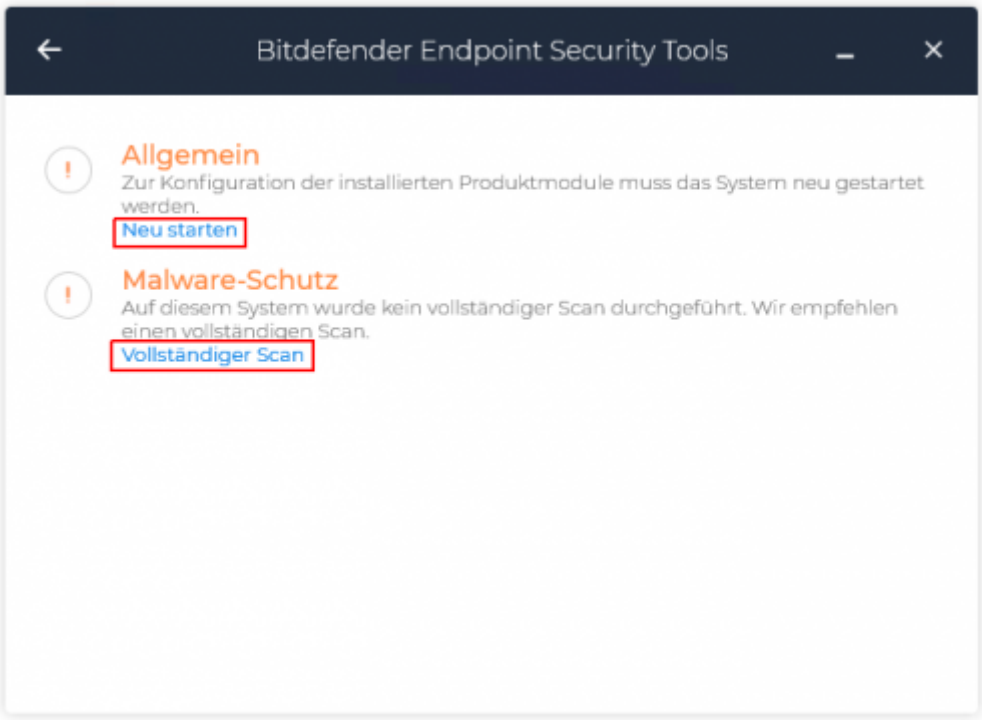


Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol und danach auf **[Anzeigen]**, um zur Client-Steuerung zu gelangen.



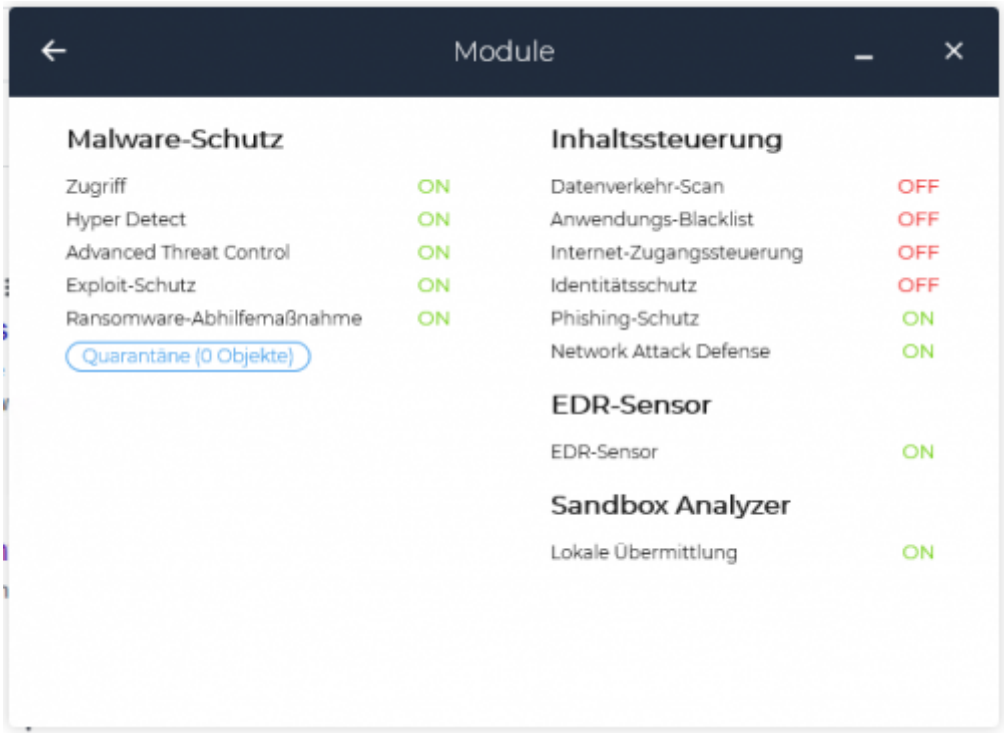
Klicken Sie im Menü auf **[Alle beheben]** und dann auf **[Vollständiger Scan]**, um das System initial zu scannen.



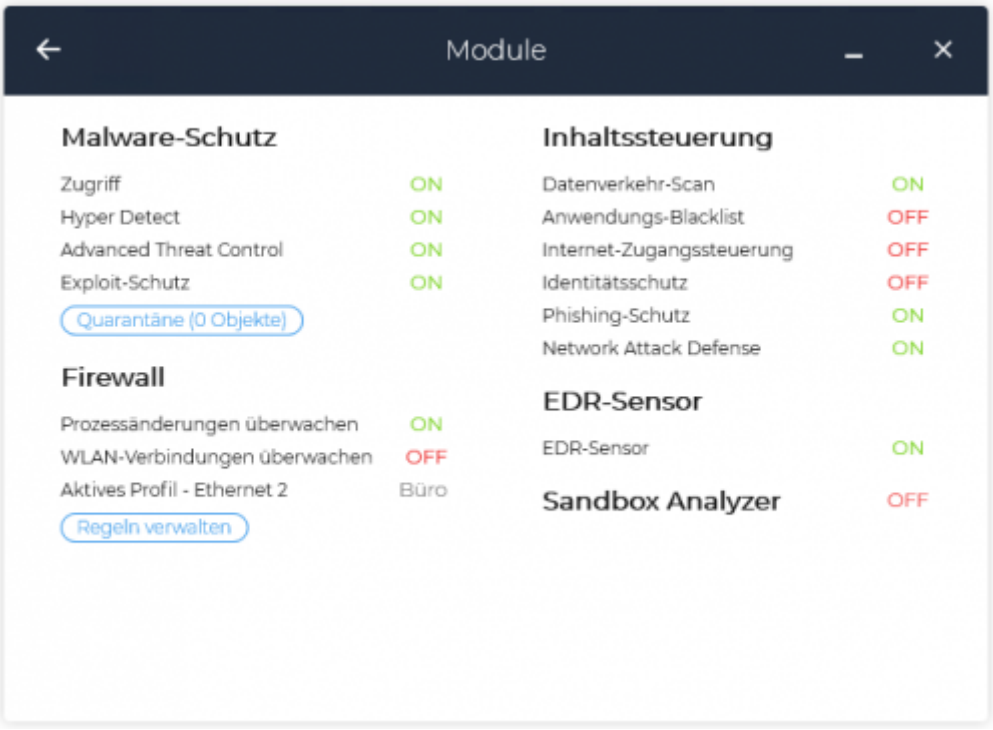


Aktive Bitdefender Module

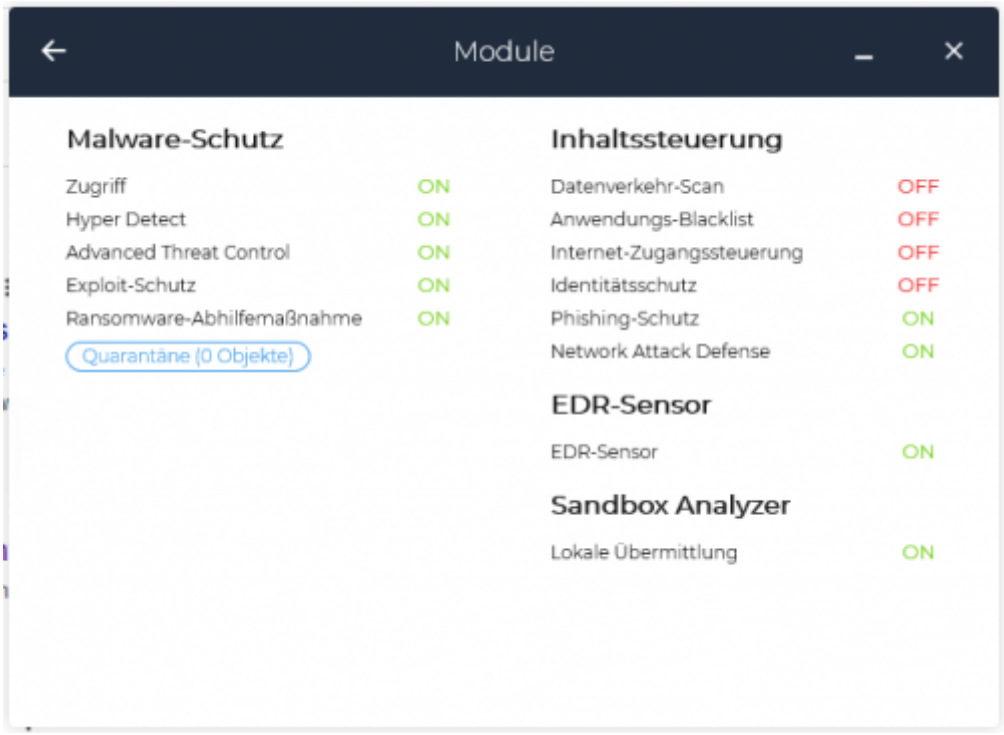
Für Bitdefender werden verschiedene Pakete verteilt, welche unter anderem verschiedene Module in Bitdefender aktiviert haben.
Nach der Installation des Pakets für ***Mitarbeiter*** sollten die Module, wie unten aufgeführt, an oder aus sein:



Nach der Installation des Pakets für ***Studenten*** sollte die Liste der Module wie folgt aussehen:



Nach der Installation des Pakets für ***Server*** sollte die Liste wie folgt aussehen:



Hinweis: Das Firewall-Modul ist nicht für Windows Server-Versionen verfügbar. Gleichgültig welches Paket Sie auf Windows Server einsetzen.

Mögliche Fehlercodes (Windows)

Es ist möglich, dass während der Installation und auch während des Betriebs Fehler in Bitdefender angezeigt werden. Entsprechend sind hier die häufigsten Fehlercodes als Hilfestellung aufgelistet.

Code	Fehler	Lösungsmöglichkeiten
-1002	Die Adresse des Bitdefender-Servers konnte nicht aufgelöst werden.	Überprüfen Sie Ihre Netzwerk- und DNS-Einstellungen und die Verbindung zu goku.rz.tu-bs.de.
-1011	Time out beim Erreichen des Update Servers.	Überprüfen Sie Ihre Netzwerk-Einstellungen bzgl. der Verbindung zu goku.rz.tu-bs.de und ob der Port 7074 in Ihrer Firewall geöffnet wurde.
-1018	Fehler beim Herunterladen der Update Dateien.	Überprüfen Sie Ihre Netzwerk-Einstellungen bzgl. der Verbindung zu goku.rz.tu-bs.de und ob der Port 7074 in Ihrer Firewall geöffnet wurde. Falls eine Verbindung besteht und Sie diesen Fehler trotzdem bekommen, schreiben Sie bitte ein Ticket an den IT-Service-Desk.

Deinstallation (Windows)

Öffnen Sie die Windows Einstellungen, gehen Sie zu **[Apps]** und klicken Sie **[Bitdefender Endpoint Security Tools]** an.
Drücken Sie anschließend auf **[Deinstallieren]**.
Für die Deinstallation werden Administratorrechte benötigt.
Bestätigen Sie die Deinstallation im nächsten Fenster, indem Sie auf **[Deinstallieren]** und dann auf **[Fortfahren]** klicken.

Bitdefender unter macOS

Installation, Deinstallation und mögliche Fehler für Bitdefender unter macOS.

Installation (macOS)

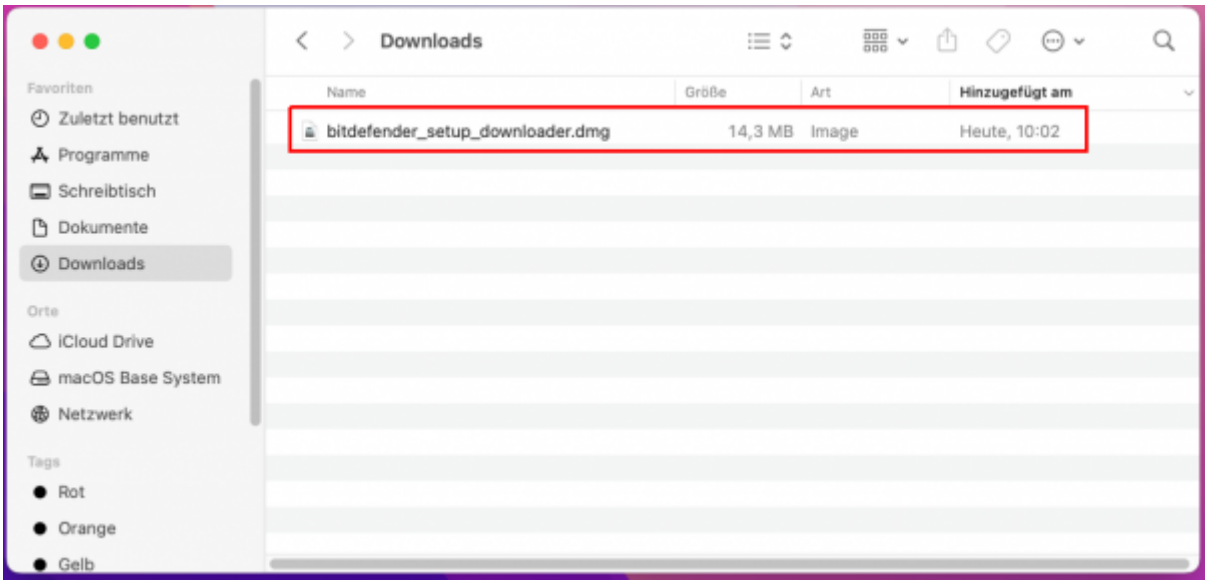
Auf der Download-Seite des Gauß-IT-Zentrums befindet sich ein vorkonfiguriertes Installationspaket für Bitdefender Endpoint Security für MacOS zum Herunterladen. Bitdefender Endpoint Security löst die Sophos Endpoint Security als Nachfolger ab. Es ist geeignet für alle MacOS-Versionen ab MacOS Mojave (10.14). Dies gilt natürlich auch für MacOS Catalina (10.15), MacOS Big Sur (11.x), MacOS Monterey (12.x) und MacOS Ventura (13.x).

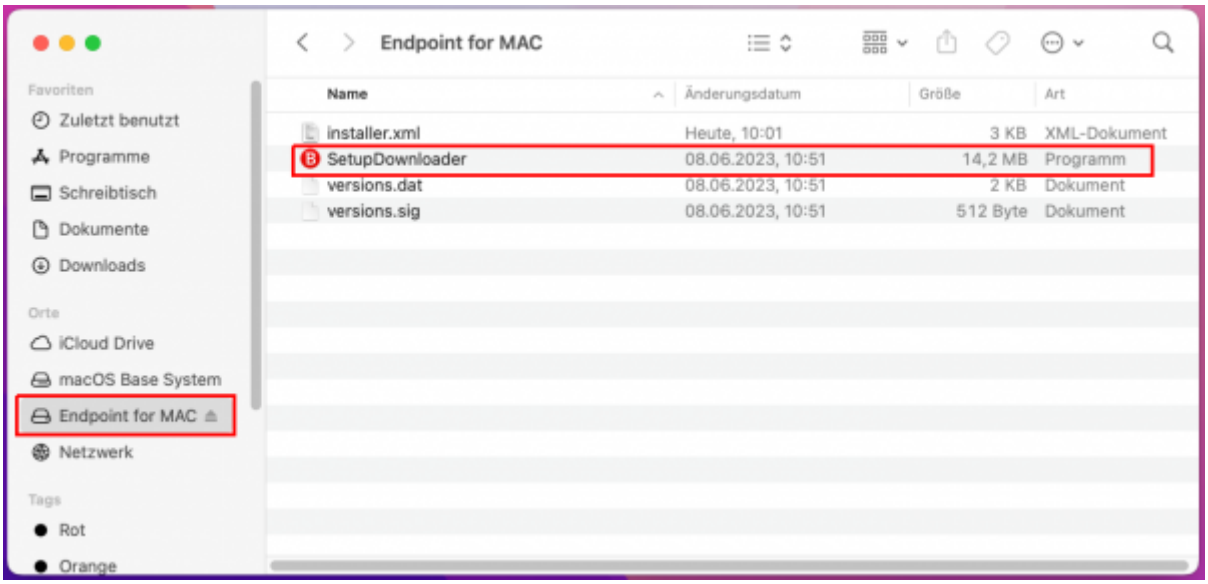
> **Für die Installation muss sich Ihr System im Netzwerk der TU Braunschweig befinden.**
> Während der Installation von Bitdefender Endpoint Security wird Sophos Endpoint Security, sowie andere Virenscanner, automatisch deinstalliert. Diese müssen im Vorfeld nicht manuell deinstalliert werden.
> Nach der Installation sollte das System gegebenenfalls neu gestartet werden.
> Starten Sie danach einen „System-Scan“ des Systems mit Bitdefender Endpoint Security.

Navigieren Sie mit Ihrem Internet-Browser zu https://www.tu-braunschweig.de/it/downloads/software/gitz-dienste und melden Sie sich unter **[Schnellzugriff]** an. Klicken Sie auf **[Virenscanner]**. Laden Sie das DMG-Archiv bei **MacOS** herunter und öffnen Sie dieses. Starten Sie die Installation mit einem Doppelklick auf das Installationsprogramm **[SetupDownloader]**. Für die Installation benötigen Sie Administratorrechte. Des Weiteren müssen Sie das Hinzufügen von Proxy-Konfigurationen und Systemerweiterungen erlauben, damit Bitdefender Endpoint Security vollumfänglich funktioniert.

Installation

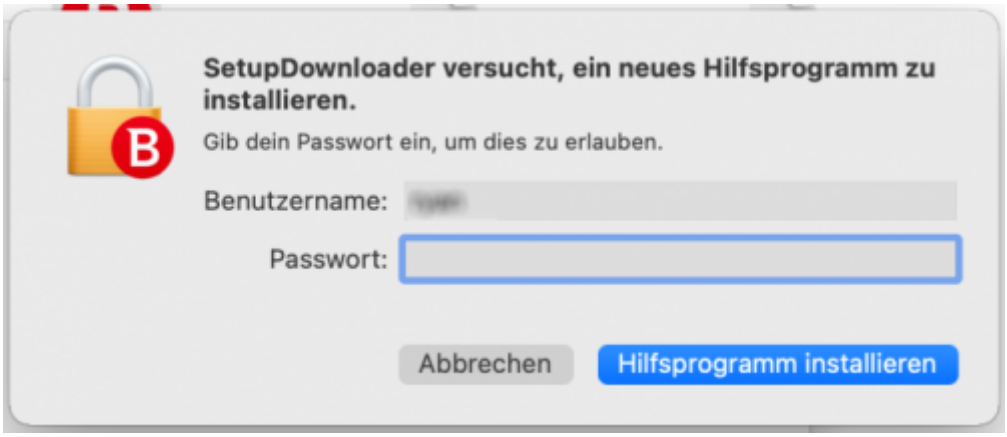
Gehen Sie im Finder zu **[Downloads]** und öffnen Sie die **[bitdefender_setup_downloader.dmg]**.
Gehen Sie dann unter **[Orte]**→ **[Endpoint for MAC]** und starten die Datei „SetupDownloader“.





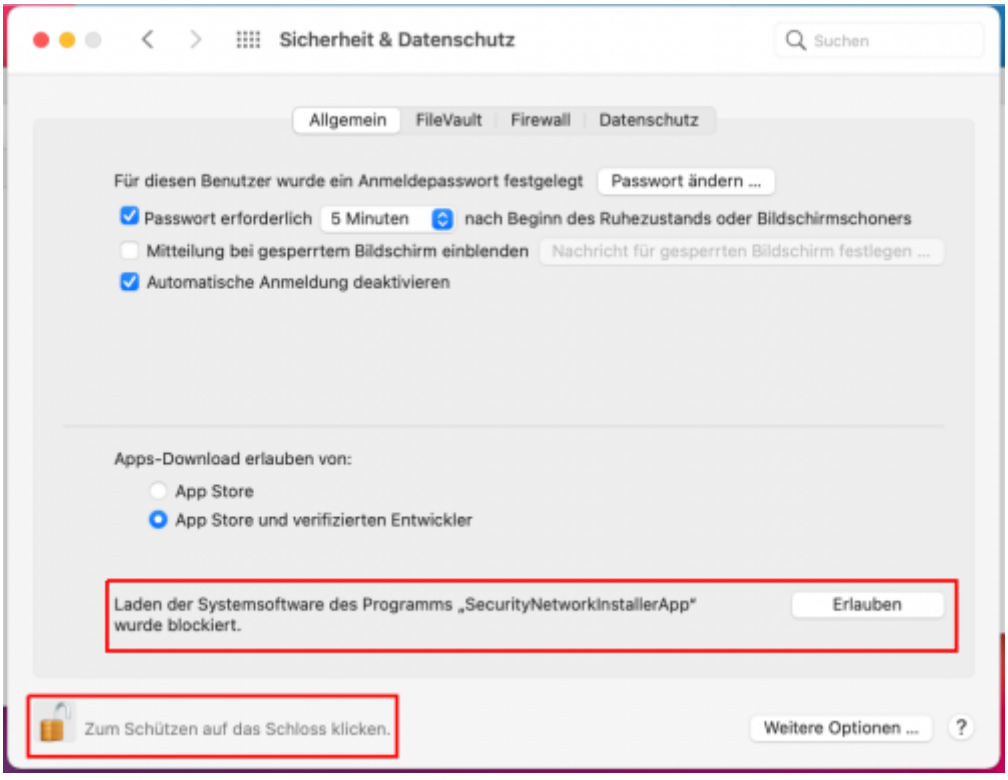
Bestätigen Sie die Ausführung und geben Sie Ihre Administratorkennung ein, um die Installation zu beginnen.



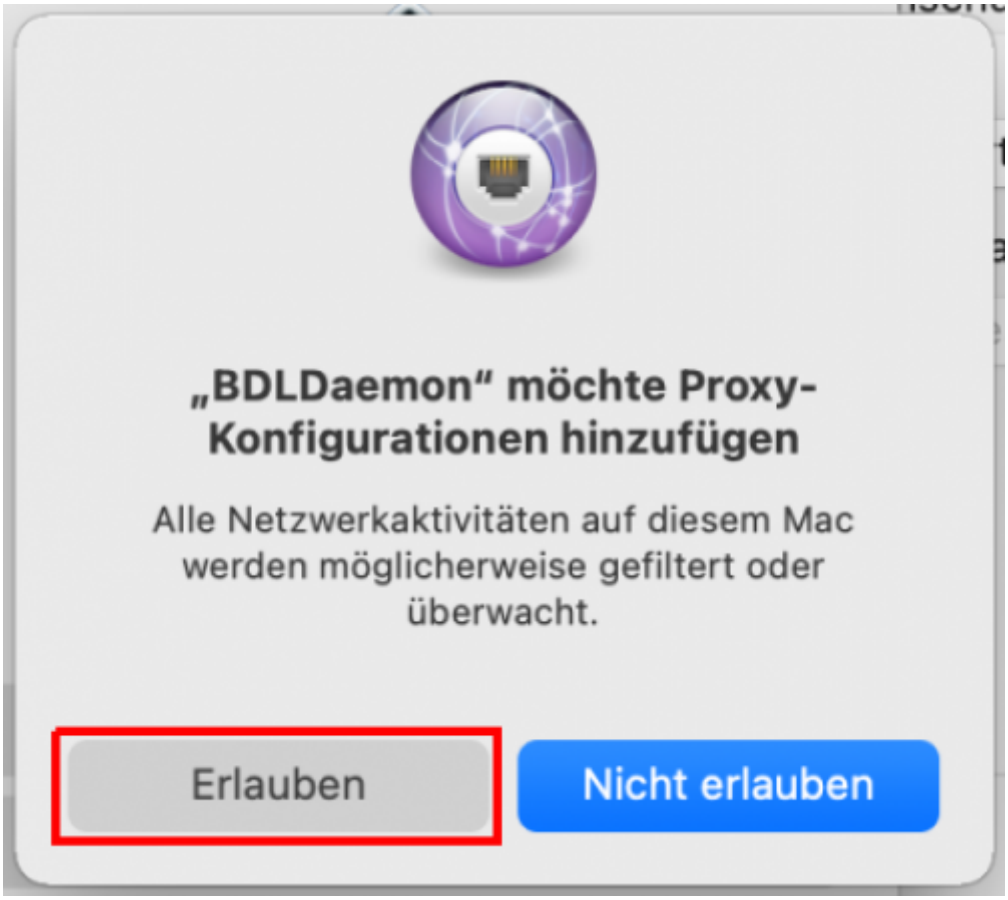


Nach der Installation werden Sie dazu aufgefordert Sicherheitseinstellungen an Ihrem Gerät zu ändern.
Öffnen Sie dazu die Systemeinstellungen **[Sicherheit]** und entsperren Sie diese über das Schloss mit Ihrer Administratorkennung.
[Erlauben] Sie das Laden des Programms „SecurityNetworkInstallerApp“.

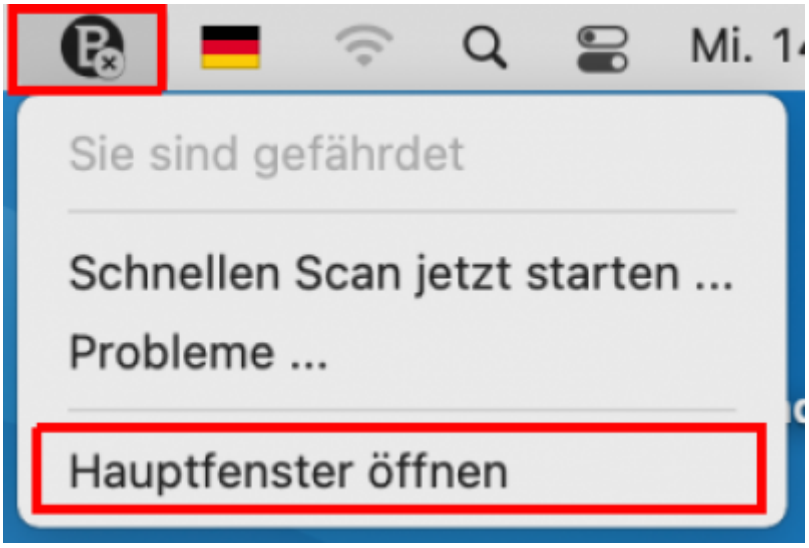


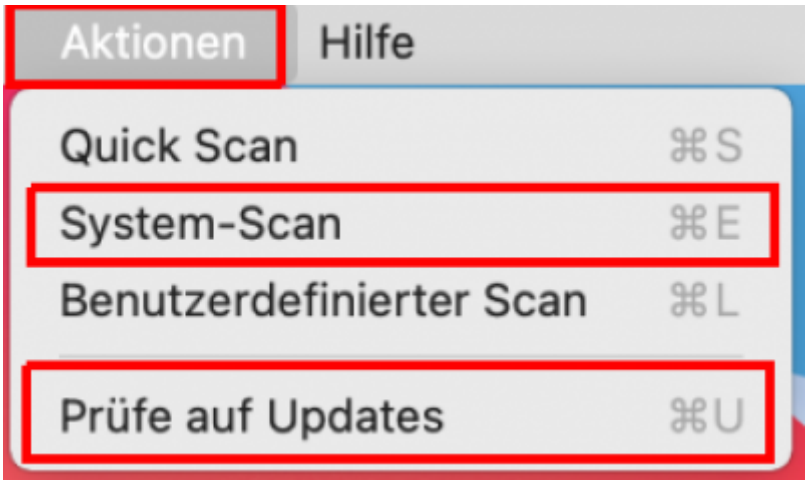


Des Weiteren werden Sie dazu aufgefordert Proxy-Konfigurationen von „BDLDaemon“ zu **[erlauben]**.
Erlauben Sie dies.



Sobald Bitdefender installiert wurde, öffnen Sie das Hauptfenster über das Bitdefender-Icon in der Taskleiste.
Starten Sie dann über **[Aktionen]** in der Taskleiste die Prüfung auf Updates und einen **[System-Scan]**.

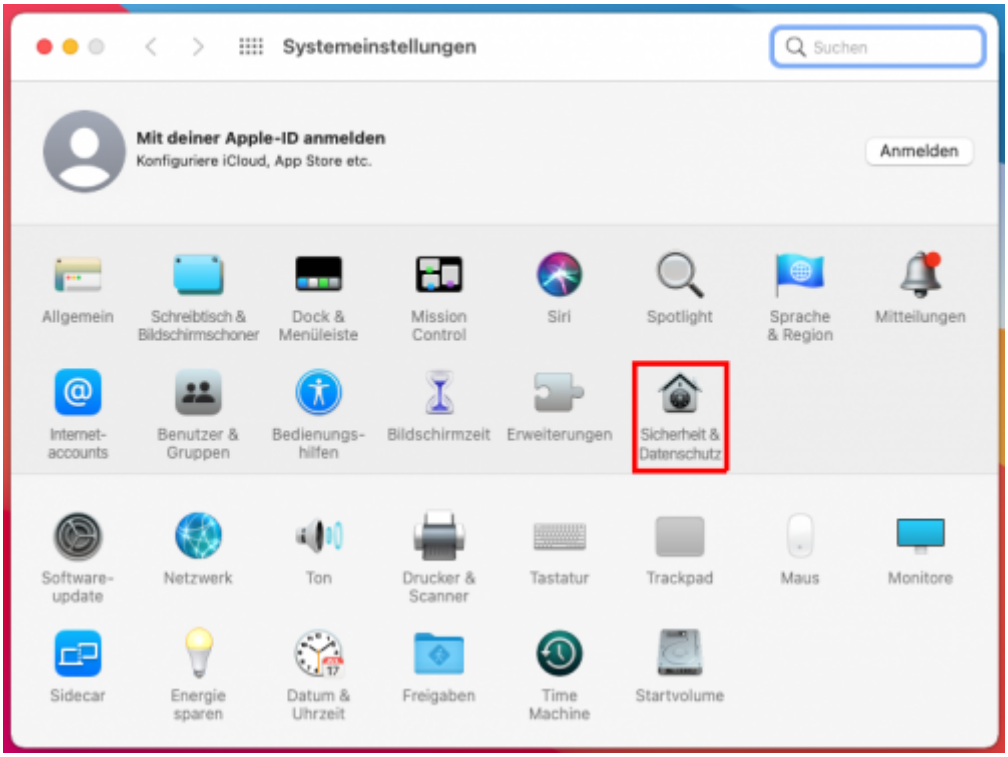




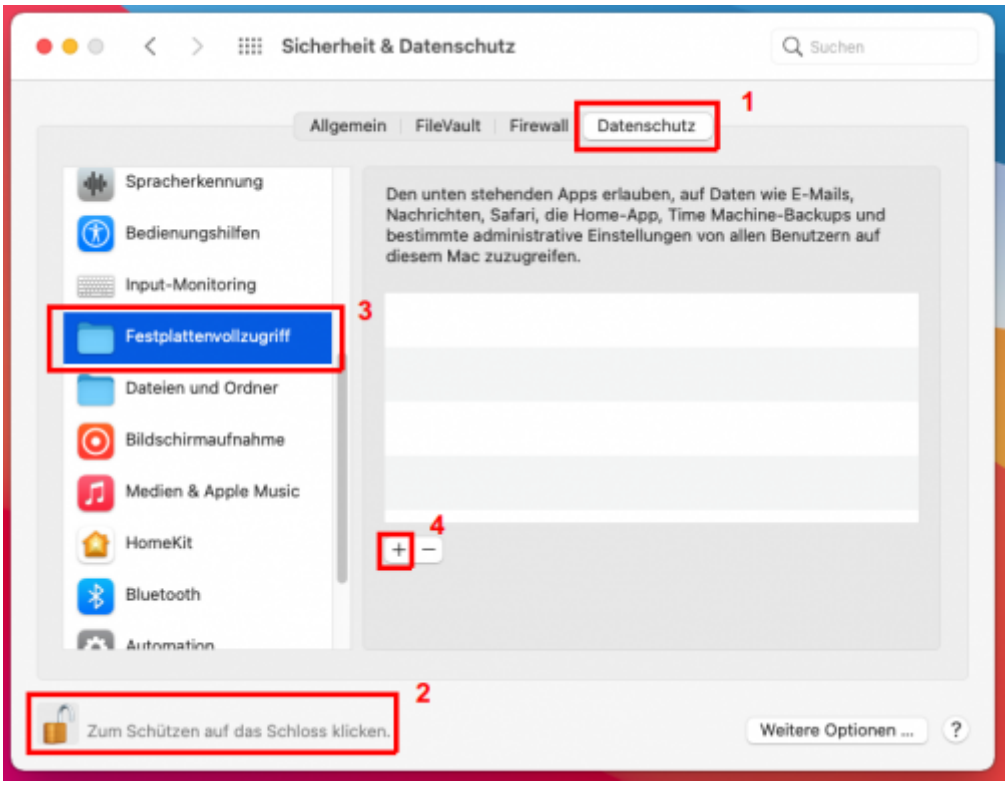
Festplattenvollzugriff für Bitdefender

Damit Bitdefender vollumfänglich funktionieren kann, benötigt dieser vollständigen Festplattenzugriff.
Nur wenn Bitdefender nachfragt, sollten Sie Bitdefender den Zugriff darauf erlauben.

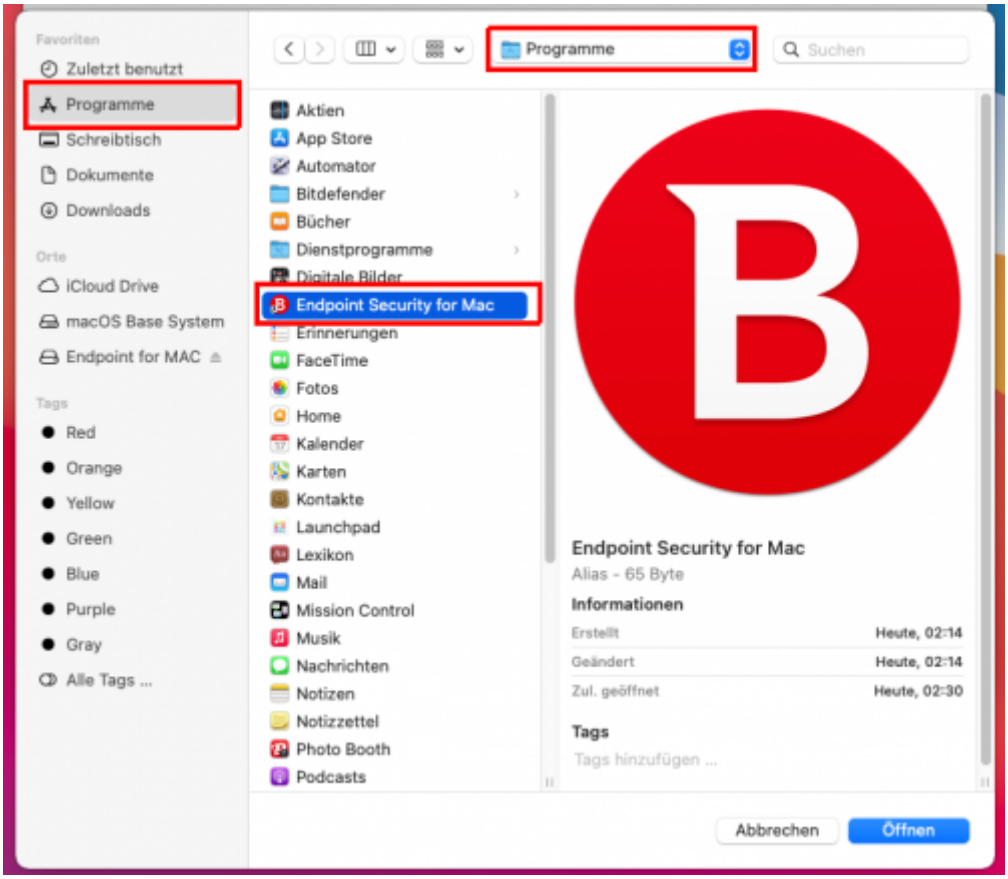
Um den Festplattenzugriff für Bitdefender zu erlauben, öffnen Sie die **[Systemeinstellungen]** und gehen zu **[Sicherheit und Datenschutz]**.



Gehen Sie dort zum Reiter **[Datenschutz]** und entsperren Sie das Menü über das Schloss.
Suchen Sie in der linken Spalte nach **[Festplattenvollzugriff]** und fügen Sie über das Plus die benötigten Programme hinzu.



Suchen Sie links unter [**Programme]** nach **[Bitdefender Security for Mac]**.
Bestätigen Sie dies anschließend mit Ihrem Passwort.

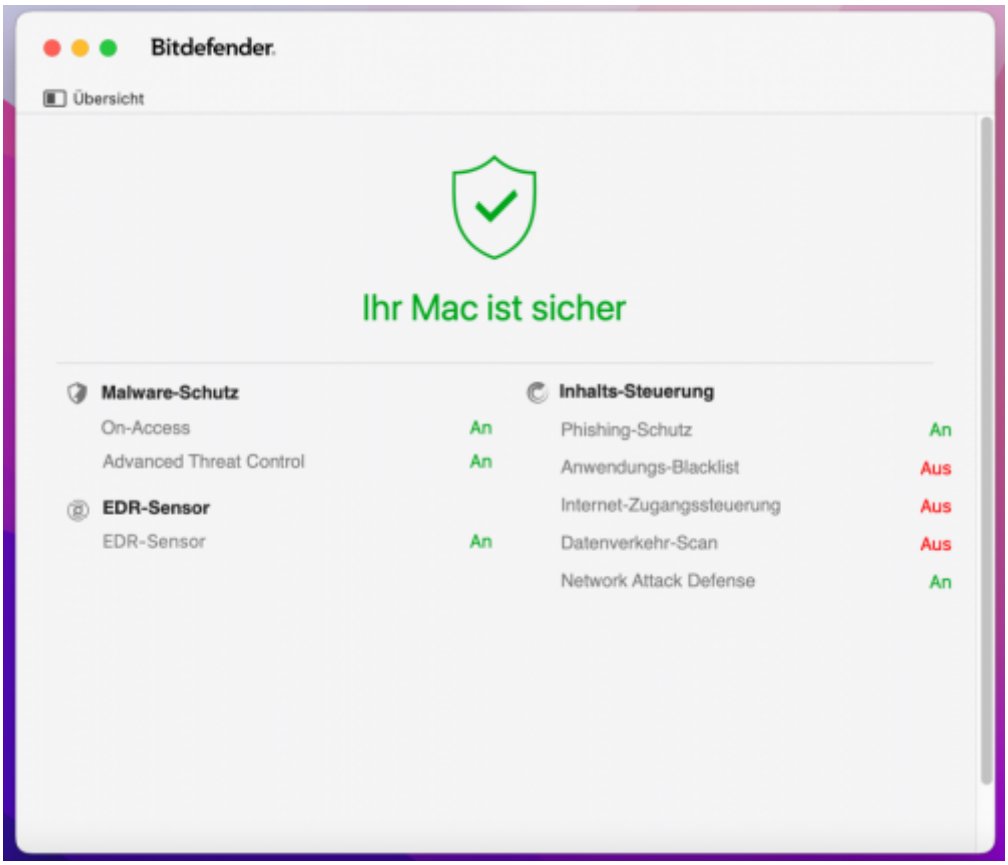


Sollte Bitdefender danach immer noch explizit nach **BDLDaemon.app** fragen, fügen Sie dies ebenfalls dort hinzu.
Wählen Sie ganz oben bei Programme Ihre **Festplatte** aus.

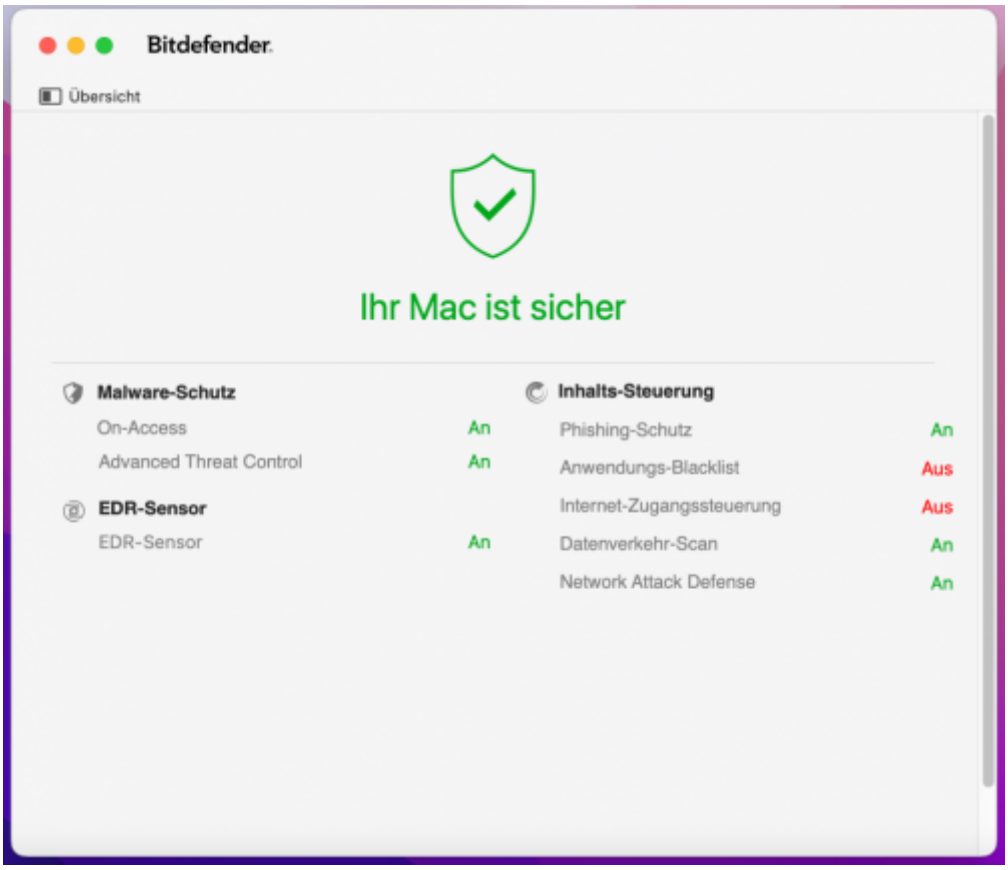
Navigieren Sie zu **[Library] → [Bitdefender] → [AVP] → [product] → [bin] → [BDLDaemon]**, um diesen Pfad hinzuzufügen.

Aktive Bitdefender Module

Für Bitdefender werden verschiedene Pakete verteilt, welche unter anderem verschiedene Module in Bitdefender aktiviert haben.
Nach der Installation des Pakets für Mitarbeiter sollten die Module, wie unten aufgeführt an oder aus sein:



Nach der Installation des Pakets für Studenten sollten die Moduleinstellungen wie folgt aussehen:


Bitdefender
Übersicht
Ihr Mac ist sicher
Malware-Schutz
On-Access
An
Advanced Threat Control
An
EDR-Sensor
EDR-Sensor
An
Inhalts-Steuerung
Phishing-Schutz
An
Anwendungs-Blacklist
Aus
Internet-Zugangssteuerung
Aus
Datenverkehr-Scan
An
Network Attack Defense
An

Mögliche Fehlercodes (macOS)

Es ist möglich, dass während der Installation und auch während des Betriebs Fehler in Bitdefender angezeigt werden. Entsprechend sind hier die häufigsten Fehlercodes als Hilfestellung aufgelistet.

Code	Fehler	Lösungsmöglichkeiten
-1002	Die Adresse des Bitdefender-Servers konnte nicht aufgelöst werden.	Überprüfen Sie Ihre Netzwerk- und DNS-Einstellungen und die Verbindung zu goku.rz.tu-bs.de
-1011	Time out beim Erreichen des Update Servers	Überprüfen Sie Ihre Netzwerk-Einstellungen bzgl. der Verbindung zu goku.rz.tu-bs.de und ob der Port 7074 in Ihrer Firewall geöffnet wurde
-1018	Fehler beim Herunterladen der Update Dateien	Überprüfen Sie Ihre Netzwerk-Einstellungen bzgl. der Verbindung zu goku.rz.tu-bs.de und ob der Port 7074 in Ihrer Firewall geöffnet wurde. Falls eine Verbindung besteht und Sie diesen Fehler trotzdem bekommen, schreiben Sie bitte ein Ticket an den IT-Service Desk

Deinstallation (macOS)

Öffnen Sie den Finder, gehen Sie zu **[Programme]** → **[Bitdefender]** (Ordner) und führen Sie **EndpointSecurityforMacUnistaller** mit einem Doppelklick aus.

Für die Deinstallation werden Administratorrechte benötigt.

Bitdefender unter Linux

Installation, Deinstallation und mögliche Fehler für Bitdefender unter Linux.

Installation (Linux)

Auf der Download-Seite des Gauß-IT-Zentrums befindet sich ein vorkonfiguriertes Installationspaket für Bitdefender Endpoint Security für Linux zum Herunterladen. Bitdefender löst die Sophos Endpoint Security als Nachfolger ab. Es ist geeignet für alle gängigen Linux-Distributionen, wie Ubuntu, Debian, Fedora, CentOS, Red Hat Enterprise Linux und deren Derivaten. Die Auflistung der offiziell unterstützten Linux-Distributionen finden Sie Hier.

> **Für die Installation muss sich Ihr System im Netzwerk der TU Braunschweig befinden.**
> Starten Sie nach der Installation einen vollständigen Scan des Systems.
> **Bitdefender Endpoint Security verfügt unter Linux über keine grafische Oberfläche.**
> **Alle Aktionen müssen Sie mit root-Rechten im Terminal ausführen.**

Navigieren Sie mit Ihrem Internet-Browser zu https://www.tu-braunschweig.de/it/downloads/software/gitz-dienste und melden Sie sich unter **[Schnellzugriff]** an. Klicken Sie auf **[Virenscanner]**. Laden Sie das TAR-Achiv bei **Linux** herunter und entpacken Sie dieses. Ändern Sie dann die Datei **installer** so ab, dass diese ausführbar wird und führen Sie diese dann mit root-Rechten aus.

Installation

Die Installation wurde hier unter Ubuntu 22.04 durchgeführt.
Möglicherweise unterscheiden sind die Installationsschritte bei anderen Linux-Distributionen.
Da Bitdefender über keine grafische Oberfläche verfügt, wird die Installation im Terminal durchgeführt.

Öffnen Sie ein Terminal mit dem Launcher (unten links) oder mit STRG + ALT + T.
Wechseln Sie in Ihren persönlichen Downloads-Ordner und entpacken Sie das TAR-Archiv.

```
cd ~/Downloads
tar -xvf installer.tar
```

Ändern Sie die Datei **installer** ab, so dass diese ausführbar wird und führen Sie diese dann mit root-Rechten aus.

```
chmod +x installer
sudo ./installer
```

Überprüfen Sie nach der Installation ob die Bitdefender Endpoint Security Daemons gestartet wurden.

```
systemctl status bdsec*
```

Führen die nach der Installation die Suche an Updates aus:

```
sudo /opt/bitdefender-security-tools/bin/bduitool update -ps
```

Starten eines manuellen Scans (Linux)

Starten Sie am besten direkt nach der Installation einen vollständigen Scan mit folgendem Befehl:

```
sudo /opt/bitdefender-security-tools/bin/bduitool scan -s full
```

Um den Status eines Scans zu überprüfen können Sie folgende Befehle nutzen:

```
# Zeigt alle Scan-Tasks an, u.a. auch die taskID
sudo /opt/bitdefender-security-tools/bin/bduitool get scantasks
# Zeigt an in welcher Status der angegebene Scan hat
sudo /opt/bitdefender-security-tools/bin/bduitool get scanstatus [taskID]
# Zeigt das Scan-Log des angegebenen Scans
sudo /opt/bitdefender-security-tools/bin/bduitool get scanlog [taskID]
```

Weitere Befehle für das Scannen mit dem bduitool können Sie auf der Internetseite des Bitdefender Supports finden
Eine Übersicht alles Befehle des bduitool finden Sie einfach mit folgenden Befehlen:

```
# Einfache Befehlsübersicht
sudo /opt/bitdefender-security-tools/bin/bduitool -h
```

Anzeigen der Quarantäne (Linux)

Die sich zur Zeit in Quarantäne befindlichen Dateien können Sie sich mit folgendem Befehl ausgeben lassen:

```
sudo /opt/bitdefender-security-tools/bin/bduitool get quar
```

> Momentan können sich in Quarantäne befindliche Dateien unter Linux nur seitens des GITZ wiederhergestellt werden.
> Bitte eröffnen Sie dafür ein Ticket mit dem Pfad ihrer Datei(en) und dem Hostnamen ihres Systems.

Mögliche Fehlercodes (Linux)

Es ist möglich, dass während der Installation und auch während des Betriebs Fehler in Bitdefender angezeigt werden. Entsprechend sind hier die häufigsten Fehlercodes als Hilfestellung aufgelistet.

Code	Fehler	Lösungsmöglichkeiten
-1002	Die Adresse des Bitdefender-Servers konnte nicht aufgelöst werden	Überprüfen Sie Ihre Netzwerk- und DNS-Einstellungen und die Verbindung zu goku.rz.tu-bs.de
-1011	Time out beim Erreichen des Update Servers	Überprüfen Sie Ihre Netzwerk-Einstellungen bzgl. der Verbindung zu goku.rz.tu-bs.de und ob der Port 7074 in Ihrer Firewall geöffnet wurde
-1018	Fehler beim Herunterladen der Update Dateien	Überprüfen Sie Ihre Netzwerk-Einstellungen bzgl. der Verbindung zu goku.rz.tu-bs.de und ob der Port 7074 in Ihrer Firewall geöffnet wurde. Falls eine Verbindung besteht und Sie diesen Fehler trotzdem bekommen, schreiben Sie bitte ein Ticket an den IT-Service Desk

Deinstallation (Linux)

Öffnen Sie ein Terminal und führen Sie dann folgenden Befehl aus:

```
sudo /opt/bitdefender-security-tools/bin/uninstall
```