Bitdefender ANTIVIRUS FOR MAC



MANUAL DE UTILIZARE

Bitdefender Antivirus for Mac Manual de utilizare

Publicat 2018.04.12

Copyright© 2018 Bitdefender

Termeni legali

Toate drepturile rezervate. Nicio parte a acestui document nu va putea fi reprodusă sau transmisă sub nicio formă și prin niciun mijloc, fie el electronic sau mecanic, inclusiv fotocopiere, înregistrare, sau orice sistem de stocare și recuperare de date, fără acordul scris al unui reprezentant autorizat al Bitdefender. Este posibilă includerea unor scurte citate în recenzii, dar numai cu condiția menționării sursei citate. Conținutul documentului nu poate fi modificat în niciun fel.

Avertisment și declinarea responsabilității. Acest produs și documentația aferentă sunt protejate de legea drepturilor de autor. Informațiile incluse în acest document sunt furnizate "ca atare", fără nicio garanție. Deși s-au luat toate măsurile de prevedere în momentul alcătuirii acestui document, autorii săi nu vor fi în niciun fel ținuți responsabili față de nicio persoană fizică sau juridică pentru pierderi sau daune cauzate sau care se presupune a fi fost cauzate, direct sau indirect, de informațiile cuprinse în acest material.

Acest document conține legături către siteuri web aparținând unor terți, care nu se află sub controlul Bitdefender; prin urmare, Bitdefender nu este responsabilă pentru conținutul respectivelor siteuri. Responsabilitatea accesării oricăruia dintre siteurile terților a căror legătură este furnizată în acest document vă aparține în totalitate. Bitdefender furnizează aceste legături exclusiv pentru ușurarea consultării documentului și prezența lor nu presupune faptul că Bitdefender sustine sau îsi asumă responsabilitatea pentru continutul siteurilor către care duc acestea.

Mărci înregistrate. Acest document poate conține nume de mărci înregistrate. Toate mărcile comerciale înregistrate sau neînregistrate din acest document aparțin exclusiv proprietarilor acestora și sunt redate ca atare.

Bitdefender

Cuprins

Cı	um să folosiți acest ghid 1. Scopul și publicul țintă 2. Cum să folosiți acest ghid 3. Convenții utilizate în ghid 3.1. Convenții tipografice 3.2. Atenționări 4. Comentarii	V v v v vi vi
1.	Instalare și dezinstalare 1.1. Cerințe de sistem 1.2. Instalarea Bitdefender Antivirus for Mac 1.2.1. Proces de instalare 1.3. Eliminare Bitdefender Antivirus for Mac	1 1 2 7
2.	Introducere 2.1. Despre Bitdefender Antivirus for Mac 2.2. Deschiderea Bitdefender Antivirus for Mac 2.3. Fereastra principală a aplicației 2.4. Pictograma aplicației din Dock	8 8 9 10
3.	Protecția împotriva softurilor periculoase	12 12 13 14 14 16 17 18 20 20 21 21
4.	Configurarea preferințelor 2 4.1. Accesarea preferințelor 2 4.2. Informații cont 2 4.3. Preferințe de protecție 2 4.3.1. Excepții scanare 2 4.4. Fișiere sigure 2 4.4.1. Administrare aplicații 2 4.5. Istoric 2 4.6. Carantină 2	22 22 22 24 25 28 28 29
5.	VPN	30 30 30 31 31 33

6. Bitdefender Central	34
6.1. Despre Bitdefender Central	. 34
6.2. Accesare Bitdefender Central	. 34
6.3. Abonamentele mele	35
6.3.1. Activare abonament	35
6.3.2. Cumpără abonament	. 35
6.4. Dispozitivele mele	. 36
6.4.1. Personalizați-vă dispozitivul	36
6.4.2. Acțiuni de la distanță	. 37
7. Întrebări frecvente	39
8. Obtinere ajutor	44
8.1. Suport	44
8.1.1. Resurse online	. 44
8.1.2. Solicitarea de asistență profesională	. 46
8.2. Informații de contact	. 46
8.2.1. Adrese Web	. 46
8.2.2. Distribuitori locali	. 47
8.2.3. Filialele Bitdefender	. 47
Tipuri de softuri periculoase	49

Cum să folosiți acest ghid

1. Scopul și publicul țintă

Acest manual se adresează tuturor utilizatorilor care au ales **Bitdefender Antivirus for Mac** ca soluție de securitate pentru calculatoarele personale. Informațiile incluse în acest manual sunt destinate nu numai utilizatorilor avansați, ci și oricărei persoane care poate lucra în sistemul Macintosh.

Veți afla cum să configurați și să utilizați Bitdefender Antivirus for Mac pentru a vă proteja împotriva virușilor și împotriva altor softuri periculoase. Veți afla cum puteți obține maximul de performanță de la Bitdefender.

Vă dorim o lectură plăcută și utilă.

2. Cum să folosiți acest ghid

Acest ghid este organizat în mai multe teme majore:

Introducere (p. 8)

Faceți cunoștință cu produsul Bitdefender Antivirus for Mac și interfața sa pentru utilizatori.

Protecția împotriva softurilor periculoase (p. 12)

Aflați cum să utilizați Bitdefender Antivirus for Mac pentru a vă proteja împotriva softurilor periculoase.

Configurarea preferințelor (p. 22)

Aflați mai multe informații despre setările favorite pentru Bitdefender Antivirus for Mac.

Obținere ajutor (p. 44)

Unde să căutați și unde să cereți ajutor în cazul în care apar situații neprevăzute.

3. Convenții utilizate în ghid

3.1. Convenții tipografice

Manualul conține diferite stiluri de text, pentru o lectură cât mai ușoară. Aspectul și semnificația acestora sunt prezentate în tabelul de mai jos.

Bitdefender Antivirus for Mac

Aspect	Descriere		
exemplu de sintaxă	Exemplele de sintaxă sunt tipărite cu caractere monospațiate.		
https://www.bitdefender.ro	Linkurile URL indică locații externe, pe serverele http sau ftp.		
documentation@bitdefender.com	Adresele de e-mail sunt inserate în text ca informație de contact.		
Cum să folosiți acest ghid (p. v)	Acesta este un link intern, către o locație din document.		
nume fișier	Numele fișierelor și ale directoarelor sunt tipărite cu caractere monospațiate.		
opțiune	Toate opțiunile produsului sunt tipărite cu caractere bold .		
cuvânt cheie	Cuvintele cheie sau frazele importante sunt evidențiate cu ajutorul caracterelor bold .		

3.2. Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.



Notă

Nota nu este decât o scurtă observație. Deși pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect asemănător.



Important

Acest lucru necesită atenția dumneavoastră și nu este recomandat să-l ocoliți. De obicei, aici se furnizează informații importante, dar nu cruciale.



Avertisment

Este vorba de informații cruciale, cărora trebuie să le acordați o mare atenție. Dacă urmați indicațiile, nu se va întâmpla nimic rău. Este indicat să citiți și să înțelegeți despre ce este vorba, deoarece aici se descrie ceva extrem de riscant.

4. Comentarii

Vă invităm să ne ajutați să îmbunătățim acest manual. Am testat și verificat toate informațiile, în măsura posibilităților noastre. Vă rugăm să ne scrieți despre orice inexactități pe care le veți găsi în această carte sau despre cum credeți că ar putea fi îmbunătățită, pentru a ne ajuta să vă oferim cea mai bună documentație.

Aveți la dispoziție adresa de e-mail documentation@bitdefender.com. Vă rugăm să scrieți în engleză sau română mailurile către adresa de mai sus pentru a le putea procesa cât mai eficient.

1. INSTALARE ȘI DEZINSTALARE

Acest capitol acoperă următoarele subiecte:

- Cerințe de sistem (p. 1)
- Instalarea Bitdefender Antivirus for Mac (p. 1)
- Eliminare Bitdefender Antivirus for Mac (p. 7)

1.1. Cerințe de sistem

Poți instala Bitdefender Antivirus for Mac exclusiv pe calculatoare Macintosh cu procesor Intel și cu sistem de operare instalat OS X Mavericks (10.9.5), OS X Yosemite (10.10.5), OS X El Capitan (10.11.6), macOS X Sierra (10.12.5 sau mai recent), , macOS High Sierra 10.13.

În plus, calculatorul dumneavoastră trebuie să îndeplinească următoarele cerințe suplimentare:

Minimum 1 GB memorie RAM

• Minim 600 MB de spațiu liber pe hard disc

Este necesar să fiți conectați la internet pentru a înregistra și actualiza Bitdefender Antivirus for Mac.

Cum să afli versiunea de macOS și informații hardware despre Mac-ul tău

Faceți clic pe pictograma Apple din colțul din stânga sus al ecranului și selectați **Despre acest Mac**. În fereastra care apare puteți vedea afișată versiunea sistemului dvs. de operare, precum și alte informații utile. Faceți clic pe **Informații suplimentare** pentru aflarea unor informații detaliate de hardware.

1.2. Instalarea Bitdefender Antivirus for Mac

Aplicația Bitdefender Antivirus for Mac poate fi instalată din contul tău Bitdefender, după cum urmează:

- 1. Conectează-te ca administrator.
- 2. Mergeți la: https://central.bitdefender.com.
- 3. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.

- 4. Selectează fereastra **Dispozitivele mele**și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA LOCALĂ**.
- 5. Alegeți una dintre cele doua opțiuni disponibile:

DESCARCĂ

Faceți clic pe buton și salvați fișierul de instalare.

Pe alt dispozitiv

Selectează **macOS** pentru a descărca produsul Bitdefender și apoi efectuează clic pe **CONTINUARE**. Introdu adresa de e-mail în câmpul corespunzător și apoi efectuează clic pe **TRIMITE**.

- 6. Rulați produsul Bitdefender descărcat.
- 7. Urmează pașii de instalare.

1.2.1. Proces de instalare

Pentru a instala Bitdefender Antivirus for Mac:

- 1. Faceți clic pe fișierul descărcat. Veți lansa astfel programul de instalare, care vă va ghida pe parcursul procesului de instalare.
- 2. Urmați programul asistent de instalare.

Pasul 1 - Fereastra de întâmpinare



Faceți clic pe Continue.

Pasul 2 - Citește Contractul de abonament



Contractul de abonament constituie un acord legal între tine și Bitdefender referitor la utilizarea Bitdefender Antivirus for Mac. Poți imprima sau salva Contractul de abonament, astfel încât să îl poți consulta ulterior.

Citește cu atenție Contractul de abonament. Pentru a continua instalarea software-ului trebuie să fii de acord cu condițiile contractului de abonament. Faceți clic pe **Continuă** și apoi pe **Sunt de acord**.

Important

Dacă nu sunteți de acord cu acești termeni și condiții, faceți clic pe **Continuă** și apoi pe **Nu sunt de acord** pentru a întrerupe procesul de instalare.

Pasul 3 - Lansați instalarea

	🥪 Instalează Bitdefender						
	Instalare standard pe "Macintosh HD"						
 Introducere Licență Selectare destinație 	Aceasta va ocupa 3,6 MB din spațiul de pe computerul dvs. Faceți clic pe Instalează pentru a efectua o instalare standard a acestui software pe discul "Macintosh HD".						
 Tip de instalare Instalare Rezumat 							
Bitdefender	Modificare destinație instalare înapoi Instalează						
Lansarea inst	Lansarea instalării						

Bitdefender Antivirus for Mac va fi instalat în Macintosh HD/Library/Bitdefender. Calea de instalare nu poate fi schimbată.

Faceți clic pe Instalează pentru a iniția instalarea.

Pasul 4 - Instalare Bitdefender Antivirus for Mac



Așteptați până când instalarea este finalizată și apoi faceți clic pe Continuă.

Pasul 5 - Finalizare



Faceți clic pe **închide** pentru a închide fereastra programului de instalare. Procesul de instalare s-a încheiat.

Important

Dacă instalezi Bitdefender Antivirus for Mac pe macOS High Sierra 10.13 sau o versiune mai nouă, va apărea notificarea Extensie de sistem blocată. Această notificare te informează că extensiile semnate de Bitdefender au fost blocate și trebuie activate manual. Faceți clic pe **OK** pentru a continua. În fereastra Bitdefender Antivirus for Mac afisată, efectuează clic pe linkul Securitate & Confidentialitate. Bifează caseta Bitdefender din listă și apoi efectuează clic pe OK.

La prima instalare a Bitdefender Antivirus for Mac, apare programul asistent pentru Fisiere sigure si Protectie Time Machine. Pentru mai multe informatii. accesează Fișiere sigure (p. 25) și Protecție Time Machine (p. 14).

Îti prezentăm caracteristica VPN. Efectuează clic pe **Continuă** pentru a continua. Pentru mai multe informații, accesează VPN (p. 30).

1.3. Eliminare Bitdefender Antivirus for Mac

Deoarece este o aplicatie complexă, Bitdefender Antivirus for Mac nu poate fi dezinstalat în modul obișnuit, prin transferarea pictogramei aplicației din directorul Applications în Trash.

Pentru a sterge Bitdefender Antivirus for Mac, urmați pașii de mai jos:

- 1. Deschide o fereastră Finder, mergi la directorul Aplicații și selectează Utilităti.
- 2. Fă dublu clic pe aplicatia Bitdefender for Mac Uninstaller pentru a o deschide.
- 3. Fă clic pe butonul **Dezinstalare** și așteaptă finalizarea procesului.
- 4. Faceti clic pe **Închide** pentru a finaliza.



Important

În cazul apariției unei erori, puteți contacta serviciul Bitdefender Customer Care, asa cum se descrie în Suport (p. 44).

2. INTRODUCERE

Acest capitol acoperă următoarele subiecte:

- Despre Bitdefender Antivirus for Mac (p. 8)
- Deschiderea Bitdefender Antivirus for Mac (p. 8)
- Fereastra principală a aplicației (p. 9)
- Pictograma aplicației din Dock (p. 10)

2.1. Despre Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac este un scanner antivirus puternic, care poate detecta și elimina toate tipurile de softuri periculoase ("malware"), incluzând:

- ransomware
- adware
- viruşi
- spyware
- Troieni
- keylogger
- 🗕 viermi

Această aplicație detectează și elimină nu numai softurile periculoase pentru Mac, ci și softurile periculoase pentru Windows, împiedicându-vă, astfel, să transmiteți fișiere infectate familiei, prietenilor și colegilor care utilizează PC-uri.

2.2. Deschiderea Bitdefender Antivirus for Mac

Aveți mai multe modalități prin care puteți deschide Bitdefender Antivirus for Mac.

- Faceți clic pe pictograma Bitdefender Antivirus for Mac în Launchpad.
- Faceți clic pe icoana
 în bara de meniu și selectați Deschide fereastra principală.
- Deschideți o fereastră Finder, mergeți la Aplicații și faceți dublu clic pe pictograma Bitdefender Antivirus for Mac.

2.3. Fereastra principală a aplicației

În fereastra principală a aplicației, poți verifica starea de securitate a calculatorului tău, poți executa scanări de sistem, îți poți securiza experiența de navigare pe internet sau te poți conecta la contul Bitdefender.



Opțiunea **Autopilot** situată în partea din dreapta sus a ferestrei principale, monitorizează în mod continuu aplicațiile ce rulează pe calculator, căutând să identifice acțiuni de tip malware și prevenind pătrunderea noilor amenințări malware în sistemul tău.

Din motive de securitate, se recomandă să păstrezi activată funcția Autopilot. Dacă aceasta este dezactivată, nu vei fi protejat în mod automat împotriva amenințărilor malware.

Bara de stare din partea de sus a ferestrei vă oferă informații privind starea de securitate a sistemului prin utilizarea unor mesaje explicite și a unor culori sugestive. În cazul în care nu există avertizări din partea Bitdefender Antivirus for Mac, bara de stare este de culoare verde. Atunci când este detectată o problemă de securitate, bara de stare își schimbă culoarea în galben. Fă clic pe butonul **Vizualizare probleme** pentru a vizualiza problemele care afectează securitatea sistemului tău. Pentru informații detaliate referitoare la probleme și la modalitățile de soluționare a acestora, consultați capitolul *Remedierea problemelor* (p. 17).

Sub bara de stare, sunt disponibile trei butoane de scanare pentru scanarea Mac-ului dumneavoastră:

- Scanare rapidă verifică dacă există programe malware în cele mai vulnerabile locații din sistemul dumneavoastră (de exemplu, folderele care conțin documentele, fişierele descărcate de pe web sau din e-mail şi fişierele temporare ale fiecărui utilizator).
- Full Scan (Scanare completă) efectuează o verificare completă a întregului sistem pentru identificarea programelor malware. Toate dispozitivele conectate vor fi, de asemenea, scanate.
- Scanare personalizată vă ajută să verificați anumite fișiere, foldere sau volume pentru a identifica programele malware.

Pentru mai multe informații, consultați capitolul *Scanarea Mac-ului dumneavoastră* (p. 13).

Alături de butoanele de scanare, sunt disponibile și opțiuni suplimentare:

- Protecție web filtrează tot traficul dumneavoastră web și blochează orice conținut periculos pentru o experiență sigură de browsing web. Pentru informații suplimentare, consultați Protecție web (p. 18).
- Mergi la contul Bitdefender fă clic pe linkul Mergi la contul tău din partea din dreapta jos a interfeței principale pentru a-ți accesa contul Bitdefender. Pentru mai multe informații, consultă *Bitdefender Central* (p. 34).
- Numărul de zile rămase afișează timpul rămas până la expirarea abonamentului. Atunci când data de expirare a fost atinsă, fă clic pe link pentru a accesa pagina web de unde îți poți reînnoi abonamentul.
- Cumpărare te redirecționează către pagina de web a Bitdefender unde poți verifica ofertele disponibile sau poți cumpăra un abonament.
- Feedback deschide o fereastră nouă în clientul dumneavoastră de e-mail implicit de unde ne puteți contacta.

2.4. Pictograma aplicației din Dock

Pictograma Bitdefender Antivirus for Mac poate fi observată în Dock, de îndată ce deschideți aplicația. Pictograma din Dock vă oferă o modalitate ușoară de a scana fișierele și folderele de programe periculoase. Pur și simplu trageți și plasați fișierul sau dosarul pe pictograma Dock și scanarea va începe imediat.



3. PROTECȚIA ÎMPOTRIVA SOFTURILOR PERICULOASE

Acest capitol acoperă următoarele subiecte:

- Recomandări de utilizare (p. 12)
- Scanarea Mac-ului dumneavoastră (p. 13)
- Activarea și dezactivarea funcției Autopilot (p. 14)
- Protecție Time Machine (p. 14)
- Asistent scanare (p. 16)
- Remedierea problemelor (p. 17)
- Protecție web (p. 18)
- Actualizări (p. 20)

3.1. Recomandări de utilizare

Pentru a vă proteja sistemul de programe periculoase și pentru a preveni infectarea accidentală a altor sisteme, respectați aceste bune practici:

- Păstrează funcția Autopilot activată pentru a permite scanarea fișierelor de sistem de către Bitdefender Antivirus for Mac.
- Păstrează Bitdefender Antivirus for Mac actualizat în permanență cu cele mai recente semnături malware și actualizări de produs, menținând funcția Autopilot activată.
- Verificați și soluționați în mod regulat problemele raportate de Bitdefender Antivirus for Mac. Pentru informații detaliate, consultați capitolul Remedierea problemelor (p. 17).
- Verificați jurnalul detaliat de evenimente privind activitatea Bitdefender Antivirus for Mac pe calculatorul dumneavoastră. De fiecare dată când are loc un eveniment relevant pentru securitatea sistemului sau a datelor dumneavoastră, se adaugă un nou mesaj la istoricul Bitdefender. Pentru mai multe informații, accesați *Istoric* (p. 28).
- Vă sugerăm să urmați aceste recomandări de utilizare:
 - Obișnuiți-vă să scanați fișierele pe care le descărcați de pe o memorie externă de stocare (precum un stick USB sau un CD), în special atunci când sursa nu vă este cunoscută.

 În cazul unui fişier DMG, instalați-l și apoi scanați conținutul acestuia (fişierele din volumul/imaginea instalată).

Cel mai ușor mod de a scana un fișier, un director sau un volum este prin folosirea funcției drag&drop pentru a îl poziționa deasupra ferestrei sau pictogramei Bitdefender Antivirus for Mac din Dock.

Nu este necesară nici o altă configurare sau acțiune. Cu toate acestea, dacă doriți, vă puteți ajusta setările și preferințele pentru a corespunde mai bine necesităților dvs. Pentru mai multe informații, consultați capitolul *Configurarea preferințelor* (p. 22).

3.2. Scanarea Mac-ului dumneavoastră

În afara caracteristicii **Autopilot**, care monitorizează permanent aplicațiile care rulează pe calculator în căutarea de acțiuni de tip malware și previne pătrunderea noilor amenințări malware în sistemul tău, îți poți scana Mac-ul sau anumite fișiere oricând dorești.

Cel mai ușor mod de a scana un fișier, un director sau un volum este prin folosirea funcției drag&drop pentru a îl poziționa deasupra ferestrei sau pictogramei Bitdefender Antivirus for Mac din Dock. Va apărea programul asistent scanare, care vă va ghida în procesul de scanare.

Puteți începe o operațiune de scanare și astfel:

- 1. Deschideți Bitdefender Antivirus for Mac.
- 2. Faceți clic pe unul dintre cele trei butoane de scanare pentru a începe scanarea dorită.
 - Scanare rapidă verifică dacă există programe malware în cele mai vulnerabile locații din sistemul dumneavoastră (de exemplu, folderele care conțin documentele, fișierele descărcate de pe web sau din e-mail și fișierele temporare ale fiecărui utilizator).
 - Full Scan (Scanare completă) efectuează o verificare completă a întregului sistem pentru identificarea programelor malware. Toate dispozitivele conectate vor fi, de asemenea, scanate.

📉 Notă

În funcție de dimensiunea hard disk-ului dumneavoastră, scanarea întregului sistem poate dura până la o oră sau chiar mai mult. Pentru o mai bună performanță, se recomandă să nu rulați această operațiune în timp ce efectuați alte operațiuni care folosesc intensiv resursele (cum ar fi editarea video).

În funcție de preferințele dumneavoastră, puteți alege să nu scanați anumite volume instalate prin adăugarea acestora la lista Excepții din fereastra de Preferințe.

 Scanare personalizată - vă ajută să verificați anumite fișiere, foldere sau volume pentru a identifica programele malware.

3.3. Activarea și dezactivarea funcției Autopilot

Pentru a activa sau dezactiva funcția Autopilot, urmează oricare dintre pașii următori:

- Deschide Bitdefender Antivirus for Mac și fă clic pe buton pentru a activa sau dezactiva funcția Autopilot.
- Faceți clic pe icoana III în bara de meniu și selectați Dezactivează funcția Autopilot.



Avertisment

Îți recomandăm să menții funcția Autopilot dezactivată cât mai puțin timp posibil. Dacă aceasta este dezactivată, nu vei fi protejat automat împotriva amenințărilor malware.

3.4. Protecție Time Machine

Protecția Time Machine Bitdefender servește drept strat suplimentar de securitate pentru unitatea ta de backup, inclusiv pentru toate fișierele pe care ai decis să le stochezi acolo, blocând accesul oricărei surse externe. În cazul în care fișierele de pe unitatea Time Machine sunt criptate de un program ransomware, le vei putea recupera fără a plăti recompensa solicitată.

Programul asistent de Protecție Time Machine

Programul asistent de Protecție Time Machine Bitdefender apare imediat de instalezi Bitdefender Antivirus for Mac pentru prima oară pe Macintosh.

•
Protecție Time Machine
Protejează backupurile Time Machine de modificările neautorizate și potențial periculoase efectuate de alte aplicații.
Funcția Time Machine nu este activată Mergeți la Time Machine Vă recomandăm să activați Time Machine. Mergeți la Time Machine
Mai târziu Activare protecție
Programul asistent de Protectie Time Machine

Trebuie să configurezi aplicația de sistem pentru backup Time Machine înainte de a activa protecția Bitdefender.

Dacă funcția Time Machine nu este activată pe sistemul tău:

1. Fă clic pe opțiunea Mergi la Time Machine.

Se va afișa fereastra Time Machine din Preferințe sistem.

2. Activează funcția și apoi selectează unde dorești să salvezi fișierele de backup.

Dacă ai nevoie de instrucțiuni suplimentare despre cum să activezi aplicația Time Machine pe sistemul tău, fă clic pe linkul **Află cum să configurezi Time Machine** din programul asistent.

Pentru a activa Protecția Time Machine Bitdefender pentru fișierele tale de backup:

1. Fă clic pe opțiunea Activare protecție.

Va apărea o fereastră de confirmare.

2. Faceți clic pe Închide.

Activarea sau dezactivarea protecției Time Machine

Pentru activa sau dezactiva protecția Time Machine:

1. Deschideți Bitdefender Antivirus for Mac.

- 2. Faceți clic pe Bitdefender Antivirus for Macîn bara de meniu și selectați **Preferințe**.
- 3. Selectați secțiunea Protecție.
- 4. Bifează sau debifează caseta Protecție Time Machine.

3.5. Asistent scanare

De fiecare dată când inițiați o operațiune de scanare, va apărea asistentul de scanare Bitdefender Antivirus for Mac.

•••		Scanare completă a sistemu	lui	
		Scanare în curs		
	/Applications/1Password.a	pp/Contents/Resou/OPSetupFold	derSyncWindowController.strings	
	8498	0	0	
	Fișiere scanate	Detectat(e)	Rezolvat(e)	
		00:00:35		
		Renunță		
~	^			
Scanare	in curs			

În timpul fiecărei scanări sunt afișate informații în timp real despre amenințările detectate și soluționate.

Așteptați ca Bitdefender Antivirus for Mac să finalizeze scanarea.

Notă Procesul de scanare poate dura cateva minute, în funcție de complexitatea scanării.

3.6. Remedierea problemelor

Bitdefender Antivirus for Mac depistează automat o serie de probleme care pot afecta securitatea sistemului și a datelor dvs. și vă informează în acest sens. În acest fel, puteți soluționa riscurile de securitate ușor și rapid.

Soluționarea problemelor indicate de Bitdefender Antivirus for Mac constituie un mod rapid și ușor de a asigura protecția optimă a sistemului și a datelor dumneavoastră.

Problemele detectate includ:

- Noile semnături de softuri periculoase și actualizările produsului nu au fost descărcate de pe serverele noastre deoarece funcția Autopilot este dezactivată.
- Au fost depistate amenințări nesoluționate în sistemul dvs.
- Funcția Autopilot este dezactivată.

Pentru a verifica și soluționa problemele detectate:

- 1. Deschideți Bitdefender Antivirus for Mac.
- 2. În cazul în care nu există avertizări din partea Bitdefender, bara de stare este de culoare verde. Atunci când este detectată o problemă de securitate, bara de stare își schimba culoarea în galben.
- 3. Verificați descrierea acesteia pentru a obține mai multe informații.
- 4. Atunci când este detectată o problemă, fă clic pe butonul Vizualizare probleme pentru a vedea informații despre problema care afectează securitatea sistemului tău. Poți întreprinde acțiuni în fereastra care se deschide.

Numele infecției	Cale către fișierul infectat
MAC.OSX.Backdoor.Jani	/Users/Shared/Janicab/RecentNews.?fdp.app/Contents/MacOS/installer
MAC.OSX.Backdoor.Jani MAC.OSX.Trojan.DNSCh MAC.OSX.Backdoor.Jani MAC.OSX.Backdoor.Jani MAC.OSX.Backdoor.Jani MAC.OSX.Backdoor.Jani	/Users/Shared/Janicab/RecentNews.?fdp.app/Contents/MacOS/installer /Users/Shared/Janicab/RecentNews.?fdp.app/Contents/Resources/Insta /Users/Shared/Janicab/RecentNews.?fdp.app/Contents/Resources/Libs /Users/Shared/Janicab/RecentNews.?fdp.app/Contents/Resources/Libs /Users/Shared/Janicab/RecentNews.?fdp.app/Contents/Resources/Libs /Users/Shared/Janicab/RecentNews.?fdp.app/Contents/Resources/Libs
Arată în Finder Ad	augă la Excluderi

Lista de amenințări nesoluționate este actualizată după fiecare operațiune de scanare a sistemului.

Puteți alege să întreprindeți următoarele acțiuni cu privire la amenințările nesoluționate:

- Arată în Finder. Întreprindeți această acțiune pentru a elimina infecțiile manual.
- Adaugă la Excluderi. Această acțiune nu este disponibilă pentru softuri periculoase care se regăsesc în arhive.

3.7. Protecție web

Bitdefender Antivirus for Mac folosește extensii TrafficLight pentru o protecție completă a experienței dumneavoastră de browsing web. Extensiile TrafficLight interceptează, procesează și filtrează întregul trafic web, blocând orice conținut periculos.

Extensiile sunt compatibile și se integrează cu următoarele browsere web: Mozilla Firefox, Google Chrome și Safari.

Activarea extensiilor TrafficLight

Pentru a activa extensiile TrafficLight, urmați pașii de mai jos:

- 1. Deschideți Bitdefender Antivirus for Mac.
- 2. Faceți clic pe Repară acum pentru a activa protecția web.

- 3. Bitdefender Antivirus for Mac va detecta browser-ul web instalat pe sistemul dumneavoastră. Pentru a instala extensia TrafficLight în browser-ul dumneavoastră, faceți clic pe **Descarcă extensia**.
- 4. Veți fi redirecționat la această locație online:

https://bitdefender.com/solutions/trafficlight.html

- 5. Selectați Descărcare gratuită.
- 6. Urmați pașii pentru instalarea extensiei TrafficLight corespunzătoare browser-ului dumneavoastră web.

Administrarea setărilor extensiilor

Sunt disponibile mai multe funcții menite să te protejeze de diferite tipuri de amenințări pe care le poți întâlni în timpul navigării pe internet. Pentru a le accesa, efectuează clic pe pictograma Semaforului de lângă setările browserului și apoi efectuează clic pe **Setări**:

Setările Semaforului Bitdefender

- Filtru pentru amenințările avansate te împiedică să accesezi site-uri web utilizate pentru atacuri malware, de tip phishing sau fraude.
- Detectorul de funcții de localizare detectează funcțiile de localizare de pe paginile internet vizitate și te informează cu privire la prezența acestora.
- Analizator rezultate căutare vă avertizează în avans cu privire la site-urile web periculoase din cadrul rezultatelor căutării efectuate de dumneavoastră.

Dacă toate setările sunt dezactivate, nu va fi scanat niciun site web.

🗕 Lista albă

Site-urile web pot fi excluse din scanarea cu motoarele Bitdefender. În câmpul corespunzător, introdu denumirea site-ului web pe care dorești să îl adaugi în lista albă și efectuează clic pe **ADAUGĂ**.

Nu se vor afișa avertizări dacă paginile excluse includ amenințări. Acesta este motivul pentru care în această listă trebuie să includeți doar site-urile web în care aveți încredere deplină.

Rating-ul de pagină și alerte

În funcție de cum clasifică TrafficLight pagina web pe care o vizualizați la momentul respectiv, una sau mai multe dintre următoarele pictograme sunt afișate în zona corespunzătoare:

Această pagină este sigură. Puteți continua.

OAceastă pagină web poate avea conținut periculos. Vizitați cu atenție această pagină.

Siți recomandăm să părăsești pagina web imediat, deoarece conține programe periculoase sau alte amenințări.

În Safari, fundalul pictogramelor Semaforului este negru.

3.8. Actualizări

În fiecare zi sunt descoperite și identificate noi programe periculoase (malware). De aceea, este foarte importantă actualizarea Bitdefender Antivirus for Mac cu ultimele semnături malware.

Păstrează funcția **Autopilot** activată pentru a permite semnăturilor malware și actualizărilor de produs să fie descărcate automat în sistemul tău. În cazul în care este detectată o actualizare, aceasta este descărcată și instalată automat pe computerul dumneavoastră.

Actualizarea semnăturilor de programe periculoase se face în zbor, ceea ce înseamnă că fișierele care trebuie actualizate sunt înlocuite progresiv. În acest fel, actualizarea nu va afecta funcționarea produsului și, în același timp, va fi exclusă orice vulnerabilitate.

- Dacă Bitdefender Antivirus for Mac este actualizat, poate detecta cele mai recente pericole descoperite şi poate curăța fişierele infectate.
- În cazul în care Bitdefender Antivirus for Mac nu este actualizat, acesta nu va putea detecta și elimina cele mai recente softuri perciuloase descoperite de Laboratoarele Bitdefender.

3.8.1. Cererea unei actualizări

Puteți efectua o actualizare la cerere oricând doriți.

Este necesară o conexiune activă la internet pentru a verifica dacă există actualizări disponibile și pentru a le descărca.

Pentru o actualizare la cerere:

- 1. Deschideți Bitdefender Antivirus for Mac.
- 2. Faceți clic pe butonul Acțiuni din bara de meniu.
- 3. Alegeți Update Virus Database.

În mod alternativ, poți solicita o actualizare manuală tastând CMD + U.

Puteți vizualiza progresul actualizării, precum și fișierele descărcate.

3.8.2. Obținerea actualizărilor prin intermediul unui server proxy

Bitdefender Antivirus for Mac se poate actualiza numai prin intermediul severelor proxy care nu necesită autentificare. Nu este necesară configurarea nici unor setări de program.

Dacă vă conectați la internet prin intermediul unui server proxy ce necesită autentificare, trebuie să treceți în mod regulat la o conexiune directă la internet pentru a putea obține actualizările semnăturilor softurilor periculoase.

3.8.3. Actualizați la o nouă versiune

Ocazional, lansăm actualizări de produse pentru a adăuga noi caracteristici și îmbunătățiri sau pentru a remedia anumite probleme legate de produs. Aceste actualizări pot necesita o repornire a sistemului, în scopul de a iniția instalarea de noi fișiere. În mod implicit, dacă o actualizare necesită repornirea computerului, Bitdefender Antivirus for Mac va continua funcționarea folosind fișierele anterioare, până când reporniți sistemul. În acest caz, procesul de actualizare nu va interfera cu activitatea utilizatorului.

Atunci când este finalizată o actualizare de produs, o fereastră pop-up vă va solicita să reporniți sistemul. Dacă ratați această această notificare, puteți fie să faceți clic pe **Repornește pentru upgrade** din bara de meniu sau să reporniți manual sistemul.

4. CONFIGURAREA PREFERINȚELOR

Acest capitol acoperă următoarele subiecte:

- Accesarea preferințelor (p. 22)
- Informații cont (p. 22)
- Preferințe de protecție (p. 22)
- Excepții scanare (p. 24)
- Fișiere sigure (p. 25)
- Istoric (p. 28)
- Carantină (p. 29)

4.1. Accesarea preferințelor

Pentru deschiderea ferestrei de preferințe a Bitdefender Antivirus for Mac:

- 1. Deschideți Bitdefender Antivirus for Mac.
- 2. Puteți proceda în oricare dintre următoarele modalități:
 - Faceți clic pe Bitdefender Antivirus for Macîn bara de meniu și selectați Preferințe.
 - Faceți clic pe icoana 🛽 în bara de meniu și selectați Preferințe.
 - Apăsați tastele comandă-virgulă (,).

4.2. Informații cont

Această fereastră cu datele de cont îți oferă informații despre abonament și contul tău Bitdefender.

Atunci când dorești să te conectezi cu un alt cont Bitdefender, fă clic pe butonul **Schimbare cont**, introdu noua adresă de e-mail și parola în fereastra de aplicație cont Bitdefender și apoi fă clic pe **AUTENTIFICARE**.

4.3. Preferințe de protecție

Fereastra de setări preferate de protecție îți permite să configurezi abordarea generală de scanare. Puteți configura acțiunile întreprinse în cazul fișierelor infectate și suspecte detectate, precum și alte setări generale.

Bitdefender Antivirus for Mac



Acțiuni pentru obiecte infectate. Atunci când detectează un virus sau un alt cod periculos, Bitdefender Antivirus for Mac va încerca în mod automat să elimine codul periculos din fișierul infectat și să reconstruiască fișierul original. Această operațiune este denumită dezinfectare. Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere.

Deși nu este recomandat, puteți seta aplicația să nu întreprindă nicio acțiune cu privire la fișierele infectate. Fișierele detectate sunt doar înregistrate.

Autopilot asigură o bună protecție împotriva softurilor periculoase, cu impact minor asupra performanței sistemului. În cazul în care există amenințări nesoluționate, le puteți vizualiza și puteți decide cum urmează să procedați în privința acestora.

Virus găsit:	EICAR-Test-File (not a	virus)			
Fișier:	eicar.com				
Cale:	/Users/Shared				
Motiv:	nu a fost setată nicio acțiune în Preferințe.				
Recomandare:	ştergeți fișierul daca nu	conține informații importante.			
	Altfel, alegeți "Exclude" p	entru a-l adauga în lista de exclude	ri. Pentru a adauga sa		
	Altfel, alegeți "Exclude" p înlătura excluderi ulterioa	entru a-l adauga în lista de exclude re deschideți meniul Preferințe.	ri. Pentru a adauga sa		
	Altfel, alegeți "Exclude" p înlătura excluderi ulterioa	entru a-l adauga în lista de exclude re deschideți meniul Preferințe. Ștergeți manual	ri. Pentru a adauga sa		
	Altfel, alegeți "Exclude" p înlătura excluderi ulterioa	entru a-l adauga în lista de exclude re deschideți meniul Preferințe. Ștergeți manual	Exclude		

 Acțiune pentru obiecte suspecte. Fișierele sunt identificate ca fiind suspecte în urma analizei euristice. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

Implicit, fișierele suspecte sunt mutate în carantină. Atunci când sunt în carantină virușii sunt inofensivi, pentru că nu pot fi executați sau citiți.

În funcție de preferințele dumneavoastră, puteți alege să ignorați fișierele suspecte. Fișierele detectate sunt doar înregistrate.

 Scanează doar fișierele noi și cele modificate. Selectați această căsuță pentru a configura Bitdefender Antivirus for Mac să scaneze exclusiv fișierele care nu au fost scanate anterior sau care au fost modificate de la ultima scanare.

Puteți alege să nu aplicați această setare în cazul scanării prin drag&drop selectând caseta corespunzătoare.

- Nu scana conținutul backupurilor. Bifează această căsuță pentru a exclude de la scanare fișierele de back-up. Dacă fișierele infectate sunt restabilite ulterior, Bitdefender Antivirus for Mac le va detecta automat și va acționa în mod corespunzător.
- Protecție Time Machine. Bifează această casetă pentru a proteja fișierele salvate în Time Machine. În cazul în care fișierele de pe unitatea Time Machine sunt criptate de un program ransomware, le vei putea recupera fără a plăti recompensa solicitată.

4.3.1. Excepții scanare

Puteți configura Bitdefender Antivirus for Mac astfel încât să nu scaneze anumite fișiere, dosare sau informațiile de pe o întreagă partiție. De exemplu, ați putea exclude de la scanare:

- Fișiere identificate eronat ca infectate (cunoscute drept "fals pozitive")
- Fișierele care duc la erori de scanare
- Volume de backup

Bitdefender Antivirus for Mac

Excluderi
Cont Securitate Fișiere sigure Excluderi Istoric Carantină
Opriți Antivirus for Mac să scaneze în aceste locații:
Clic pe butonul Adaugă sau trageți un fișier, dosar sau disc pe lista de mai jos.
Cale
+ -
Excepții scanare

Lista de excepții conține căile de acces către fișierele ce au fost excluse de la scanare.

Există două modalități de a stabili o excepție:

- Trageți fișierele, dosarele sau partițiile peste lista de excepții (prin metoda drag&drop).
- Faceți clic pe butonul marcat cu semnul plus (+), ce se află sub lista excepțiilor. Apoi alegeți fișierul, folderul sau volumul care urmează a fi exclus din operațiunea de scanare.

Pentru a dezactiva o excepție, selectați-o din listă și faceți clic pe butonul marcat cu minus (-), ce se află sub lista excepțiilor.

4.4. Fișiere sigure

Ransomware este un program periculos care atacă sistemele vulnerabile blocându-le și solicită bani pentru a permite utilizatorului să reia controlul asupra sistemului. Acest software periculos acționează inteligent prin afișarea unor mesaje false pentru a panica utilizatorul, solicitându-i să efectueze plata cerută.

Folosind cea mai recentă tehnologie, Bitdefender asigură integritatea sistemului prin protejarea zonelor de sistem de importanță critică împotriva

atacurilor ransomware, fără a afecta sistemul. Cu toate acestea, este posibil să vrei să-ți protejezi și fișierele personale, cum ar fi documentele, fotografiile sau filmele, împotriva accesării lor de către aplicații nesigure. Cu Bitdefender Fișiere sigure, poți să-ți menții în siguranță fișierele personale și să configurezi singur ce aplicații ar trebui să aibă dreptul de a efectua modificări asupra fișierelor protejate și ce aplicații nu ar trebui să aibă astfel de drepturi.

Îți prezentăm caracteristica Fișiere sigure
Fișiere sigure este un strat de protecție preventivă împotriva programelor ransomware care încearcă să cripteze informațiile sensibile pe Mac-ul tău. Această caracteristică se asigură că numai aplicațiile sigure pot modifica fișierele tale cele mai importante. Nu trebuie decât să adaugi căile pe care dorești să le protejezi și ți vom menține fișierele în siguranță:
//Jsers/Tester/Pictures //Jsers/Tester/Pictures //Jsers/Shared/
+ -
Mai târziu Activează
Asistent Fișiere sigure

Asistentul Bitdefender Fișiere sigure apare imediat după instalarea Bitdefender Antivirus for Mac pe Mac-ul tău. Selectează sau adaugă noi locații pe care dorești să le protejezi și apoi efectuează clic pe **Activare Fișiere Sigure**.

Bitdefender Antivirus for Mac

Fişiere sigure	
Cont Securitate Fișiere sigure Excluderi Istoric Carantină	
Fişier sigure: activat	Dezactivează Fișiere sigure
Permite accesul în locațiile protejate numai aplicațiilor sigure.	
Selectează fișierele pe care dorești să le protejezi:	
/Users/Shared	
JUsers/tester1/Desktop	
/Users/tester1/Documents	
JUsers/tester1/Downloads	
+ - Efectuează clic pe Adăugare (+) pentru a proteja un nou fișier, director s	au disc.
Selectesză anlicatiile cărora doraști să le	Administrare enlicetii
nermiti sau să le blochezi accesul la fisierele	Aurimistrare aplicății
tale proteiate.	
T '	
Fișiere sigure	
,	

Există două modalități de a adăuga ulterior fișiere în mediul protejat:

- Glisează și fixează (drag-and-drop) un fișier, director sau volum în fereastra Fișiere sigure.
- Efectuează clic pe butonul marcat cu semnul plus (+), ce se află sub lista fișierelor protejate. Apoi, selectează fișierul, directorul sau volumul de protejat în cazul în care se încearcă accesarea lor de către programele ransomware.

Pentru a evita încetinirea sistemului, îți recomandăm să adaugi cel mult 30 de directoare sau să salvezi mai multe fișiere într-un singur director.

În mod implicit, directoarele Fotografii, Documente, Desktop și Fișiere descărcate sunt protejate contra atacurilor amenințărilor.

Notă

Directoarele personalizate pot fi protejate doar pentru utilizatorii curenți. Unitățile, sistemele și fișierele aplicațiilor externe nu pot fi adăugate la mediul de protecție.

Vei fi informat de fiecare dată când o aplicație necunoscută având un comportament neobișnuit va încerca să modifice fișierele adăugate.

Efectuează clic pe **Permite** sau **Blochează** pentru a o adăuga în lista Administrare aplicații list.

4.4.1. Administrare aplicații

Aplicațiile care încearcă să modifice sau să șteargă fișierele protejate pot fi marcate ca fiind potențial nesigure și adăugate în lista de aplicații blocate. Dacă o astfel de aplicație este blocată și ești sigur că comportamentul acesteia este normal, poți să-i permiți accesul efectuând clic pe butonul **Administrare aplicații** și modificând apoi starea acesteia în Permis.

Aplicațiile cu starea Permis pot fi setate și pe valoarea Blocat.

Folosește metoda de glisare și fixare (drag&drop) sau efectuează clic pe semnul plus (+) pentru a adăuga în listă mai multe aplicații.

4.5. Istoric

Bitdefender menține un jurnal detaliat de evenimente privind activitatea sa pe calculatorul tău. De fiecare dată când are loc un eveniment relevant pentru securitatea sistemului sau a datelor tale, se adaugă un nou mesaj la istoricul Bitdefender Antivirus for Mac, așa cum îți apare un nou e-mail în Inbox.

Evenimentele reprezintă un instrument extrem de important pentru monitorizarea și gestionarea protecției Bitdefender. De exemplu, poți verifica rapid dacă actualizarea a fost finalizată cu succes, dacă au fost detectate programe malware pe calculatorul tău, dacă o aplicație neautorizată a încercat să acceseze unitatea Time Machine etc.

Sunt afișate detalii privind activitatea produsului.



Oricând doriți să ștergeți istoricul, faceți clic pe butonul Curăță istoricul.

Butonul **Copiază** vă oferă posibilitatea să copiați aceste informații în clipboard.

4.6. Carantină

Bitdefender Antivirus for Mac permite izolarea fișierelor infectate sau suspecte într-o zonă sigură, numită carantină. Atunci când sunt în carantină virușii sunt inofensivi, pentru că nu pot fi executați sau citiți.

		_	_	Carantir	nă	
			Fueludari		Sec.	
Cont	Securitate	Fișiere sigure	Excluderi	Istoric	Carantina	
Nume	e amenințare	Cale i	nițială			
Res	staurează	Şterge				Număr de obiecte: 0
Sta	are:			Nu există	á nicio selectie	
Pro	oprietar:			Nu existà	á nicio selecție	
Uti	lizator:			Nu există	á nicio selecție	
Dat	tă:			Nu există	á nicio selecție	
ici	oro m	utata îr	o o a ra	ntir	ŭ	

Secțiunea Carantină afișează toate fișierele izolate în directorul Carantină.

Pentru a șterge un fișier aflat în carantină, selectați-l și faceți clic pe **Șterge**. Dacă doriți să restaurați un fișier aflat în carantină în locația sa originală, selectați-l și faceți clic pe **Restaurează**.

5. VPN

Acest capitol acoperă următoarele subiecte:

- Despre VPN (p. 30)
- Instalarea VPN (p. 30)
- Deschiderea aplicației VPN (p. 31)
- Interfata (p. 31)
- Abonamente (p. 33)

5.1. Despre VPN

Cu Bitdefender VPN își menții confidențialitatea datelor atunci când te conectezi la rețele wireless nesecurizate în aeroporturi, mall-uri, cafenele sau hoteluri. În acest fel, pot fi evitate situațiile nefericite cum ar fi furtul de date personale sau tentativele de a face IP-ul tău accesibil de către hackeri.

VPS acționează ca tunel între dispozitivul tău și rețeaua la care te conectezi, securizându-ți conexiunea, criptându-ți datele prin criptare la nivel de bancă și ascunzându-ți adresa IP oriunde te-ai afla. Traficul tău este redirecționat prin intermediul unui server separat, ceea ce face ca dispozitivul tău să fie imposibil de identificat între multitudinea de alte dispozitive care folosesc serviciile noastre. Mai mult decât atât, în timp ce ești conectat la internet prin intermediul aplicației Bitdefender VPN, poți accesa conținut care în mod normal este restricționat în anumite zone.

Notă

Unele țări cenzurează conținutul online și, prin urmare, utilizarea soluțiilor VPN pe teritoriul lor a fost interzisă prin lege. Pentru a evita consecințele juridice, este posibil să se afișeze un mesaj de avertizare atunci când încercați să folosiți aplicația VPN Bitdefender pentru prima dată. Prin continuarea utilizării aplicației, confirmi că ai cunoștință de reglementările aplicabile țării respective și riscurile la care te-ai putea expune.

5.2. Instalarea VPN

Aplicația VPN poate fi instalată din fereastra principală Bitdefender, după cum urmează:

1. Deschideți Bitdefender Antivirus for Mac.

- 2. Fă clic pe Obține-l acum în colțul din dreapta jos.
- 3. În fereastra cu descrierea aplicației VPN, citește **Contractul de abonament** și apoi fă clic pe **Instalare VPN**. Dacă nu ești de acord cu aceste condiții, fă clic pe **Mai târziu** pentru a anula instalarea.
- 4. Fă clic pe Am înțeles pentru a finaliza procesul de instalare.

5.3. Deschiderea aplicației VPN

Pentru a deschide aplicația Bitdefender VPN, fă clic pe pictograma @ din bara de meniu. În plus față de aceasta, poți accesa directorul Aplicații, deschide directorul Bitdefender folder și apoi fă dublu clic pe pictograma Bitdefender VPN.

5.4. Interfata

Interfața VPN afișează starea aplicației, respectiv dacă este conectată sau deconectată. Locația serverului pentru utilizatorii versiunii gratuite este setată automat de Bitdefender la cel mai apropiat server, în timp ce utilizatorii versiunii Premium au posibilitatea de a modifica locația serverului la care doresc să se conecteze selectând-o din lista **SELECTARE LOCAȚIE**. Pentru detalii despre abonamentele VPN, accesează *Abonamente* (p. 33).

Pentru conectare sau deconectare, nu trebuie decât să efectuezi clic pe starea afișată în partea de sus a ecranului. Pictograma din bara de meniu devine neagră atunci când conexiunea VPN este activă și albă atunci când conexiunea VPN este inactivă.

Bitdefender Antivirus for Mac

Bitdefender VPN Bazată pe Hotspot Shield	¢
CONECTARE	
SELECTEAZĂ LOCAȚIA	
Automat 🝷	
Interfața VPN	

Când ești conectat, timpul scurs este afișat în partea de jos a interfeței. Pentru a avea acces la mai multe opțiuni, efectuează clic pe pictograma din partea de sus dreapta:

- Contul meu sunt afişate detalii despre contul tău Bitdefender şi abonamentul VPN. Efectuează clic pe Schimbare cont dacă doreşti să te conectezi cu alt cont.
- Setări în funcție de nevoile tale, poți personaliza comportamentul produsului tău:
 - poți seta funcția VPN să ruleze la pornirea sistemului
 - poți primi notificări atunci când funcția VPN se conectează sau se deconectează automat

- Efectuează upgrade la Premium dacă folosești versiunea gratuită a produsului, poți face upgrade la abonamentul Premium de aici. Efectuează clic peEFECTUEAZĂ UPGRADE ACUM pentru a fi redirecționat către o pagină web de unde poți cumpăra un abonament.
- Suport ești redirecționat către platforma noastră Support Center unde poți citi un articol util despre cum sa folosești Bitdefender VPN.
- Despre sunt afișate informații despre versiunea instalată.
- Închidere ieși din aplicație.

5.5. Abonamente

Bitdefender VPN oferă o cotă de trafic zilnică de 200 MB pe dispozitiv pentru a-ți securiza conexiunea oricând ai nevoie, conectându-te automat la locația optimă a serverului.

Pentru a obține trafic nelimitat și acces nerestricționat la conținutul din întreaga lume alegând o locație de server în funcție de preferințe, efectuează upgrade la versiunea Premium.

Poți face oricând upgrade la versiunea Bitdefender Premium VPN efectuând clic pe butonul **OBȚINE TRAFIC NELIMITAT** disponibil în interfața produsului.

Abonamentul Bitdefender Premium VPN este independent de abonamentul Bitdefender Antivirus for Mac, ceea ce înseamnă că îl vei putea folosi pe toată durata de valabilitate, indiferent de starea abonamentului antivirus. În cazul în care abonamentul Bitdefender Premium VPN expiră, dar există în continuare un abonament activ pentru Bitdefender Antivirus for Mac, vei reveni la planul gratuit.

6. BITDEFENDER CENTRAL

Acest capitol acoperă următoarele subiecte:

- Despre Bitdefender Central (p. 34)
- Abonamentele mele (p. 35)
- Dispozitivele mele (p. 36)

6.1. Despre Bitdefender Central

Bitdefender Central este platforma web de pe care aveți acces la funcțiile online ale produsului și la servicii și de pe care puteți efectua de la distanță sarcini importante pe dispozitivele pe care este instalat Bitdefender. Vă puteți autentifica la contul Bitdefender de pe orice calculator sau dispozitiv mobil conectat la Internet, accesând https://central.bitdefender.com. După accesare, puteți face următoarele:

- Descarcă și instalează Bitdefender pe sistemele de operare Windows, macOS, iOS și Android. Produsele disponibile pentru descărcare sunt:
 - Bitdefender Antivirus for Mac
 - Linia de produse Windows Bitdefender
 - Bitdefender Mobile Security pentru Android
 - Bitdefender Mobile Security for iOS
 - Bitdefender Parental Advisor
- Administrați și reînnoiți abonamentele Bitdefender.
- Adăugați dispozitive noi la rețeaua dvs. și administrați-le oriunde v-ați afla.

6.2. Accesare Bitdefender Central

Există mai multe moduri de accesare aBitdefender Central. În funcție de sarcina pe care doriți să o efectuați, puteți utiliza oricare dintre următoarele posibilități:

• Din interfața principală Bitdefender Antivirus for Mac:

- 1. Fă clic pe linkul **Mergi la contul tău** situat în partea din dreapta jos a ecranului.
- Din browser-ul web:

- 1. Deschideți un browser web pe orice dispozitive cu acces la Internet.
- 2. Mergeți la: https://central.bitdefender.com.
- Conectați-vă la contul dumneavoastră cu ajutorul adresei de e-mail și parolei.

6.3. Abonamentele mele

Platforma Bitdefender Central vă oferă posibilitatea de a administra cu ușurință abonamentele deținute pentru toate dispozitivele.

6.3.1. Activare abonament

Un abonament poate fi activat în timpul procesului de instalare folosind contul Bitdefender. Concomitent cu procesul de activare, începe să curgă și perioada de valabilitate a abonamentului.

Dacă ați achiziționat un cod de activare de la unul dintre distribuitorii noștri sau l-ați primit cadou, puteți adăuga valabilitatea acestuia la abonamentul Bitdefender.

Pentru a activa un abonament folosind un cod de activare, urmați pașii de mai jos:

- 1. Accesați Bitdefender Central.
- 2. Fă clic pe pictograma E situată în colțul din stânga sus al ferestrei și apoi selectați panoul **Abonamentele mele**.
- 3. Apăsați pe butonul **COD DE ACTIVARE**, apoi introduceți codul în câmpul corespunzător.
- 4. Efectuați clic pe COD DE ACTIVARE pentru a continua.

Abonamentul este acum activat.

Pentru a începe instalarea produsului pe dispozitivele tale, consultă *Instalarea Bitdefender Antivirus for Mac* (p. 1).

6.3.2. Cumpără abonament

Poți achiziționa un abonament direct din contul tău Bitdefender urmând acești pași:

1. Accesați Bitdefender Central.

- 2. Fă clic pe pictograma situată în colțul din stânga sus al ferestrei și apoi selectați panoul **Abonamentele mele**.
- 3. Fă clic pe linkul **Cumpără acum**. Vei fi redirecționat către o pagină web de unde poți face achiziția.

Imediat ce ai finalizat procesul, disponibilitatea abonamentului va fi vizibilă în colțul din dreapta jos al interfeței principale a produsului.

6.4. Dispozitivele mele

Zona **Dispozitivele mele** din contul Bitdefender îți oferă posibilitatea de a instala, administra și efectua operațiuni de la distanță pentru produsul Bitdefender de pe orice dispozitiv pornit și conectat la internet. Secțiunile cu dispozitive afișează numele dispozitivului, starea protecției și dacă există riscuri de securitate ce afectează protecția dispozitivelor tale.

6.4.1. Personalizați-vă dispozitivul

Pentru a vă identifica ușor dispozitivele, puteți personaliza denumirea acestora:

- 1. Accesați Bitdefender Central.
- 2. Selectați secțiunea Dispozitivele mele.
- 3. Efectuează clic pe fila dispozitivului dorit și apoi pe pictograma [‡] din colțul din dreapta sus al ecranului.
- 4. Selectează Setări.
- 5. Introdu o nouă denumire în câmpul **Denumire dispozitiv** și apoi selectează **SALVARE**.

Puteți crea și aloca un deținător pentru fiecare dintre dispozitivele dumneavoastră pentru o mai bună gestionare a acestora:

- 1. Accesați Bitdefender Central.
- 2. Selectați secțiunea Dispozitivele mele.
- 3. Efectuează clic pe fila dispozitivului dorit și apoi pe pictograma [‡] din colțul din dreapta sus al ecranului.
- 4. Selectează Profil.

- Efectuează clic pe Adăugare deținător și completează câmpurile corespunzătoare. Personalizează-ți profilul adăugând o fotografie, selectând data nașterii și adăugând o adresă de e-mail și un număr de telefon.
- 6. Faceți clic pe ADAUGĂ pentru a salva profilul.
- 7. Selectați deținătorul dorit din lista **Deținător dispozitiv**, apoi faceți clic pe **ALOCARE**.

6.4.2. Acțiuni de la distanță

Pentru a actualiza Bitdefender de la distanță pe un dispozitiv:

- 1. Accesați Bitdefender Central.
- 2. Selectați secțiunea Dispozitivele mele.
- 3. Efectuează clic pe fila dispozitivului dorit și apoi pe pictograma [‡] din colțul din dreapta sus al ecranului.
- 4. Selectează Actualizare.

Pentru a activa de la distanță funcția Autopilot:

- 1. Accesați Bitdefender Central.
- 2. Selectați secțiunea Dispozitivele mele.
- 3. Efectuează clic pe fila dispozitivului dorit și apoi pe pictograma [‡] din colțul din dreapta sus al ecranului.
- 4. Selectează **Setări**. Fă clic pe butonul corespunzător pentru a activa funcția Autopilot.

După ce ați făcut clic pe cardul dispozitivului, sunt disponibile următoarele secțiuni:

Panou de bord. În această ferestră, poți vizualiza detalii despre dispozitivul selectat, poți verifica starea de protecție a acestuia și câte amenințări au fost blocate în ultimele șapte zile. Starea de protecție poate fi fie verde, atunci când nu există probleme care îți afectează dispozitivul, fie galbenă, atunci când dispozitivul necesită o intervenție din partea ta, fie roșie, atunci când dispozitivul este supus unor riscuri. Dacă există probleme care afectează dispozitivul tău, fă clic pe săgeata jos din zona de stare din

partea de sus pentru a afla mai multe detalii. De aici, poți remedia manual problemele care afectează securitatea dispozitivelor tale.

Protecție. Din această fereastră puteți rula de la distanță o operațiune de Scanare rapidă sau completă a dispozitivelor. Faceți clic pe butonul SCANARE pentru a iniția procesul. Puteți, de asemenea, verifica momentul la care a avut loc ultima scanare a dispozitivului, fiind, de asemenea, disponibil și un raport al celei mai recente scanări care conține cele mai importante informații. Pentru mai multe informații despre aceste 2 procese de scanare, consultați Scanarea Mac-ului dumneavoastră (p. 13).

7. ÎNTREBĂRI FRECVENTE

Cum pot încerca Bitdefender Antivirus for Mac înainte de a solicita un abonament?

Ești un client nou Bitdefender și dorești să încerci produsul nostru înainte de a-l cumpăra. Perioada de evaluare este de 30 de zile și poți utiliza în continuare produsul instalat numai dacă achiziționezi un abonament Bitdefender. Pentru a încerca Bitdefender Antivirus for Mac, trebuie să:

- 1. Creează-ți un cont Bitdefender urmând acești pași:
 - Mergeți la: https://central.bitdefender.com.
 - Introduceți informațiile solicitate în câmpurile corespunzătoare și apoi faceți clic pe butonul CREARE CONT.

Informațiile furnizate aici vor rămâne confidențiale.

- 2. Descarcă Bitdefender Antivirus for Mac astfel:
 - Selectează fereastra Dispozitivele meleși apoi efectuează clic pe INSTALEAZĂ PROTECȚIA LOCALĂ.
 - Alegeți una dintre cele doua opțiuni disponibile:
 - DESCARCĂ

Faceți clic pe buton și salvați fișierul de instalare.

Pe alt dispozitiv

Selectează **macOS** pentru a descărca produsul Bitdefender și apoi efectuează clic pe **CONTINUARE**. Introdu adresa de e-mail în câmpul corespunzător și efectuează clic pe **TRIMITE**.

• Rulați produsul Bitdefender descărcat.

Am deja un cont de activare. Cum adaug valabilitatea acestuia la abonamentul meu?

Dacă ați achiziționat un cod de activare de la unul dintre distribuitorii noștri sau l-ați primit cadou, puteți adăuga valabilitatea acestuia la abonamentul Bitdefender.

Pentru a activa un abonament folosind un cod de activare, urmați pașii de mai jos:

1. Accesați Bitdefender Central.

- 2. Fă clic pe pictograma situată în colțul din stânga sus al ferestrei și apoi selectați panoul **Abonamentele mele**.
- 3. Apăsați pe butonul **COD DE ACTIVARE**, apoi introduceți codul în câmpul corespunzător.
- 4. Faceți clic din nou pe butonul COD DE ACTIVARE.

Extensia este acum vizibilă în contul tău Bitdefender și în produsul tău Bitdefender Antivirus for Mac instalat, în partea din dreapta jos a ecranului.

Jurnalul de scanare indică faptul că există încă o serie de obiecte nesoluționate. Cum le șterg?

Obiectele nesoluționate din jurnalul de scanare pot fi:

• acces restricționat arhive (xar, rar, etc.)

Soluție: Utilizați opțiunea **Arată în Finder** pentru a identifica fișierul și pentru a-l șterge manual. Goliți folderul Trash.

• acces restricționat cutii poștale (Thunderbird, etc.)

Soluție: Utilizați aplicația pentru a șterge înregistrarea care conține fișierul infectat.

• Conținut din back-up-uri

Soluție: Activează opțiunea **Nu scana conținutul backupurilor** din Preferințele de protecție sau **Adaugă la excepții** fișierele detectate.

Dacă fișierele infectate sunt restabilite ulterior, Bitdefender Antivirus for Mac le va detecta automat și va acționa în mod corespunzător.

🔨 Notă

Fișierele cu acces restricționat sunt fișiere pe care Bitdefender Antivirus for Mac le poate doar deschide, însă pe care nu le poate modifica.

Unde pot vedea detalii despre activitatea produsului?

Bitdefender păstrează un jurnal al tuturor acțiunilor importante, al tuturor modificărilor de stare și al altor mesaje importante cu privire la activitatea sa. Pentru a accesa aceste informații, deschideți fereastra Preferințe Bitdefender Antivirus for Mac:

- 1. Deschideți Bitdefender Antivirus for Mac.
- 2. Puteți proceda în oricare dintre următoarele modalități:

- Faceți clic pe Bitdefender Antivirus for Macîn bara de meniu și selectați Preferințe.
- Faceți clic pe icoana 🛽 în bara de meniu și selectați **Preferințe**.
- Apăsați tastele comandă-virgulă (,).
- 3. Selectează fila Istoric.

Sunt afișate detalii privind activitatea produsului.

Pot actualiza Bitdefender Antivirus for Mac printr-un server proxy?

Bitdefender Antivirus for Mac se poate actualiza numai prin servere proxy care nu necesită autentificare. Nu este necesară configurarea vreunor setări de program.

Dacă vă conectați la internet prin intermediul unui server proxy ce necesită autentificare, trebuie să treceți în mod regulat la o conexiune directă la internet pentru a putea obține actualizările semnăturilor softurilor periculoase.

Cum dezinstalez Bitdefender Antivirus for Mac?

Pentru a șterge Bitdefender Antivirus for Mac, urmați pașii de mai jos:

- 1. Deschide o fereastră Finder, mergi la directorul Aplicații și selectează Utilități.
- 2. Fă dublu clic pe aplicația Bitdefender Uninstaller.
- 3. Faceți clic pe Dezinstalează pentru a continua.
- 4. Așteaptă terminarea procesului și apoi fă clic pe **închidere** pentru finalizare.

🔿 Important

În cazul apariției unei erori, puteți contacta serviciul Bitdefender Customer Care, așa cum se descrie în *Suport* (p. 44).

Cum șterg extensiile TrafficLight din browser-ul meu web?

- Pentru a şterge extensiile TrafficLight din Mozilla Firefox, urmaţi paşii de mai jos:
 - 1. Deschideți browser-ul Mozilla Firefox.
 - 2. Mergeți la Instrumente și selectați Add-ons.
 - 3. Selectați Extensii din coloana din partea stângă.
 - 4. Selectați extensia și faceți clic pe Ștergere.

Bitdefender Antivirus for Mac

- 5. Reporniți browser-ul pentru finalizarea procesului de ștergere.
- Pentru a şterge extensiile TrafficLight din Google Chrome, urmaţi paşii de mai jos:
 - 1. Deschideți browser-ul Google Chrome.
 - 2. În colțul din dreapta sus, efectuează clic pe Mai mult
 - 3. Mergi la Mai multe instrumente și selectează Extensii.
 - 4. Efectuează clic pe pictograma **Dezinstalează din Chrome...** de lângă extensia pe care dorești să o ștergi.
 - 5. Efectuează clic pe **Dezinstalare** pentru a confirma procesul de stergere.
- Pentru a şterge Bitdefender TrafficLight din Safari, urmaţi paşii de mai jos:
 - 1. Deschideți browser-ul Safari.
 - Faceți click pe in din bara de instrumente a browserului și faceți clic pe Preferences.
 - 3. Selectați tab-ul **Extensii** și identificați extensia **Bitdefender TrafficLight în Safari** în listă.
 - 4. Selectați extensia și faceți clic pe Dezinstalare.
 - 5. Faceți clic pe Dezinstalare pentru a confirma procesul de ștergere.

Când ar trebui să folosesc Bitdefender VPN?

Trebuie să procedezi cu atenție atunci când accesezi, descarci sau încarci conținut pe Internet. Pentru a te asigura că rămâi în siguranță în timp ce navighezi pe internet, îți recomandăm să folosești Bitdefender VPN în următoarele situații:

- când dorești să te conectezi la rețele wireless publice
- când dorești să accesezi conținut care în mod normal este restricționat în anumite zone, indiferent dacă ești acasă sau în străinătate
- când dorești să-ți păstrezi confidențialitatea datelor tale personale (nume de utilizator, parole, datele cardului de credit etc.)
- când dorești să-ți ascunzi adresa IP

Bitdefender VPN va avea un impact negativ asupra nivelului de încărcare a bateriei dispozitivului meu?

Funcția Bitdefender VPN este proiectată pentru a-ți proteja datele personale, pentru a-ți ascunde adresa IP atunci când ești conectat la rețele wireless nesecurizate și pentru a-ți permite să accesezi conținut restricționat în anumite țări. Pentru a evita consumarea inutilă a bateriei, îți recomandăm să folosești funcția VPN numai atunci când ai nevoie de ea și să te deconectezi atunci când ești offline.

De ce este redusă viteza de navigare pe internet atunci când sunt conectat prin Bitdefender VPN?

Funcția Bitdefender VPN este proiectată pentru a-ți oferi o experiență de navigare pe internet cu impact redus asupra resurselor, însă, cu toate acestea, conexiunea la internet sau distanța serverului la care te conectezi pot cauza încetiniri. În acest caz, dacă este absolut necesar să te conectezi din locația ta la un server găzduit la mare distanță (de ex. din SUA la China), îți recomandăm să permiți funcției Bitdefender VPN să te conecteze automat la cel mai apropiat server sau să găsească un server mai apropiat de locația ta actuală.

8. OBȚINERE AJUTOR

Acest capitol acoperă următoarele subiecte:

- Suport (p. 44)
- Informații de contact (p. 46)

8.1. Suport

Bitdefender se străduiește să ofere clienților săi un nivel neegalat în ceea ce privește rapiditatea și acuratețea suportului tehnic. Dacă vă confruntați cu o problemă sau aveți o întrebare referitoare la produsul Bitdefender deținut, puteți utiliza un număr de resurse online pentru a găsi rapid o soluție sau un răspuns. Sau, dacă preferați, puteți contacta serviciul de asistență clienți al Bitdefender. Reprezentanții noștri vă vor răspunde la întrebări la timp și vă vor oferi asistența de care aveți nevoie.

8.1.1. Resurse online

Sunt disponibile mai multe resurse online pentru a vă ajuta la soluționarea problemelor și întrebărilor referitoare la produsul Bitdefender.

• Centrul de asistență Bitdefender :

https://www.bitdefender.ro/support/consumer.html

• Forum asistență Bitdefender:

https://forum.bitdefender.com

• Portalul de securitate informatică HOTforSecurity:

https://www.hotforsecurity.com

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare privind securitatea calculatoarelor, produsele și compania Bitdefender.

Centrul de asistență Bitdefender

Centrul de asistență Bitdefender este un depozit online ce conține informații despre produsele Bitdefender. Acesta stochează, într-un format ușor accesibil, rapoarte privind rezultatele unor activități continue de asistență tehnică și remediere ale echipelor de asistență și dezvoltare Bitdefender, alături de articole mai generale referitoare la prevenirea virușilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Centrul de asistență Bitdefender este deschis publicului și pot fi realizate căutări în mod liber. Prin intermediul informațiilor extinse pe care le conține, putem oferi clienților Bitdefender cunoștințele tehnice și înțelegerea de care au nevoie. Toate solicitările valide de informații sau rapoarte de eroare care vin din partea clienților Bitdefender ajung la Centrul de asistență Bitdefender sub formă de rapoarte de remediere a erorilor, notițe de evitare a erorilor sau articole informative pentru a completa fișierele de ajutor ale produsului.

Centrul de asistență Bitdefender este disponibil în orice moment la următoarea adresă: https://www.bitdefender.ro/support/consumer.html.

Forum asistență Bitdefender

Forumul de suport al Bitdefender le oferă utilizatorilor Bitdefender o modalitate facilă de a obține ajutor și de a-i ajuta pe alții. Puteți posta orice probleme sau întrebări legate de produsul dumneavoastră Bitdefender.

Reprezentanții de suport tehnic ai Bitdefender monitorizează forumul pentru a verifica noile postări cu scopul de a vă ajuta. De asemenea, puteți obține un răspuns sau o soluție de la un utilizator Bitdefender cu mai multă experiență.

Înainte de a posta problema sau întrebarea, sunteți rugat să verificați în forum existența unui subiect similar sau corelat.

Forumul de suport al Bitdefender este disponibil la https://forum.bitdefender.com, în 5 limbi diferite: engleză, germană, franceză, spaniolă și română. Faceți clic pe linkul **Home & Home Office Protection** pentru a accesa secțiunea dedicată produselor pentru consumatori individuali.

Portalul HOTforSecurity

Portalul Malware City constituie o sursă bogată de informații privind securitatea informatică. Aici puteți afla informații despre diversele pericole la care este expus calculatorul dumneavoastră atunci când este conectat la internet (malware, phishing, spam, infracțiuni cibernetice). Un dicționar util vă ajută la înțelegerea termenilor de securitate a calculatoarelor cu care nu sunteți familiarizați. Se postează în mod regulat noi articole pentru a vă ține la curent cu cele mai recente pericole descoperite, tendințele actuale din domeniul securității și alte informații din domeniul securității calculatoarelor.

Vizitați pagina de web HOTforSecurity accesând https://www.hotforsecurity.com.

8.1.2. Solicitarea de asistență profesională

Ne puteți contacta pentru asistență prin intermediul Centrului de asistență online:

- 1. Mergeți la https://www.bitdefender.ro/support/consumer.html.
- 2. Căutați în Centrul de asistență articole care vă pot ajuta să soluționați problema cu care vă confruntați.
- 3. Citiți articolele sau documentele relevante și încercați soluțiile propuse.
- Dacă nu ați găsit o soluție, faceți clic pe Contactați-ne în partea de jos a ferestrei.
- 5. Folosiți formularul de contact pentru a deschide un tichet de asistență prin e-mail sau accesați o altă opțiune de contact disponibilă.

8.2. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. Din 2001, BITDEFENDER a câștigat o reputație indisputabilă, căutând în mod constant mijloace pentru o comunicare mai bună în vederea depășirii așteptărilor clienților și partenerilor noștri. Dacă ai nelămuriri, nu ezita să ne contactezi.

8.2.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro Centrul de asistență:https://www.bitdefender.ro/support/consumer.html Documentație: documentation@bitdefender.com Distribuitori locali:https://www.bitdefender.ro/partners Program de Parteneriat: partners@bitdefender.com Relații media: pr@bitdefender.com Cariere: jobs@bitdefender.com Subscrieri viruși: virus_submission@bitdefender.com Subscrieri spam: spam_submission@bitdefender.com Raportare abuz: abuse@bitdefender.com Sit web:https://www.bitdefender.ro

8.2.2. Distribuitori locali

Distribuitorii locali Bitdefender sunt pregătiți să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale.

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

- 1. Mergeți la https://www.bitdefender.ro/partners.
- 2. Mergeți la Localizare partener.
- 3. Datele de contact ale distribuitorilor locali Bitdefender ar trebui să fie afișate automat. În caz contrar, selectați țara de reședință pentru a accesa aceste informații.
- 4. În cazul în care nu găsiți un distribuitor Bitdefender în țara dumneavoastră, nu ezitați să ne contactați prin e-mail la adresa sales@bitdefender.com. Vă rugăm să scrieți mesajul în română sau engleză pentru a ne da posibilitatea să vă ajutăm cu promptitudine.

8.2.3. Filialele Bitdefender

Sucursalele Bitdefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale. Adresele lor precum și modul în care pot fi contactate sunt date mai jos.

U.S.A

Bitdefender, LLC

6301 NW 5th Way, Suite 4300 Fort Lauderdale, Florida 33309 Telefon (birou&vânzări): 1-954-776-6262 Vânzări: sales@bitdefender.com Suport tehnic: https://www.bitdefender.com/support/consumer.html Web: https://www.bitdefender.com

Emiratele Arabe Unite

Dubai Internet City Building 17, Office # 160 Dubai, UAE Telefon vânzări: 00971-4-4588935 / 00971-4-4589186 E-mail vânzări: mena-sales@bitdefender.com Suport tehnic: https://www.bitdefender.com/support/consumer.html Sit web: https://www.bitdefender.com

Germania

Bitdefender GmbH

TechnoPark Schwerte Lohbachstrasse 12 D - 58239 Schwerte Birou: +49 2304 9 45 - 162 Fax: +49 2304 9 45 - 169 Vânzări: vertrieb@bitdefender.de Suport tehnic: https://www.bitdefender.de/support/consumer.html Web: https://www.bitdefender.de

Spania

Bitdefender España, S.L.U.

C/Bailén, 7, 3-D 08010 Barcelona Fax: +34 93 217 91 28 Telefon: +34 902 19 07 65 Vânzări: comercial@bitdefender.es Suport tehnic: https://www.bitdefender.es/support/consumer.html Sit web: https://www.bitdefender.es

România

BITDEFENDER SRL

Complex DV24, Building A, 24 Delea Veche Street, Sector 2 Bucharest Fax: +40 21 2641799 Telefon vânzări: +40 21 2063470 E-mail vânzări: sales@bitdefender.ro Suport tehnic: https://www.bitdefender.ro/support/consumer.html Sit web: https://www.bitdefender.ro

Tipuri de softuri periculoase

adware

Adware-ul este adesea combinat cu o aplicație gazdă, care este oferită gratuit dacă utilizatorul acceptă adware. Deoarece aplicațiile adware sunt, de obicei, instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere sau abonament care explică scopul aplicației, nu este comisă nicio infracțiune.

Totuși, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanțele sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le adună pot reprezenta motive de îngrijorare pentru utilizatorii care nu cunosc în întregime condițiile contractului de licențiere sau abonament.

Keylogger

Un keylogger este o aplicație care înregistrează orice tastați.

Keylogger-urile nu sunt periculoase prin natura lor. Acestea pot fi utilizate în scopuri legitime, ca de exemplu pentru monitorizarea activității copiilor sau a angajaților. Totuși, sunt folosite din ce în ce mai mult de infractorii cibernetici în scopuri negative (ca de exemplu, pentru a colecta date personale, cum ar fi acreditările de înregistrare și codurile numerice personale).

Ransomware

Ransomware este un program periculos care încearcă să obțină bani de la utilizatori prin blocarea sistemelor vulnerabile. CryptoLocker, CryptoWall și TeslaWall sunt doar câteva variante care vânează sistemele personale ale utilizatorilor.

Infecția se poate extinde prin accesarea mesajelor spam, descărcarea atașamentelor e-mail sau instalarea de aplicații, fără ca utilizator să afle ce se întâmplă pe sistemul său. Utilizatorii și companiile sunt vizate zilnic de către hackerii ransomware.

Rootkit

Un rootkit este un set de unelte soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la unelte recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, loginuri și jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde aplicații malițioase sau prezența intrușilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la Internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și un virus troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victima unei aplicații spyware este acela de a descărca anumite produse de schimb de fișiere peer-to-peer, care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

Troian

Este un program distructiv care este deghizat sub forma unei aplicații benigne. Spre deosebire de viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai deghizați troieni este acela care pretinde că elimină virușii de pe computerul tău, dar în loc de aceasta, introduce viruși pe computerul tău.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul orașului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.

Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a virușilor se pot și înmulți. Toți virușii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar și un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus și mai periculos este acela care este capabil să se răspândească în rețea și poate să treacă de sistemele de securitate.

Virus polimorf

Reprezintă un virus care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruși sunt greu de identificat.