

Bitdefender[®] FAMILY PACK



MANUAL DE UTILIZARE



iOS



Bitdefender Family Pack Manual de utilizare

Publicat 13.12.2019

Copyright© 2019 Bitdefender

Termeni legali

Toate drepturile rezervate. Nicio parte a acestui document nu va putea fi reproducă 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 nici o 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 linkuri 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 al căror link este furnizat în acest document îți aparține în totalitate. Bitdefender furnizează aceste linkuri exclusiv pentru ușurarea consultării documentului și prezența lor nu presupune faptul că Bitdefender susține sau își asumă responsabilitatea pentru conținutul 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 recunoscute ca atare.



Cuprins

Despre acest Ghid	x
1. Scopul și publicul țintă	x
2. Cum să folosești acest ghid	x

Total Security pentru PC 1

1. Instalare	2
1.1. Pregătirea pentru instalare	2
1.2. Cerințe de sistem	2
1.3. Instalarea produsului tău Bitdefender	3
1.3.1. Instalează din Bitdefender Central	4
1.3.2. Instalare de pe discul de instalare	6
2. Primii pași	11
2.1. Informații de bază	11
2.1.1. Notificări	13
2.1.2. Profile	14
2.1.3. Protecție cu parolă pentru setările Bitdefender	15
2.1.4. Rapoarte despre produs	16
2.1.5. Notificări privind ofertele speciale	16
2.2. Interfața Bitdefender	17
2.2.1. Pictograma barei de sistem	17
2.2.2. Meniu de navigare	19
2.2.3. Panou de bord	20
2.2.4. Secțiunile Bitdefender	23
2.2.5. Asistent de securitate	28
2.2.6. Modifică limba produsului	30
2.3. Bitdefender Central	30
2.3.1. Autentificare în doi pași	31
2.3.2. Abonamentele mele	34
2.3.3. Dispozitivele mele	36
2.3.4. Activitate	38
2.3.5. Notificări	39
2.4. Actualizarea permanentă a Bitdefender	39
2.4.1. Cum verificați dacă Bitdefender este actualizat	40
2.4.2. Efectuarea unei actualizări	40
2.4.3. Activarea sau dezactivarea actualizării automate	41
2.4.4. Ajustarea setărilor de actualizare	42
2.4.5. Actualizări permanente	42
3. Cum să	44
3.1. Instalare	44
3.1.1. Cum instalez Bitdefender pe un al doilea calculator?	44
3.1.2. Cum reinstalez Bitdefender?	44
3.1.3. De unde se poate descărca produsul Bitdefender?	45
3.1.4. Cum pot modifica limba produsului meu Bitdefender?	46
3.1.5. Cum folosesc abonamentul Bitdefender după un upgrade Windows?	46
3.1.6. Cum pot face upgrade la cea mai recentă versiune Bitdefender?	49



3.2. Bitdefender Central	50
3.2.1. Cum mă autentific în contul Bitdefender cu un alt cont?	50
3.2.2. Cum pot dezactiva mesajele de ajutor pentru Bitdefender Central?	50
3.2.3. Am uitat parola setată pentru contul meu Bitdefender. Cum se resetează?	51
3.2.4. Cum pot gestiona sesiunile de autentificare asociate contului meu Bitdefender?	51
3.3. Scanarea cu Bitdefender	52
3.3.1. Cum scanez un fișier sau un director?	52
3.3.2. Cum îmi scanez sistemul?	52
3.3.3. Cum programez o scanare?	53
3.3.4. Cum creez o activitate de scanare personalizată?	54
3.3.5. Cum exclud un director de la procesul de scanare?	55
3.3.6. Ce să fac atunci când Bitdefender a detectat un fișier curat ca fiind infectat?	56
3.3.7. Cum aflu ce amenințări au fost detectate de Bitdefender?	57
3.4. Control Parental	58
3.4.1. Cum îmi protejez copiii împotriva amenințărilor online?	58
3.4.2. Cum blochez accesul copilului meu la un anumit site web?	59
3.4.3. Cum îmi împiedic copilul să folosească anumite aplicații?	60
3.4.4. Cum îmi împiedic copilul să intre în contact cu persoane care nu sunt de încredere?	60
3.4.5. Cum pot seta o locație ca fiind sigură sau restricționată pentru copilul meu?	61
3.4.6. Cum blochez accesul copilului meu la dispozitivele alocate în timpul activităților zilnice?	62
3.4.7. Cum blochez accesul copilului meu la dispozitivele asociate ziua sau noaptea?	62
3.4.8. Ștergerea profilului de copil	63
3.4.9. Cum pot face upgrade la Bitdefender Parental Control Premium?	63
3.5. Protecție confidențialitate	64
3.5.1. Cum mă asigur că tranzacțiile mele online sunt securizate?	64
3.5.2. Ce pot face dacă mi-a fost furat dispozitivul?	65
3.5.3. Cum utilizez seifurile pentru fișiere?	66
3.5.4. Cum șterg definitiv un fișier cu ajutorul Bitdefender?	67
3.5.5. Cum îmi protejez de hackeri camera web?	68
3.5.6. Cum pot restabili manual fișierele criptate atunci când procesul de restabilire eșuează?	68
3.6. Instrumente de optimizare	69
3.6.1. Cum pot îmbunătăți performanța sistemului meu?	69
3.6.2. Cum pot îmbunătăți timpul de pornire al sistemului meu?	70
3.7. Informații utile	70
3.7.1. Cum îmi testez soluția de securitate?	70
3.7.2. Cum dezinstalez Bitdefender?	71
3.7.3. Cum dezinstalez Bitdefender VPN?	72
3.7.4. Cum dezinstalez extensia Bitdefender Anti-tracker?	73
3.7.5. Cum închid automat calculatorul după finalizarea operațiunii de scanare?	74
3.7.6. Cum pot configura Bitdefender să utilizeze o conexiune la internet de tip proxy?	75



3.7.7. Utilizez o versiune Windows pe 32 biți sau pe 64 biți?	76
3.7.8. Cum pot afișa elementele ascunse din Windows?	77
3.7.9. Cum elimin celelalte soluții de securitate?	77
3.7.10. Cum pot să repornesc sistemul în Safe Mode?	79
4. Administrarea securității dumneavoastră	81
4.1. Protecție antivirus	81
4.1.1. Scanare la accesare (protecție în timp real)	82
4.1.2. Scanare la cerere	87
4.1.3. Scanarea automată a suporturilor media amovibile	96
4.1.4. Scanare fișier de configurare a gazdelor	98
4.1.5. Configurarea excepțiilor de scanare	98
4.1.6. Gestionarea fișierelor aflate în carantină	101
4.2. Advanced Threat Defense	102
4.3. Online Threat Prevention	104
4.4. Antispam	106
4.4.1. Detalii privind modulul Antispam	107
4.4.2. Activarea sau dezactivarea protecției antispam	109
4.4.3. Utilizarea barei de instrumente antispam în fereastra de client de e-mail	109
4.4.4. Configurarea listei de prieteni	111
4.4.5. Configurarea listei de spammeri	113
4.4.6. Se configurează filtrele locale antispam	114
4.4.7. Configurarea setărilor cloud	115
4.5. Firewall	115
4.5.1. Administrarea regulilor pentru aplicații	116
4.5.2. Administrarea setărilor de conectare	119
4.5.3. Configurarea setărilor avansate	120
4.6. Vulnerabilități	121
4.6.1. Scanarea sistemului pentru identificarea vulnerabilităților	122
4.6.2. Cu ajutorul monitorizării automate a vulnerabilităților	123
4.6.3. Evaluare securitate rețele Wi-Fi	125
4.7. Protecție video și audio	129
4.7.1. Protecție cameră web	129
4.7.2. Monitorizare microfon	132
4.8. Protecție Fișiere	133
4.8.1. Activarea și dezactivarea caracteristicii Protecție Fișiere	134
4.8.2. Protejați fișierele personale contra atacurilor ransomware	134
4.8.3. Configurarea accesului la aplicații	135
4.8.4. Protecție la pornire	136
4.9. Remediere ransomware	136
4.10. File Encryption	139
4.11. Protecția datelor de autentificare cu Password Manager	143
4.12. Anti-tracker	150
4.13. VPN	153
4.14. Securitate Safepay pentru tranzacțiile online	156
4.15. Data Protection	161
4.16. Control Parental	162
4.16.1. Accesarea funcției Control parental - Copiii mei	163
4.16.2. Creează profiluri pentru copiii tăi	164



4.16.3. Configurarea profilurilor de Control parental	169
4.16.4. Abonamente Bitdefender Parental Control	177
4.17. Antifurt	178
4.18. Bitdefender USB Immunizer	181
5. Optimizare de sistem	182
5.1. Instrumente	182
5.1.1. Optimizați viteza sistemului cu un singur clic	182
5.1.2. Optimizarea timpului de pornire al calculatorului dvs.	183
5.1.3. Se optimizează discul	184
5.2. Profiluri	186
5.2.1. Profil Lucru	187
5.2.2. Profil Film	188
5.2.3. Profil Joc	189
5.2.4. Profil Wi-Fi public	191
5.2.5. Profil mod baterie	191
5.2.6. Optimizare în timp real	192
6. Remedierea problemelor	193
6.1. Soluționarea problemelor frecvente	193
6.1.1. Sistemul meu funcționează lent	193
6.1.2. Nu începe scanarea	195
6.1.3. Nu mai pot utiliza o aplicație	197
6.1.4. Ce trebuie făcut atunci când Bitdefender blochează un site web, un domeniu, o adresă IP sau o aplicație online care sunt sigure	198
6.1.5. Ce trebuie să faci dacă Bitdefender detectează ca ransomware o aplicație sigură	199
6.1.6. Nu mă pot conecta la internet	199
6.1.7. Nu pot accesa un dispozitiv din rețeaua mea	200
6.1.8. Conexiunea mea la internet este lentă	202
6.1.9. Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet ..	203
6.1.10. Serviciile Bitdefender nu răspund	204
6.1.11. Filtrul Antispam nu funcționează corespunzător	204
6.1.12. Funcția Completare automată din Portofel nu funcționează	209
6.1.13. Nu s-a reușit deinstalarea Bitdefender	210
6.1.14. Sistemul meu nu pornește după ce am instalat Bitdefender	211
6.2. Eliminarea amenințărilor din sistemul dumneavoastră	214
6.2.1. Bitdefender Modul de recuperare (Mediul de recuperare în Windows 10)	215
6.2.2. Ce trebuie să faci atunci când Bitdefender detectează amenințări pe computerul tău?	218
6.2.3. Cum elimin o amenințare dintr-o arhivă?	220
6.2.4. Cum elimin o amenințare dintr-o arhivă de e-mail?	221
6.2.5. Ce trebuie să fac dacă suspectez că un fișier este periculos?	222
6.2.6. Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?	223
6.2.7. Ce reprezintă elementele omise din jurnalul de scanare?	223
6.2.8. Ce reprezintă fișierele supracomprimate din jurnalul de scanare?	223
6.2.9. De ce Bitdefender a șters în mod automat un fișier infectat?	224

Antivirus pentru Mac **225**



7. Instalare și deinstalare	226
7.1. Cerințe de sistem	226
7.2. Instalarea Bitdefender Antivirus for Mac	226
7.2.1. Proces de instalare	227
7.3. Eliminarea Bitdefender Antivirus for Mac	231
8. Introducere	232
8.1. Despre Bitdefender Antivirus for Mac	232
8.2. Deschiderea Bitdefender Antivirus for Mac	232
8.3. Fereastră principală aplicație	233
8.4. Pictogramă aplicație în Dock	234
8.5. Meniu de navigare	234
8.6. Mod întunecat	235
9. Protecția împotriva softurilor periculoase	236
9.1. Recomandări de utilizare	236
9.2. Scanarea Mac-ului dumneavoastră	237
9.3. Asistent scanare	238
9.4. Carantină	239
9.5. Bitdefender Shield (protecție în timp real)	240
9.6. Excepții scanare	241
9.7. Protecție web	242
9.8. Anti-tracker	243
9.8.1. Interfața Anti-tracker	245
9.8.2. Dezactivarea Bitdefender Anti-tracker	245
9.8.3. Permiteți urmărirea unui site web	245
9.9. Protecție Fișiere	246
9.9.1. Administrare aplicații	247
9.10. Protecție Time Machine	248
9.11. Remedierea problemelor	248
9.12. Notificări	250
9.13. Actualizări	251
9.13.1. Cererea unei actualizări	251
9.13.2. Obținerea actualizărilor prin intermediul unui server proxy	252
9.13.3. Actualizați la o nouă versiune	252
9.13.4. Cum găsești informații despre Bitdefender Antivirus for Mac	252
10. Configurarea preferințelor	253
10.1. Accesarea preferințelor	253
10.2. Preferințe de protecție	253
10.3. Preferințe avansate	254
10.4. Oferte speciale	254
11. VPN	255
11.1. Despre VPN	255
11.2. Deschiderea conexiunii VPN	255
11.3. Interfața	256
11.4. Abonamente	258
12. Bitdefender Central	259
12.1. Despre Bitdefender Central	259



12.2. Accesare Bitdefender Central	260
12.3. Autentificare în doi pași	260
12.4. Adăugarea dispozitivelor sigure	262
12.5. Abonamentele mele	262
12.5.1. Activare abonament	262
12.5.2. Cumpără abonament	263
12.6. Dispozitivele mele	263
12.6.1. Personalizați-vă dispozitivul	263
12.6.2. Acțiuni de la distanță	264
13. Întrebări frecvente	266
Mobile Security pentru iOS	271
14. Ce este Bitdefender Mobile Security for iOS	272
15. Introducere	273
16. VPN	277
16.1. Abonamente	278
17. Protecție web	280
17.1. Alerte Bitdefender	280
17.2. Abonamente	281
18. Confidențialitate cont	283
19. Bitdefender Central	285
Mobile Security pentru Android	290
20. Funcții de protecție	291
21. Introducere	292
22. Scanare malware	297
23. Protecție web	300
24. VPN	302
25. Funcții Antifurt	305
26. Confidențialitate cont	309
27. Blocare Aplicații	311
28. Rapoarte	316
29. WearON	317
30. Despre	318
31. Bitdefender Central	319
32. Întrebări frecvente	326



Contactați-ne	332
33. Solicitarea ajutorului	333
34. Resurse online	336
34.1. Centrul de asistență Bitdefender	336
34.2. Forumul de suport al Bitdefender	337
34.3. Portalul HOTforSecurity	337
35. Informații de contact	338
35.1. Adrese web	338
35.2. Distribuitori locali	338
35.3. Filialele Bitdefender	338
Vocabular	341



Despre acest Ghid

1. Scopul și publicul țintă

Abonamentul tău Bitdefender Family Pack acoperă până la 15 dispozitive dintr-o locuință, incluzând PC-urile, Mac-urile, smartphone-urile și tabletele Android și iOS deținute de familia ta.

Poți administra dispozitivele tale protejate prin intermediul contului tău Bitdefender, care trebuie să fie asociat unui abonament activ.

Acest ghid oferă asistență pentru configurarea și utilizarea produselor incluse în abonamentul tău: Bitdefender Total Security (pentru Windows), Bitdefender Antivirus for Mac (pentru macOS), Bitdefender Mobile Security (pentru Android) și Bitdefender Mobile Security for iOS.

Poți afla cum să configurezi Bitdefender pe diferite dispozitive pentru a le menține protejate de toate tipurile de amenințări.

2. Cum să folosești acest ghid

Acest ghid este organizat în jurul a patru produse incluse în Bitdefender Family Pack:

- „Total Security pentru PC” (p. 1)

Află cum poți utiliza produsul pe PC-urile și laptop-urile tale cu sistem de operare Windows.

- „Antivirus pentru Mac” (p. 225)

Află cum poți utiliza produsul pe Mac-urile tale.

- „Mobile Security pentru iOS” (p. 271)

Află cum poți utiliza produsul pe smartphone-urile și tabletele tale cu sistem de operare iOS.

- „Mobile Security pentru Android” (p. 290)

Află cum poți utiliza produsul pe smartphone-urile și tabletele tale cu sistem de operare Android.

- „Contactați-ne” (p. 332)

Află unde poți găsi ajutor dacă apare o problemă neașteptată.



TOTAL SECURITY PENTRU PC



1. INSTALARE

1.1. Pregătirea pentru instalare

Pentru a instala Bitdefender Total Security fără probleme, trebuie să parcurgi acești pași prealabili:

- Asigurați-vă dacă calculatorul pe care doriți să instalați Bitdefender îndeplinește cerințele de sistem. În cazul în care calculatorul nu întrunește toate cerințele de sistem, Bitdefender nu va fi instalat sau nu va funcționa în mod corespunzător, determinând reducerea vitezei de funcționare și instabilitatea sistemului. Pentru o listă completă a cerințelor de sistem, consultați *„Cerințe de sistem”* (p. 2).
- Autentifica-te pe calculator cu datele unui cont de administrator.
- Dezinstalează orice alt program similar de pe computer. Dacă se detectează ceva în timpul procesului de instalare Bitdefender, vei primi o notificare de dezinstalare. Rularea simultană a două programe de securitate poate afecta funcționarea lor și poate provoca probleme majore ale sistemului. Windows Defender va fi dezactivat în timpul instalării.
- Dezactivează sau dezinstalează orice alt program firewall de pe calculator. Rularea simultană a două programe firewall poate afecta funcționarea lor și poate provoca probleme majore ale sistemului. Windows Firewall va fi dezactivat în timpul instalării.
- Se recomandă ca, în timpul instalării, computerul tău să fie conectat la internet, chiar atunci când instalarea se face de pe un CD/DVD. Dacă sunt disponibile versiuni mai noi ale fișierelor aplicației decât cele incluse în pachetul de instalare, Bitdefender le va descărca și le va instala.

1.2. Cerințe de sistem

Poți instala Bitdefender Total Security doar pe calculatoare pe care rulează următoarele sisteme de operare:

- Windows 7 cu Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10



- 2,5 GB spațiu liber disponibil pe hard disk (cel puțin 800 MB pe unitatea de sistem)
- Intel Core Duo (2 GHz) sau procesor echivalent
- 2 GB de memorie (RAM)



Notă

Pentru a afla pe ce sistem de operare funcționează calculatorul tău și informațiile referitoare la hardware:

- În **Windows 7**, efectuează clic dreapta pe **My Computer** de pe desktop și selectează **Properties** din meniu.
- În **Windows 8**, din ecranul de Start al Windows, localizează Computer (de exemplu, poți începe să tastezi **Computer** direct în ecranul de Start) și efectuează clic dreapta pe pictograma acestuia. În **Windows 8.1**, localizează **Acest PC**.

Selectează **Proprietăți** din meniul din partea de jos. Caută în zona **Sistem** pentru a afla informații referitoare la tipul de sistem.

- În **Windows 10**, introdu **Sistem** în caseta de căutare din bara de sarcini și efectuează clic pe pictograma aferentă. Caută în zona **Sistem** pentru a afla informații referitoare la tipul de sistem.

Cerințe software

Pentru a putea utiliza Bitdefender și toate funcțiile sale, computerul tău trebuie să îndeplinească următoarele cerințe software:

- Microsoft Edge 40 sau superior
- Internet Explorer 10 sau o variantă mai recentă
- Mozilla Firefox 51 și o versiune mai recentă
- Google Chrome 34 și o versiune mai recentă

1.3. Instalarea produsului tău Bitdefender

Poți instala Bitdefender folosind CD-ul de instalare sau aplicația web descărcată pe calculatorul tău **Bitdefender Central**.

Dacă produsul achiziționat acoperă mai multe calculatoare, repetă procesul de instalare și activează produsul utilizând același cont pe fiecare calculator. Contul pe care trebuie să-l folosești este cel care conține abonamentul dvs. activ pentru Bitdefender.



1.3.1. Instalează din Bitdefender Central

Din Bitdefender Central puteți descărca kitul de instalare corespunzător abonamentului achiziționat. Odată ce procesul de instalare s-a finalizat, Bitdefender Total Security este dezactivat.

Pentru a descărca Bitdefender Total Security din Bitdefender Central:

1. Accesați **Bitdefender Central**.
2. Selectează fereastra **Dispozitivele mele** și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA**.
3. Alegeți una dintre cele două opțiuni disponibile:
 - **Protejează acest dispozitiv**
 - a. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
 - b. Salvează fișierul de instalare.
 - **Protejează alte dispozitive**
 - a. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
 - b. Selectează **TRIMITE LINKUL PENTRU DESCĂRCARE**.
 - c. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**.

Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.
 - d. Pe dispozitivul pe care dorești să instalezi produsul Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.
4. Așteaptă să se finalizeze descărcarea și apoi execută aplicația de instalare.

Validarea instalării

Bitdefender verifică mai întâi sistemul tău pentru a valida instalarea.

Dacă sistemul tău nu îndeplinește cerințele de sistem pentru instalarea Bitdefender, vei fi informat cu privire la zonele ce necesită să fie îmbunătățite înainte să poți continua.



Dacă este detectat o soluție antivirus necompatibilă sau o versiune mai veche a Bitdefender, vi se va cere să le ștergeți de pe sistemul dumneavoastră. Vă rugăm să urmați instrucțiunile pentru a șterge software-ul din sistemul dumneavoastră, evitând astfel apariția problemelor pe viitor. Este posibil să fie nevoie să reporniți calculatorul pentru a finaliza dezinstalarea soluțiilor antivirus detectate.

Pachetul de instalare Bitdefender Total Security este actualizat constant.



Notă

Descărcarea fișierelor de instalare poate dura foarte mult, cu precădere în cazul conexiunilor internet mai lente.

După validarea instalării, se afișează asistentul de configurare. Urmați pașii pentru instalarea Bitdefender Total Security.

Pasul 1 - Instalarea Bitdefender

Înainte de a începe instalarea, este necesar să îți exprimi acordul cu privire la Contractul de abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Total Security.

Dacă nu ești de acord cu acești termeni, închide fereastra. Procesul de instalare va fi abandonat și vei ieși din fereastra de instalare.

În cadrul acestui pas se pot efectua două sarcini suplimentare:

- Menține opțiunea **Trimite rapoarte despre produs** activă. Prin permiterea acestei opțiuni, sunt trimise rapoarte către serverele Bitdefender, conținând informații despre modul în care utilizezi produsul. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să îți oferim produse și mai bune pe viitor. Rapoartele nu conțin date confidențiale, cum ar fi numele tău sau adresa IP, și nu vor fi folosite în scopuri comerciale.
- Selectează limba în care dorești să instalezi produsul.

Efectuează clic pe **INSTALARE** pentru a lansa procesul de instalare al produsului tău Bitdefender.

Pasul 2 - Instalare în curs de desfășurare

Așteaptă până când instalarea este finalizată. Sunt afișate informații detaliate cu privire la evoluția instalării.



Pasul 3 - Instalare finalizată

Produsul tău Bitdefender s-a instalat cu succes.

Este afișat rezumatul instalării. Dacă, în timpul instalării, este detectată și deinstalată o amenințare, poate fi necesară o repornire a sistemului. Pentru a continua, efectuează clic pe **ÎNCEPE SĂ FOLOSEȘTI Bitdefender**.

Pasul 4 - Primii pași

În fereastra **Primii pași**, poți vizualiza detaliile abonamentului tău activ.

Faceți clic pe **FINALIZARE** pentru a accesa interfața Bitdefender Total Security.

1.3.2. Instalare de pe discul de instalare

Pentru a instala Bitdefender de pe discul de instalare, introdu CD-ul în unitatea optică.

În câteva momente se va afișa fereastra de instalare. Urmează instrucțiunile pentru a începe instalarea.

Dacă nu apare ecranul de instalare, utilizează Windows Explorer pentru a parcurge directorul rădăcină al CD-ului și efectuează dublu clic pe fișierul `autorun.exe`.

În cazul în care viteza ta de internet este slabă sau sistemul tău nu este conectat la internet, efectuează clic pe butonul **Instalare de pe CD/DVD**. În acest caz, va fi instalat produsul Bitdefender disponibil pe disc și o versiune mai nouă se va descărca de pe serverele Bitdefender prin intermediul actualizărilor de produs.

Validarea instalării

Bitdefender verifică mai întâi sistemul tău pentru a valida instalarea.

Dacă sistemul tău nu îndeplinește cerințele de sistem pentru instalarea Bitdefender, vei fi informat cu privire la zonele ce necesită să fie îmbunătățite înainte să poți continua.

Dacă este detectat o soluție antivirus incompatibilă sau o versiune mai veche a Bitdefender, vi se va cere să le ștergeți de pe sistemul dumneavoastră. Vă rugăm să urmați instrucțiunile pentru a șterge software-ul din sistemul dumneavoastră, evitând astfel apariția problemelor pe viitor.



Este posibil să fie nevoie să reporniți calculatorul pentru a finaliza dezinstalarea soluțiilor antivirus detectate.



Notă

Descărcarea fișierelor de instalare poate dura foarte mult, cu precădere în cazul conexiunilor internet mai lente.

După validarea instalării, se afișează asistentul de configurare. Urmăți pașii pentru instalarea Bitdefender Total Security.

Pasul 1 - Instalarea Bitdefender

Înainte de a începe instalarea, este necesar să îți exprimi acordul cu privire la Contractul de abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender.

Dacă nu ești de acord cu acești termeni, închide fereastra. Procesul de instalare va fi abandonat și vei ieși din fereastra de instalare.

În cadrul acestui pas se pot efectua două sarcini suplimentare:

- Menține opțiunea **Trimite rapoarte despre produs** activă. Prin permiterea acestei opțiuni, sunt trimise rapoarte către serverele Bitdefender, conținând informații despre modul în care utilizezi produsul. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să îți oferim produse și mai bune pe viitor. Rapoartele nu conțin date confidențiale, cum ar fi numele tău sau adresa IP, și nu vor fi folosite în scopuri comerciale.
- Selectează limba în care dorești să instalezi produsul.

Efectuează clic pe **INSTALARE** pentru a lansa procesul de instalare al produsului tău Bitdefender.

Pasul 2 - Instalare în curs de desfășurare

Așteaptă până când instalarea este finalizată. Sunt afișate informații detaliate cu privire la evoluția instalării.



Pasul 3 - Instalare finalizată

Este afișat rezumatul instalării. Dacă, în timpul instalării, este detectată și deinstalată o amenințare, poate fi necesară o repornire a sistemului. Pentru a continua, efectuează clic pe **ÎNCEPE SĂ FOLOSEȘTI Bitdefender**.

Pasul 4 - Contul Bitdefender

După finalizarea instalării inițiale, se va afișa fereastra Contului Bitdefender. Este necesar un cont Bitdefender pentru a activa produsul și pentru a folosi caracteristicile online ale acestuia. Pentru mai multe informații, consultați capitolul „*Bitdefender Central*” (p. 30).

Continuă în funcție de situația ta.

● **Doresc să creez un cont Bitdefender**

1. Introduceți informațiile solicitate în câmpurile corespunzătoare. Informațiile furnizate aici vor rămâne confidențiale. Parola trebuie să aibă o lungime de minimum 8 caractere, să includă cel puțin o cifră sau un simbol și să includă litere mici și mari.
2. Înainte de a merge mai departe este necesar să îți exprimi acordul cu privire la Termenii de utilizare. Accesează secțiunea Termeni de utilizare și citește termenii cu atenție întrucât conțin termenii și condițiile care îți permit utilizarea Bitdefender.

Suplimentar, poți accesa și citi Politica de confidențialitate.

3. Efectuează clic pe **CREARE CONT**.

Notă

O dată ce contul este creat, poți utiliza adresa de e-mail și parola furnizate pentru a te autentifica în contul tău la <https://central.bitdefender.com> sau în aplicația Bitdefender Central dacă aceasta este instalată pe unul dintre dispozitivele tale Android sau iOS. Pentru a instala aplicația Bitdefender Central pe Android, este necesar să accesezi Google Play, să cauți Bitdefender Central, iar apoi să apeși pe opțiunea de instalare corespunzătoare. Pentru a instala aplicația Bitdefender Central pe iOS, este necesar să accesezi App Store, să cauți Bitdefender Central, iar apoi să apeși pe opțiunea de instalare corespunzătoare.

● **Deja am un cont Bitdefender**

1. Faceți clic pe **Accesează**.



2. Introdu adresa de e-mail în câmpul corespunzător, apoi fă clic pe **MAI DEPARTE**.

3. Introdu parola și apoi efectuează clic pe **AUTENTIFICARE**.

Dacă ai uitat parola contului tău sau dacă pur și simplu dorești să o resetezi pe cea existentă deja:

a. Faceți clic pe **Ați uitat parola?**

b. Introdu adresa ta de e-mail, apoi selectează opțiunea **ÎNAINTE**.

c. Verificați-vă contul de e-mail, introduceți codul de securitate primit și apoi faceți clic pe **MAI DEPARTE**.

Alternativ, puteți face clic pe **Schimbare parolă** din mesajul e-mail pe care vi l-am trimis.

d. Introduceți noua parolă pe care doriți să o setați și apoi introduceți-o din nou. Efectuează clic pe **SALVARE**.



Notă

Dacă ai deja un cont MyBitdefender, îl poți folosi pentru a-ți accesa contul Bitdefender. Dacă v-ați uitat parola, este necesar să accesați <https://my.bitdefender.com> pentru a o reseta. Apoi, utilizați datele de autentificare actualizate pentru a-ți accesa contul Bitdefender.

● Doresc să mă autentific prin intermediul contului de Microsoft, Facebook sau Google

Pentru autentificare cu contul tău de Microsoft, Facebook sau Google:

1. Selectați serviciul pe care doriți să îl utilizați. Veți fi redirectionat către pagina de autentificare a aceluși serviciu.

2. Urmați instrucțiunile oferite de serviciul selectat pentru a face legătura dintre contul dumneavoastră și Bitdefender.



Notă

Bitdefender nu are acces la informații confidențiale, precum parola contului pe care te autentifici de obicei sau datele personale ale prietenilor și contactelor.



Pasul 5 - Activați-vă produsul



Notă

Această etapă apare dacă ai selectat crearea unui nou cont Bitdefender pe parcursul etapei anterioare sau dacă te-ai autentificat utilizând un cont aferent unui abonament care a expirat.

Este necesară o conexiune activă la internet pentru a finaliza activarea produsului.

Procedați în funcție de situația dumneavoastră:

● Am un cod de activare

În acest caz, activează produsul urmând acești pași:

1. Introdu codul de activare în câmpul **Am un cod de activare** și apoi fă clic pe **CONTINUĂ**.



Notă

Iată cum poți găsi codul tău de activare:

- pe eticheta de la CD/DVD.
- pe certificatul de înregistrare al produsului.
- în e-mailul de achiziționare online.

2. Doresc să evaluez Bitdefender

În acest caz, puteți utiliza produsul pe o perioadă de 30 de zile. Pentru a începe perioada de evaluare, selectează **Nu am abonament, doresc să încerc produsul gratuit** și apoi fă clic pe **CONTINUĂ**.

Pasul 6 - Primii pași

În fereastra **Primii pași**, poți vizualiza detaliile abonamentului tău activ.

Faceți clic pe **FINALIZARE** pentru a accesa interfața Bitdefender Total Security.



2. PRIMII PAȘI

2.1. Informații de bază

Odată ce ai instalat Bitdefender Total Security, calculatorul tău este protejat împotriva tuturor tipurilor de amenințări (cum ar fi programe periculoase, programe spion, ransomware, exploatări, botnet-uri și troieni) și a amenințărilor de pe internet (cum ar fi hackeri, atacurile de tip phishing și mesajele spam).

Aplicația utilizează tehnologia Photon pentru a mări viteza și performanțele procesului de scanare a amenințărilor. Funcționează prin preluarea modelelor de utilizare ale aplicațiilor din sistemul dvs. pentru a ști ce anume și când să scaneze, reducând astfel la minimum impactul asupra performanțelor sistemului dvs.

Conectarea fără protecție la rețele wireless publice din aeroporturi, mall-uri, cafenele sau hoteluri poate fi periculoasă pentru dispozitivul și datele tale. Principalul motiv pentru aceasta este faptul că cei care comit fraude ar putea să-ți monitorizeze activitatea și să găsească cel mai bun moment pentru a-ți fura datele personale, dar și faptul că oricine îți poate vedea adresa IP, transformând astfel sistemul tău într-o victimă a viitoarelor atacuri cibernetice. Pentru a evita astfel de situații nefericite, instalează și utilizează aplicația „VPN” (p. 153).

Poți menține evidența parolelor și a conturilor tale online salvându-le cu „Protecția datelor de autentificare cu Password Manager” (p. 143) într-un portofel. Cu o singură parolă generală îți poți proteja confidențialitatea de intrușii care ar putea încerca să te lase fără bani.

„Protecție cameră web” (p. 129) Împiedică aplicațiile nesigure să acceseze camera ta video, evitând astfel orice încercare de hacking. În funcție de alegerea utilizatorilor Bitdefender, accesul aplicațiilor folosite în mod frecvent la camera dvs. web va fi permis sau blocat.

Pentru a te proteja de potențialii curioși și spioni atunci când dispozitivul tău este conectat la o rețea wireless nesecurizată, Bitdefender analizează nivelul său de securitate și, dacă este necesar, oferă recomandări pentru a spori siguranța activităților tale online. Pentru instrucțiuni despre cum îți poți păstra în siguranță datele personale, consultați secțiunea „Evaluare securitate rețele Wi-Fi” (p. 125).



Fișierele tale personale stocate local, cum ar fi documente, fotografiile sau filme, și cele stocate în cloud pot rămâne acum departe de cele mai periculoase amenințări din zilele noastre, și anume ransomware-ul. Pentru informații despre cum să-ți pui la adăpost fișierele personale, consultați *„Protecție Fișiere”* (p. 133).

Fișierele criptate de ransomware pot fi acum recuperate fără a cheltui bani pe recompense. Pentru informații despre modul de recuperare a fișierelor criptate, accesează *„Remediere ransomware”* (p. 136).

În timp ce lucrați, jucați jocuri sau vizionați filme, Bitdefender vă poate oferi o experiență neîntreruptă a utilizatorului prin amânarea sarcinilor de întreținere, eliminarea întreruperilor și ajustarea efectelor vizuale ale sistemului. Puteți beneficia de toate acestea activând și configurând opțiunea *„Profiluri”* (p. 186).

Bitdefender va lua majoritatea deciziilor legate de securitate în locul dumneavoastră și va afișa rareori alerte pop-up. În fereastra Notificări sunt disponibile detalii despre acțiunile aplicate și informații cu privire la funcționarea programului. Pentru mai multe informații, consultați capitolul *„Notificări”* (p. 13).

Din când în când, trebuie să deschideți Bitdefender și să remediați oricare din problemele existente. Este posibil să fie nevoie să configurați anumite componente ale Bitdefender sau să luați măsuri preventive pentru a vă proteja calculatorul și datele dumneavoastră.

Pentru a folosi caracteristicile online ale Bitdefender Total Security și pentru administrarea abonamentelor și dispozitivelor dumneavoastră, accesați-vă contul Bitdefender. Pentru mai multe informații, consultați capitolul *„Bitdefender Central”* (p. 30).

În secțiunea *„Cum să”* (p. 44) veți găsi instrucțiuni pas cu pas de efectuare a sarcinilor obișnuite. Dacă vă confrunțați cu probleme în utilizarea Bitdefender, accesați secțiunea *„Soluționarea problemelor frecvente”* (p. 193) pentru soluții posibile la cele mai frecvente probleme.

Deschiderea ferestrei Bitdefender

Pentru a accesa interfața principală a Bitdefender Total Security, urmați pașii de mai jos:

● În Windows 7:


1. Faceți clic pe **Start** și mergeți la **Toate programele**.




2. Faceți clic pe **Bitdefender**.

3. Faceți clic pe **Bitdefender Total Security** sau, mai rapid, faceți dublu clic pe pictograma Bitdefender  din bara de sistem.

● În Windows 8 și Windows 8.1:

Din ecranul de Start al Windows, localizează Bitdefender (de exemplu, poți începe să tastezi "Bitdefender" direct în ecranul de Start) și fă clic pe pictograma acestuia. În mod alternativ, deschideți aplicația pentru desktop și faceți dublu clic pe pictograma Bitdefender  din bara de sistem.

● În Windows 10:

Introduceți "Bitdefender" în caseta de căutare din bara de sarcini și apoi faceți clic pe pictogramă. Alternativ, faceți dublu clic pe pictograma Bitdefender  din tava de sistem.

Pentru mai multe informații despre fereastra și pictograma Bitdefender de pe bara de sistem, consultați „*Interfața Bitdefender*” (p. 17).

2.1.1. Notificări

Bitdefender menține un jurnal detaliat al evenimentelor legate de activitatea sa pe computerul dumneavoastră. Ori de câte ori se întâmplă un lucru important pentru securitatea sistemului sau datelor dumneavoastră, se adaugă un nou mesaj la Notificările Bitdefender, ca și când ați primi un e-mail nou în Inbox-ul dumneavoastră.

Notificările reprezintă un instrument important pentru monitorizarea și gestionarea protecției Bitdefender. De exemplu, poți verifica cu ușurință dacă actualizarea a fost efectuată cu succes, dacă au fost detectate amenințări sau vulnerabilități pe calculatorul tău, etc. În plus, puteți lua măsuri suplimentare dacă este cazul sau puteți modifica măsurile luate prin intermediul Bitdefender.

Pentru a accesa jurnalul de Notificări, efectuează clic pe **Notificări** din meniul de navigare al interfeței **Bitdefender**. De fiecare dată când se produce un eveniment critic, se poate observa modificarea conturului pe pictograma



În funcție de tip și severitate, notificările sunt grupate în:

- Evenimentele **critice** indică probleme critice. Acestea ar trebui verificate imediat.



- Evenimentele de tip **Avertizare** indică probleme care nu sunt de foarte mare importanță. Ar trebui să verificați și să le remediați atunci când aveți timp.
- Evenimentele de tip **Informații** indică operațiile finalizate cu succes.

Fă clic pe fiecare filă pentru mai multe detalii despre evenimentele generate. Detaliile pe scurt sunt afișate la un singur clic pe titlul fiecărui eveniment, respectiv: o scurtă descriere, acțiunea pe care Bitdefender a întreprins-o atunci când a survenit, precum și data și ora producerii evenimentului. Pot fi setate diverse opțiuni prin intermediul cărora să fie aplicații și alte acțiuni, dacă este necesar.

Pentru a vă ajuta să gestionați cu ușurință evenimentele înregistrate, ferestra Notificări oferă opțiuni de ștergere sau marcare ca citite a tuturor evenimentelor din secțiunea respectivă.

2.1.2. Profiluri

Unele activități efectuate pe calculator, cum ar fi jocurile online sau prezentările video, necesită o viteză sporită de reacție și funcționare superioară a sistemului, fără întreruperi. Când laptopul dvs se alimentează de la baterie, este recomandat să amânați operațiile cu consum mare de energie până când laptopul este conectat din nou la o priză.

Opțiunea Profiluri Bitdefender alocă mai multe resurse din sistem aplicațiilor care rulează prin modificarea temporară a setărilor de protecție și ajustarea configurației sistemului. Prin urmare, impactul sistemului asupra activității dumneavoastră este redus la minimum.

Pentru adaptarea la diferite activități, Bitdefender este furnizat cu următoarele profiluri:

Profil Lucru

Optimizează eficiența activității dumneavoastră prin identificarea și ajustarea setărilor produsului și ale sistemului.

Profil Film

Spoarește efectele vizuale și elimină întreruperile în timpul vizionării filmelor.

Profil Joc

Spoarește efectele vizuale și elimină întreruperile în timpul jocurilor.



Profil Wi-Fi public

Aplică setările de produs pentru a beneficia de protecție completă în timpul conexiunii la o rețea wireless nesecurizată.

Profil mod baterie

Aplică setările de produs și menține redusă activitatea din fundal pentru a economisi bateria.

Configurează activarea automată a profilurilor

Pentru o experiență ușor de utilizat, poți configura Bitdefender pentru gestionarea profilului tău de lucru. În acest caz, Bitdefender detectează automat activitatea derulată și aplică setările de optimizare a sistemului și produsului.

Pentru a permite Bitdefender să activeze profilurile:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.
3. Folosiți butonul corespunzător pentru a activa funcția **Activați profilurile automat**.

Dacă nu doriți activarea automată a Profilurilor, opriți funcția de la buton.

Pentru a activa manual un profil, pornește butonul corespunzător. Dintre primele trei profiluri, doar unul poate fi activat manual imediat.

Pentru mai multe informații despre Profiluri, consultă „*Profiluri*” (p. 186)

2.1.3. Protecție cu parolă pentru setările Bitdefender

Dacă nu sunteți singura persoană cu drepturi administrative care folosește acest calculator, este recomandat să vă protejați setările Bitdefender cu o parolă.

Pentru a configura protecția cu parolă pentru setările Bitdefender:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Din fereastra **General**, activează **Protecția cu parolă**.
3. Introdu parola în cele două câmpuri și efectuează clic pe **OK**. Parola trebuie să aibă cel puțin 8 caractere.

După ce ai setat o parolă, aceasta va trebuie introdusă de fiecare dată când cineva încearcă să modifice setările Bitdefender.



Important

Vă sfătuim să rețineți parola sau să o notați și să o păstrați într-un loc sigur. Dacă ați uitat parola, trebuie să reinstalați programul sau să contactați Bitdefender pentru asistență.

Pentru a elimina protecția cu parolă:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Din fereastra **General**, dezactivează **Protecția cu parolă**.
3. Introdu parola și efectuează clic pe **OK**.



Notă

Pentru a modifica parola produsului tău, efectuează clic pe **Modificare parolă**. Introdu parola actuală și apoi efectuează clic pe **OK**. În fereastra afișată, introduceți noua parolă pe care doriți să o utilizați de acum înainte pentru a restricționa accesul la setările produsului dumneavoastră Bitdefender.

2.1.4. Rapoarte despre produs

Rapoartele de produs conțin informații despre modul în care utilizezi produsul Bitdefender pe care l-ai instalat. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să vă oferim produse și mai bune pe viitor.

Te rugăm să reții că aceste rapoarte nu conțin date confidențiale, cum ar fi numele sau adresa ta IP și că acestea nu vor fi utilizate în scopuri comerciale.

Dacă ai ales în timpul procesului de instalare să expediezi astfel de rapoarte către serverele Bitdefender, iar acum dorești să oprești procesul:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Avansat**.
3. Dezactivează opțiunea **Rapoarte produs**.

2.1.5. Notificări privind ofertele speciale

Atunci când sunt disponibile oferte promoționale, produsul Bitdefender este configurat să vă notifice prin intermediul unei ferestre de tip pop-up. Aceasta vă oferă oportunitatea de a beneficia de prețuri avantajoase și de a vă menține dispozitivele protejate pentru o perioadă mai lungă de timp.

Pentru a activa sau dezactiva notificările privind ofertele speciale:



1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. În fereastra **General**, pornește sau oprește butonul corespunzător.
Opțiunea de Oferte speciale și notificări de produse este activată implicit.

2.2. Interfața Bitdefender

Bitdefender Total Security îndeplinește deopotrivă cerințele persoanelor experimentate și pe cele ale începătorilor în utilizarea calculatorului. Interfața sa grafică este proiectată pentru a se potrivi fiecărei categorii de utilizatori.

Pentru a parcurge interfața Bitdefender, în partea din stânga sus este afișat un asistent de introducere care conține detalii despre cum să interacționezi cu produsul și cum să îl configurezi. Selectează săgeata dreapta pentru a continua să primești indicații sau **Renunță la tur** pentru a închide asistentul.


Pictograma din bara de sistem Bitdefender este disponibilă în orice moment, indiferent dacă dorești să deschizi fereastra principală, să rulezi o actualizare de produs sau să vizualizezi informațiile referitoare la versiunea instalată.

Fereastra principală îți oferă informații cu privire la starea ta de securitate. În funcție de utilizarea și necesitățile dispozitivului tău, **Autopilot** afișează aici diferite tipuri de recomandări care să te ajute să îmbunătățești securitatea și performanța dispozitivului tău. Mai mult, poți adăuga acțiunile rapide pe care le utilizezi cel mai mult, astfel încât să le poți avea la îndemână oricând ai nevoie de ele.

Din meniul de navigare din partea stângă poți accesa **contul tău Bitdefender**, zona de setări, notificări și **secțiunile Bitdefender** pentru o configurare detaliată și sarcini administrative avansate. De asemenea, ne poți contacta pentru asistență în cazul în care ai întrebări sau intervine ceva neașteptat.

Dacă doriți să monitorizați în permanență informațiile de securitate esențiale și să aveți acces rapid la principalele setări, adăugați **Widget-ul de securitate** pe desktop.

2.2.1. Pictograma barei de sistem


Pentru a administra întregul produs mai rapid, puteți folosi iconița Bitdefender  din bara de sistem.



Notă

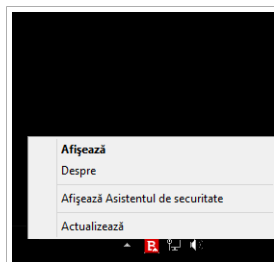
Este posibil ca pictograma Bitdefender să nu fie vizibilă întotdeauna. Pentru afișarea permanentă a pictogramei:



- În **Windows 7, Windows 8 și Windows 8.1**:
 1. Faceți clic pe săgeata  din colțul din dreapta jos al ecranului.
 2. Faceți clic pe **Personalizare...** pentru a deschide fereastra Pictogramelor din zona notificărilor.
 3. Selectați opțiunea **Afișare pictograme și notificări** pentru pictograma **Agent Bitdefender**.
- În **Windows 10**:
 1. Clic dreapta pe bara de activități și selectează **Setări bară de activități**
 2. Derulează în jos și accesează link-ul **Alege ce pictograme apar în bara de activități** din **Zona de notificări**.
 3. Activați butonul de lângă **Agent Bitdefender**.

Dacă faceți dublu-clic pe această iconiță, se va deschide fereastra Bitdefender. De asemenea, făcând clic-dreapta pe iconiță, un meniu contextual vă va oferi posibilitatea unei administrări rapide a Bitdefender.



- **Arată** - deschide fereastra principală a Bitdefender.
- **Despre** - se deschide o fereastră din care poți afla informații despre Bitdefender, poți afla unde poți căuta dacă ai nevoie de ajutor în cazul în care apare o situație neașteptată, unde poți accesa și vizualiza Contractul de abonament, Componentele Terților și Politica de Confidențialitate.



Pictogramă în bară

- **Ascunde/ Afișează asistentul de securitate** - activează / dezactivează **widget-ul de securitate**.
- **Actualizează** - inițiază o actualizare imediată. Puteți urmări starea actualizării pe panoul de actualizare din **fereastra Bitdefender** principală.

Iconița Bitdefender din bara de sistem vă informează despre problemele care vă afectează calculatorul sau despre funcționarea produsului, prin afișarea unui simbol special, după cum urmează:








-  Nu există probleme care afectează securitatea sistemului tău.
-  Probleme grave de securitate afectează calculatorul dvs. Acestea necesită atenția dvs imediat și trebuie remediate în cel mai scurt timp.




Dacă Bitdefender nu funcționează, pictograma din bara de sistem apare pe un fundal gri: **B**. Acest lucru se întâmplă de obicei când expiră abonamentul. O altă cauză poate fi faptul că serviciile Bitdefender nu răspund sau că alte erori afectează funcționarea normală a Bitdefender.

2.2.2. Meniu de navigare

În partea stângă a interfeței Bitdefender se află meniul de navigare, care îți permite să accesezi rapid caracteristicile și instrumentele Bitdefender de care ai nevoie pentru a îți gestiona produsul. Secțiunile disponibile în această zonă sunt:

-  **Panou de bord.** De aici, poți rezolva rapid problemele de securitate, poți vizualiza recomandările în funcție de necesitățile sistemului tău și modelele de utilizare, poți realiza acțiuni rapide și poți instala Bitdefender pe alte dispozitive.
-  **Securitate.** De aici, poți lansa și configura scanări antivirus, poți accesa setările Firewall, poți proteja fișiere și aplicații împotriva atacurilor ransomware, poți recupera datele în cazul criptării acestora de către un program ransomware și poți configura protecția în timp ce navighezi pe internet.
-  **Confidențialitate.** De aici, poți crea configurații Password Manager pentru conturile tale online, poți proteja accesul la camera ta web de privirile indiscrete, poți efectua plăți online într-un mediu sigur, poți deschide aplicația VPN și îți poți proteja copiii prin vizualizarea și restricționarea activității lor online.
-  **Instrumente.** De aici, poți îmbunătăți viteza sistemului și poți configura caracteristica Anti-furt pentru dispozitivele tale.
-  **Notificări.** De aici, ai acces la notificările generate.
-  **Contul meu.** De aici, îți poți accesa contul tău Bitdefender pentru a verifica abonamentele și a efectua sarcinile de securitate pe dispozitivele pe care le administrezi. Sunt de asemenea disponibile detalii despre contul Bitdefender și despre abonamentul în curs.
-  **Setări.** De aici, ai acces la setările generale.



-  **Asistență.** De aici, oricând ai nevoie de asistență pentru a soluționa o anumită situație cu produsul Bitdefender Total Security, poți contacta departamentul de Asistență Tehnică Bitdefender.

2.2.3. Panou de bord

Fereastra panou de control îți permite să efectuezi sarcini obișnuite, să rezolvi rapid problemele de securitate, să vizualizezi informații despre utilizarea produsului și să accesezi secțiunile din care poți configura setările produsului.

Puteți accesa orice opțiune prin doar câteva clicuri.

Fereastra conține trei secțiuni principale:

Zonă stare securitate

De aici poți verifica starea de securitate a calculatorului tău.

Autopilot


De aici poți verifica recomandările Autopilot pentru a asigura funcționarea corectă a sistemului.

Acțiuni rapide

Aici poți executa diverse sarcini pentru a-ți menține sistemul protejat și capabil să funcționeze la viteză optimă. Poți de asemenea instala Bitdefender pe alte dispozitive, cu condiția ca abonamentul tău să aibă suficiente sloturi disponibile.

Zonă stare securitate

Bitdefender utilizează un sistem de monitorizare a problemelor pentru a detecta și pentru a vă informa în legătură cu aspectele care pot afecta securitatea computerului și datelor dumneavoastră. Problemele depistate pot include setări de protecție importante care au fost dezactivate, precum și alte condiții care pot reprezenta un risc de securitate.

Oricând există probleme care afectează securitatea calculatorului tău, starea care apare în partea superioară a **interfeței Bitdefender** se modifică în roșu. Starea afișată indică tipul problemelor care îți afectează sistemul. De asemenea, pictograma **barei de sistem** se modifică în  și dacă muți cursorul mouse-ului peste pictogramă, o fereastră pop-up va confirma existența unor probleme.



Întrucât problemele detectate pot împiedica Bitdefender să te protejeze împotriva amenințărilor sau reprezintă un risc major de securitate, îți recomandăm să fii atent și să le rezolvi în cel mai scurt timp. Pentru a rezolva o problemă, efectuează clic pe butonul de lângă problema detectată.

Autopilot

Pentru a îți oferi o funcționare eficientă și protecție sporită în timp ce realizezi diferite activități, Bitdefender Autopilot va acționa ca un consultant personal de securitate. În funcție de activitatea pe care o realizezi, fie că lucrezi, fie că efectuezi plăți online, urmărești filme sau joci jocuri, Bitdefender Autopilot va veni cu recomandări contextuale pe baza nivelului de utilizare și necesităților dispozitivului tău. Recomandările propuse pot fi de asemenea legate de acțiuni pe care trebuie să le efectuezi pentru a îți menține produsul funcțional la capacitate maximă.

Pentru a începe să utilizezi o funcție sugerată sau să faci îmbunătățiri la produsul tău, efectuează clic pe butonul corespunzător.

Dezactivarea notificărilor Autopilot

Pentru a te informa cu privire la recomandările Autopilot, produsul Bitdefender este setat să te notifice printr-o fereastră pop-up.


Pentru a dezactiva notificările Autopilot:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. În fereastra **General**, dezactivează **Notificări de recomandare**.

Acțiuni rapide

Utilizând acțiuni rapide poți lansa rapid sarcini pe care le consideri importante pentru păstrarea protecției sistemului tău și pentru rularea la viteză optimă.

Implicit, Bitdefender sosește cu câteva acțiuni rapide care pot fi înlocuite cu cele pe care știi că le utilizezi cel mai des. Pentru a înlocui o acțiune rapidă:

1. Efectuează clic pe pictograma  din colțul din dreapta sus al cardului pe care dorești să îl îndepartezi.
2. Plasează sarcina pe care dorești să o adaugi la interfața principală și apoi efectuează clic pe **ADĂUGARE**.

Sarcinile pe care le poți adăuga în interfața principală sunt:



- **Procesul de Scanare Rapidă.** Rulează o scanare rapidă pentru a detecta cu promptitudine amenințările posibile care ar putea fi prezente pe calculatorul tău.
- **Scanare Sistem.** Efectuează o scanare de sistem pentru a te asigura că nu există amenințări în calculatorul tău.
- **Scanare Vulnerabilități.** Scanați calculatorul pentru identificarea vulnerabilităților, pentru a vă asigura că toate aplicațiile instalate, precum și Sistemul de operare, sunt actualizate și funcționează corespunzător.
- **Verifică securitatea rețelei Wi-Fi.** Deschide Consultantul de Securitate Wi-Fi pentru a verifica dacă rețeaua wireless de acasă la care ești conectat este sigură sau nu și dacă are vulnerabilități.
- **Portofele.** Vizualizează și administrează portofelele tale.
- **Deschide Safepay.** Deschideți Bitdefender Safepay™ pentru a vă proteja datele confidențiale, în timpul tranzacțiilor online.
- **Deschide VPN.** Deschide Bitdefender VPN pentru a adăuga un strat suplimentar de protecție când ești conectat la internet.
- **Instrument de eliminare a fișierelor.** Lansează instrumentul de Distrugere a Fișierelor pentru a îndepărta urmele de date sensibile din calculatorul tău.
- **Seifuri pentru fișiere.** Creează seifuri de fișiere în care poți stoca documente confidențiale și sensibile.
- **Deschide OneClick Optimizer.** Eliberează spațiu pe disc, remediază erorile de înregistrare și protejează-ți confidențialitatea ștergând fișierele care nu mai sunt utile, cu un singur clic pe buton.
- **Deschide Startup Optimizer.** Îmbunătățește timpul de pornire al sistemului prin excluderea aplicațiilor care nu sunt necesare la pornire.
- **Curăță-mi dispozitivul.** Fă loc pentru date noi prin ștergerea fișierelor care nu mai sunt necesare.

Pentru a începe să protejezi dispozitive suplimentare cu Bitdefender:

1. Efectuează clic pe **Instalează pe alt dispozitiv.**

O nouă fereastră apare pe ecran.

2. Selectează **TRIMITE LINK-UL.**

3. Urmează pașii de pe ecran pentru a instala Bitdefender.

În funcție de alegerea dumneavoastră, se vor instala următoarele produse Bitdefender:

- Bitdefender Total Security pe dispozitive pe platformă Windows.



- Bitdefender Antivirus for Mac pe dispozitive pe platformă macOS.
- Bitdefender Mobile Security pe dispozitive pe platformă Android.
- Bitdefender Mobile Security pe dispozitive pe platformă iOS.

2.2.4. Secțiunile Bitdefender

Produsul Bitdefender este livrat cu trei secțiuni împărțite în mai multe caracteristici utile pentru a vă ajuta să rămâneți protejat în timp ce lucrați, să navigați pe Internet sau să efectuați plăți online, să îmbunătățiți viteza sistemului și multe altele.

Atunci când dorești să accesezi caracteristicile pentru o anumită secțiune sau să începi configurarea produsului tău, accesează următoarele pictograme situate în meniul de navigare al **interfeței Bitdefender**:

-  **Protecție**
-  **Confidențialitate**
-  **Instrumente**

Protecție

În secțiunea Securitate poți configura setările avansate de securitate, poți administra prietenii și spammer-ii, poți vizualiza și modifica setările de conexiune la rețea, poți configura caracteristicile Protecție Fișiere și Online Threat Prevention, poți verifica și remedia potențiale vulnerabilități de sistem și poți evalua securitatea rețelelor wireless la care te conectezi.

Caracteristicile pe care le poți administra în secțiunea Securitate sunt:

ANTIVIRUS

Protecția antivirus reprezintă fundația securității dumneavoastră. Bitdefender te protejează în timp real și la cerere împotriva tuturor tipurilor de amenințări, precum malware, troieni, programe de tip spyware, adware etc.

Din funcția Antivirus, poți accesa cu ușurință următoarele sarcini de scanare:

- Scanare Rapidă
- Scanare Sistem
- Administrare Scanări
- Modul de recuperare (Mediul de recuperare în Windows 10)



Pentru mai multe informații referitoare la activitățile de scanare și modul de configurare a protecției antivirus, consultați *„Protecție antivirus”* (p. 81).

ONLINE THREAT PREVENTION

Online Threat Prevention te ajută să te protejezi contra atacurilor de tip phishing, tentativelor de fraudă și scurgerilor de date personale în timp ce navighezi pe internet.

Pentru mai multe informații referitoare la modul de configurare Bitdefender pentru a vă proteja activitatea online, consultați *„Online Threat Prevention”* (p. 104).

FIREWALL

Firewall-ul vă protejează în timp ce sunteți conectat la rețele și la internet, filtrând toate tentativele de conectare.

Pentru mai multe informații cu privire la configurarea firewall-ului, consultați *„Firewall”* (p. 115).

ADVANCED THREAT DEFENSE

Funcția Advanced Threat Defense îți protejează sistemul împotriva amenințărilor precum ransomware, programe spion și troieni, analizând comportamentul tuturor aplicațiilor instalate. Procesele suspecte sunt identificate și, dacă este cazul, blocate.

Pentru mai multe informații referitoare la modul în care vă puteți menține sistemul protejat împotriva amenințărilor, consultați *„Advanced Threat Defense”* (p. 102).

ANTISPAM

Caracteristica antispam a Bitdefender se asigură că nu intră e-mail-uri nedorite în directorul cu mesaje primite, filtrând traficul de e-mail POP3.

Pentru mai multe informații referitoare la protecția antispam, consultați *„Antispam”* (p. 106).

VULNERABILITATE

Funcția Vulnerabilități te ajută să-ți menții actualizarea sistemului de operare și a aplicațiilor pe care le folosești în mod regulat și să identifici rețelele wireless nesigure la care te conectezi.

Faceți clic pe **Scanare vulnerabilități** în funcția Vulnerabilități pentru a identifica actualizările Windows critice, actualizările aplicațiilor, parole slabe aferente conturilor Windows și rețele wireless care nu sunt sigure.



Efectuează clic pe **Securitate Wi-fi** pentru a vizualiza lista rețelelor wireless la care te conectezi, împreună cu evaluarea reputației fiecăreia dintre acestea și acțiunile pe care le poți întreprinde pentru a te proteja de eventualii curioși.

Pentru informații suplimentare referitoare la configurarea protecției la vulnerabilitate, consultați „*Vulnerabilități*” (p. 121).

PROTECȚIE FIȘIERE

Caracteristica Protecție Fișiere se asigură că toate fișierele tale personale rămân protejate de atacurile ransomware.

Pentru mai multe informații privind configurarea modulului Protecție fișiere pentru a-ți proteja fișierele personale contra atacurilor de tip ransomware, consultă „*Protecție Fișiere*” (p. 133).

REMEDIERE RANSOMWARE

Funcția Remediere ransomware te ajută să recuperezi fișierele în cazul în care acestea sunt criptate de ransomware.

Pentru informații suplimentare despre modul de recuperare a fișierelor criptate, accesează „*Remediere ransomware*” (p. 136).

Confidențialitate

În secțiunea Confidențialitate, poți deschide aplicația Bitdefender VPN, îți poți cripta datele tale personale, îți proteja tranzacțiile online, îți poți securiza camera web și experiența de navigare și îți poți proteja copiii vizualizându-le și restricționându-le activitatea.

Caracteristicile pe care le puteți administra în secțiunea Confidențialitate sunt:

VPN

VPN îți securizează activitatea online și îți ascunde adresa IP de fiecare dată când te conectezi la rețele wireless nesecurizate în timp ce ești prin aeroporturi, mall-uri, cafenele sau hoteluri. În mod suplimentar, poți accesa conținut care în mod normal este restricționat în anumite zone.

Pentru mai multe informații despre această caracteristică, accesează „*VPN*” (p. 153).



FILE ENCRYPTION

Creați pe computerul dumneavoastră partiții logice criptate și protejate prin parolă (sau seifuri), unde puteți stoca în deplină siguranță documentele dumneavoastră importante și confidențiale.

Pentru mai multe informații cu privire la crearea de partiții logice criptate și protejate cu parolă (sau seifuri) pe calculatorul dumneavoastră, consultați *„File Encryption”* (p. 139).

PROTECȚIE VIDEO ȘI AUDIO

Protecția audio și video îți menține camera web în siguranță prin blocarea accesului la aplicații nesigure și te notifică atunci când aplicațiile încearcă să obțină acces la microfonul dispozitivului tău.

Pentru informații suplimentare despre cum să îți protejezi camera web împotriva accesului neautorizat și cum să setezi Bitdefender astfel încât să-ți transmită notificări în legătură cu activitatea microfonului, accesează *„Protecție video și audio”* (p. 129).

ADMINISTRATOR PAROLE

Bitdefender Password Manager îți permite să îți administrezi parolele, îți protejează confidențialitatea și își oferă o experiență de navigare sigură.

Pentru mai multe informații referitoare la configurarea modulului Password Manager, consultă *„Protecția datelor de autentificare cu Password Manager”* (p. 143).

SAFEPAY

Browser-ul Bitdefender Safepay™ vă ajută să vă mențineți tranzacțiile de online, e-shopping și orice alte tipuri de tranzacții confidențiale și sigure.

Pentru mai multe informații despre Bitdefender Safepay™, consultați *„Securitate Safepay pentru tranzacțiile online”* (p. 156).

CONTROL PARENTAL

Aplicația Control parental Bitdefender îți permite să monitorizezi activitățile copiilor tăi pe computerul lor. În cazul conținutului necorespunzător, puteți decide să restricționați accesul copilului la internet sau la anumite aplicații.

Efectuați clic pe **Configurează** din secțiunea Asistență parentală pentru a începe să configurați dispozitivele copiilor dvs. și a le monitoriza activitatea indiferent unde vă aflați.



Pentru mai multe informații referitoare la configurarea aplicației Control parental, accesează „*Control Parental*” (p. 162).

DATA PROTECTION

Caracteristica Data Protection îți permite să ștergi definitiv fișiere. Dă clic pe opțiunea **Ștergere definitivă fișiere** în panoul Data Protection pentru a porni un asistent care îți va permite să elimini complet fișierele din sistem.

Pentru informații suplimentare privind configurarea caracteristicii Data Protection, consultă „*Data Protection*” (p. 161).

ANTI-TRACKER

Funcția Anti-tracker previne tracking-ul, astfel încât datele tale rămân private în timp ce navighezi online, reducând totodată timpul de încărcare al site-urilor web.

Pentru mai multe informații despre această funcție, consultă „*Anti-tracker*” (p. 150).

Instrumente

În secțiunea Instrumente, poți îmbunătăți viteza sistemului și poți administra dispozitivele tale.

Instrumente de optimizare

Bitdefender Total Security asigură nu numai securitate, ci te ajută de asemenea să menții performanțele computerului tău la un nivel ridicat.

Instrumentele de optimizare disponibile sunt:

- Optimizare rapidă
- Startup Optimizer
- Curățare disc

Pentru mai multe informații privind instrumentele de optimizare a performanței, consultă „*Instrumente*” (p. 182).

Antifurt

Bitdefender Anti-Theft îți protejează calculatorul și datele împotriva furtului sau a pierderii. În cazul unui eveniment de acest tip, opțiunea îți permite să localizezi sau să blochezi de la distanță calculatorul. De asemenea, poți șterge toate datele din sistem.

Funcția anti-furt Bitdefender îți oferă următoarele opțiuni:

- Localizare de la distanță



- Blocare de la distanță
- Ștergere de la distanță
- Alertă de la distanță

Pentru mai multe informații referitoare la modul în care îți poți proteja sistemul, consultă „*Antifurt*” (p. 178).

2.2.5. Asistent de securitate

Widget-ul de securitate reprezintă cea mai rapidă și ușoară metodă pentru monitorizarea și controlul Bitdefender Total Security. Adăugând acest widget la desktop, veți putea vizualiza informații importante și veți putea efectua sarcini cheie în orice moment:

- deschideți fereastra principală a Bitdefender.
- monitorizarea activității de scanare în timp real
- monitorizarea stării de securitate a sistemului dumneavoastră și remediarea problemelor existente
- vedeți când există actualizări în curs.
- vizualizarea notificărilor și acces la cele mai recente evenimente raportate de Bitdefender.
- scanarea fișierelor și directoarelor prin tragerea și fixarea unuia sau a mai multor elemente în widget.



Starea generală de securitate a calculatorului dumneavoastră este afișată **în partea centrală** a widget-ului. Starea este indicată de culoarea și forma pictogramei afișate în această zonă.



Probleme critice afectează securitatea sistemului dumneavoastră.

Acestea necesită atenția dvs imediat și trebuie remediate în cel mai scurt timp. Faceți clic pe pictograma de stare pentru a începe remediarea problemelor raportate.



Probleme care nu sunt critice afectează securitatea sistemului dumneavoastră. Ar trebui să verificați și să le remediați atunci când aveți timp. Faceți clic pe pictograma de stare pentru a începe remedierea problemelor raportate.




Sistemul dumneavoastră este protejat.



Atunci când o operațiune de scanare la cerere este în curs, se afișează această pictogramă animată.

Atunci când se raportează erori, faceți clic pe pictograma de stare pentru a lansa Asistentul de remediere a problemelor.


În partea de jos a widget-ului se afișează contorul evenimentelor necitite (numărul de evenimente nerezolvate raportate de Bitdefender, dacă există). Faceți clic pe contorul de evenimente, de exemplu  pentru un eveniment necitit, pentru a deschide fereastra Notificări. Pentru mai multe informații, consultați capitolul „Notificări” (p. 13).

Scanarea fișierelor și directoarelor

Puteți utiliza Widget-ul de securitate pentru a scana rapid fișiere și directoare. Trageți și fixați orice fișier sau director pe care doriți să-l scanați direct în **Widget-ul de securitate**.

Vă apărea **Asistentul de scanare** care vă va ghida de-a lungul procesului de scanare. Opțiunile de scanare sunt pre-configurate pentru a obține rata maximă de detecție și nu pot fi modificate. Atunci când se detectează fișiere infectate, Bitdefender va încerca să le curețe (să elimine codul periculos). Dacă această acțiune de curățare eșuează, asistentul de scanare Antivirus vă va permite să specificați alte acțiuni pentru a fi aplicate în cazul fișierelor infectate.

Ascundere / afișare Widget de securitate

Dacă nu mai doriți ca widget-ul să fie vizibil, faceți clic pe .

Pentru a reactiva Asistentul de securitate, utilizați una dintre următoarele metode:

● Din bara de sistem:

1. Clic dreapta pe pictograma Bitdefender din **bara de sistem**.



2. Faceți clic pe **Afișare widget de securitate** din meniul contextual afișat.

● Din interfața Bitdefender:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.

2. În fereastra **General**, activează **Widget de securitate**.

Asistentul de securitate Bitdefender este dezactivat în mod implicit.

2.2.6. Modifică limba produsului

Interfața Bitdefender este disponibilă în mai multe limbi și poate fi modificată urmând acești pași:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.

2. În fereastra **General**, selectează **Schimbă limba**.

3. Selectează din listă limba dorită și apoi clic pe **SALVEAZĂ**.

4. Așteaptă câteva momente până când se aplică setările.

2.3. Bitdefender Central

Bitdefender Central este platforma din care ai acces la funcțiile și serviciile online ale produsului și din care poți executa de la distanță sarcini importante pe dispozitivele pe care este instalat Bitdefender. Te poți conecta la contul tău Bitdefender de la orice computer conectat la internet accesând <https://central.bitdefender.com> sau direct din aplicația Bitdefender Central de pe dispozitivele Android și iOS.

Pentru a instala aplicația Bitdefender Central pe dispozitivele tale:

● **Pe Android** - caută Bitdefender Central în Google Play și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.

● **Pe iOS** - caută Bitdefender Central în App Store și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.

După autentificare, poți face următoarele:

● Descărcați și instalați Bitdefender pe sistemele de operare Windows, macOS, iOS și Android. Produsele disponibile pentru descărcare sunt:

● Bitdefender Total Security

● Bitdefender Antivirus pentru Mac

● Bitdefender Mobile Security pentru Android



- Bitdefender Mobile Security for iOS
- Bitdefender Control parental
- Administrați și reînnoiți abonamentele Bitdefender.
- Adăugați dispozitive noi la rețeaua dvs. și administrați-le oriunde v-ați afla.
- Protejați-vă dispozitivele din rețea și datele de pe acestea împotriva furtului sau a pierderii cu ajutorul funcției **Anti-Theft**.
- Configurați setările de **Control parental** pentru dispozitivele copiilor tăi și monitorizează activitatea acestora oriunde te-ai afla.

Accesare Bitdefender Central

Există mai multe moduri de accesare a Bitdefender Central:

- Din interfața principală Bitdefender:
 1. Dă clic pe **Contul meu** din meniul de navigare al **interfeței Bitdefender**.
 2. Selectează **Accesează Bitdefender Central**.
 3. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
- Din browser-ul web:
 1. Deschide un browser web pe orice dispozitiv cu acces la internet.
 2. Mergeți la: <https://central.bitdefender.com>.
 3. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
- De pe dispozitivul tău Android sau iOS:

Deschide aplicația Bitdefender Central pe care ai instalat-o.



Notă

În acest material sunt prezentate opțiunile disponibile în platforma web și instrucțiunile aferente.

2.3.1. Autentificare în doi pași

Metoda de autentificare în doi pași adaugă un strat suplimentar de securitate contului tău Bitdefender, solicitând un cod de autentificare suplimentar pe lângă datele tale de conectare. În acest fel, vei evita ca altcineva să preia




controlul asupra contului tău și veți ține la distanță atacuri cibernetice precum keyloggere, atacuri de tip „brute-force” sau pe bază de dicționar.

Activați autentificarea de tip „two-factor”

Prin activarea autentificării în doi pași, contul tău Bitdefender devine mult mai sigur. Identitatea ta va fi verificată de fiecare dată când te vei conecta de la diferite dispozitive pentru a instala unul dintre produsele Bitdefender, pentru a verifica starea abonamentului tău sau pentru a executa sarcini de la distanță pe dispozitivele tale.

Pentru a activa autentificarea de tip „two-factor”:

1. Accesați **Bitdefender Central**.
2. Faceți clic pe icoana  din partea dreapta de sus al ecranului.
3. Selectează **Cont Bitdefender** din meniul derulant.
4. Selectează fila **Parolă și securitate**.
5. Selectează **Autentificare în doi pași**.
6. Selectează **PRIMII PAȘI**.

Selectează una dintre următoarele metode:

- **Aplicație de autentificare** - folosește o aplicație de autentificare pentru a genera un cod de fiecare dată când dorești să te conectezi la contul tău Bitdefender.

Dacă dorești să utilizezi o aplicație de autentificare, dar nu ești sigur ce să alegi, îți punem la dispoziție o listă cu aplicațiile de autentificare pe care le recomandăm.

- a. Selectează **UTILIZEAZĂ O APLICAȚIE DE AUTENTIFICARE** pentru a începe.
- b. Pentru a te autentifica pe un dispozitiv cu sistem de operare Android sau iOS, folosește dispozitivul tău pentru a scana codul QR.

Pentru a te autentifica pe un laptop sau computer, poți adăuga manual codul afișat.

Faceți clic pe **CONTINUĂ**.

- c. Introdu codul furnizat de aplicație sau cel afișat la pasul anterior, apoi selectează **ACTIVARE**.



- **E-mail** - de fiecare dată când te conectezi la contul tău Bitdefender, se va trimite un cod de verificare către căsuța ta de e-mail. Verifică contul de e-mail și introdu codul primit.
 - a. Selectează **UTILIZEAZĂ ADRESA DE E-MAIL** pentru a începe.
 - b. Verifică-ți contul de e-mail și introdu codul furnizat.

Reține că ai cinci minute la dispoziție pentru a-ți verifica contul de e-mail și pentru a introduce codul generat. Dacă timpul expiră, trebuie să generezi unul nou urmând aceiași pași.
 - c. Selectează **ACTIVARE**.
 - d. Ai la dispoziție zece coduri de activare. Poți copia, descărca sau tipări lista pentru a o utiliza ulterior în cazul în care îți pierzi adresa de e-mail sau nu te poți conecta. Fiecare cod poate fi folosit o singură dată.
 - e. Selectează **FINALIZAT**.

Dacă nu mai dorești să folosești Autentificarea în doi pași:

1. Selectează opțiunea **DEZACTIVEAZĂ AUTENTIFICAREA ÎN DOI PAȘI**.
2. Verifică aplicația sau contul de e-mail și introdu codul primit.


Dacă ai optat pentru a primi codul de autentificare prin e-mail, ai cinci minute la dispoziție pentru a-ți verifica contul de e-mail și pentru a introduce codul generat. Dacă timpul expiră, trebuie să generezi unul nou urmând aceiași pași.

3. Confirmă alegerea.

Adăugarea dispozitivelor sigure

Pentru a ne asigura că tu ești singura persoană care poate accesa contul tău Bitdefender, este posibil să îți solicităm mai întâi un cod de securitate. Dacă dorești să omiți acest pas de fiecare dată când te conectezi de pe același dispozitiv, îți recomandăm să îl setezi ca dispozitiv sigur.

Pentru a adăuga dispozitive marcate ca fiind sigure:

1. Accesați **Bitdefender Central**.
2. Faceți clic pe icoana  din partea dreapta de sus al ecranului.
3. Selectează **Cont Bitdefender** din meniul derulant.
4. Selectează fila **Parolă și securitate**.



5. Selectează opțiunea **Dispozitive sigure**.
6. Se afișează lista cu dispozitivele pe care este instalat Bitdefender. Selectează dispozitivul dorit.

Poți adăuga oricât de multe dispozitive dorești, cu condiția ca pe acestea să fie instalat Bitdefender și abonamentul tău să fie valid.

2.3.2. Abonamentele mele

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

Verificați abonamentele disponibile

Pentru a verifica abonamentele disponibile:

1. Accesați **Bitdefender Central**.
2. Selectați fereastra **Abonamentele mele**.

Aici aveți informații referitoare la disponibilitatea abonamentelor pe care le dețineți și la numărul de dispozitive care utilizează fiecare dintre aceste abonamente.

Puteți adăuga dispozitive unui abonament sau îl puteți reînnoi selectând un card de abonament.



Notă

Puteți avea mai multe abonamente în contul dumneavoastră cu condiția ca acestea să fie pentru platforme diferite (Windows, macOS, iOS sau Android).

Adaugă dispozitiv nou

Dacă abonamentul dvs. acoperă mai multe dispozitive, puteți adăuga un dispozitiv nou și puteți instala Bitdefender Total Security pe acesta, după cum urmează:

1. Accesați **Bitdefender Central**.
2. Selectează fereastra **Dispozitivele mele** și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA**.
3. Alegeți una dintre cele două opțiuni disponibile:
 - **Protejează acest dispozitiv**



Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.

● Protejează alte dispozitive

Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.

Selectează **TRIMITE LINKUL PENTRU DESCĂRCARE**. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.

Pe dispozitivul pe care dorești să instalezi produsul Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

4. Așteaptă să se finalizeze descărcarea și apoi execută aplicația de instalare.

Reînnoire abonament

Dacă ai dezactivat reînnoirea automată a abonamentului Bitdefender, îl poți reînnoi manual parcurgând pașii următori:

1. Accesați **Bitdefender Central**.
2. Selectați fereastra **Abonamentele mele**.
3. Selectați cardul de abonare dorit.
4. Fă clic pe **Reînnoire** pentru a continua.

Se deschide o pagină web în browser-ul dvs., de unde puteți reînnoi abonamentul Bitdefender.

Activare abonament

Un abonament poate fi activat în timpul procesului de instalare, folosind contul Bitdefender. După activare, începe și calcularea perioadei de valabilitate rămase.

Dacă ați achiziționat un cod de activare de la unul dintre distribuitorii noștri sau l-ați primit cadou, puteți adăuga valabilitatea acestuia la abonamentul actual Bitdefender disponibil în cont, cu condiția să fie destinat aceleiași produs.

Pentru a activa un abonament folosind un cod de activare:



1. Accesați **Bitdefender Central**.
2. Selectați fereastra **Abonamentele mele**.
3. Apăsați pe butonul **COD DE ACTIVARE**, apoi introduceți codul în câmpul corespunzător.
4. Efectuează clic pe **ACTIVARE** pentru a continua.


Abonamentul este acum activat. Accesează secțiunea **Dispozitivele mele** și selectează **INSTALARE PROTECȚIE** pentru a instala produsul pe unul dintre dispozitivele tale.

2.3.3. Dispozitivele mele

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

Pentru a vizualiza lista dispozitivelor tale sortate în funcție de starea acestora sau utilizatori, efectuează clic pe săgeata jos din colțul din dreapta-sus al ecranului.


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 alocă 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**.
5. Efectuează clic pe **Adăugare proprietar** și completează câmpurile corespunzătoare. Personalizează-ți profilul adăugând o fotografie și selectând data nașterii.
6. Faceți clic pe **ADAUGĂ** pentru a salva profilul.
7. Selectați deținătorul dorit din lista **Deținător dispozitiv**, apoi faceți clic pe **ALOCARE**.

Pentru a actualiza Bitdefender de la distanță pe un dispozitiv Windows:

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 mai multe operațiuni ce pot fi efectuate de la distanță și informații referitoare la produsul Bitdefender instalat pe un anumit dispozitiv, efectuează clic pe fila dispozitivului dorit.

După ce ai efectuat clic pe fila dispozitivului, sunt disponibile următoarele secțiuni:

- **Panou de bord.** În această fereastră, poți vizualiza detalii despre dispozitivul selectat, poți verifica starea sa de protecție, starea funcției VPN Bitdefender 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. Atunci când există probleme care îți afectează dispozitivul, efectuează clic pe săgeata din zona de stare din partea de sus pentru a afla mai multe detalii. De aici, puteți remedia manual problemele care afectează securitatea dispozitivelor.
- **Securitate.** Din această fereastră, puteți executa de la distanță o Scanare rapidă sau de sistem pe dispozitive. Faceți clic pe butonul **SCANARE** pentru a începe procesul. De asemenea, puteți afla data ultimei scanări a



dispozitivului și puteți primi un raport cu privire la cea mai recentă scanare, cu cele mai importante informații disponibile. Pentru mai multe informații referitoare la aceste două proceduri de scanare, consultați *„Executarea unei scanări a sistemului”* (p. 88) și *„Rularea unei scanări rapide”* (p. 87).

- **Optimizator.** Aici puteți îmbunătăți performanța sistemului de la distanță prin scanarea rapidă, detectarea și curățarea fișierelor inutile. Faceți clic pe butonul **START** și apoi selectați zonele pe care doriți să le optimizați. Faceți din nou clic pe butonul **START** pentru a începe procesul de optimizare. Fă clic pe **Mai multe detalii** pentru a accesa un raport detaliat despre problemele remediate.

În plus, poți îmbunătăți pornirea dispozitivului identificând acele aplicații care consumă multe resurse de sistem. Apasă pe **MAI MULTE DETALII** și apoi selectează cum dorești să procedezi cu aplicațiile detectate. Pentru mai multe detalii despre aceste caracteristici, consultă *„Optimizăți viteza sistemului cu un singur clic”* (p. 182) și *„Optimizarea timpului de pornire al calculatorului dvs.”* (p. 183).

- **Antifurt.** Dacă nu știți unde ați pus aparatul, dacă vă este furat sau îl pierdeți, cu funcția Antifurt puteți localiza dispozitivul pentru a lua măsuri de la distanță. Faceți clic pe **LOCALIZARE** pentru a afla unde se află dispozitivul. Se va afișa ultima poziție cunoscută, alături de oră și dată. Pentru detalii despre această funcție, consultă *„Antifurt”* (p. 178).
- **Vulnerabilități.** Pentru a verifica existența unor vulnerabilități pe un dispozitiv, cum ar fi lipsa actualizărilor Windows, aplicații expirate sau parole slabe, faceți clic pe butonul **SCANARE** din secțiunea Vulnerabilități. Vulnerabilitățile nu pot fi remediate de la distanță. În cazul în care se identifică o vulnerabilitate, trebuie să executați o nouă scanare pe dispozitivul respectiv și apoi să întreprindeți acțiunile recomandate. Fă clic pe **Mai multe detalii** pentru a accesa un raport detaliat despre problemele identificate. Pentru detalii despre această funcție, consultă *„Vulnerabilități”* (p. 121).

2.3.4. Activitate

În secțiunea Activitate, ai acces la informații despre dispozitivele pe care este instalat Bitdefender.

Când accesezi fereastra **Activitate**, vor deveni disponibile următoarele carduri:

- **Dispozitivele mele.** Aici poți vedea numărul dispozitivelor conectate împreună cu starea lor de protecție. Pentru a remedia problemele de la




distanță de pe dispozitivele detectate, selectează **Remediere probleme** și apoi **SCANARE ȘI REMEDIERE PROBLEME**.

Pentru a vizualiza detaliile referitoare la problemele detectate, selectează **Vizualizează problemele**.

Informațiile despre amenințările detectate nu pot fi extrase de pe dispozitivele cu iOS.

- **Amenințări blocate.** Aici poți vizualiza un grafic care prezintă statistici globale, ce includ informații despre amenințările blocate în ultimele 24 de ore și șapte zile. Informațiile afișate sunt preluate în funcție de comportamentul periculos detectat în cazul fișierelor, aplicațiilor și adreselor URL accesate.
- **Principalii utilizatori cu amenințări blocate.** Aici poți vedea un top al utilizatorilor la care au fost detectate cele mai multe amenințări.
- **Principalele dispozitive cu amenințări blocate.** Aici poți vedea un top al dispozitivelor pe care au fost detectate cele mai multe amenințări.

2.3.5. Notificări

Pentru a vă ajuta să fiți la curent cu ceea ce se întâmplă pe dispozitivele asociate contului dumneavoastră, aveți la dispoziție pictograma . Odată ce efectuați clic pe aceasta, veți avea o imagine de ansamblu ce constă în informații despre activitatea produselor Bitdefender instalate pe dispozitivele dumneavoastră.

2.4. Actualizarea permanentă a Bitdefender

Zi de zi sunt descoperite și identificate noi amenințări. De aceea este foarte important ca Bitdefender să fie actualizat cu cea mai recentă bază de date cu amenințări.

Dacă sunteți conectat la internet, prin bandă largă sau ADSL, Bitdefender se ocupă singur de actualizări. În mod implicit, acesta caută actualizări la pornirea sistemului, precum și după fiecare **oră**. În cazul în care este detectată o actualizare, aceasta este descărcată și instalată automat pe computerul dumneavoastră.

Procesul de actualizare este realizat progresiv, ceea ce înseamnă că fișierele care trebuie actualizate sunt înlocuite unul câte unul. Astfel, procesul de



actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.



Important

Mențineți funcția Actualizare automată activată pentru a fi protejat împotriva celor mai noi amenințări.

În anumite cazuri este necesară intervenția dumneavoastră pentru ca protecția oferită de Bitdefender să fie actualizată:

- Dacă computerul dumneavoastră este conectat la internet printr-un server proxy, trebuie să configurați setările proxy, după cum se specifică în *„Cum pot configura Bitdefender să utilizeze o conexiune la internet de tip proxy?”* (p. 75).
- Dacă vă conectați la internet prin dial-up, atunci este recomandat să actualizați manual Bitdefender în mod regulat. Pentru mai multe informații, consultați capitolul *„Efectuarea unei actualizări”* (p. 40).

2.4.1. Cum verificați dacă Bitdefender este actualizat

Pentru a verifica momentul ultimei actualizări a Bitdefender tău:

1. Efectuează clic pe **Notificări** din meniul de navigare al interfeței Bitdefender.
2. În fila **Toate**, selectează notificarea privind ultima actualizare.

Puteți afla când anume au fost inițiate actualizări, precum și informații despre acestea (dacă au fost finalizate cu succes, dacă este necesară o repornire pentru a finaliza instalarea). Dacă este necesar, reporniți sistemul cât mai curând posibil.

2.4.2. Efectuarea unei actualizări

Pentru efectuarea actualizărilor este necesară existența unei conexiuni la internet.

Pentru a porni o actualizare, efectuează clic dreapta pe pictograma Bitdefender **B** din **bara de sistem** și apoi selectează opțiunea **Actualizează acum**.

Funcția Actualizare se va conecta la serverul de actualizare al Bitdefender și va căuta noi actualizări. În cazul în care este detectată o actualizare, în



funcție de **setările de actualizare**, vi se va cere fie să confirmați actualizarea, fie aceasta va fi realizată automat.




Important

Poate fi necesar ca după realizarea unei actualizări să reporniți calculatorul. Vă recomandăm să faceți acest lucru cât mai repede cu putință.

De asemenea, puteți efectua actualizări ale dispozitivelor dumneavoastră și de la distanță, cu condiția ca acestea să fie pornite și conectate la internet.

Pentru a actualiza Bitdefender de la distanță pe un dispozitiv Windows:

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**.

2.4.3. Activarea sau dezactivarea actualizării automate

Pentru activa sau dezactiva actualizarea automată:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Actualizare**.
3. Activează sau dezactivează butonul corespunzător.
4. Se deschide o fereastră de avertizare. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării actualizării automate. Poți dezactiva actualizarea automată pentru 5, 15 sau 30 de minute, pentru o oră sau până la repornirea sistemului.



Avertisment

Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați actualizarea automată pentru cât mai puțin timp posibil. Dacă nu este actualizat în mod regulat, Bitdefender nu va putea să vă protejeze împotriva ultimelor amenințări apărute.



2.4.4. Ajustarea setărilor de actualizare

Actualizările pot fi realizate din rețeaua locală, de pe internet, direct sau printr-un server proxy. Implicit, Bitdefender va căuta actualizări la fiecare oră, pe internet, și va instala actualizările disponibile fără a vă mai avertiza.

Setările de actualizare implicite sunt potrivite pentru majoritatea utilizatorilor, și, în mod normal, nu este nevoie să le modificați.

Pentru a ajusta setările de actualizare:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectează fila **Actualizare** și ajustează setările conform preferințelor tale.

Frecvența actualizărilor

Bitdefender este configurat să verifice din oră în oră dacă există actualizări. Pentru a modifica frecvența actualizărilor, trageți de cursor de-a lungul scalei pentru a stabili perioada dorită de timp la care ar trebui să intervină actualizarea.

Reguli de procesare a actualizării

De fiecare dată când este disponibilă o actualizare, Bitdefender va descărca și implementa automat actualizarea fără notificări vizibile. Dezactivează opțiunea **Actualizare silențioasă** dacă dorești să fii notificat de fiecare dată când este disponibilă o nouă actualizare.

Anumite actualizări necesită o repornire a computerului pentru a finaliza procesul de instalare.

Implicit, dacă o actualizare necesită repornirea computerului, Bitdefender va continua să funcționeze cu fișierele vechi până în momentul în care utilizatorul repornește computerul. În acest fel, procesul de actualizare a Bitdefender nu interferează cu operațiile utilizatorului.

Dacă dorești să fii notificat atunci când o actualizare necesită repornirea calculatorului, activează opțiunea **Repornește notificări**.

2.4.5. Actualizări permanente

Pentru a vă asigura că folosiți cea mai recentă versiune, Bitdefender verifică automat actualizările de produs. Aceste actualizări pot introduce noi caracteristici și îmbunătățiri, pot remedia erori ale produsului sau pot realiza



un upgrade automat la o nouă versiune. Atunci când noua versiune Bitdefender este disponibilă prin intermediul actualizării, se salvează setările personalizate și se evită procedura de dezinstalare și reinstalare.

Aceste actualizări necesită repornirea sistemului cu scopul de a iniția instalarea de noi fișiere. Atunci când este finalizată o actualizare de produs, o fereastră pop-up vă va solicita să reporniți sistemul. Dacă ratați această notificare, puteți fie să efectuați clic pe **REPORNEȘTE ACUM** în fereastra **Notificări** unde este menționată cea mai recentă actualizare, fie să reporniți manual sistemul.



Notă

Actualizările care includ noi caracteristici și îmbunătățiri vor fi livrate numai către utilizatorii care au Bitdefender 2019 instalat.



3. CUM SĂ

3.1. Instalare

3.1.1. Cum instalez Bitdefender pe un al doilea calculator?

Dacă abonamentul achiziționat acoperă mai mult de un calculator, puteți utiliza contul dvs. Bitdefender pentru a activa un al doilea calculator.

Pentru a instala Bitdefender pe un al doilea calculator:

1. Dă clic pe **Instalare pe alt dispozitiv** din colțul din stânga-jos al **interfeței Bitdefender**.

O nouă fereastră apare pe ecran.

2. Selectează **TRIMITE LINK-UL**.
3. Urmează instrucțiunile de pe ecran pentru a instala Bitdefender.

Noul dispozitiv pe care l-ați instalat pe produsul Bitdefender va apărea în panoul de control Bitdefender Central.

3.1.2. Cum reinstalez Bitdefender?

Printre cazurile care ar putea necesita reinstalarea Bitdefender se numără următoarele:

- ați reinstalat sistemul de operare.
- doresc să remediez problemele care este posibil să fi cauzat încetiniri ale proceselor sau căderi de sistem.
- produsul dumneavoastră Bitdefender nu pornește sau nu funcționează corespunzător.

În cazul în care vă aflați într-una dintre situațiile menționate mai sus, urmați acești pași:

- În **Windows 7**:

1. Faceți clic pe **Start** și mergeți la **Toate programele**.
2. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
3. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
4. După finalizarea procesului, va fi necesară repornirea calculatorului.



● În Windows 8 și Windows 8.1:

1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
5. După finalizarea procesului, va fi necesară repornirea calculatorului.

● În Windows 10:

1. Faceți clic pe **Start**, apoi pe Setări.
2. Faceți clic pe pictograma **Sistem** din zona Setări și selectați **Aplicații & funcții**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Efectuați clic pe **REINSTALEAZĂ**.
6. După finalizarea procesului, va fi necesară repornirea calculatorului.



Notă

Urmând această procedură de reinstalare, setările personalizate sunt salvate și vor fi disponibile în noul produs instalat. Celelalte setări pot fi restabilite la configurația implicită.

3.1.3. De unde se poate descărca produsul Bitdefender?

Puteți instala Bitdefender folosind CD-ul de instalare sau aplicația de instalare web pe care o puteți descărca pe calculatorul dumneavoastră din platforma Bitdefender Central.



Notă

Înainte de a rula aplicația de instalare, vă recomandăm să dezinstalați orice soluție de securitate de pe sistemul dumneavoastră. Atunci când utilizați mai multe soluții de securitate pe același calculator, sistemul devine instabil.

Pentru a instala Bitdefender din Bitdefender Central:

1. Accesați **Bitdefender Central**.



2. Selectează fereastra **Dispozitivele mele** și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA**.
3. Alegeți una dintre cele două opțiuni disponibile:
 - **Protejează acest dispozitiv**

Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
 - **Protejează alte dispozitive**

Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.

Selectează **TRIMITE LINKUL PENTRU DESCĂRCARE**. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.

Pe dispozitivul pe care dorești să instalezi produsul Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.
4. Rulați produsul Bitdefender descărcat.

3.1.4. Cum pot modifica limba produsului meu Bitdefender?

Interfața Bitdefender este disponibilă în mai multe limbi și poate fi modificată urmând acești pași:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. În fereastra **General**, selectează **Schimbă limba**.
3. Selectează din listă limba dorită și apoi clic pe **SALVEAZĂ**.
4. Așteaptă câteva momente până când se aplică setările.

3.1.5. Cum folosesc abonamentul Bitdefender după un upgrade Windows?

Această situație apare atunci când faceți un upgrade al sistemului de operare și doriți utilizați în continuare abonamentul Bitdefender.

Dacă folosiți versiunea anterioară a Bitdefender, puteți trece gratuit la cea mai recentă versiune a Bitdefender, după cum urmează:



- De la versiunea anterioară Antivirus Bitdefender până la cea mai recentă versiune Antivirus Bitdefender disponibilă.
- De la o versiune anterioară de Securitate Internet Bitdefender până la cea mai recentă versiune de Securitate pe Internet Bitdefender disponibilă.
- De la o versiune de Securitate totală Bitdefender anterioară până la cea mai recentă versiune de Securitate totală Bitdefender disponibilă.

Pot apărea două situații:

- Ați făcut upgrade la sistemul de operare folosind Windows Update și ați observat că Bitdefender nu mai funcționează.

În acest caz, este necesar să reinstalați produsul urmând acești pași:

● În Windows 7:

1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
2. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
3. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
4. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

Deschideți interfața noului produs Bitdefender instalat pentru a avea acces la caracteristicile sale.

● În Windows 8 și Windows 8.1:

1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
5. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

Deschideți interfața noului produs Bitdefender instalat pentru a avea acces la caracteristicile sale.

● În Windows 10:



1. Faceți clic pe **Start**, apoi pe Setări.
2. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează **Aplicații**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
6. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

Deschideți interfața noului produs Bitdefender instalat pentru a avea acces la caracteristicile sale.



Notă

Urmând această procedură de reinstalare, setările personalizate sunt salvate și vor fi disponibile în noul produs instalat. Celelalte setări pot fi restabilite la configurația implicită.

- Ați modificat sistemul dumneavoastră și doriți să utilizați în continuare protecția Bitdefender. Prin urmare, trebuie să reinstalați produsul folosind cea mai recentă versiune.

Pentru a rezolva această problemă:

1. Descărcați fișierul de instalare:
 - a. Accesați **Bitdefender Central**.
 - b. Selectează fereastra **Dispozitivele mele** și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA**.
 - c. Alegeți una dintre cele două opțiuni disponibile:
 - **Protejează acest dispozitiv**
Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
 - **Protejează alte dispozitive**
Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
Selectează **TRIMITE LINKUL PENTRU DESCĂRCARE**. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE**



E-MAIL. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.

Pe dispozitivul pe care dorești să instalezi produsul Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

2. Rulați produsul Bitdefender descărcat.

Pentru mai multe informații cu privire la procesul de instalare Bitdefender, consultați „*Instalarea produsului tău Bitdefender*” (p. 3).

3.1.6. Cum pot face upgrade la cea mai recentă versiune Bitdefender?

De acum înainte, actualizarea la cea mai recentă versiune este posibilă fără a urma procedura de dezinstalare și reinstalare manuală. Mai exact, noul produs care include noi caracteristici și îmbunătățiri majore de produs este livrat prin intermediul actualizărilor de produs și, dacă aveți deja un abonament Bitdefender activ, produsul se activează automat.

Dacă folosești versiunea 2019, poți face upgrade la cea mai nouă versiune urmând acești pași:

1. Efectuați clic pe **REPORNEȘTE ACUM** în fereastra de notificare în care sunt afișate informațiile privind actualizarea. Dacă ați ratat-o, accesați fereastra **Notificări**, identificați cea mai recentă actualizare și apoi efectuați clic pe butonul **REPORNEȘTE ACUM**. Așteaptă repornirea calculatorului.

Se va afișa fereastra **Ce este nou** conținând informațiile despre caracteristicile noi și îmbunătățite.

2. Efectuați clic pe link-urile **Citiți mai multe** pentru redirectare către pagina noastră dedicată conținând mai multe detalii și articole utile.

3. Închideți fereastra **Ce este nou** pentru a accesa interfața noi versiuni instalate.

Utilizatorii care doresc să facă upgrade gratuit de la Bitdefender 2016 sau o versiune anterioară la cea mai recentă versiune Bitdefender trebuie să dezinstaleze versiunea lor actuală din Control Panel și apoi să descarce cel mai recent fișier de instalare de pe site-ul Bitdefender accesând următoarea adresă: <https://www.bitdefender.com/Downloads/>. Activarea este posibilă numai dacă există un abonament valabil.



3.2. Bitdefender Central

3.2.1. Cum mă autentific în contul Bitdefender cu un alt cont?

Ați creat un nou cont Bitdefender și doriți să începeți să-l folosiți.

Pentru a vă autentifica cu alt cont Bitdefender:

1. Dă clic pe **Contul meu** din meniul de navigare al **interfeței Bitdefender**.
2. Selectează **Schimbă contul** din colțul din dreapta sus al ecranului pentru a schimba contul asociat computerului respectiv.
3. Introdu adresa de e-mail în câmpul corespunzător, apoi fă clic pe **MAI DEPARTE**.
4. Introdu parola și apoi efectuează clic pe **AUTENTIFICARE**.



Notă


Produsul Bitdefender de pe dispozitivul dvs. trece automat la abonamentul asociat noului cont Bitdefender.

Dacă nu există niciun abonament disponibil asociat noului cont Bitdefender sau dacă doriți să îl transferați pe contul anterior, puteți contacta Bitdefender pentru asistență, în modul descris în secțiunea „*Solicitarea ajutorului*” (p. 333).

3.2.2. Cum pot dezactiva mesajele de ajutor pentru Bitdefender Central?

Pentru a te ajuta să înțelegi cum să folosești fiecare opțiune din Bitdefender Central, în panoul de bord sunt afișate mesaje de ajutor.

Dacă dorești să nu mai vezi acest tip de mesaje:

1. Accesați **Bitdefender Central**.
2. Faceți clic pe icoana  din partea dreapta de sus al ecranului.
3. Fă clic pe **Contul meu** în meniul derulant.
4. Selectează opțiunea **Setări** din meniul derulant.
5. Dezactivează opțiunea **Activează/dezactivează mesajele de ajutor**.



3.2.3. Am uitat parola setată pentru contul meu Bitdefender. Cum se resetează?

Există două posibilități pentru a seta o nouă parolă pentru contul dumneavoastră Bitdefender:

● Din interfața Bitdefender:

1. Dă clic pe **Contul meu** din meniul de navigare al **interfeței Bitdefender**.
2. Selectează **Schimbă contul** din colțul din dreapta sus al ecranului.
Se afișează o nouă fereastră.
3. Faceți clic pe **Ați uitat parola?**.
4. Introduceți adresa de e-mail și selectează **ÎNAINTE**.
5. Verificați-vă contul de e-mail, introduceți codul de securitate primit și apoi faceți clic pe **MAI DEPARTE**.
Alternativ, puteți face clic pe **Schimbare parolă** din mesajul e-mail pe care vi l-am trimis.
6. Introduceți noua parolă pe care doriți să o setați și apoi introduceți-o din nou. Efectuează clic pe **SALVARE**.

● Din browser-ul web:

1. Mergeți la: <https://central.bitdefender.com>.
2. Selectează **AUTENTIFICARE**.
3. Introduceți adresa ta de e-mail, apoi selectează opțiunea **ÎNAINTE**.
4. Faceți clic pe **Ați uitat parola?**.
5. Verifică-ți contul de e-mail și urmărește instrucțiunile furnizate pentru a seta o nouă parolă pentru contul tău Bitdefender.


Pentru a accesa ulterior contul Bitdefender, introduceți adresa e-mail și noua parolă setată.

3.2.4. Cum pot gestiona sesiunile de autentificare asociate contului meu Bitdefender?

În contul dumneavoastră Bitdefender, aveți posibilitatea de a vizualiza cele mai recente sesiuni de autentificare active și inactive de pe dispozitivele



asociate contului dumneavoastră. În plus, vă puteți deconecta de la distanță urmând acești pași:

1. Accesați **Bitdefender Central**.
2. Faceți clic pe icoana  din partea dreapta de sus al ecranului.
3. Fă clic pe **Contul meu** în meniul derulant.
4. Selectează **Administrare sesiuni** din meniul glisant.
5. În secțiunea **Sesiuni active**, selectați opțiunea **Deconectare** din dreptul dispozitivului pe care doriți să încheiați sesiunea.

3.3. Scanarea cu Bitdefender

3.3.1. Cum scanez un fișier sau un director?

Cea mai ușoară metodă de a scana un fișier sau un director este de a face clic dreapta pe un obiect pe care doriți să-l scanați, alegeți Bitdefender și selectați **Scanează cu Bitdefender** din meniu.

Pentru finalizarea procesului de scanare, urmați pașii asistentului de scanare antivirus. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate.

Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Iată câteva situații în care este recomandată folosirea acestei metode de scanare:

- Suspectați un anumit fișier sau director că este infectat.
- Atunci când descărcați fișiere de pe internet considerate că ar putea fi periculoase.
- Scanați un director comun din rețea înainte de a copia fișiere din acesta pe calculatorul dumneavoastră.

3.3.2. Cum îmi scanez sistemul?

Pentru a realiza o scanare completă a sistemului:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTIVIRUS**, efectuează clic pe **Scanare sistem**.




3. Urmați programul asistent Scanare Sistem pentru a încheia scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate.

Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultați capitolul „*Asistentul de scanare antivirus*” (p. 92).

3.3.3. Cum programez o scanare?

Puteți configura Bitdefender să activeze scanarea locațiilor importante de sistem când nu vă aflați la calculator.

Pentru a programa o scanare:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTIVIRUS**, efectuează clic pe **Administrare scanări**.
3. Selectează  în dreptul tipului de scanare pe care dorești să o programezi, respectiv Scanare de sistem sau Scanare rapidă.

Ca metodă alternativă, poți crea un tip de scanare care să corespundă necesităților tale selectând **Creează o nouă sarcină de scanare**.

4. Activează opțiunea **Programează sarcina de scanare**.

Selectați una dintre opțiunile corespunzătoare pentru a seta un program:

- La pornirea sistemului
- Zilnic
- Săptămânal
- Lunar

Dacă selectezi Zilnic, Lunar sau Săptămânal, trage de cursor pentru a seta perioada de timp dorită pentru începerea scanării.

Dacă alegi să creezi o nouă scanare personalizată, se va afișa fereastra **Sarcină de scanare**. De aici poți selecta locațiile care dorești să fie scanate.



3.3.4. Cum creez o activitate de scanare personalizată?

Dacă doriți să scanați anumite locații de pe computer sau pentru a configura opțiunile de scanare, puteți configura și rula o sarcină de scanare personalizată.

Pentru a crea o activitate de scanare personalizată, procedați după cum urmează:

1. În panoul **ANTIVIRUS**, efectuează clic pe **Administrare scanări**.
2. Selectează **Creează o nouă sarcină de scanare**.
3. În câmpul **Nume sarcină**, introdu o denumire pentru scanarea respectivă, apoi selectează locațiile care dorești să fie scanate și apasă pe **ÎNAINTE**.
4. Configurează următoarele opțiuni generale:
 - **Scanează doar aplicații**. Poți configura Bitdefender astfel încât să scaneze numai aplicațiile accesate.
 - **Prioritate sarcină de scanare**. Poți alege impactul pe care procesul de scanare ar trebui să îl aibă asupra performanței sistemului.
 - **Automat** - Prioritatea procesului de scanare va depinde de activitatea sistemului. Pentru a te asigura că procesul de scanare nu va afecta activitatea sistemului, Bitdefender va decide dacă procesul de scanare trebuie să se execute cu prioritate mare sau mică.
 - **Ridicat** - Prioritatea procesului de scanare va fi ridicată. Selectând această opțiune, vei permite executarea altor programe cu o viteză redusă, micșorând perioada de timp necesară pentru finalizarea scanării.
 - **Redus** - Prioritatea procesului de scanare va fi redusă. Selectând această opțiune, vei permite executarea altor programe cu o viteză mai mare, măbind perioada de timp necesară pentru finalizarea scanării.
 - **Acțiuni post-scanare**. Alege acțiunea care trebuie întreprinsă de Bitdefender în cazul în care nu sunt identificate niciun fel de amenințări:
 - Afișează fereastra Sumar
 - Închide dispozitivul
 - Închide fereastra Scanare



5. Dacă dorești să configurezi în detaliu opțiunile de scanare, selectează **Afișează opțiuni avansate**.

Selectează **ÎNAINTE**.

6. Activează **Programează sarcina de scanare** și apoi precizează când ar trebui să pornească sarcina personalizată pe care ai creat-o.

- La pornirea sistemului
- Zilnic
- Lunar
- Săptămânal

Dacă selectezi Zilnic, Lunar sau Săptămânal, trage de cursor pentru a seta perioada de timp dorită pentru începerea scanării.

7. Selectează **SALVEAZĂ** pentru a salva setările și a închide fereastra de configurare.

Procesul de scanare poate dura ceva timp, în funcție de locațiile ce vor fi scanate. Dacă se vor găsi amenințări în timpul procesului de scanare, îți se va solicita să alegi acțiunile care trebuie întreprinse în cazul fișierelor detectate.

Dacă doriți, puteți relua rapid rularea scanării personalizate anterioare, făcând clic pe înregistrarea corespunzătoare din lista valabilă.

3.3.5. Cum exclud un director de la procesul de scanare?

Bitdefender permite excluderea de la scanare a anumitor fișiere, directoare sau extensii de fișiere.

Excepțiile vor fi folosite de către utilizatorii care au cunoștințe avansate privind computerele sau doar în situațiile următoare:

- Aveți un director mare pe sistemul dumneavoastră în care există filme și muzică
- Aveți o arhivă mare pe sistemul dumneavoastră în care păstrați diferite date.
- Păstrați un director în care să instalați diverse tipuri de software-uri și aplicații în scopuri de testare. Scanarea directorului poate duce la pierderea anumitor date.

Pentru a adăuga un director în lista de Excepții:



1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
3. Dă clic pe fila **Excepții**.
4. Dă clic meniul expandabil **Lista fișierelor și directoarelor excluse de la scanare** și apoi pe **Adăugare**.
5. Dă clic pe **RĂSFOIRE**, selectează directorul care dorești să fie exclus de la scanare și apoi selectează tipul scanării de la care să fie exclus.
6. Dă clic pe **ADĂUGARE** pentru a salva modificările și închide fereastra.

3.3.6. Ce să fac atunci când Bitdefender a detectat un fișier curat ca fiind infectat?

Pot exista situații în care Bitdefender marchează în mod greșit un fișier legitim ca fiind o amenințare (un fals pozitiv). Pentru a corecta această eroare, adaugă fișierul în secțiunea de Excepții a Bitdefender:

1. Dezactivați protecția antivirus în timp real a Bitdefender:
 - a. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
 - b. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
 - c. În fereastra **Shield**, dezactivează opțiunea **Bitdefender Shield**.

Se deschide o fereastră de avertizare. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real. Puteți dezactiva protecția în timp real pentru 5, 15 sau 30 de minute, pentru o oră, permanent sau doar până la repornirea sistemului.
2. Afișați elementele ascunse din Windows. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot afișa elementele ascunse din Windows?”* (p. 77).
3. Restaurați fișierul din zona de carantină:
 - a. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
 - b. În secțiunea **ANTIVIRUS**, efectuați clic pe **Carantină**.
 - c. Selectați fișierul și faceți clic pe **RESTABILIRE**.



4. Aduagă fișierul în lista de Excepții. Pentru a afla cum poți face acest lucru, consultă secțiunea „*Cum exclud un director de la procesul de scanare?*” (p. 55).
5. Activați protecția antivirus în timp real a Bitdefender.
6. Contactați un reprezentant al echipei noastre de asistență tehnică și solicitați eliminarea actualizării informațiilor privind amenințările. Pentru a afla cum poți face acest lucru, consultă secțiunea „*Solicitarea ajutorului*” (p. 333).

3.3.7. Cum aflu ce amenințări au fost detectate de Bitdefender?

De fiecare dată când se efectuează o operațiune de scanare, se creează un jurnal în care Bitdefender înregistrează toate problemele detectate.

Raportul de scanare conține informații detaliate despre procesul de scanare înregistrat, cum ar fi opțiunile de scanare, locațiile scanate, amenințările găsite și acțiunile luate asupra acestor amenințări.

Poți deschide raportul de scanare direct din asistentul de scanare, după ce scanarea a luat sfârșit, apăsând **AFIȘEAZĂ JURNAL**.

Pentru a verifica un jurnal de scanări sau orice infecție detectată ulterior:

1. Efectuează clic pe **Notificări** din meniul de navigare al interfeței **Bitdefender**.
2. În fila **Toate**, selectează notificarea privind ultima scanare.
Aici puteți găsi toate evenimentele de scanare, inclusiv amenințările detectate prin scanarea la accesare, prin scanarea inițiată de utilizator, precum și modificările de stare rezultate de scanările automate.
3. În lista de notificări puteți verifica ce operațiuni de scanare au fost realizate recent. Faceți clic pe o notificare pentru a vizualiza detaliile acesteia.
4. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**.




3.4. Control Parental

3.4.1. Cum îmi protejez copiii împotriva amenințărilor online?

Aplicația Control parental Bitdefender îți oferă posibilitatea de a restricționa accesul la internet și la anumite aplicații, astfel încât copiii tăi să nu poată vizualiza conținut neadecvat atunci când nu ești prin preajmă să-i supraveghezi.

Pentru a configura funcția Control parental:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **CONTROL PARENTAL**, selectează **Configurare**.
Sunteți redirecționat(ă) la pagina web a contului Bitdefender. Asigură-te că ești conectat(ă) cu datele tale de autentificare.
3. Se deschide panoul de control pentru funcția Control parental. De aici puteți verifica și configura setările funcției de Control Parental.
4. Selectează opțiunea **CREAZĂ UN PROFIL DE COPIL** din fereastra **Copiii mei**.
5. Introdu informații specifice, cum ar fi numele, data nașterii sau sexul. Pentru a adăuga o imagine la profilul copilului tău, accesează pictograma  din colțul din dreapta jos al opțiunii **Fotografie de profil**. Selectează **SALVEAZĂ** pentru a continua.

În baza standardelor de dezvoltare a copilului, setarea datei nașterii copilului încarcă automat setările de căutare web considerate corespunzătoare pentru categoria sa de vârstă.

6. Selectează opțiunea **SĂ ADĂUGĂM UN DISPOZITIV**.
7. Dacă dispozitivul copilului tău are deja instalat un produs Bitdefender, selectează dispozitivul acestuia din lista disponibilă și apoi contul pe care dorești să-l monitorizezi. Selectează opțiunea **TRIBUIE**.

În cazul în care copilul tău nu are instalat niciun produs Bitdefender pe dispozitivul pe care îl folosește, selectează **Instalează pe un dispozitiv nou** și apoi **TRIMITE LINKUL PENTRU DESCĂRCARE**. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că



linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.

Pe dispozitivul pe care dorești să instalezi Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.



Important

Pe dispozitivele Windows și macOS pe care nu este instalat niciun produs Bitdefender, se va instala tracker-ul de monitorizare Bitdefender Parental Control astfel încât să poți monitoriza activitățile online ale copiilor tăi.

Pe dispozitivele Android și iOS, se va descărca și instala aplicația Bitdefender Parental Control.

3.4.2. Cum blochez accesul copilului meu la un anumit site web?

Funcția Control parental Bitdefender îți permite să controlezi conținutul accesat de copilul tău atunci când folosește dispozitivul și să blochezi accesul la anumite site-uri web.

Pentru a bloca accesul la un site web, trebuie să-l adaugi în lista de Excepții, după cum urmează:

1. Mergeți la: <https://central.bitdefender.com>.
2. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
3. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
4. Selectați profilul copilului dumneavoastră din fereastra **Copiii mei**.
5. Selectează fila **Site-uri web** și apoi accesează opțiunea **ADMINISTRARE**.
6. Introduceți pagina web pe care dorești să o blochezi în câmpul corespunzător.
7. Selectați **Permite** sau **Blocare**.
8. Faceți clic pe **Finalizare** pentru a salva modificările.



Notă

Pot fi setate restricții numai pentru dispozitivele Android, macOS și Windows.



3.4.3. Cum îmi împiedic copilul să folosească anumite aplicații?

Bitdefender Parental Control îți permite să controlezi conținutul pe care îl accesează copiii tăi în timp ce utilizează dispozitivele.

Pentru a bloca accesul la o aplicație:

1. Mergeți la: <https://central.bitdefender.com>.
2. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
3. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
4. Selectează un profil de copil din fereastra **Copiii mei**.
5. Selectați fila **Aplicații**.
6. Este afișată lista dispozitivelor asociate.
Selectează panoul dispozitivului pentru care dorești să restricționezi accesul la aplicații.
7. Apasă pe **Administrare aplicații utilizate de....**
Se afișează o listă a aplicațiilor instalate.
8. Selectează **Blocat** din dreptul aplicațiilor care dorești să nu mai fie folosite de copilul tău.
9. Selectează **SALVEAZĂ** pentru a aplica noile setări.



Notă

Pot fi setate restricții numai pentru dispozitivele Android, macOS și Windows.

3.4.4. Cum îmi împiedic copilul să intre în contact cu persoane care nu sunt de încredere?


Bitdefender Parental Control îți oferă posibilitatea de a bloca apelurile din lista de contacte de pe telefonul copilului tău. Restricțiile pentru apeluri pot fi configurate numai pentru dispozitivele iOS adăugate în profilul copilului tău și se aplică exclusiv apelurilor primite.

Pentru a bloca un anumit contact pe un dispozitiv pe care este instalată aplicația Bitdefender Parental Control:

1. Mergeți la: <https://central.bitdefender.com>.



2. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
3. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
4. Selectați profilul copilului în legătură cu care doriți să stabiliți restricțiile. Asigură-te că profilul selectat utilizează dispozitivul Android asociat.
5. Selectați fila **Contacte telefon**.
Se afișează o listă cu carduri. Card-urile reprezintă contactele din telefonul copilului dumneavoastră.
6. Selectați cardul cu numărul de telefon pe care doriți să îl blocați.

Pictograma  indică faptul că numărul de telefon selectat nu poate lua legătura cu copilul tău.

3.4.5. Cum pot seta o locație ca fiind sigură sau restricționată pentru copilul meu?

Funcția Control parental Bitdefender îți permite să setezi o locație ca fiind sigură sau restricționată pentru copilul tău.

Pentru a seta o locație:

1. Mergeți la: <https://central.bitdefender.com>.
2. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
3. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
4. Selectați profilul copilului dumneavoastră din fereastra **Copiii mei**.
5. Selectați fila **Locație copil**.
6. Efectuați clic pe **Dispozitive** în cadrul disponibil în fereastra **Locație copil**.
7. Faceți clic pe **SELECTARE DISPOZITIVE** și apoi selectați dispozitivul pe care doriți să îl configurați.
8. În fereastra **Zone**, faceți clic pe butonul **ADĂUGARE ZONĂ**.
9. Selectați tipul locației **SIGURĂ** sau **RESTRICȚIONATĂ**.
10. Introduceți un nume valid pentru zona pe care copilul dumneavoastră o poate sau nu accesa.



11. Stabiliți raza care urmează a fi aplicată pentru monitorizare din bara glisantă **Rază**.

12. Faceți clic pe **ADĂUGARE ZONĂ** pentru a salva setările.

De fiecare dată când doriți să setați o locație restricționată ca locație sigură sau o locație sigură ca restricționată, faceți clic pe aceasta și apoi selectați butonul **EDITARE ZONĂ**. În funcție de modificarea pe care doriți să o efectuați, selectați opțiunea **SIGUR(Ă)** sau **RESTRICȚIONAT(Ă)** și apoi faceți clic pe **ACTUALIZARE ZONĂ**.

3.4.6. Cum blochez accesul copilului meu la dispozitivele alocate în timpul activităților zilnice?

Control parental Bitdefender îți permite să limitezi accesul copilului tău la dispozitivele asociate în timpul activităților zilnice, cum ar fi în timpul programului de școală, în intervalul de timp alocat temelor sau somnului.

Pentru a configura restricțiile de timp:

1. Mergeți la: <https://central.bitdefender.com>.
2. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
3. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
4. Din fereastra **Copiii mei**, selectează profilul copilului pentru care dorești să setezi restricții.
5. Selectează fila **Timpul petrecut în fața ecranului**.
6. Selectează **Verificare restricții de timp**.
7. În secțiunea **Setare restricții de timp**, selectează **Adăugare restricție nouă**.
8. Introdu o denumire pentru restricția pe care dorești să o configurezi (de exemplu, ora de culcare, teme, lecții de tenis etc.).
9. Setează intervalul orar și zilele pentru care se vor aplica restricțiile, apoi selectează **ADĂUGARE** pentru a salva setările.

3.4.7. Cum blochez accesul copilului meu la dispozitivele asociate ziua sau noaptea?

Aplicația Control parental Bitdefender îți permite să limitezi accesul copilului tău la dispozitivele asociate în anumite intervale orare pe parcursul unei zile.




Pentru a seta limita zilnică de utilizare:

1. Mergeți la: <https://central.bitdefender.com>.
2. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
3. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
4. Din fereastra **Copiii mei**, selectează profilul copilului pentru care dorești să setezi restricții.
5. Selectează fila **Timpul petrecut în fața ecranului**.
6. Selectează **Verificare restricții de timp**.
7. În secțiunea **Setare limită de utilizare zilnică**, selectează **Adăugare limită zilnică nouă**.
8. Setează intervalul orar și zilele pentru care se vor aplica restricțiile, apoi selectează **SALVARE** pentru a salva setările.

3.4.8. Ștergerea profilului de copil

Dacă dorești să ștergi un profil de copil existent:

1. Mergeți la: <https://central.bitdefender.com>.
2. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
3. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
4. Faceți clic pe pictograma  de pe profilul de copil pe care doriți să îl ștergeți și apoi selectați **Ștergere**.
5. Confirmă alegerea.

3.4.9. Cum pot face upgrade la Bitdefender Parental Control Premium?

Cu abonamentul Bitdefender Parental Control Premium, poți fi informat în timp real în legătură cu amenințările la care sunt expuși copiii tăi în timp ce aceștia utilizează rețelele de socializare, precum WhatsApp, Facebook Messenger sau Instagram. Mai exact, de fiecare dată când în conversațiile online sunt detectate următoarele comportamente:

- Fotografii ce conțin nuditate.



- Mesaje text răutăcioase.
- Divulgarea datelor cu caracter personal (adresa de domiciliu, parole, numerele cardurilor de credit, codurile numerice personale etc.).
- Solicitări de întâlnire primite din partea unor persoane străine.

Abonamentul Bitdefender Parental Control Premium acoperă un număr nelimitat de dispozitive Windows, macOS, Android și iOS atribuite copiilor.

Pentru a face upgrade la Bitdefender Parental Control Premium:

1. Accesați **Bitdefender Central**.
2. Selectează secțiunea **Control parental**.
3. Selectează **AFLĂ MAI MULTE** din bannerul afișat deasupra profilurilor copiilor tăi.
4. Selectează **CUMPĂRĂ VERSIUNEA PREMIUM**.

Ești redirecționat către site-ul web Bitdefender unde poți continua procesul de cumpărare.



Notă

Poți face upgrade la Bitdefender Parental Control Premium numai dacă te afli într-una din următoarele țări: SUA, Canada, Regatul Unit, Irlanda, Africa de Sud, Australia sau Noua Zeelandă. Această listă de țări va fi actualizată de îndată ce produsul va fi disponibil pentru utilizare în noi regiuni.

3.5. Protecție confidențialitate

3.5.1. Cum mă asigur că tranzacțiile mele online sunt securizate?

Pentru a asigura confidențialitatea operațiunilor pe care le efectuați online, puteți folosi browserul furnizat de Bitdefender, care vă protejează tranzacțiile și aplicațiile de home banking.


Bitdefender Safepay™ este un browser securizat proiectat pentru a vă proteja informațiile referitoare la cardul de credit, numărul de cont sau orice alte date sensibile pe care le introduceți când accesați alte locații online.

Pentru a menține securitatea și confidențialitatea activității tale online:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.



2. În secțiunea **SAFEPLAY**, selectează **Deschide Safeplay**.

3. Faceți clic pe butonul  pentru a accesa **Tastatura virtuală**.

Folosiți **Tastatura virtuală** atunci când introduceți informații confidențiale, cum ar fi parolele.

3.5.2. Ce pot face dacă mi-a fost furat dispozitivul?


Furtul de dispozitive mobile - indiferent dacă este vorba despre un smartphone, o tabletă sau un laptop - este una dintre principalele probleme care afectează în prezent indivizii și organizațiile din întreaga lume.


Bitdefender Anti-Theft vă permite nu numai să localizați și să blocați dispozitivul furat, dar și să ștergeți toate datele pentru a vă asigura că acestea nu vor fi folosite de autorii furtului.

Pentru a accesa caracteristicile Anti-Theft din contul tău:

1. Accesați **Bitdefender Central**.
2. Selectați secțiunea **Dispozitivele mele**.
3. Efectuează clic pe fila dispozitivului dorit și selectează **Antifurt**.
4. Selectați funcția pe care doriți să o folosiți:

● **LOCALIZARE** - afișează locația dispozitivului dumneavoastră pe Google Maps.

●  **Alertă** - trimiterea unei alerte pe dispozitiv.

●  **Blocare** - blocați calculatorul și setați un cod PIN de deblocare. O altă variantă este să activezi opțiunea corespunzătoare pentru a permite Bitdefender să fotografieze persoanele care încearcă să-ți acceseze contul.

●  **Ștergere** - șterge toate datele de pe calculatorul dumneavoastră.



Important

După ce ștergeți un dispozitiv, este oprită funcționarea tuturor funcțiilor Anti-Theft.

● **Afișează IP** - afișează ultima adresă IP a dispozitivului selectat.



3.5.3. Cum utilizez seifurile pentru fișiere?

Funcția Criptare fișiere a Bitdefender vă permite să creați pe calculatorul dumneavoastră partiții logice criptate și protejate prin parolă (seifuri), unde puteți stoca în deplină siguranță documentele dumneavoastră confidentiale. La nivel fizic, seiful este de fapt un fișier criptat de pe hard-discul dumneavoastră, având extensia .bvd.

Atunci când creați un seif, două aspecte sunt importante: dimensiunea și parola. Spațiul implicit de 100 MB ar trebui să fie suficient pentru documentele dumneavoastră personale, fișierele Excel și alte date similare. Cu toate acestea, pentru fișiere video sau alte fișiere de mari dimensiuni, este posibil să aveți nevoie de mai mult spațiu.

Pentru a vă stoca în siguranță fișierele sau directoarele confidentiale în seifurile pentru fișiere Bitdefender:

● Creați un seif pentru fișiere și stabiliți o parolă complexă pentru acesta.

Pentru a crea un seif, clic dreapta pe o zonă liberă de pe desktop sau într-un director de pe computer, selectează **Bitdefender > Bitdefender CRIPTARE FIȘIERE** și selectează **Creează seif pentru fișiere**.

Se afișează o nouă fereastră. Procedați astfel:

1. Faceți clic pe **Caută**, selectați locația seifului și salvați fișierul seif cu numele dorit.
2. Selectați din meniu o literă pentru partiție. Atunci când deschideți seiful, puteți vedea în **My Computer** o partiție virtuală denumită cu litera selectată.
3. Introduceți parola seifului în câmpul **Parolă și Confirmare**.
4. Dacă dorești să modifice dimensiunea implicită (100 MB) a seifului, folosește săgețile sus/jos din caseta **Mărime seif (MB)**.
5. Faceți clic pe **Creează**.



Notă

Atunci când deschideți seiful, puteți vedea o partiție virtuală în **My Computer**. Partiția este denumită cu litera atribuită seifului.

● Adăugați în seif fișierele sau directoarele pe care doriți să le protejați.

Pentru a adăuga un fișier într-un seif, trebuie mai întâi să deschideți seiful.



1. Localizați fișierul .bvd corespunzător seifului.
2. Faceți clic-dreapta pe seiful pentru fișiere, duceți cursorul deasupra opțiunii Seif Bitdefender pentru fișiere și selectați **Deschide**.
3. În fereastra afișată introdu parola, selectează litera care urmează să fie atribuită seifului și fă clic pe **OK**.

Acum puteți efectua operațiuni pe unitatea corespunzătoare seifului pentru fișiere cu ajutorul Windows Explorer, așa cum ați face și în cazul unei unități obișnuite. Pentru a adăuga un fișier într-un seif deschis, puteți de asemenea să faceți clic-dreapta pe fișier, să duceți cursorul deasupra opțiunii Seif Bitdefender pentru fișiere și să selectați **Adaugă în Seiful pentru fișiere**.

● **Țineți seiful închis în permanență.**

Deschideți seifurile numai atunci când trebuie să le accesați sau să le administrați conținutul. Pentru a închide un seif, faceți clic-dreapta pe partiția virtuală corespunzătoare din **My Computer**, duceți cursorul deasupra opțiunii **Seif Bitdefender pentru fișiere** și selectați **Închide**.

● **Fișierul .bvd corespunzător seifului nu trebuie șters.**

Ștergerea fișierului duce de asemenea la ștergerea conținutului seifului.

Pentru mai multe informații privind utilizarea seifurilor pentru fișiere, consultați „*File Encryption*” (p. 139).

3.5.4. Cum șterg definitiv un fișier cu ajutorul Bitdefender?

Dacă doriți să ștergeți definitiv un fișier din sistemul dumneavoastră, este necesar să ștergeți fizic datele de pe hard disk.

Funcția Ștergere definitivă fișiere a Bitdefender vă permite să ștergeți definitiv și rapid fișiere și directoare din computerul dumneavoastră cu ajutorul meniului contextual Windows urmând pașii de mai jos:

1. Faceți clic dreapta pe fișierul sau directorul pe care doriți să-l ștergeți definitiv, alegeți Bitdefender și selectați **Ștergere definitivă fișiere**.
2. Efectuează clic pe **ȘTERGE DEFINITIV** și apoi confirmă că dorești să continui procesul.

Așteptați ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.

3. Sunt afișate rezultatele. Efectuați clic pe **Finalizare** pentru a părăsi asistentul.




3.5.5. Cum îmi protejerez de hackeri camera web?

Puteti configura produsul Bitdefender pentru a permite sau bloca accesul aplicațiilor instalate la camera web urmând acești pași:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În pagina **PROTECȚIE VIDEO ȘI AUDIO**, selectează **Acces cameră web**.

Aici este afișată lista cu aplicațiile care au solicitat acces la camera web.

3. Identificați aplicația căreia doriți să-i permiteți sau să-i blocați accesul și apoi efectuați clic pe butonul corespunzător.

Pentru a vizualiza ce opțiuni au ales ceilalți utilizatori Bitdefender pentru aplicația selectată, efectuați clic pe pictograma . Vei primi o notificare de fiecare dată când una dintre aplicațiile incluse în listă este blocată de către utilizatorii Bitdefender.

Pentru a adăuga manual aplicații în această listă, efectuați clic pe linkul **Adaugă în listă o nouă aplicație**.

3.5.6. Cum pot restabili manual fișierele criptate atunci când procesul de restabilire eșuează?

În cazul în care fișierele criptate nu pot fi restabilite automat, le poți restabili manual urmând acești pași:

1. Efectuează clic pe **Notificări** din meniul de navigare al **interfeței Bitdefender**.
2. În fila **Toate**, selectează notificarea privind cel mai recent comportament ransomware detectat, apoi apasă pe **Fișiere criptate**.
3. Este afișată lista fișierelor criptate.

Pentru a continua, selectează **RECUPERARE FIȘIERE**.

4. În cazul în care procesul de restabilire eșuează, fie complet, fie parțial, trebuie să selectezi locația în care să fie salvate fișierele decriptate. Apasă pe **LOCAȚIE RESTAURARE** și apoi selectează o locație de pe PC-ul tău.
5. Va apărea o fereastră de confirmare.

Selectează **FINALIZARE** pentru a încheia procesul de restabilire.

Fișierele cu următoarele extensii pot fi restabilite în cazul în care sunt criptate:



.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb; .doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html; .ico; .jar; .java; .jpeg; .jpg; .js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp; .odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

3.6. Instrumente de optimizare

3.6.1. Cum pot îmbunătăți performanța sistemului meu?

Performanța sistemului nu depinde numai de configurația hardware, cum ar fi încărcarea procesorului, utilizarea memoriei și spațiul de pe hard disk. Are de asemenea legătură directă cu configurația software și cu modul de administrare a datelor.

Acestea sunt acțiunile principale pe care le puteți efectua cu Bitdefender pentru a îmbunătăți viteza și performanța sistemului dumneavoastră:

- *„Optimizați performanțele sistemului printr-un singur clic”* (p. 69)
- *„Scanați periodic sistemul”* (p. 70)

Optimizați performanțele sistemului printr-un singur clic

Opțiunea Oneclick Optimizer economisește timp prețios când doriți o modalitate de a vă îmbunătăți performanțele sistemului prin scanarea rapidă, detectare și eliminarea fișierelor inutile.

Pentru a lansa procesul Oneclick Optimizer:

1. Efectuează clic pe **Instrumente** din meniul de navigare al interfeței **Bitdefender**.
2. Efectuează clic pe **OPTIMIZEAZĂ-MI DISPOZITIVUL**.
3. Lasă Bitdefender să caute fișiere care pot fi șterse, apoi faceți clic pe butonul **Optimizare** pentru a încheia procesul.

Pentru informații suplimentare referitoare la modul în care puteți îmbunătăți viteza calculatorului dvs. printr-un singur clic, consultați *„Optimizați viteza sistemului cu un singur clic”* (p. 182).



Scanați periodic sistemul

Amenințările pot afecta, de asemenea, viteza sistemului dumneavoastră, precum și comportamentul general al acestuia.

Scanați sistemul periodic, cel puțin o dată pe săptămână.

Este recomandat să utilizați procesul de scanare a sistemului deoarece acesta scanează toate tipurile de amenințări care pun în pericol securitatea sistemului tău, scanând de asemenea și în interiorul arhivelor.

Pentru a porni Scanarea sistemului:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTIVIRUS**, efectuează clic pe **Scanare sistem**.
3. Urmați pașii asistentului.

3.6.2. Cum pot îmbunătăți timpul de pornire al sistemului meu?

Aplicațiile care nu sunt necesare și care vă încetinesc în mod supărător timpul de pornire la deschiderea calculatorului pot fi dezactivate sau amânate folosind opțiunea Startup Optimizer, care vă ajută să economisiți timp prețios.

Pentru a utiliza funcția Startup Optimizer:

1. Efectuează clic pe **Instrumente** din meniul de navigare al interfeței **Bitdefender**.
2. Efectuează clic pe **OPTIMIZEAZĂ BOOT DISPOZITIV**.
3. Selectați aplicațiile pe care doriți să le amânați la pornirea sistemului.

Pentru informații suplimentare privind modalitatea de optimizare a timpului de pornire al calculatorului dvs., consultați „*Optimizarea timpului de pornire al calculatorului dvs.*” (p. 183).

3.7. Informații utile

3.7.1. Cum îmi testez soluția de securitate?

Pentru a vă asigura că produsul Bitdefender funcționează corespunzător, vă recomandăm să utilizați testul Eicar.



Testul Eicar vă permite să vă verificați soluția de securitate folosind un fișier de siguranță conceput special pentru acest scop.

Pentru a testa soluția de securitate:

1. Descărcați testul din pagina oficială a organizației EICAR <http://www.eicar.org/>.
2. Faceți clic pe fila **Fișier de testare anti-malware**.
3. Faceți clic pe **Descărcare** în meniul din stânga.
4. Din zona de Download **folosind protocolul standard http** faceți clic pe fișierul de testare **eicar.com**.
5. Veți primi notificarea că pagina pe care încercați să o accesați conține fișierul de testare EICAR (și nu o amenințare).

Dacă faceți clic pe **Înțeleg riscurile, vreau să continui oricum**, descărcarea pachetului de testare va începe automat și o fereastră pop-up Bitdefender vă va informa că a fost detectată o amenințare.

Faceți clic pe **Mai multe detalii** pentru a afla mai multe informații despre această acțiune.

Dacă nu primiți nicio alertă Bitdefender, vă recomandăm să contactați Bitdefender pentru asistență, așa cum este indicat la secțiunea „*Solicitarea ajutorului*” (p. 333).

3.7.2. Cum dezinstalez Bitdefender?

Dacă dorești să dezinstalezi Bitdefender Total Security:

● În Windows 7:

1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
2. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
3. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
4. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

● În Windows 8 și Windows 8.1:

1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.



2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
5. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

● În **Windows 10**:

1. Faceți clic pe **Start**, apoi pe **Setări**.
2. Efectuează clic pe pictograma **Sistem** din secțiunea **Setări**, apoi selectează **Aplicații**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
6. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.



Notă

Această procedură de reinstalare va șterge definitiv setările personalizate.

3.7.3. Cum dezinstalez Bitdefender VPN?

Procedura de dezinstalare a aplicației Bitdefender VPN este similară celei utilizate pentru ștergerea altor programe din calculatorul tău:

● În **Windows 7**:

1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
2. Găsește **Bitdefender VPN** și selectează **Dezinstalare**.
Așteptați până când procesul de dezinstalare este finalizat.

● În **Windows 8 și Windows 8.1**:

1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Găsește **Bitdefender VPN** și selectează **Dezinstalare**.
Așteptați până când procesul de dezinstalare este finalizat.




● În Windows 10:

1. Faceți clic pe **Start**, apoi pe Setări.
2. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.
3. Găsește **Bitdefender VPN** și selectează **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
Așteptați până când procesul de dezinstalare este finalizat.


3.7.4. Cum dezinstalez extensia Bitdefender Anti-tracker?

În funcție de browserul web pe care îl utilizezi, urmează acești pași pentru a dezinstala extensia Bitdefender Anti-tracker:


● Internet Explorer

1. Accesează  din dreptul barei de căutare și apoi Administrare add-on-uri.
Se va afișa o listă cu extensiile instalate.
2. Selectează Bitdefender Anti-tracker.
3. Selectează **Dezactivare** din dreapta jos.

● Google Chrome

1. Accesează  din dreptul barei de căutare.
2. Selectează **Mai multe instrumente** și apoi **Extensii**.
Se va afișa o listă cu extensiile instalate.
3. Selectează **Dezinstalează** din caseta Bitdefender Anti-tracker.
4. Selectează opțiunea **Dezinstalează** din fereastra care se deschide.

● Mozilla Firefox

1. Accesează  din dreptul barei de căutare.
2. Selectează **Add-on-uri** și apoi **Extensii**.
Se va afișa o listă cu extensiile instalate.
3. Selectează **Dezinstalează** din caseta Bitdefender Anti-tracker.




3.7.5. Cum închid automat calculatorul după finalizarea operațiunii de scanare?

Bitdefender oferă mai multe opțiuni de scanare pe care le puteți folosi pentru a vă asigura că sistemul dumneavoastră nu este infectat cu amenințări. Scanarea întregului calculator poate dura destul de mult timp, în funcție de configurația hardware și software a sistemului dumneavoastră.

Din acest motiv, Bitdefender vă permite să vă configurați produsul să închidă sistemul imediat după finalizarea scanării.


Spre exemplu: v-ați terminat lucrul la calculator și vreți să mergeți la culcare. Doriți să efectuați o verificare integrală a sistemului dumneavoastră în vederea detectării amenințărilor cu ajutorul Bitdefender.

Pentru a opri computerul în momentul finalizării unei sarcini de Scanare rapidă sau Scanare de sistem:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTIVIRUS**, efectuează clic pe **Administrare scanări**.
3. Accesează  din dreptul opțiunilor de Scanare rapidă sau Scanare de sistem.
4. Din lista **Acțiuni post-scanare**, selectează **Închide dispozitivul** și apoi **ÎNAINTE**.
5. Activează opțiunea **Programează sarcina de scanare** și apoi alege când dorești să înceapă execuția.

Dacă selectezi Zilnic, Lunar sau Săptămânal, trage de cursor pentru a seta perioada de timp dorită pentru începerea scanării.

Pentru a opri computerul la finalizarea unei sarcini personalizate:

1. Selectează opțiunea  din dreptul sarcinii personalizate pe care ai creat-o.
2. În fereastra **Sarcină de scanare**, selectează **ÎNAINTE**.
3. Din lista **Acțiuni post-scanare**, selectează **Închide dispozitivul**.
4. Selectează **ÎNAINTE** și apoi **SALVARE**.

Dacă nu este detectată nicio amenințare, calculatorul se va închide.



Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultați capitolul „*Asistentul de scanare antivirus*” (p. 92).

3.7.6. Cum pot configura Bitdefender să utilizeze o conexiune la internet de tip proxy?

Dacă computerul dumneavoastră se conectează la internet prin intermediul unui server proxy, trebuie să configurați Bitdefender cu setările proxy. În mod normal, Bitdefender detectează și importă în mod automat setările proxy ale sistemului dumneavoastră.



Important

Conexiune de internet de acasă nu sunt folosite, în mod normal, ca server proxy. Ca regulă de bază, verificați și configurați setările conexiunii proxy ale programului Bitdefender atunci când nu funcționează actualizările. Dacă Bitdefender poate folosi actualizări, înseamnă că este configurat corespunzător pentru a se conecta la internet.

Pentru a administra setările proxy:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Avansat**.
3. Activează opțiunea **Server proxy**.
4. Dă clic pe **Modificare proxy**.
5. Există două opțiuni de configurare a setărilor proxy:

- **Importă setări proxy din browserul implicit** - setări proxy ale utilizatorului curent, extrase din browserul implicit. Dacă serverul proxy necesită un nume de utilizator și o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.



Notă

Bitdefender poate importa setări proxy de la browserele cele mai des folosite, inclusiv cele mai noi versiuni de Microsoft Edge, Internet Explorer, Mozilla Firefox și Google Chrome.

- **Setări proxy personalizate** - setări proxy pe care le puteți configura cum doriți. Următoarele setări trebuie specificate:
 - **Adresă** - introduceți adresa IP a serverului proxy.



- **Port** - introduceți portul folosit Bitdefender pentru a se conecta la serverul proxy.
- **Utilizator** - introduceți un nume de utilizator recunoscut de proxy.
- **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.

6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Bitdefender va folosi setările proxy disponibile până când va reuși să se conecteze la internet.

3.7.7. Utilizez o versiune Windows pe 32 biți sau pe 64 biți?

Pentru a afla dacă ai un sistem de operare pe 32 sau 64 de biți:

● În Windows 7:

1. Faceți clic pe **Start**.
2. Localizați **Computer** din meniul **Start**.
3. Faceți clic-dreapta pe **Computer** și selectați **Properties**.
4. Sub **System** veți găsi informații referitoare la sistemul dumneavoastră.

● Pentru Windows 8:

1. Din ecranul de Start al Windows, localizați **Computer** (de exemplu, puteți începe să tastați „Computer” direct în ecranul de Start) și faceți clic dreapta pe pictograma acestuia.

În **Windows 8.1**, localizează **Acest PC**.

2. Selectează **Proprietăți** din meniul din partea de jos.
3. Mergeți la secțiunea Sistem pentru a vedea tipul sistemului.

● În Windows 10:

1. Introduceți "System" în caseta de căutare din bara de sarcini și faceți clic pe pictogramă.
2. Căutați în zona System pentru a afla informații referitoare la tipul de sistem.



3.7.8. Cum pot afișa elementele ascunse din Windows?

Acești pași sunt utili în acele cazuri în care aveți de-a face cu o situație în care este implicată o amenințare și trebuie să găsiți și să eliminați fișierele infectate, care pot fi ascunse.

Urmați acești pași pentru a afișa obiectele ascunse din Windows:

1. Faceți clic pe **Start** și mergeți la **Panoul de control**.

În **Windows 8** și **Windows 8.1**: Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.

2. Selectează **Opțiunile dosarului**:
3. Mergeți la fila **View**.
4. Selectați **Show hidden files and folders**.
5. Debifați **Hide extensions for known file types**.
6. Debifați **Hide protected operating system files**.
7. Faceți clic pe **Aplică** și apoi pe **OK**.

În **Windows 10**:

1. Introduceți "Show hidden files and folders" în caseta de căutare din bara de sarcini și faceți clic pe pictogramă.
2. Selectați **Show hidden files, folders, and drives**.
3. Debifați **Hide extensions for known file types**.
4. Debifați **Hide protected operating system files**.
5. Faceți clic pe **Aplică** și apoi pe **OK**.

3.7.9. Cum elimin celelalte soluții de securitate?

Principalul motiv pentru utilizarea unei soluții de securitate este de a asigura protecția și siguranța datelor dumneavoastră. Ce se întâmplă însă când aveți mai multe produse de securitate instalate în același sistem?

Atunci când utilizați mai multe soluții de securitate pe același calculator, sistemul devine instabil. Programul de instalare a Bitdefender Total Security detectează în mod automat alte programe de securitate și vă oferă opțiunea de a le dezinstala.



Dacă nu ați deinstalat celelalte soluții de securitate în timpul instalării inițiale:

● În Windows 7:

1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
2. Așteptați câteva momente până când este afișată lista programelor instalate.
3. Găsiți numele programului pe care doriți să-l deinstalați și selectați **Dezinstalare**.
4. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

● În Windows 8 și Windows 8.1:

1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Așteptați câteva momente până când este afișată lista programelor instalate.
4. Găsiți numele programului pe care doriți să-l deinstalați și selectați **Dezinstalare**.
5. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

● În Windows 10:

1. Faceți clic pe **Start**, apoi pe Setări.
2. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează **Aplicații**.
3. Găsiți numele programului pe care doriți să-l deinstalați și selectați **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

Dacă nu reușiți să eliminați cealaltă soluție de securitate, descărcați instrumentul de dezinstalare de pe site-ul furnizorului sau contactați-l direct pentru a vă oferi instrucțiuni cu privire la dezinstalare.



3.7.10. Cum pot să repornesc sistemul în Safe Mode?

Safe Mode este un mod de funcționare de diagnosticare, utilizat în principal pentru depanarea problemelor care afectează funcționarea normală a sistemului Windows. Printre astfel de probleme se numără driverele incompatibile și amenințările ce împiedică pornirea normală a sistemului Windows. În Safe Mode funcționează numai câteva aplicații, iar Windows încarcă doar driverele de bază și un minim de componente ale sistemului de operare. Acesta este motivul pentru care majoritatea amenințărilor sunt inactice atunci când Windows se află în Safe Mode și pot fi eliminate cu ușurință.

Pentru a porni Windows în Safe Mode:

● În **Windows 7**:

1. Reporniți calculatorul.
2. Apăsați tasta **F8** de mai multe ori înainte ca Windows să pornească pentru a avea acces la meniul de pornire.
3. Selectați **Safe Mode** din meniul de pornire sau **Safe mode with Networking** dacă doriți să aveți acces la internet.
4. Apăsați **Enter** și așteptați până când Windows se încarcă în Safe Mode.
5. Acest proces se finalizează cu un mesaj de confirmare. Faceți clic pe **OK** pentru a confirma.
6. Pentru a porni Windows în mod normal, reporniți pur și simplu sistemul.

● În **Windows 8, Windows 8.1 și Windows 10**:

1. Lansează aplicația de **Configurare sistem (System Configuration)** din Windows apăsând simultan tastele **Windows + R**.
2. Tastează **msconfig** în caseta de dialog **Deschidere (Open)** și apoi fă clic pe **OK**.
3. Selectați secțiunea **Boot**.
4. În secțiunea **Opțiuni pornire**, bifează caseta **Pornire sigură**.
5. Faceți clic pe **Rețea** și apoi pe **OK**.
6. Fă clic pe **OK** în fereastra **Configurare sistem (System Configuration)** care vă informează că sistemul trebuie repornit pentru ca modificările să poată fi implementate.



Sistemul tău este în curs de repornire în Safe Mode with Networking.
Pentru a reporni sistemul în modul normal, restabilește setările inițiale lansând din nou funcția **Operare sistem** și debifând caseta **Pornire sigură**. Fă clic pe **OK** și apoi pe **Repornire**. Așteaptă aplicarea noilor setări.



4. ADMINISTRAREA SECURITĂȚII DUMNEAVOASTRĂ

4.1. Protecție antivirus

Bitdefender vă protejează calculatorul împotriva oricăror amenințări (malware, troieni, aplicații spyware, rootkituri și altele). Protecția oferită de Bitdefender se împarte în două categorii:

- **Scanarea la accesare** - previne pătrunderea noilor amenințări în sistemul dumneavoastră. Bitdefender va scana, de exemplu, un document Word atunci când îl deschideți și un mesaj e-mail atunci când îl primiți.

Procesul de scanare la accesare asigură protecție în timp real împotriva amenințărilor, fiind o componentă esențială a oricărui program de securitate pentru calculatoare.



Important

Pentru a preveni infectarea computerului, păstrați activată funcția de **scanare la accesare**.

- **Scanarea la cerere** - permite detectarea și eliminarea amenințărilor care există deja în sistemul dumneavoastră. Acesta este modul clasic de scanare, inițiată de utilizator – dumneavoastră alegeți partițiile, directoarele sau fișierele pe care trebuie să le scaneze Bitdefender, iar Bitdefender le scanează – la cerere.

Bitdefender scanează în mod automat orice fișier media amovibil care este conectat la computer pentru a vă asigura că este sigur să îl accesați. Pentru mai multe informații, consultați capitolul *„Scanarea automată a suporturilor media amovibile”* (p. 96).

Utilizatorii avansați pot configura excepțiile de scanare în cazul în care nu doresc ca anumite fișiere sau tipuri de fișiere să fie scanate. Pentru mai multe informații, consultați capitolul *„Configurarea excepțiilor de scanare”* (p. 98).

Atunci când detectează o amenințare, Bitdefender 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. Pentru mai multe informații, consultați capitolul *„Gestionarea fișierelor aflate în carantină”* (p. 101).



În cazul în care calculatorul dumneavoastră a fost infectat cu amenințări, consultați „*Eliminarea amenințărilor din sistemul dumneavoastră*” (p. 214). Pentru a vă ajuta să vă curățați computerul de amenințările care nu pot fi eliminate din sistemul de operare Windows, Bitdefender vă pune la dispoziție „*Bitdefender Modul de recuperare (Mediul de recuperare în Windows 10)*” (p. 215). Acesta este un mediu sigur, creat în special pentru eliminarea amenințărilor, care vă permite să porniți computerul în mod independent de Windows. Atunci când computerul rulează în Modul de recuperare (mediul de recuperare în Windows 10), amenințările Windows sunt inactive și, în consecință, pot fi șterse cu ușurință.

4.1.1. Scanare la accesare (protecție în timp real)

Bitdefender oferă protecție în timp real contra unei game extinse de amenințări, scanând toate fișierele și mesajele e-mail accesate.

Activarea sau dezactivarea protecției în timp real

Pentru a activa sau dezactiva protecția în timp real împotriva amenințărilor:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
3. În fereastra **Shield**, activează sau dezactivează opțiunea **Bitdefender Shield**.
4. Dacă doriți să dezactivați protecția în timp real, se afișează o fereastră de avertizare. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real. Puteți dezactiva protecția în timp real pentru 5, 15 sau 30 de minute, pentru o oră, permanent sau doar până la repornirea sistemului. Protecția în timp real se va activa automat la expirarea intervalului de timp selectat.



Avertisment

Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați protecția în timp real pentru cât mai puțin timp posibil. Dacă protecția în timp real este dezactivată, nu veți mai fi protejat împotriva amenințărilor.



Configurarea setărilor avansate de protecție în timp real

Utilizatorii avansați pot beneficia în urma ofertelor Bitdefender în ceea ce privește setările de scanare. Puteți configura setările protecției în timp real în detaliu prin crearea unui nivel de protecție personalizat.

Pentru a configura setările avansate de protecție în timp real:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
3. În fereastra **Shield**, dă clic pe meniul expandabil **Afișează setările avansate**.
Se afișează o fereastră compusă din mai multe panouri.
4. Defilează în jos pentru a configura setările de scanare după cum este necesar.

Informații cu privire la opțiunile de scanare

Aceste informații vă pot fi de folos:

- **Scanează doar aplicații.** Poți configura Bitdefender astfel încât să scaneze numai aplicațiile accesate.
- **Scanare pentru identificarea aplicațiilor potențial nedorite .** Selectează această opțiune pentru a efectua o scanare în vederea identificării aplicațiilor nedorite. O aplicație potențial nedorită (PUA - potentially unwanted application) sau un program potențial nedorit (PUP - potentially unwanted program) reprezintă un software care, de obicei, vine la pachet cu un software freeware și care afișează ferestre pop-up sau instalează un toolbar în browserul implicit. Unele dintre acestea modifică pagina de pornire sau motorul de căutare, altele execută mai multe procese în fundal încetinind PC-ul sau afișează numeroase reclame. Aceste programe pot fi instalate fără consimțământul tău (numite și adware), sau sunt incluse în mod implicit în kit-ul de instalare rapidă (ad-supported).
- **Scanează pentru detectarea scripturilor.** Funcția Scanează pentru detectarea scripturilor permite Bitdefender să scaneze scripturile powershell și documentele Office care ar putea conține malware bazat pe scripturi.
- **Scanează directoare comune din rețea.** Pentru a accesa în siguranță de la computerul tău o rețea de la distanță, îți recomandăm să păstrezi activată opțiunea Scanează directoare comune din rețea.



- **Deschide arhive.** Scanarea în interiorul arhivelor este un proces lent și care necesită multe resurse, nefiind recomandată, prin urmare, pentru protecția în timp real. Arhivele ce conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului dumneavoastră. Amenințările vă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția în timp real.

Dacă decizi să utilizezi această opțiune, activeaz-o și apoi trage cursorul pentru a exclude de la scanare arhivele care depășesc o anumită valoare în MB (megaocteți).

- **Scanează e-mailuri.** Pentru a împiedica descărcarea amenințărilor pe calculatorul tău, Bitdefender scanează automat e-mail-urile primite și trimise.

Deși nu se recomandă, poți dezactiva scanarea amenințărilor pentru e-mail pentru a extinde performanțele sistemului. Dacă dezactivezi opțiunile de scanare corespunzătoare, e-mail-urile și fișierele primite nu vor fi scanate, permițând astfel fișierelor infectate să fie salvate pe calculatorul tău. Aceasta nu reprezintă o amenințare majoră deoarece protecția în timp real va bloca amenințările atunci când fișierele infectate sunt accesate (deschise, mutate, copiate sau executate).

- **Scanare sectoare de boot.** Puteți seta Bitdefender să scaneze sectoarele de boot ale hard-diskului. Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot. Atunci când o amenințare infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.
- **Scanează numai fișierele noi și modificate.** Prin scanarea exclusivă a fișierelor noi și a acelor modificate, poți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
- **Scanare după keyloggers.** Selectați această opțiune pentru a scana sistemul în vederea identificării aplicațiilor de tip keylogger. Aplicațiile keyloggers înregistrează ceea ce introduceți de pe tastatură și trimit raporte pe internet către o persoană rău intenționată (hacker). Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.
- **Scanare preliminară la încărcarea sistemului.** Selectați opțiunea de **Scanare la pornirea sistemului** pentru a scana sistemul la inițializare, imediat după încărcarea tuturor sistemelor critice. Misiunea acestei caracteristici este



de a îmbunătăți detecția amenințărilor la pornirea sistemului și timpul de încărcare a sistemului dumneavoastră.

Acțiuni aplicate pentru amenințările detectate

Poți configura acțiunile inițiate de protecția în timp real urmând acești pași:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
3. În fereastra **Shield**, dă clic pe meniul expandabil **Afișează setările avansate**.
Se afișează o fereastră compusă din mai multe panouri.
4. Derulează în jos până când vezi opțiunea **Acțiuni în cazul amenințărilor**.
5. Configurați setările de scanare după cum este nevoie.

Următoarele acțiuni pot fi inițiate de protecția în timp real în Bitdefender:

Aplică acțiunile optime

Bitdefender va aplica acțiunile recomandate în funcție de tipul fișierului detectat:

- **Fișiere infectate.** Fișierele detectate ca fiind infectate se potrivesc cu o informație privind amenințările din Baza de Date cu Informații privind Amenințările a Bitdefender. Bitdefender va încerca în mod automat să elimine codul malițios din fișierul infectat și să refacă fișierul original. Această operațiune este denumită dezinfectare.

Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispăre riscul de a fi infectat. Pentru mai multe informații, consultați capitolul „*Gestionarea fișierelor aflate în carantină*” (p. 101).



Important

Pentru anumite tipuri de amenințări, dezinfectia nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

- **Fișiere 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. Acestea vor fi mutate în carantină pentru a preveni o posibilă infectare.

Implicit, fișierele aflate în carantină sunt trimise automat către Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender în materie de amenințări. Dacă se confirmă prezența unei amenințări, este lansată o actualizare a informațiilor privind amenințarea pentru a permite ștergerea amenințării.

● Arhive ce conțin fișiere infectate.

- Arhivele care conțin doar fișiere infectate sunt șterse în mod automat.
- Dacă o arhivă conține atât fișiere infectate cât și fișiere curate, Bitdefender va încerca să șteargă fișierele infectate cu condiția să poată apoi reface arhiva cu fișierele curate. Dacă reconstrucția arhivei nu este posibilă, veți fi notificat de faptul că nu poate fi aplicată nicio acțiune astfel încât să se evite pierderea fișierelor curate.

Mută în carantină

Mută fișierele detectate în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Pentru mai multe informații, consultați capitolul „*Gestionarea fișierelor aflate în carantină*” (p. 101).

Interzice accesul

În caz că un fișier este infectat, accesul la acesta va fi interzis.

Restaurarea setărilor implicite

Setările implicite de protecție în timp real asigură o bună protecție împotriva amenințărilor cu un impact minor asupra performanțelor sistemului.

Pentru a restaura setările implicite pentru protecția în timp real:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
3. În fereastra **Shield**, dă clic pe meniul expandabil **Afișează setările avansate**.
Se afișează o fereastră compusă din mai multe panouri.



4. Defilează în jos până când vezi opțiunea **Resetare setări**. Selectați această opțiune pentru a reseta setările antivirus la valorile implicite.

4.1.2. Scanare la cerere

Principalul obiectiv Bitdefender este protejarea calculatorului dumneavoastră de amenințări. Aceasta se face nepermițând amenințărilor noi să pătrundă în sistem, prin scanarea mesajelor e-mail și a fișierelor descărcate sau copiate pe calculator.

Există însă riscul ca o amenințare să fi fost în sistem înainte de instalarea Bitdefender. Din acest motiv, este indicat să vă scanați calculatorul de amenințări după instalarea Bitdefender. Și este, de asemenea, recomandat să vă scanați sistemul periodic.

Scanarea la cerere se bazează pe sarcinile de scanare. Sarcinile de scanare sunt cele care specifică opțiunile de scanare și obiectele care să fie scanate. Puteți scana computerul oricând doriți prin rularea sarcinilor implicite sau a propriilor sarcini de scanare (sarcini definite de utilizator). Dacă doriți să scanați anumite locații de pe computerul dumneavoastră sau să configurați opțiunile de scanare, puteți configura și rula o scanare personalizată.

Scanarea unui fișier sau a unui director pentru detectarea amenințărilor

Trebuie să scanați fișierele și directoarele ori de câte ori considerați că acestea pot fi infectate. Faceți clic dreapta pe fișierul sau directorul pe care doriți să îl scanați, indicați **Bitdefender** și selectați **Scanează cu Bitdefender**. Va apărea **Asistentul de scanare** care vă va ghida de-a lungul procesului de scanare. După finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.

Rularea unei scanări rapide

Scanarea rapidă utilizează o tehnologie de scanare "in-the-cloud" (online) pentru a detecta amenințările ce rulează pe sistemul dumneavoastră. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o mică parte din resursele de sistem necesare pentru o scanare antivirus obișnuită.

Pentru a rula o scanare rapidă:



1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, efectuați clic pe **Scanare rapidă**.
3. Urmați **programul asistent de scanare antivirus** pentru a finaliza scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate. Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Executarea unei scanări a sistemului

Sarcina de Scanare a sistemului scanează întregul calculator pentru identificarea tuturor tipurilor de amenințări care îi pun în pericol securitatea, cum ar fi programele malware, aplicațiile spion, adware, rootkiturile și altele.



Notă

Deoarece opțiunea de **Scanare a sistemului** efectuează o scanare atentă a întregului sistem, aceasta poate dura un timp. În consecință, este recomandat să executați această activitate într-un moment când nu utilizați computerul.

Înainte de a executa o Scanare a sistemului, se recomandă următoarele:

- Asigurați-vă că Bitdefender are actualizate bazele de date cu informațiile privind actualizările. Scanarea calculatorului folosind informații vechi despre amenințări poate împiedica Bitdefender să detecteze noi amenințări descoperite după ultima actualizare efectuată. Pentru mai multe informații, consultați capitolul *„Actualizarea permanentă a Bitdefender”* (p. 39).
- Închideți toate programele deschise.

Dacă doriți să scanați anumite locații de pe computer sau pentru a configura opțiunile de scanare, puteți configura și rula o sarcină de scanare personalizată. Pentru mai multe informații, consultați capitolul *„Configurarea unei scanări personalizate”* (p. 89).

Pentru a rula scanarea completă a sistemului:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTIVIRUS**, efectuează clic pe **Scanare sistem**.
3. La prima rulare a Scanării Sistemului ți se prezintă această caracteristică. Efectuează clic pe **OK, AM ÎNȚELES** pentru a continua.



4. Urmați **programul asistent de scanare antivirus** pentru a finaliza scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate. Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Configurarea unei scanări personalizate

În fereastra **Administrare scanări**, poți configura Bitdefender pentru a executa scanări ori de câte ori consideri că computerul tău are nevoie de o verificare pentru depistarea unor potențiale amenințări. Poți opta pentru programarea unei **Scanări de sistem** sau a unei **Scanări rapide**, sau poți crea o sarcină personalizată la alegerea ta.

Când accesezi această fereastră, sunt disponibile următoarele pictograme:



Sarcina de scanare programată este dezactivată.



Sarcina de scanare programată este activată.



Configurarea detaliată se poate face de aici.



Șterge scanarea selectată. Această opțiune este disponibilă numai pentru noile scanări personalizate.

Pentru a configura în detaliu o nouă scanare personalizată:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTIVIRUS**, efectuează clic pe **Administrare scanări**.
3. Selectează **Creează o nouă sarcină de scanare**.
4. În câmpul **Nume sarcină**, introdu o denumire pentru scanarea respectivă, apoi selectează locațiile care dorești să fie scanate și apasă pe **ÎNAINTE**.
5. Configurează următoarele opțiuni generale:
 - **Scanează doar aplicații**. Poți configura Bitdefender astfel încât să scaneze numai aplicațiile accesate.
 - **Prioritate sarcină de scanare**. Poți alege impactul pe care procesul de scanare ar trebui să îl aibă asupra performanței sistemului.
 - **Automat** - Prioritatea procesului de scanare va depinde de activitatea sistemului. Pentru a te asigura că procesul de scanare nu va afecta activitatea sistemului, Bitdefender va decide dacă procesul de scanare trebuie să se execute cu prioritate mare sau mică.



- **Ridicat** - Prioritatea procesului de scanare va fi ridicată. Selectând această opțiune, vei permite executarea altor programe cu o viteză redusă, micșorând perioada de timp necesară pentru finalizarea scanării.
 - **Redus** - Prioritatea procesului de scanare va fi redusă. Selectând această opțiune, vei permite executarea altor programe cu o viteză mai mare, mărirind perioada de timp necesară pentru finalizarea scanării.
 - **Acțiuni post-scanare.** Alege acțiunea care trebuie întreprinsă de Bitdefender în cazul în care nu sunt identificate niciun fel de amenințări:
 - Afișează fereastra Sumar
 - Închide dispozitivul
 - Închide fereastra Scanare
6. Dacă dorești să configurezi în detaliu opțiunile de scanare, selectează **Afișează opțiuni avansate**. Poți găsi informații referitoare la scanările incluse în listă la sfârșitul acestei secțiuni.
- Selectează **ÎNAINTE**.
7. Activează **Programează sarcina de scanare** și apoi precizează când ar trebui să pornească sarcina personalizată pe care ai creat-o.
- La pornirea sistemului
 - Zilnic
 - Lunar
 - Săptămânal
- Dacă selectezi Zilnic, Lunar sau Săptămânal, trage de cursor pentru a seta perioada de timp dorită pentru începerea scanării.
8. Selectează **SALVEAZĂ** pentru a salva setările și a închide fereastra de configurare.
- Procesul de scanare poate dura ceva timp, în funcție de locațiile ce vor fi scanate. Dacă se vor găsi amenințări în timpul procesului de scanare, îți se va solicita să alegi acțiunile care trebuie întreprinse în cazul fișierelor detectate.



Informații cu privire la opțiunile de scanare

Aceste informații vă pot fi de folos:

- Dacă nu sunteți familiarizat cu anumiți termeni, verificați-i în **glosar**. De asemenea, puteți găsi informații utile pe internet.
- **Scanare pentru identificarea aplicațiilor potențial nedorite** . Selectează această opțiune pentru a efectua o scanare în vederea identificării aplicațiilor nedorite. O aplicație potențial nedorită (PUA - potentially unwanted application) sau un program potențial nedorit (PUP - potentially unwanted program) reprezintă un software care, de obicei, vine la pachet cu un software freeware și care afișează ferestre pop-up sau instalează un toolbar în browserul implicit. Unele dintre acestea modifică pagina de pornire sau motorul de căutare, altele execută mai multe procese în fundal încetinind PC-ul sau afișează numeroase reclame. Aceste programe pot fi instalate fără consimțământul tău (numite și adware), sau sunt incluse în mod implicit în kit-ul de instalare rapidă (ad-supported).
- **Deschide arhive**. Arhivele ce conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului dumneavoastră. Amenințările vă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția în timp real. Cu toate acestea, se recomandă să utilizați această opțiune pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

Trage cursorul pentru a exclude de la scanare arhivele care depășesc o anumită valoare în MB (megaocți).



Notă

Scanarea fișierelor arhivate crește timpul total necesar pentru scanare și necesită mai multe resurse de sistem.

- **Scanează numai fișierele noi și modificate**. Prin scanarea exclusivă a fișierelor noi și a acelor modificate, poți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
- **Scanare sectoare de boot**. Puteți seta Bitdefender să scaneze sectoarele de boot ale hard-diskului. Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot. Atunci când o amenințare infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.



- **Scanează memoria.** Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului dumneavoastră.
- **Scanează regiștrii.** Selectați această opțiune pentru a scana cheile de regiștri. Regiștrii Windows sunt o bază de date care stochează setările de configurare și opțiunile pentru componentele sistemului de operare Windows, precum și pentru aplicațiile instalate.
- **Scanează fișiere cookie.** Selectați această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe computerul dumneavoastră.
- **Scanare după keyloggers.** Selectați această opțiune pentru a scana sistemul în vederea identificării aplicațiilor de tip keylogger. Aplicațiile keyloggers înregistrează ceea ce introduceți de pe tastatură și trimit raporte pe internet către o persoană rău intenționată (hacker). Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.

Asistentul de scanare antivirus

Ori de câte ori inițiați o scanare la cerere (de exemplu, faceți clic pe un director, evidențiați Bitdefender și selectați **Scanează cu Bitdefender**), se inițiază asistentul de Scanare antivirus Bitdefender. Urmați instrucțiunile asistentului pentru a finaliza procesul de scanare.

Notă

Dacă asistentul de scanare nu apare, este posibil ca scanarea să fie configurată să ruleze discret, în fundal. Căutați iconița de scanare în curs **B** în **bara de sistem**. Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

Pasul 1 - Realizarea scanării

Bitdefender va începe scanarea obiectelor selectate. Puteți vedea informații în timp real cu privire la starea scanării precum și statistici (inclusiv timpul consumat, o estimare a timpului rămas și numărul de amenințări detectate).

Așteptați ca Bitdefender să finalizeze scanarea. Procesul de scanare poate dura câteva minute, în funcție de complexitatea scanării.

Oprirea sau întreruperea temporară a scanării. Puteți opri scanarea oricând doriți făcând clic pe **STOP**. Veți trece direct la ultimul pas al asistentului de scanare. Pentru a opri temporar procesul de scanare, faceți clic pe **ÎNTRERUPE**. Va trebui să faceți clic pe **RELUARE** pentru a relua scanarea.



Arhive protejate prin parolă. Atunci când este identificată o arhivă protejată prin parolă, în funcție de setările de scanare, este posibil să fiți rugat să introduceți parola. Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizați parola. Sunt disponibile următoarele opțiuni:

- **Parolă.** Dacă doriți ca Bitdefender să scaneze arhiva, selectați această opțiune și introduceți parola. Dacă nu cunoașteți parola, selectați una dintre celelalte opțiuni.
- **Nu solicita parola și ignoră acest obiect la scanare.** Selectând această opțiune, arhiva nu fi scanată.
- **Ignoră toate articolele protejate prin parolă, fără a le scana.** Selectați această opțiune dacă doriți să nu vi se mai solicite introducerea parolei pentru arhivele protejate prin parolă. Bitdefender nu le va putea scana, dar va păstra o înregistrare în raportul de scanare.

Alegeți opțiunea dorită și faceți clic pe **OK** pentru a continua scanarea.

Pasul 2 - Selectarea acțiunilor

După finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.



Notă

Atunci când executați o scanare rapidă sau o scanare a sistemului, Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor în timpul scanării. Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Obiectele infectate sunt afișate în grupuri, în funcție de amenințarea cu care sunt infectate. Faceți clic pe linkul corespunzător unei amenințări pentru a afla mai multe informații despre obiectele infectate.

Puteți alege o acțiune globală care să fie aplicată pentru rezolvarea tuturor problemelor găsite, sau puteți alege acțiuni separate pentru fiecare grup de probleme. Una sau mai multe dintre opțiunile următoare pot apărea în meniu:

Aplică acțiunile optime

Bitdefender va aplica acțiunile recomandate în funcție de tipul fișierului detectat:

- **Fișiere infectate.** Fișierele detectate ca fiind infectate se potrivesc cu o informație privind amenințările din Baza de Date cu Informații privind Amenințările a Bitdefender. Bitdefender va încerca în mod automat



să elimine codul malițios din fișierul infectat și să refacă fișierul original. Această operațiune este denumită dezinfectare.

Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Pentru mai multe informații, consultați capitolul „*Gestionarea fișierelor aflate în carantină*” (p. 101).



Important

Pentru anumite tipuri de amenințări, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

- **Fișiere 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. Acestea vor fi mutate în carantină pentru a preveni o posibilă infectare.

Implicit, fișierele aflate în carantină sunt trimise automat către Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender în materie de amenințări. Dacă se confirmă prezența unei amenințări, este lansată o actualizare a informațiilor pentru a permite ștergerea amenințării.

- **Arhive ce conțin fișiere infectate.**

- Arhivele care conțin doar fișiere infectate sunt șterse în mod automat.
- Dacă o arhivă conține atât fișiere infectate cât și fișiere curate, Bitdefender va încerca să șteargă fișierele infectate cu condiția să poată apoi reface arhiva cu fișierele curate. Dacă reconstrucția arhivei nu este posibilă, veți fi notificat de faptul că nu poate fi aplicată nicio acțiune astfel încât să se evite pierderea fișierelor curate.

Ștergere

Îndepărtează fișierele identificate ca fiind infectate de pe disc.

Dacă într-o arhivă sunt stocate fișiere infectate împreună cu fișiere curate, Bitdefender va încerca să șteargă fișierele infectate și să refacă arhiva incluzând doar fișierele curate. Dacă reconstrucția arhivei nu este



posibilă, veți fi notificat de faptul că nu poate fi aplicată nicio acțiune astfel încât să se evite pierderea fișierelor curate.

Nicio acțiune

Nu se va lua nicio acțiune asupra fișierelor detectate. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.

Faceți clic pe **Continuă** pentru a aplica acțiunile specificate.

Pasul 3 - Rezumat

Atunci când Bitdefender a remediat toate problemele apărute, rezultatele scanării vor fi afișate într-o nouă fereastră. Dacă doriți informații complete cu privire la procesul de scanare, faceți clic pe **AFIȘEAZĂ JURNAL** pentru a vizualiza jurnalul de scanare.



Important

În majoritatea cazurilor, Bitdefender va dezinfecța fișierele infectate detectate sau le va izola. Cu toate acestea, există anumite probleme care nu pot fi rezolvate automat. Dacă este necesar, reporniți sistemul pentru a finaliza procesul de curățare. Pentru mai multe informații și instrucțiuni privind modul de eliminare a amenințărilor în mod manual, consultați *„Eliminarea amenințărilor din sistemul dumneavoastră”* (p. 214).

Examinarea jurnalelor de scanare

De fiecare dată când efectuați o scanare, se creează un jurnal de scanare și Bitdefender înregistrează problemele identificate în fereastra Antivirus. Raportul de scanare conține informații detaliate despre procesul de scanare înregistrat, cum ar fi opțiunile de scanare, locațiile scanate, amenințările găsite și acțiunile luate asupra acestor amenințări.

Poți deschide raportul de scanare direct din asistentul de scanare, după ce scanarea a luat sfârșit, apăsând **AFIȘEAZĂ JURNAL**.

Pentru a verifica un jurnal de scanări sau orice infecție detectată ulterior:

1. Efectuează clic pe **Notificări** din meniul de navigare al interfeței **Bitdefender**.
2. În fila **Toate**, selectează notificarea privind ultima scanare.



Aici puteți găsi toate evenimentele de scanare, inclusiv amenințările detectate prin scanarea la accesare, prin scanarea inițiată de utilizator, precum și modificările de stare rezultate de scanările automate.

3. În lista de notificări puteți verifica ce operațiuni de scanare au fost realizate recent. Faceți clic pe o notificare pentru a vizualiza detaliile acesteia.
4. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**.

4.1.3. Scanarea automată a suporturilor media amovibile

Bitdefender detectează automat când conectezi o unitate de stocare amovibilă la calculatorul tău și o scanează în fundal atunci când este activată opțiunea Scanare automată. Acest lucru este recomandat pentru a preveni pătrunderea amenințărilor pe calculatorul tău.

Unitățile detectate fac parte din următoarele categorii:

- CD-uri/DVD-uri
- Unitățile de stocare USB, cum ar fi memoriile flash sau hard discurile externe
- unități de rețea mapate (la distanță)

Puteți configura scanarea automată separat pentru fiecare categorie de dispozitive de stocare. Scanarea automată a partițiilor rețelei mapate este dezactivată implicit.

Cum funcționează?

Când detectează un dispozitiv de stocare amovibil, Bitdefender inițiază scanarea pentru depistarea amenințărilor (cu condiția ca scanarea automată să fie activată pentru acel tip de dispozitiv). Veți fi notificat prin intermediul unei ferestre pop-up că a fost detectat un nou dispozitiv și că aceasta este scanat.

O pictogramă de scanare Bitdefender **B** se va afișa în **tăvița de sistem**. Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

În momentul în care scanarea este finalizată, va apărea fereastra cu rezultatele scanării care vă va informa dacă puteți accesa în siguranță fișierele regăsite pe suportul media amovibil.

În majoritatea cazurilor, Bitdefender elimină automat amenințările detectate sau izolează fișierele infectate în carantină. Dacă există amenințări



nesoluționate după finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.



Notă

Luăți în considerare faptul că nu se poate întreprinde nicio acțiune împotriva fișierelor suspecte detectate pe CD-uri/DVD-uri. De asemenea, nu se poate întreprinde nicio acțiune împotriva fișierelor infectate sau suspecte detectate pe unități mapate de rețea în absența privilegiilor respective.

Următoarele informații vă pot fi de folos:

- Vă rugăm să acordați atenție maximă atunci când folosiți un CD/DVD infectat cu amenințări, deoarece o amenințare nu poate fi ștearsă de pe CD/DVD (suportul media este de tip read-only). Asigurați-vă că protecția în timp real este activată pentru a preveni răspândirea amenințărilor în cadrul sistemului dvs. Cea mai bună metodă este să copiați datele importante de pe CD pe sistemul dumneavoastră și apoi să aruncați CD-ul.
- Există posibilitatea ca, în unele cazuri, Bitdefender să nu poată elimina amenințările din anumite fișiere din cauza unor constrângeri tehnice sau legale. Un astfel de exemplu este reprezentat de fișierele arhivate cu ajutorul unei tehnologii brevetate (acest lucru se întâmplă din cauză că arhiva nu poate fi recreată corect).

Pentru a afla cum poți gestiona amenințările, consultă *„Eliminarea amenințărilor din sistemul dumneavoastră”* (p. 214).

Administrarea scanării a fișierelor media amovibile

Pentru a administra scanarea automată a suporturilor media amovibile:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
3. Selectează fila **Partiții și dispozitive**.

Opțiunile de scanare sunt pre-configurate pentru a obține rata maximă de detecție. În cazul în care sunt detectate fișiere infectate, Bitdefender va încerca să le dezinfecțeze (să elimine codul malițios) sau să le mute în carantină. Dacă ambele acțiuni eșuează, asistentul de scanare Antivirus vă va permite să specificați alte acțiuni pentru a fi aplicate în cazul fișierelor infectate. Opțiunile de scanare sunt standard și nu le puteți modifica.



Pentru cea mai bună protecție, este recomandat să activezi opțiunea **Scanare automată** pentru toate tipurile de dispozitive de stocare amovibile.

4.1.4. Scanare fișier de configurare a gazdelor

Fișierul de configurare a gazdelor vine implicit cu instalarea sistemului de operare și este folosit pentru a mapa numele de gazdă pentru adresele IP de fiecare dată când accesezi o nouă pagină web, te conectezi la FTP sau la alte servere de internet. Este un fișier simplu de tip text, iar programele periculoase îl pot modifica. Utilizatorii avansați știu cum să-l utilizeze pentru a bloca reclamele deranjante, bannerele, cookie-urile terților sau hackerii.

Pentru a configura scanarea fișierului de configurare gazde:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Avansat**.
3. Activează sau dezactivează opțiunea **Scanare fișier de configurare a gazdelor**.

4.1.5. Configurarea excepțiilor de scanare

Bitdefender permite excluderea de la scanare a anumitor fișiere, directoare sau extensii de fișiere. Această caracteristică are scopul de a evita interferențele cu munca dumneavoastră și poate ajuta la îmbunătățirea performanței sistemului. Excepțiile vor fi folosite de către utilizatorii care au cunoștințe avansate în ceea ce privește computerele. În caz contrar, pot fi folosite urmând recomandările unui reprezentant Bitdefender.

Poți configura setările astfel încât excepțiile să se aplice doar în cazul scanării la accesare sau al scanării la cerere, sau în cazul ambelor scanări. Obiectele excluse de la scanarea la accesare nu vor fi scanate, indiferent dacă acestea sunt accesate de către tine sau de către o aplicație.



Notă

Excepțiile NU se vor aplica în cazul scanării contextuale. Scanarea contextuală este o metodă de scanare la cerere: faceți clic-dreapta pe fișierul sau directorul pe care doriți să-l scanați și selectați **Scanează cu Bitdefender**.

Excluderea fișierelor și directoarelor de la scanare

Pentru a exclude anumite fișiere și directoare de la scanare:



1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
3. Selectează fila **Excepții**.
4. Dă clic meniul expandabil **Lista fișierelor și directorelor excluse de la scanare**. În fereastra care va apărea, poți administra fișierele și directoratele excluse de la scanare.
5. Pentru a adăuga excepții, urmează pașii de mai jos:
 - a. Faceți clic pe **Add**.
 - b. Dă clic pe **RĂSFOIRE**, selectează fișierul sau directorul care dorești să fie exclus de la scanare și apoi dă clic pe **ADĂUGARE**. Ca o alternativă, puteți introduce (sau copia și lipi) calea către fișier sau director în câmpul editabil.
 - c. În mod implicit, fișierul sau directorul selectat este exclus atât de la scanarea la accesare cât și de la scanarea la cerere. Pentru a modifica când anume se aplică aceste excepții, selectează una dintre celelalte opțiuni.
 - d. Faceți clic pe **Add**.

Excluderea de la scanare a extensiilor de fișiere

În momentul în care o extensie de fișier este exclusă de la scanare, Bitdefender nu va mai scana fișierele cu acea extensie, indiferent de locația acestora pe computer. Excepțiile pot fi aplicate, de asemenea, pentru fișierele aflate pe suporturi amovibile, cum ar fi CD-urile, DVD-urile, dispozitivele USB sau unitățile de rețea.



Important

Aționează cu grijă atunci când setezi excepții de scanare pentru extensiile de fișiere deoarece asemenea excepții pot face computerul vulnerabil în fața amenințărilor.

Pentru a exclude extensii de fișiere de la scanare:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.



3. Selectează fila **Excepții**.
4. Dă clic pe meniul expandabil **Lista extensiilor excluse de la scanare**. În fereastra care va apărea, poți administra extensiile de fișiere excluse de la scanare.
5. Pentru a adăuga excepții, urmează pașii de mai jos:
 - a. Faceți clic pe **Add**.
 - b. Introdu extensiile care dorești să fie excluse de la scanare, separându-le prin punct și virgulă (;). Iată un exemplu:
txt;avi;jpg
 - c. În mod implicit, toate fișierele care au extensiile specificate sunt excluse atât de la scanarea la accesare cât și de la scanarea la cerere. Pentru a modifica când anume se aplică aceste excepții, selectează una dintre celelalte opțiuni.
 - d. Efectuează clic pe **ADĂUGARE**.

Administrarea excepțiilor de scanare

Dacă excepțiile de scanare configurate nu mai sunt necesare, se recomandă să le ștergi sau să dezactivezi excepțiile de scanare.

Pentru a administra excepțiile de scanare:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
3. Selectează fila **Excepții**.
4. Folosește opțiunile din meniul expandabil **Lista de fișiere și directoare excluse de la scanare** pentru a administra excepțiile de scanare.
5. Pentru a șterge sau edita excepțiile de scanare, dă clic pe unul dintre link-urile disponibile. Procedați astfel:
 - Pentru a șterge un element de pe listă, selectați-l și faceți clic pe **Ștergere**.
 - Pentru a edita o înregistrare din tabel, dă dublu clic pe aceasta (sau selectează-o și dă clic pe **Editare**). Se afișează o nouă fereastră unde poți schimba extensia sau calea care va fi exclusă, precum și tipul de



scanare de la care acestea să fie excluse. Efectuează modificările necesare, apoi dă clic pe **MODIFICĂ**.

4.1.6. Gestionarea fișierelor aflate în carantină

Bitdefender izolează fișierele infectate cu amenințări ce nu pot fi dezinfectate, precum și fișierele suspecte într-o zonă sigură numită carantină. Atunci când sunt în carantină, amenințările sunt inofensive, pentru că nu pot fi executate sau citite.

Implicit, fișierele aflate în carantină sunt trimise automat către Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender în materie de amenințări. Dacă se confirmă prezența unei amenințări, este lansată o actualizare a informațiilor pentru a permite ștergerea amenințării.

În plus, Bitdefender scanează fișierele din carantină după fiecare actualizare a bazei de date cu amenințări. Fișierele curățate sunt mutate automat în locația lor originală.

Pentru a verifica și gestiona fișierele din carantină:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, efectuați clic pe **Carantină**.

Aici poți vizualiza denumirile fișierelor în carantină, localizarea lor originală și denumirea amenințărilor detectate.

3. Fișierele aflate în carantină sunt gestionat în mod automat de Bitdefender, în funcție de setările implicite pentru carantină.

Deși nu este recomandat, poți modifica setările de carantină în funcție de preferințele tale efectuând clic pe **Vizualizare setări**.

Faceți clic pe comutatoare pentru a activa sau dezactiva:

Scanează din nou carantina după actualizarea informațiilor despre amenințări

Mențineți activată această opțiune pentru a scana în mod automat fișiere aflate în carantină după fiecare actualizare a bazei de date cu informații privind amenințările. Fișierele curățate sunt mutate automat în locația lor originală.

Ștergere conținutul mai vechi de 30 de zile

Fișierele aflate în carantină mai vechi de 30 de zile sunt șterse automat.



Creează excepții pentru fișierele restabilite

Fișierele pe care le restabilești din carantină sunt mutate înapoi în locația lor inițială fără a fi reparate și sunt automat excluse de la scanările următoare.

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

4.2. Advanced Threat Defense

Bitdefender Advanced Threat Defense este o tehnologie inovatoare de detecție proactivă, care folosește metode euristice avansate pentru a detecta programele ransomware și alte potențiale amenințări în timp real.

Advanced Threat Defense monitorizează continuu aplicațiile care rulează pe calculatorul dumneavoastră, căutând amenințări. Fiecare dintre aceste acțiuni are un anumit punctaj iar punctajul global este calculat pentru fiecare proces.

Ca o măsură de siguranță, vei fi anunțat de fiecare dată când se detectează și se blochează amenințări și procese potențial periculoase.

Activarea sau dezactivarea funcției Advanced Threat Defense

Pentru a activa sau dezactiva funcția Advanced Threat Defense

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ADVANCED THREAT DEFENSE**, activează sau dezactivează butonul.

Notă

Pentru a-ți menține sistemul protejat de ransomware și toate celelalte amenințări, îți recomandăm să dezactivezi funcția Advanced Threat Defense cât mai puțin timp posibil.

Verificarea atacurilor malware detectate

Ori de câte ori sunt detectate amenințări sau procese potențial dăunătoare, Bitdefender le va bloca pentru a preveni infectarea computerului cu



ransomware sau cu alte programe malware. Poți verifica în orice moment lista atacurilor malware detectate urmând acești pași:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ADVANCED THREAT DEFENSE**, efectuează clic pe **Apărare împotriva amenințărilor**.
3. La prima utilizare a funcției Protecție împotriva programelor de tip ransomware, ți se prezintă această funcție. Efectuează clic pe **OK, AM ÎNȚELES** pentru a continua.

Sunt afișate atacurile detectate în ultimele 90 de zile. Pentru a afla detalii despre tipul de ransomware detectat, calea procesului periculos, sau dacă dezinfectarea a fost efectuată cu succes, efectuează clic pe acesta.

Adăugarea proceselor în lista de excepții

Poți configura regulile de excludere pentru aplicațiile sigure astfel încât funcția Advanced Threat Defense să nu le blocheze dacă întreprind acțiuni ce pot părea amenințătoare.

Pentru a începe adăugarea proceselor în lista de excepții a funcției Advanced Threat Defense:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ADVANCED THREAT DEFENSE**, efectuează clic pe **Setări**.
3. În secțiunea **Excepții**, selectează **Adăugare aplicații în lista de excepții**.
4. Găsește și selectează aplicația care dorești să fie exceptată și dă clic pe **OK**.

Pentru a șterge o înregistrare din listă, efectuează clic pe opțiunea **Ștergere** din dreptul său.

Detecție exploatări

Una dintre metodele folosite de hackeri pentru a pătrunde în sisteme este de a profita de anumite erori sau vulnerabilități prezente în software-ul (aplicații sau plugin-uri) și hardware-ul computerelor. Pentru a te asigura că computerul tău este protejat de astfel de atacuri, care în mod normal se



răspândesc foarte rapid, Bitdefender utilizează cele mai noi tehnologii anti-exploit-uri.

Activarea sau dezactivarea funcției de detecție exploit-uri

Pentru a activa sau dezactiva funcția de detecție exploit-uri:

- Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
- În panoul **ADVANCED THREAT DEFENSE**, efectuează clic pe **Setări**.
- Folosește butonul corespunzător de activare sau dezactivare.



Notă

Opțiunea Detecție exploit-uri este activată în mod implicit.

4.3. Online Threat Prevention

Bitdefender Online Threat Prevention asigură o experiență de navigare sigură alertându-te cu privire la paginile web potențial periculoase.

Bitdefender oferă funcția de prevenire în timp real a amenințărilor pentru:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Pentru a configura setările Online Threat Prevention:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ONLINE THREAT PREVENTION**, efectuează clic pe **Setări**.

În fereastra **Protecție cameră web**, efectuează clic pe butoane pentru a activa sau dezactiva opțiunea.

- Funcția de prevenire a atacurilor web blochează amenințările care vin de pe internet, inclusiv descărcările neintenționate.



- Asistență pentru căutare, o componentă care clasifică rezultatele căutărilor efectuate cu ajutorul motoarelor de căutare și link-urile publicate în rețelele sociale prin afișarea unei pictograme în dreptul fiecărui rezultat:

- Nu este recomandat să vizitați această pagină web.

- ⚠ Această pagină web poate avea conținut periculos. Vizitați cu atenție această pagină.

- Această pagină este sigură.

Funcția de Asistență pentru căutare clasifică rezultatele generate de următoarele motoare de căutare:

- Google
- Yahoo!
- Bing
- Baidu

Funcția de Asistență pentru căutare clasifică link-urile publicate pe următoarele site-uri de socializare:

- Facebook
- Twitter

- Scanare web criptată.

Atacurile mai sofisticate pot folosi trafic de web securizat pentru a induce în eroare victimele. Prin urmare, îți recomandăm să păstrezi activată opțiunea Scanare web criptată.

- Protecție împotriva fraudelor.
- Protecție antiphishing.

În fereastra **Prevenire amenințări rețea**, există opțiunea **Prevenire amenințări rețea**. Pentru a îți păstra calculatorul protejat împotriva atacurilor programelor periculoase (cum ar fi ransomware) prin exploatarea vulnerabilităților, păstrează activă această opțiune.

Poți crea o listă de site-uri, domenii și adrese IP care nu vor fi scanate de motoarele contra amenințărilor, tentativelor de phishing și antifraudă Bitdefender. Lista trebuie să conțină numai site-uri web, domenii și adrese IP în care aveți încredere deplină.

Pentru a configura și administra site-urile web, domeniile și adresele IP folosind funcția Online Threat Prevention pusă la dispoziție de Bitdefender:



1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ONLINE THREAT PREVENTION**, dă clic pe **Excepții**.
3. Introdu în câmpul corespunzător denumirea site-ului web, numele domeniului sau adresa IP pe care dorești să o adaugi la excepții, apoi selectează **ADAUGĂ**.

Pentru a șterge o înregistrare din listă, selectează-o și apoi clic pe **Șterge**.

Efectuează clic pe **SALVEAZĂ** pentru a memora schimbările și a închide fereastra.

Alertele Bitdefender sunt afișate în browser

De fiecare dată când încercați să vizitați un site web clasificat ca fiind nesigur, acesta este blocat și este deschisă o pagină de avertizare în browser-ul dumneavoastră.

Pagina conține informații precum URL-ul site-ului web și amenințarea detectată.

Trebuie să decideți ce veți face în continuare. Sunt disponibile următoarele opțiuni:

- Părăsește site-ul web respectiv dând clic pe **REVENIRE LA O PAGINĂ SIGURĂ**.
- Accesați site-ul web, în ciuda avertismentului, făcând clic pe **Înțeleg riscurile și doresc să accesez această pagină**.
- Dacă ești sigur că pagina web detectată este sigură, selectează **TRIMITE** pentru a o adăuga în lista de excepții. Îți recomandăm să adaugi numai pagini web în care ai deplină încredere.

4.4. Antispam

Spam este un termen utilizat pentru a descrie un e-mail nesolicitat. Spamul este o problemă în creștere, atât pentru individ cât și pentru organizații. Nu este interesant, nu ați dori să fie văzut de către copii, puteți fi concediat din cauza lui (pentru pierdere de timp prin primirea de mesaje cu conținut sexual pe adresa de serviciu) și nu puteți împiedica trimiterea sa. Cel mai bun lucru pe care îl puteți face este, evident, să nu îl mai primiți. Din păcate, acesta există în cantități mari, într-o gamă largă de forme și mărimi.



Bitdefender Antispam utilizează remarcabile inovații tehnologice și filtre antispam standard pentru a ține la distanță spamul de căsuțele de mesaje ale utilizatorilor. Pentru mai multe informații, consultați capitolul „*Detalii privind modulul Antispam*” (p. 107).

Protecția antispam Bitdefender este disponibilă numai pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3. POP3 este unul dintre cele mai des folosite protocoale de descărcare a mesajelor e-mail de pe un server de mail.



Notă

Bitdefender nu asigură protecție antispam pentru conturile de e-mail pe care le accesați prin intermediul serviciilor de e-mail oferite pe internet.

Mesajele spam detectate de Bitdefender sunt marcate cu prefixul [spam] în subiect. Bitdefender mută în mod automat mesajele spam într-un anumit director, după cum urmează:

- În Microsoft Outlook, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Deleted Items**. Folderul **Spam** este creat atunci când un e-mail este etichetat drept spam.
- În Mozilla Thunderbird, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Trash**. Folderul **Spam** este creat atunci când un e-mail este etichetat drept spam.

Dacă utilizați alt client de mail, trebuie să creați o regulă pentru a muta mesajele e-mail marcate ca [spam] de Bitdefender într-un anumit director de carantină. Dacă folderele Ștergere articole sau Coș de gunoi sunt șterse, folderul Spam va fi șters și el. Cu toate acestea, se va crea un nou folder Spam imediat ce un e-mail este etichetat drept spam.

4.4.1. Detalii privind modulul Antispam

Filtrele Antispam

Motorul antispam Bitdefender include protecție cloud și diverse alte filtre care vă protejează de mesajele de tip SPAM, cum ar fi **Lista de prieteni**, **Lista de spammeri** și **Filtrul de caractere**.

Lista de prieteni/Lista de spanmmeri

Majoritatea oamenilor comunică în mod regulat cu un grup de cunoștințe sau chiar primesc mesaje de la companii sau organizații cu același domeniu



de activitate. Prin utilizarea **listei de prieteni sau de spammeri**, puteți clasifica ușor persoanele de la care doriți să primiți e-mail-uri (prieteni) indiferent de conținutul mesajului sau persoanele de la care nu mai doriți să primiți deloc mesaje (spammeri).



Notă

Vă recomandăm să adăugați numele și adresele prietenilor la **Lista de prieteni**. Bitdefendernu blochează mesajele persoanelor aflate în această listă; de aceea, adăugarea prietenilor în listă asigură primirea mesajelor legitime.

Filtrul de caractere

Multe mesaje Spam sunt scrise cu caractere chirilice și / sau asiatice. Filtrul de caractere detectează acest tip de mesaje și le marchează ca SPAM.

Funcționarea Antispam

Motorul antispam al Bitdefender utilizează concomitent toate filtrele antispam pentru a determina dacă un anumit mesaj e-mail ar trebui să ajungă în directorul **Inbox (Mesaje primite)** sau nu.

Fiecare mesaj e-mail pe care îl primiți este întâi verificat de filtrul **Lista de prieteni/Lista de spammeri**. Dacă adresa expeditorului se regăsește în **Lista de prieteni** mesajul este trimis direct în **Inbox**.

În caz contrar, filtrul **Lista de spammer-i** va verifica dacă adresa expeditorului se află pe această listă. Dacă adresa este găsită, e-mail-ul este etichetat ca SPAM și este mutat în directorul **Spam**.

Altfel, **Filtrul de caractere** va verifica dacă mesajul este scris cu caractere Chirilice sau Asiatice. În acest caz, e-mail-ul este etichetat ca SPAM și mutat în directorul **Spam**.



Notă

Dacă mesajul este etichetat ca SEXUALLY EXPLICIT în subiect, Bitdefender îl va considera SPAM.

Clienți și protocoale de e-mail compatibile

Protecția antispam este oferită pentru toți clienții de mail POP3/SMTP. Bara de comenzi antispam însă este integrată doar în:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 sau mai recent



4.4.2. Activarea sau dezactivarea protecției antispam

Protecția antispam este activată implicit.

Pentru a activa sau dezactiva caracteristica Antispam:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTISPAM**, activează sau dezactivează butonul.

4.4.3. Utilizarea barei de instrumente antispam în fereastra de client de e-mail

În partea de sus a ferestrei clientului dumneavoastră de mail, puteți vedea bara de comenzi antispam. Bara de comenzi antispam vă ajută să administrați protecția antispam direct din clientul dumneavoastră de mail. Puteți corecta Bitdefender cu ușurință dacă acesta a marcat un mesaj legitim ca SPAM.



Important


Bitdefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, consultați „*Clienți și protocoale de e-mail compatibile*” (p. 108).


Fiecare buton al barei de comenzi este explicat mai jos:


- ⚙️ **Setări** - deschide o fereastră în care puteți configura filtrele antispam și setările barei de instrumente.
- 🗑️ **Este Spam** - indică faptul că mesajul e-mail selectat este spam. Mesajul e-mail va fi mutat imediat în directorul **Spam**. Dacă serviciile antispam cloud sunt activate, mesajul va fi trimis către Bitdefender Cloud pentru a fi analizat în detaliu.
- 📧 **Nu este spam** - indică faptul că mesajele e-mail selectate nu sunt de tip spam și Bitdefender nu ar fi trebuit să le eticheteze astfel. E-mailul va fi mutat din directorul **Spam** în directorul **Inbox** (Mesaje primite). Dacă serviciile antispam cloud sunt activate, mesajul va fi trimis către Bitdefender Cloud pentru a fi analizat în detaliu.





Important

Butonul  **Nu este Spam** este activ doar când selectați un mesaj etichetat ca SPAM de către Bitdefender (în mod normal aceste mesaje se găsesc în directorul **Spam**).

 **Adaugă Spammer** - adaugă expeditorul e-mailului selectat pe Lista de spammeri. Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare. Mesajele e-mail primite de la adrese de pe Lista de spammeri sunt marcate automat ca [spam].


 **Adaugă prieten** - adaugă expeditorul e-mailului selectat pe Lista de prieteni. Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare. Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.

 **Spammeri** - deschide **lista de spammeri** care conține adrese de e-mail de la care nu doriți să primiți mesaje, indiferent de conținutul acestora. Pentru mai multe informații, consultați capitolul „*Configurarea listei de spammeri*” (p. 113).

 **Prieteni** - deschide **lista de prieteni** care conține adrese de e-mail de la care doriți întotdeauna să primiți mesaje, indiferent de conținutul acestora. Pentru mai multe informații, consultați capitolul „*Configurarea listei de prieteni*” (p. 111).

Indicarea erorilor de detecție

Dacă folosiți un client de e-mail compatibil, puteți corecta cu ușurință filtrul antispam (indicând ce mesaje e-mail nu ar fi trebuit marcate ca fiind de tip [spam]). Astfel, veți îmbunătăți eficiența filtrului antispam. Urmați acești pași:


1. Deschideți clientul dumneavoastră de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele legitime pe care Bitdefender le-a marcat incorect ca [spam].
4. Faceți clic pe butonul  **Adaugă prieten** din bara de instrumente antispam Bitdefender, pentru a adăuga expeditorul pe Lista de prieteni. Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare. Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.




5. Faceți clic pe butonul  **Nu este spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail). Mesajul e-mail va fi mutat în directorul Mesaje primite.

Indicarea mesajelor spam nedetectate



Dacă folosiți un client de mail admis, puteți indica cu ușurință care mesaje e-mail ar fi trebuit detectate ca spam. Astfel, veți îmbunătăți eficiența filtrului antispam. Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți la directorul Inbox.
3. Selectați mesajele spam nedetectate.
4. Faceți clic pe butonul  **Spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail). Acestea sunt marcate imediat ca [spam] și mutate în directorul de mesaje nesolicitate (junk).

Configurarea setărilor barei de instrumente

Pentru a configura setările barei de instrumente antispam pentru clientul de e-mail, faceți clic pe butonul  **Setări** din bara de instrumente și apoi pe fila **Setări bară din instrumente**.

Aici aveți la dispoziție următoarele opțiuni:

- **Marchează e-mail-urile spam ca 'citite'** - marchează, în mod automat, mesajele e-mail de tip spam ca fiind citite, astfel încât să nu fiți deranjat la primirea unui astfel de mesaj.
- Puteți alege dacă să fie afișate sau nu ferestrele de confirmare când faceți clic pe butoanele  **Adaugă Spammer** și  **Adaugă prieten** din bara de instrumente antispam.

Ferestrele de confirmare pot preveni adăugarea accidentală a expeditorilor de mesaje e-mail la lista de prieteni/contacte care trimit mesaje spam.

4.4.4. Configurarea listei de prieteni


Lista de Prieteni este o listă care conține toate adresele de e-mail de la care doriți să primiți mesaje, indiferent de conținutul acestora. Mesajele de la prieteni nu vor fi etichetate ca Spam, chiar dacă au conținut asemănător mesajelor Spam.



Notă

Orice mesaj venit de la o adresă inclusă pe **lista de prieteni** va fi trimis automat în directorul Inbox, fără a mai fi procesat.

Pentru a configura și administra lista de prieteni:

- Dacă utilizați Microsoft Outlook sau Thunderbird, faceți clic pe butonul  **Prieteni** de pe **bara de instrumente antispam Bitdefender**
- Alternativ:
 1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
 2. În panoul **ANTISPAM**, efectuează clic pe **Administrare prieteni**.

Pentru a adăuga o adresă de e-mail, selectează opțiunea **Adresă e-mail**, introdu adresa și apoi efectuează clic pe **ADAUGĂ**. Sintaxă: nume@domeniu.com.

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectează opțiunea **Nume domeniu**, introdu numele domeniului și efectuează clic pe **Adaugă**. Sintaxă:

- @domain.com și domain.com - toate mesajele primite de la domain.com vor ajunge în directorul **Inbox** indiferent de conținut;
- domeniu - toate mesajele primite de la domeniu (indiferent de sufixul domeniului) vor fi etichetate ca SPAM;
- com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate ca SPAM;

Se recomandă să evitați adăugarea de domenii, însă acest lucru poate fi util în anumite situații. De exemplu, puteți adăuga domeniul de e-mail al companiei pentru care lucrați sau pe cele ale partenerilor dumneavoastră de încredere.

Pentru a șterge un element de pe listă, faceți clic pe link-ul **Elimină** corespunzător. Pentru a șterge toate înregistrările din listă, efectuează clic pe **ȘTERGERE LISTĂ**.

Puteți salva Lista de prieteni într-un fișier, astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului. Pentru a salva Lista de prieteni, faceți clic pe butonul **Salvează** și salvați-o în locația dorită. Fișierul va avea extensia .bwl.

Pentru a încărca o Listă de prieteni memorată anterior, efectuează clic pe **ÎNCARCĂ** și deschide fișierul corespunzător .bwl. Pentru a reseta conținutul




listei curente atunci când încărcați o listă salvată anterior, selectați **Suprascrie lista curentă**.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

4.4.5. Configurarea listei de spammeri

Lista de spammeri este o listă care conține toate adresele de e-mail de la care nu doriți să primiți mesaje, indiferent de conținutul acestora. Orice mesaj primit de la o adresă din **lista de spammeri** va fi automat etichetat ca Spam, fără altă procesare.

Pentru a configura și administra lista de spammeri:

- Dacă utilizați Microsoft Outlook sau Thunderbird, faceți clic pe butonul  **Spammeri** de pe **bara de instrumente antisпам Bitdefender** integrată în clientul dumneavoastră de e-mail.
- Alternativ:
 1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
 2. În panoul **ANTISPAM**, efectuează clic pe **Administrare spammeri**.

Pentru a adăuga o adresă de e-mail, selectează opțiunea **Adresă e-mail**, introdu adresa și apoi efectuează clic pe **ADAUGĂ**. Sintaxă: nume@domeniu.com.

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectează opțiunea **Nume domeniu**, introdu numele domeniului și efectuează clic pe **Adaugă**. Sintaxă:

- @domain.com și domain.com - toate mesajele primite de la domain.com vor ajunge în directorul **Inbox** indiferent de conținut;
- domeniu - toate mesajele primite de la domeniu (indiferent de sufixul domeniului) vor fi etichetate ca SPAM;
- com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate ca SPAM.

Se recomandă să evitați adăugarea de domenii, însă acest lucru poate fi util în anumite situații.

Avertisment

Nu adăugați nume de domenii legitime ale unor servicii de e-mail bazate pe web (Yahoo, Gmail, Hotmail sau altele asemenea) pe Lista de spammeri. În caz contrar, mesajele e-mail primite de la orice utilizator înregistrat al unui



astfel de serviciu va fi detectat ca spam. Dacă, de exemplu, adăugați yahoo.com pe Lista de spammeri, toate mesajele e-mail care provin de la adrese yahoo.com vor fi marcate ca [spam].

Pentru a șterge un element de pe listă, faceți clic pe link-ul **Elimină** corespunzător. Pentru a șterge toate înregistrările din listă, efectuează clic pe **ȘTERGERE LISTĂ**.

Puteți salva Lista de spammeri într-un fișier astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului. Pentru a salva Lista de spammeri, faceți clic pe butonul **Salvează** și salvați-o în locația dorită. Fișierul va avea extensia .bwl.

Pentru a încărca o Listă de spammeri memorată anterior, efectuează clic pe **ÎNCARCĂ** și deschide fișierul corespunzător .bwl. Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior, selectați **Suprascrie lista curentă**.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

4.4.6. Se configurează filtrele locale antispam

Conform descrierii de la „*Detalii privind modulul Antispam*” (p. 107), Bitdefender utilizează o combinație de diferite filtre antispam pentru a identifica mesajele spam. Filtrele antispam sunt preconfigurate pentru asigurarea unei protecții eficiente.



Important

Dacă primiți e-mailuri legitime scrise cu caractere asiatice sau chirlice, dezactivați setarea care blochează în mod automat aceste e-mailuri. Setarea corespunzătoare este dezactivată pentru versiunile localizate ale programului care utilizează astfel de seturi de caractere (de exemplu, în cazul versiunii în limba rusă sau chineză).

Pentru a configura filtrele locale antispam:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTISPAM**, efectuează clic pe **Setări**.
3. Efectuează clic pe butoanele de pornire și oprire corespunzătoare.

În cazul în care utilizați Microsoft Outlook sau Thunderbird, puteți configura filtrele locale antispam direct din clientul de e-mail. Faceți clic pe butonul 



Setări din bara de instrumente antisпам Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail) și apoi pe fila **Filtre antisпам**.

4.4.7. Configurarea setărilor cloud

Detecția cloud folosește serviciile Bitdefender Cloud pentru a vă oferi protecție antisпам eficientă și întotdeauna actualizată.

Protecția cloud funcționează cât timp funcția Antisпам a Bitdefender este menținută activă.

Mostre de mesaje e-mail legitime și de tip spam pot fi trimise către Bitdefender Cloud în cazul în care identificați erori de detecție sau mesaje e-mail de tip spam nedetectate. Acest lucru vă ajută să îmbunătățiți rata de detecție antisпам a Bitdefender.

Configurați trimiterea mostrelor de e-mail către Bitdefender Cloud selectând opțiunile dorite și urmărind pașii de mai jos:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTISPAM**, efectuează clic pe **Setări**.
3. Efectuează clic pe butoanele de pornire și oprire corespunzătoare.

În cazul în care utilizați Microsoft Outlook sau Thunderbird, puteți configura detecția cloud direct de la clientul dumneavoastră de e-mail. Faceți clic pe butonul * **Setări** din bara de instrumente antisпам Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail) și apoi pe fila **Setări Cloud**.

4.5. Firewall

Firewall-ul vă protejează calculatorul contra tentativelor de conectare interne și externe neautorizate, atât în rețele locale, cât și pe internet. Este asemănător unui paznic - ține evidența tentativelor de conectare și decide pe care să le permite și pe care să le blocheze.

Firewall-ul Bitdefender folosește un set de reguli pentru a filtra datele transmise către și de la sistemul dumneavoastră.

În condiții normale, Bitdefender creează în mod automat o regulă de fiecare dată când o aplicație încearcă să acceseze internetul. De asemenea, puteți edita sau adăuga manual reguli pentru aplicații.



Ca măsură de securitate, vei fi notificat de fiecare dată când o aplicație potențial periculoasă este blocată de la a accesa internetul.

Bitdefender alocă automat un nou tip fiecărei conexiuni la rețea detectate. În funcție de tipul de rețea, protecția firewall este setată la nivelul corespunzător pentru fiecare conexiune.

Pentru a afla mai multe despre setările firewall pentru fiecare tip de rețea și despre modul în care puteți edita setările rețelei, consultați „*Administrarea setărilor de conectare*” (p. 119).

Activarea sau dezactivarea protecției firewall.

Pentru a activa sau dezactiva protecția firewall:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **FIREWALL**, activează sau dezactivează butonul.



Avertisment

Deoarece vă expune computerul unor conexiuni neautorizate, dezactivarea firewallului trebuie să fie doar o măsură temporară. Reactivați firewall-ul cât mai repede posibil.

4.5.1. Administrarea regulilor pentru aplicații

Pentru a vizualiza și a administra regulile pentru firewall, ce controlează accesul aplicațiilor la resursele rețelei și la internet:


1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **FIREWALL**, dă clic pe **Acces aplicație**.
3. La prima accesare a funcției Firewall, ți se prezintă această funcție. Efectuează clic pe **OK, AM ÎNȚELES** pentru a continua.

Poți vedea cele mai recente 15 programe (proces) care au trecut prin Firewall-ul Bitdefender și rețeaua de internet la care ești conectat. Pentru a vedea regulile create pentru o anumită aplicație, efectuează clic pe aceasta și apoi accesează linkul **Vezi regulile aplicației**. Se deschide fereastra **Reguli**.

Pentru fiecare regulă sunt afișate următoarele informații:



- **REȚEA** - procesul și tipurile de adaptoare de rețea (Acasă/Birou, Public sau Toate) pentru care se aplică regula. Regulile sunt create automat pentru a filtra accesul la rețea sau internet prin oricare adaptor. În mod implicit, regula se aplică oricărei rețele. Pentru a filtra accesul aplicațiilor la rețea și internet printr-un anumit adaptor (de exemplu, printr-un adaptor de rețea wireless), puteți crea reguli manual sau puteți edita regulile existente.
- **PROTOCOL** - protocolul IP căruia i se aplică regula. În mod implicit, regula se aplică oricărui protocol.
- **TRAFIC** - regula se aplică în ambele direcții, atât traficului de intrare și celui de ieșire.
- **PORTURI** - protocolul de PORTURI căruia i se aplică regula. În mod implicit, regula se aplică tuturor porturilor.
- **IP** - protocolul de internet (IP) căruia i se aplică regula. În mod implicit, regula se aplică tuturor adreselor IP.
- **ACCES** - dacă accesul aplicației la rețea sau la internet este permis sau respins în condițiile precizate.

Pentru a modifica sau șterge regulile pentru aplicațiile selectate, efectuează clic pe pictograma .

- **Modificare regulă** - deschide o fereastră în care puteți modifica regula curentă.
- **Ștergere regulă** - poți alege să ștergi setul de reguli curent pentru aplicația selectată.

Adăugare reguli pentru aplicații

Pentru adăugarea unei reguli pentru aplicație:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **FIREWALL**, efectuează clic pe **Setări**.
3. În fereastra **Reguli**, efectuează clic pe **Adăugare regulă**.

În fereastra **Setări**, poți aplica următoarele modificări:

- **Aplică această regulă tuturor aplicațiilor**. Activează acest buton pentru a aplica regula creată tuturor aplicațiilor.



- **Cale program.** Efectuează clic pe **CAUȚĂ** și selectează aplicația căreia i se aplică regula.
- **Permișiune.** Selectați una dintre permisiunile disponibile:

Permișiune	Descriere
Permite	Aplicației specificate îi va fi permis accesul la rețea / internet în condițiile specificate.
Interzice	Aplicației specificate îi va fi refuzat accesul la rețea / internet în condițiile specificate.

- **Tip rețea.** Selectați tipul de rețea pentru care se aplică regula. Puteți modifica tipul deschizând meniul vertical **Tip de rețea** și selectând unul dintre tipurile disponibile din listă.

Tip rețea	Descriere
Orice rețea	Permite tot traficul dintre calculatorul tău și alte calculatoare indiferent de tipul rețelei.
Acasă/Birou	Permite tot traficul dintre calculatorul dumneavoastră și calculatoarele din rețeaua locală.
Publică	Tot traficul este filtrat.

- **Protocol.** Selectați din meniu protocolul IP căruia i se aplică regula.
 - Dacă doriți ca regula să fie aplicată tuturor protocoalelor, selectați **Oricare**.
 - Dacă doriți ca regula să fie aplicată pentru TCP, selectați **TCP**.
 - Dacă doriți ca regula să fie aplicată pentru UDP, selectați **UDP**.
 - Dacă dorești ca regula să fie aplicată pentru ICMP, selectează **ICMP**.
 - Dacă dorești ca regula să fie aplicată pentru IGMP, selectează **IGMP**.
 - Dacă doriți ca o regulă să se aplice unui anumit protocol, introduceți în câmpul gol numărul alocat protocolului pe care doriți să-l filtrați.



Notă

Numerele protocoalelor IP sunt atribuite de către Internet Assigned Numbers Authority (IANA). Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa <http://www.iana.org/assignments/protocol-numbers>.

- **Direcție.** Selectați din meniu direcția traficului căreia i se aplică regula.

Direcție	Descriere
La ieșire	Regula nu se va aplica decât pentru traficul la ieșire.
La intrare	Regula nu se aplica decât pentru traficul la intrare.
Ambele	Regula se va aplica în ambele direcții.

În fereastra **Avansat** poți personaliza următoarele setări:

- **Adresă locală personalizată.** Specificați adresa IP locală și portul local cărora li se aplică regula.
- **Adresă remote personalizată.** Specificați adresa IP și portul la distanță cărora li se aplică regula.

Pentru a îndepărta setul actual de reguli și a restabili regulile implicite, efectuează clic pe **Resetați reguli** din fereastra **Reguli**.

4.5.2. Administrarea setărilor de conectare

Indiferent că te conectezi la internet printr-un adaptor Wi-Fi sau printr-un adaptor Ethernet, poți configura setările care dorești să fie aplicate pentru o navigare sigură. Opțiunile disponibile sunt următoarele:

- **Dinamic** – tipul rețelei va fi setat automat în funcție de profilul rețelei conectate, Acasă/Birou sau Public. Atunci când se întâmplă acest lucru, se vor aplica numai regulile de Firewall valabile pentru tipul de rețea respectiv sau cele definite pentru a se aplica tuturor tipurilor de rețea.
- **Acasă/Birou** – tipul de rețea va fi întotdeauna Acasă/Birou, indiferent de profilul rețelei conectate. Atunci când se întâmplă acest lucru, se vor aplica numai regulile de Firewall pentru modul Acasă/Birou sau cele definite pentru a se aplica tuturor tipurilor de rețea.



- **Public** - tipul de rețea va fi întotdeauna Public, indiferent de profilul rețelei conectate. Atunci când se întâmplă acest lucru, se vor aplica numai regulile de Firewall pentru modul Public sau cele definite pentru a se aplica tuturor tipurilor de rețea.

Pentru a configura adaptoarele de rețea:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **FIREWALL**, efectuează clic pe **Setări**.
3. Selectează secțiunea **Adaptoare rețea**.
4. Selectează setările care dorești să fie aplicate atunci când te conectezi la următoarele adaptoare:
 - Wi-Fi
 - Ethernet

4.5.3. Configurarea setărilor avansate

Pentru a configura setări avansate de firewall:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **FIREWALL**, efectuează clic pe **Setări**.
3. Selectați tabul **Setări**.

Pot fi configurate următoarele caracteristici:

- **Protecția scanării porturilor** - detectează și blochează tentativele de a afla ce porturi sunt deschise.
Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculatorul dumneavoastră. Dacă este detectat un port vulnerabil, aceștia pot pătrunde în calculatorul dumneavoastră.
- **Mod alertă** - alertele sunt indicate de fiecare dată când o aplicație încearcă să se conecteze la internet. Selectați **Permite** sau **Blocare**. Când Modul alertă este pornit, funcția **Profiluri** este dezactivată automat. Modul de alertă poate fi folosit în același timp cu **Modul baterie**.
- **Permite accesul la rețeaua de domeniu** - permiteți sau refuză accesul la resurse și locații partajate definite de controllerele de domeniu.



- **Mod ascuns** - dacă puteți fi detectat de alte calculatoare. Efectuează clic pe **Modificare setări mod ascuns** pentru a selecta când dispozitivul tău ar trebui și când nu ar trebui să fie vizibil pentru alte calculatoare.
- **Comportament implicit al aplicației** - permite Bitdefender să aplice setările automate pentru aplicațiile fără reguli definite. Efectuează clic pe **Modificare reguli implicite** pentru a selecta dacă setările automate trebuie aplicate sau nu.
 - Automat - accesul aplicațiilor va fi permis sau blocat pe baza setărilor automate de Firewall și a regulilor utilizatorului.
 - Permite - se va permite în mod automat accesul aplicațiilor care nu au definită nicio regulă de Firewall.
 - Blochează - se va bloca în mod automat accesul aplicațiilor care nu au definită nicio regulă de Firewall.

4.6. Vulnerabilități

Un pas important în protejarea calculatorului dumneavoastră împotriva acțiunilor și aplicațiilor periculoase este de a menține actualizat sistemul de operare și aplicațiile pe care le utilizați în mod regulat. Mai mult, pentru a împiedica accesul fizic neautorizat la calculatorul tău, este necesară configurarea de parole puternice (parole ce nu pot fi ghicite cu ușurință) pentru fiecare cont de utilizator Windows, precum și pentru rețelele Wi-Fi la care te conectezi.

Bitdefender verifică automat dacă există vulnerabilități în sistemul dumneavoastră și vă informează în legătură cu acestea. Acesta scanează următoarele:

- aplicații neactualizate din calculatorul tău.
- actualizări Windows lipsă.
- parolele simple ale conturilor de utilizator Windows.
- rețele wireless și routere nesecurizate.

Bitdefender permite remedierea cu ușurință a vulnerabilităților sistemului dumneavoastră prin oricare dintre cele două metode de mai jos:

- Puteți scana sistemul pentru a identifica vulnerabilitățile acestuia și le puteți remedia pas cu pas folosind opțiunea **Scanare vulnerabilitate**.



- Prin intermediul monitorizării automate a vulnerabilităților, puteți verifica și remedia vulnerabilitățile detectate, în fereastra **Notificări**.

Ar trebui să verificați și să remediați vulnerabilitățile sistemului săptămânal sau o dată la două săptămâni.

4.6.1. Scanarea sistemului pentru identificarea vulnerabilităților

Pentru a detecta vulnerabilitățile sistemului, Bitdefender necesită o conexiune activă la internet.

Pentru a-ți scana sistemul în vederea identificării vulnerabilităților:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **VULNERABILITATE**, efectuează clic pe **Scanare vulnerabilitate**.
3. Prima dată când accesezi funcția Detectare vulnerabilități, ți se va face o introducere referitoare la această caracteristică. Selectează **PORNIRE SCANARE** pentru a continua, apoi așteaptă ca Bitdefender să verifice sistemul tău pentru a detecta eventualele vulnerabilități.

● Actualizări Windows importante

Se afișează o listă de actualizări Windows importante care nu sunt instalate pe computerul tău. Ar putea fi necesară repornirea sistemului pentru a permite finalizarea instalării de către Bitdefender.

Reține că instalarea actualizărilor poate dura câteva minute.

● Actualizări aplicații

Pentru a vedea informațiile despre aplicația care urmează a fi actualizată, clic pe numele acesteia din listă.

Dacă o aplicație nu este la zi, accesează **DESCĂRCARE VERSIUNE NOUĂ** pentru a descărca versiunea ce mai recentă.

● Conturi Windows vulnerabile

Puteti vedea lista conturilor de utilizator Windows configurate pe calculatorul dumneavoastră și nivelul de protecție asigurat de parola acestora.

Puteți să-i solicitați utilizatorului să schimbe parola la următoarea autentificare sau puteți schimba dumneavoastră parola imediat.



Pentru a seta o nouă parolă pentru sistemul tău, selectează **Schimbă parola acum**.

Pentru a crea o parolă puternică, îți recomandăm să utilizezi o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, \$ sau @).

● **Rețele Wi-Fi și routere**

Pentru a afla mai multe despre rețeaua wireless și routerul la care ești conectat, clic pe numele acesteia din listă. Dacă se recomandă să setezi o parolă mai puternică pentru rețeaua ta de acasă, asigură-te că urmezi instrucțiunile noastre, astfel încât să poți rămâne conectat fără să-ți faci griji cu privire la confidențialitatea datelor tale.

Atunci când sunt disponibile și alte recomandări, urmează instrucțiunile pentru a te asigura că rețeaua ta de acasă este protejată de ochii iscoditori ai hackerilor.

4.6.2. Cu ajutorul monitorizării automate a vulnerabilităților

Bitdefender scanează sistemul împotriva vulnerabilităților la intervale regulate, în fundal și păstrează înregistrări ale problemelor detectate în fereastra **Notificări**.

Pentru a verifica și soluționa problemele detectate:

1. Efectuează clic pe **Notificări** din meniul de navigare al interfeței **Bitdefender**.
2. În fila **Toate**, selectează notificarea privind scanarea Vulnerabilităților.
3. Puteți vizualiza informații detaliate cu privire la vulnerabilitățile sistemului detectate. În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedați după cum urmează:
 - Dacă sunt disponibile actualizări Windows, efectuează clic pe **Instalare**.
 - Dacă actualizarea automată Windows este dezactivată, faceți clic **Activare**.
 - Dacă o aplicație nu este actualizată, efectuează clic pe **Actualizează acum** pentru a găsi un link către pagina furnizorului, de unde poți instala cea mai recentă versiune a aplicației respective.
 - Dacă un cont de utilizator Windows are o parolă slabă, faceți clic pe **Modificare parolă** pentru a forța utilizatorul să modifice parola la



următoarea conectare sau schimbați-o chiar dumneavoastră. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, \$ sau @).

- Dacă funcția de executare automată Windows este activată, faceți clic pe **Remediere** pentru a o dezactiva.
- Dacă routerul pe care l-ai configurat are configurată o parolă slabă, efectuează clic pe **Modificare parolă** pentru a accesa interfața din care poți configura o parolă puternică.
- Dacă rețeaua la care ești conectat conține vulnerabilități care pot supune sistemul tău unor riscuri, fă clic pe **Modificare setări Wi-Fi**.

Pentru a configura setările de monitorizare a vulnerabilităților:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În modulul **VULNERABILITATE**, efectuează clic **Setări**.



Important

Pentru a primi informații automate cu privire la vulnerabilitățile sistemului sau aplicației, mențineți opțiunea **Vulnerabilitate** activată.

3. Selectați vulnerabilitățile sistemului care doriți să fie verificate în mod regulat, cu ajutorul comutatoarelor corespunzătoare.

Actualizări Windows

Verificați dacă sistemul de operare Windows are instalate cele mai recente actualizări de securitate importante de la Microsoft.

Actualizări aplicații

Verificați dacă aplicațiile instalate pe sistemul dvs. sunt actualizate. Aplicațiile neactualizate pot fi exploatare de software-uri periculoase, expunându-vă computerul la atacuri din exterior.

Parole utilizatori

Verifică dacă parolele pentru conturile de Windows și routerele configurate pe sistem sunt ușor de descoperit sau nu. Setând parole care sunt greu de ghicit (parole puternice), va fi mai mult mai dificil pentru hackeri să pătrundă în sistemul dumneavoastră. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, \$ sau @).



Redare automată

Verificați starea caracteristicii de executare automată Windows. Această caracteristică permite pornirea aplicațiilor în mod automat direct de pe CD, DVD, unități USB sau alte dispozitive externe.

Anumite tipuri amenințări folosesc funcția de executare automată pentru a se răspândi de la suporturile media amovibile în computer. De aceea se recomandă să dezactivați această caracteristică Windows.

Evaluare securitate rețele Wi-Fi

Verifică dacă rețeaua wireless de acasă la care ești conectat este sigură sau nu și dacă are vulnerabilități. De asemenea, verifică dacă parola routerului de acasă este suficient de puternică și află cum o poți face mai sigură.

Majoritatea rețelelor wireless neprotejate sunt nesigure, permițând astfel hackerilor să aibă acces la activitățile tale private.



Notă

Dacă dezactivați monitorizarea pentru o anumită vulnerabilitate, posibilele probleme aferente nu vor mai fi înregistrate în fereastra Notificări.

4.6.3. Evaluare securitate rețele Wi-Fi

Atunci când te deplasezi, lucrezi dintr-o cafenea sau aștepți în aeroport, conectarea la o rețea wireless publică pentru a face plăți, verifica e-mail-ul sau conturile pe rețelele sociale poate fi soluția cea mai rapidă. Însă pot exista curioși care să încerce să-ți fure datele personale, urmărind informațiile care trec prin rețea.

Datele personale includ parolele și numele de utilizator pe care le folosești pentru a-ți accesa conturile online, cum ar fi căsuțele de e-mail, conturile bancare, conturile de rețele sociale, dar și mesajele pe care le trimiți.

De obicei, rețelele wireless publice sunt cel mai probabil nesigure deoarece nu necesită parolă la autentificare sau, dacă au parolă, aceasta poate fi pusă la dispoziția oricui dorește să se conecteze. Mai mult, pot exista rețele periculoase sau de tip honeypot, care reprezintă o țintă pentru infractorii cibernetici.

Pentru a te proteja împotriva pericolelor hotspot-urilor wireless publice nesecurizate sau necriptate, funcția Asistență securitate Wi-Fi Bitdefender



analizează cât de sigură este o rețea wireless și, atunci când este nevoie, îți recomandă să utilizezi **Bitdefender VPN**.

Funcția Asistență Securitate Wi-Fi Bitdefender oferă informații despre:

- **Rețele Wi-Fi acasă**
- **Rețele Wi-Fi de la birou**
- **Rețele Wi-Fi publice**

Activarea sau dezactivarea notificărilor pentru Asistență Securitate Wi-Fi

Pentru a activa sau dezactiva notificările pentru Asistență Securitate Wi-Fi:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În modulul **VULNERABILITATE**, efectuează clic **Setări**.
3. În fereastra **Setări**, activează sau dezactivează opțiunea **Evaluare securitate rețele Wi-Fi**.

Configurarea rețelei Wi-Fi de acasă

Pentru a porni configurarea rețelei tale de acasă:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **VULNERABILITĂȚI**, efectuează clic pe **Securitate Wi-Fi**.
3. În secțiunea **Wi-Fi acasă**, accesează **SELECTEAZĂ WI-FI ACASĂ**.

Se va afișa o listă a rețelelor wireless la care te-ai conectat până în prezent.

4. Găsește rețeaua ta de acasă și apoi fă clic pe **SELECTEAZĂ**.

Dacă o rețea de acasă este considerată nesecurizată sau nesigură, sunt afișate recomandări de configurare pentru îmbunătățirea securității.

Pentru a șterge rețeaua wireless pe care ai setat-o ca fiind rețeaua ta de acasă, fă clic pe butonul **ȘTERGERE**.

Pentru a adăuga o nouă rețea wireless ca rețea de acasă, accesează opțiunea **Selectează o nouă rețea Wi-Fi acasă**.



Configurarea rețelei Wi-Fi de acasă

Pentru a începe configurarea rețelei tale de la birou:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **VULNERABILITĂȚI**, efectuează clic pe **Securitate Wi-Fi**.
3. În fila **Wi-Fi birou**, accesează opțiunea **SELECTEAZĂ WI-FI BIROU**.
Se va afișa o listă a rețelelor wireless la care te-ai conectat până în prezent.
4. Găsește rețeaua ta de la birou și apoi clic pe **SELECTEAZĂ**.

Dacă o rețea de birou este considerată nesecurizată sau nesigură, sunt afișate recomandări de configurare pentru îmbunătățirea securității.

Pentru a șterge rețeaua wireless pe care ai setat-o ca fiind rețeaua ta de birou, accesează opțiunea **ȘTERGE**.

Pentru a adăuga o nouă rețea wireless ca rețea de birou, accesează opțiunea **Selectează o nouă rețea Wi-Fi de birou**.

Wi-Fi Public

Atunci când ești conectat la o rețea nesecurizată sau nesigură, este activat profilul Wi-Fi public. Cât timp acest profil este activ, Bitdefender Total Security este configurat pentru a pune în aplicare automat următoarele setări:

- Funcția Advanced Threat Defense este activă
- Firewall-ul Bitdefender este pornit și următoarele setări sunt aplicate pentru adaptorul tău wireless:
 - Mod ascuns - PORNIT
 - Tipul rețelei - Public
- Următoarele setări din Online Threat Prevention sunt activate:
 - Scanare web criptată
 - Protecție împotriva fraudelor
 - Protecție împotriva tentativelor de phishing
- Devine disponibil un buton care deschide Bitdefender Safepay™. În acest caz, protecția Hotspot pentru rețele nesecurizate este activată în mod implicit.



Verificarea informațiilor despre rețelele Wi-Fi

Pentru a verifica informațiile despre rețelele wireless la care te conectezi de obicei:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **VULNERABILITĂȚI**, efectuează clic pe **Securitate Wi-Fi**.
3. În funcție de informațiile de care ai nevoie, selectează una dintre următoarele trei secțiuni: **Wi-Fi acasă**, **Wi-Fi birou** sau **Wi-Fi public**.
4. Fă clic pe **Vizualizare detalii** din dreptul rețelei despre care dorești să afli mai multe informații.

Există trei tipuri de rețele wireless filtrate în funcție de importanța lor, fiecare marcat printr-o anumită pictogramă:

■ ❌ ■ **Rețeaua Wi-Fi este nesigură** - indică faptul că nivelul de securitate al rețelei este scăzut. Aceasta înseamnă că utilizarea ei prezintă un nivel ridicat de risc și nu se recomandă să efectuezi plăți sau să-ți verifici conturile bancare fără o protecție suplimentară. În astfel de situații, îți recomandăm să utilizezi Bitdefender Safepay™ cu funcția de protecție Hotspot pentru rețele nesecurizate activată.

■ ■ ■ **Rețeaua Wi-Fi este nesigură** - indică faptul că nivelul de securitate al rețelei este moderat. Aceasta înseamnă că poate avea vulnerabilități și nu se recomandă să efectuezi plăți sau să-ți verifici conturile bancare fără o protecție suplimentară. În astfel de situații, îți recomandăm să utilizezi Bitdefender Safepay™ cu funcția de protecție Hotspot pentru rețele nesecurizate activată.

■ ■ ■ **Rețeaua Wi-Fi este sigură** - indică faptul că rețeaua pe care o folosești este sigură. În acest caz, poți folosi date confidențiale pentru realizarea operațiunilor online.

Atunci când efectuați clic pe link-ul **Vizualizare detalii** din dreptul fiecărei rețele, se afișează următoarele detalii:

- **Securitate** - aici puteți vedea dacă rețeaua selectată este securizată sau nu. Rețelele necriptate pot face ca datele pe care le folosești să fie expuse.
- **Tip de criptare** - aici poți vedea tipul de criptare folosit de rețeaua selectată. Unele tipuri de criptare pot fi nesigure. Prin urmare, îți recomandăm să verifici informațiile despre tipul de criptare afișat pentru a te asigura că ești protejat în timp de navighezi pe internet.



- **Canal/Frecvență** - aici poți vizualiza frecvența canalului utilizat de rețeaua selectată.
- **Complexitatea parolei** - aici poți vedea cât de puternică este parola. Te rugăm să reții că rețelele cu parole slabe reprezintă o țintă pentru infractorii cibernetici.
- **Tipul autentificării** - aici poți verifica dacă rețeaua selectată este sau nu protejată prin parolă. Se recomandă să te conectezi numai la rețele cu parole puternice.
- **Tip de autentificare** - aici poți vedea tipul de autentificare folosit de rețeaua selectată.

4.7. Protecție video și audio

Din ce în ce mai multe amenințări sunt concepute astfel încât să acceseze camerele web și microfoanele încorporate. Pentru a împiedica accesul neautorizat la camera web și pentru a te informa ce aplicații nesigure accesează microfonul dispozitivului tău și când, Bitdefender Video & Audio include:

- **Protecție cameră web**
- **Monitorizare Microfon**

4.7.1. Protecție cameră web

Faptul că hackerii pot prelua controlul asupra camerei web pentru a vă spiona nu mai este o noutate, iar soluțiile de protejare a acesteia, cum ar fi revocarea drepturilor aplicațiilor, dezactivarea camerei integrate a dispozitivului sau acoperirea ei nu sunt foarte practice. Pentru a împiedica eventualele încercări de a obține controlul asupra confidențialității dumneavoastră, funcția Bitdefender Webcam Protection monitorizează în permanență aplicațiile care încearcă să obțină acces la camera web și le blochează pe acelea care nu figurează ca fiind sigure.

Ca măsură de siguranță, vei fi notificat de fiecare dată când o aplicație nesigură va încerca să obțină acces la camera ta.

Activarea sau dezactivarea funcției Webcam Protection

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.



2. În secțiunea **PROTECȚIE VIDEO ȘI AUDIO**, selectează opțiunea **Setări**.
3. În fereastra **Webcam**, pornește sau oprește butonul corespunzător.

Configurarea funcției Webcam Protection

Acum puteți configura ce reguli să fie aplicate atunci când o aplicație încearcă să obțină acces la camera dvs. web, urmând acești pași:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PROTECȚIE VIDEO ȘI AUDIO**, selectează opțiunea **Setări**.
3. Selectați secțiunea **Cameră web**.

Sunt disponibile următoarele opțiuni:

Reguli pentru blocarea aplicațiilor

- **Blochează orice acces la camera web** - nicio aplicație nu va putea accesa camera dvs. web.
- **Blocați accesul browserelor la camera web** - niciun browser web în afară de Internet Explorer și Microsoft Edge nu va avea acces la camera dvs. web. Datorită procedurii aplicațiilor din Windows Store de a rula în cadrul unui singur proces, Internet Explorer și Microsoft Edge nu pot fi detectate de Bitdefender ca fiind browsere web, prin urmare sunt exceptate de la această setare.
- **Setează drepturile de acces pentru aplicații pe baza preferințelor comunității** - dacă majoritatea utilizatorilor Bitdefender consideră o aplicație utilizată în mod frecvent ca fiind inofensivă, atunci accesul acesteia la camera web va fi setat automat pe Permite. Dacă o aplicație folosită în mod frecvent este considerată ca fiind periculoasă de mulți utilizatori, atunci accesul acesteia va fi setat automat pe Blocat.

Vei fi informat de fiecare dată când una dintre aplicațiile tale instalate vor fi incluse în lista de aplicații blocate de către majoritatea utilizatorilor Bitdefender.

Notificări

- **Notificare în momentul în care aplicațiile permise se conectează la camera web** - vei fi notificat de fiecare dată când o aplicație permisă îți va accesa camera web.




Adăugarea aplicațiilor în lista Webcam Protection

Aplicațiile care încearcă să se conecteze la camera web sunt detectate automat în funcție de comportamentul lor și preferințele comunității, iar accesul acestora este permis sau blocat. Cu toate acestea, puteți configura manual ce acțiune doriți să fie întreprinsă urmând acești pași:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PROTECȚIE VIDEO ȘI AUDIO**, selectează **Acces cameră web**.
3. La prima utilizare a funcției Webcam Protection, ți se prezintă această funcție.
4. Efectuează clic pe link-ul dorit:
 - **Selectează aplicațiile Windows Store pentru a adăuga la lista de permisiuni** - este afișată o listă cu aplicațiile Windows Store detectate. Activează butoanele de lângă aplicațiile pe care dorești să le adaugi pe listă.
 - **Începe să adaugi aplicații la lista de acces pentru webcam** - mergi la fișierul de tip .exe pe care dorești să îl adaugi în listă, apoi efectuează clic pe **OK**.



Pentru a adăuga aplicații suplimentare, faceți clic pe **Adaugați în listă o nouă aplicație**.

Pentru a vizualiza ce opțiuni au ales utilizatorii Bitdefender pentru aplicația selectată, efectuați clic pe pictograma .

În această fereastră se vor afișa aplicațiile care vor solicita acces la camera web, alături de data și ora ultimei activități.

Vei fi notificat de fiecare dată când una dintre aplicațiile permise este blocată de către utilizatorii Bitdefender.

Pentru a opri accesul unei aplicații adăugate la camera dvs. web, faceți clic

pe pictograma . Pictograma se transformă în , ceea ce înseamnă că aplicația selectată nu va avea acces la camera dvs. web.



4.7.2. Monitorizare microfon

Aplicațiile de tip rogue pot accesa microfonul inclus în mod silențios sau în fundal fără consimțământul dvs. Pentru a vă face conștient cu privire la posibilele programe malițioase de tip exploits, monitorizare Bitdefender Microphone vă va notifica despre aceste evenimente. Astfel, nicio aplicație nu va putea obține acces la microfonul dvs. fără ca dvs. să știți acest lucru.

Activarea sau dezactivarea monitorului pentru Microfon

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PROTECȚIE VIDEO ȘI AUDIO**, selectează opțiunea **Setări**.
3. Selectați fila **Microfon**.
4. În fereastra **Microfon**, porniți sau opriți butonul corespunzător.

Configurarea notificărilor pentru monitorul de Microfon

Pentru a configura ce notificări ar trebui să apară când aplicațiile încearcă să obțină acces la microfonul dvs., urmați pașii de mai jos:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PROTECȚIE VIDEO ȘI AUDIO**, selectează opțiunea **Setări**.
3. Selectați fila **Microfon**.

Notificări

- **Anunță-mă atunci când aplicația încearcă să acceseze microfonul**
- **Anunță-mă atunci când browser-ele accesează microfonul**
- **Anunță-mă atunci când aplicații nesecurizate îmi accesează microfonul**
- **Afișați notificația în baza alegerii utilizatorilor Bitdefender**


Adăugarea de aplicații în lista de monitorizare a Microfonului

Aplicațiile care vor încerca să se conecteze la microfonul dvs. vor fi detectate automat și adăugate la lista de Notificări. Cu toate acestea, puteți configura manual individual dacă o notificare trebuie afișată sau nu prin respectarea următorilor pași:





1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PROTECȚIE VIDEO ȘI AUDIO**, selectează **Monitorizare microfon**.
3. La prima accesare a Monitorizării pentru microfon, vi se prezintă această funcție.
4. Efectuează clic pe link-ul dorit:
 - **Selectați aplicațiile Windows Store de adăugat în listă** - este afișată o listă cu aplicațiile detectate din Windows Store. Activează butoanele de lângă aplicațiile pe care dorești să le adaugi pe listă.
 - **Începe să adaugi aplicații în listă** - navighează la fișierul de tip .exe pe care dorești să îl adaugi în listă, apoi selectează **OK**.

Pentru a adăuga aplicații suplimentare, faceți clic pe **Adaugați în listă o nouă aplicație**.

Pentru a vizualiza ce opțiuni au ales utilizatorii Bitdefender pentru aplicația selectată, efectuați clic pe pictograma .

În această fereastră se vor afișa aplicațiile care vor solicita acces la microfon, alături de data și ora ultimei activități.

Pentru a nu mai primi notificări cu privire la activitatea unei aplicații adăugate,

faceți clic pe pictograma . Pictograma se transformă în , ceea ce înseamnă că nicio notificare Bitdefender nu va fi afișată când aplicația selectată va încerca să vă acceseze microfonul.

4.8. Protecție Fișiere

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.

Infestarea se poate împrăști prin e-mail-uri, prin descărcarea fișierelor atașate sau prin vizitarea site-urilor infestate și instalarea unor aplicații malițioase fără a informa utilizatorul ce se întâmplă cu sistemul.



Aplicațiile ransomware pot avea unul dintre următoarele comportamente care împiedică utilizatorul să acceseze sistemul:

- Crijtează fișierele sensibile și personale și nu permite descrierea decând după plata răscumpărării de către victimă.
- Blochează ecranul calculatorului și afișează un mesaj prin care se solicită o anumită sumă de bani. În acest caz, niciun fișier nu este criptat, utilizatorul este forțat să efectueze plata.
- Blochează funcționarea aplicațiilor.

Cu ajutorul modulului Bitdefender Protecție Fișiere, îți poți proteja fișierele personale, precum documente, fotografiile sau filme, împotriva atacurilor ransomware.



Notă

Advanced Threat Defense și Protecție Fișiere reprezintă două straturi de protecție împotriva programelor ransomware. Caracteristica Advanced Threat Defense este cea care oprește atacurile ransomware în zonele de importanță critică ale sistemului tău, în timp ce caracteristica Protecție Fișiere se asigură că niciun fișier important de pe calculatorul tău nu este criptat.

4.8.1. Activarea și dezactivarea caracteristicii Protecție Fișiere

Pentru a activa sau dezactiva caracteristica Protecție Fișiere:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **PROTECȚIE FIȘIERE**, activează sau dezactivează opțiunea.

De fiecare dată când o aplicație încearcă să acceseze unul dintre fișierele protejate, se afișează o fereastră pop-up Bitdefender. Poți permite sau bloca accesul.



Notă

Caracteristica Protecție Fișiere nu este activată în mod implicit.

4.8.2. Protejați fișierele personale contra atacurilor ransomware

Dacă dorești să creezi un paravan de protecție pentru fișierele tale personale:



1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **PROTECȚIE FIȘIERE**, efectuează clic pe **Directoare protejate**.
3. La prima accesare a Directoarelor protejate, ți se prezintă această funcție. Efectuează clic pe **PROTEJEAZĂ MAI MULTE DIRECTOARE** pentru a continua.
4. Selectează directorul pe care dorești să-l protejezi și apoi efectuează clic pe **OK**.

Pentru a adăuga directoare suplimentare, efectuează clic pe linkul **Protejează mai multe directoare**. În mod alternativ, glisează directoarele în această fereastră.

În mod implicit, directoarele Pictures, Videos, Documents și Music sunt protejate împotriva atacurilor. Datele personale stocate în fișierul online care găzduiește servicii cum ar fi Box, Dropbox, Google Drive și OneDrive sunt, de asemenea, incluse în mediul protejat, cu condiția ca aplicațiile să fie instalate în sistem.

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



Notă

Directoarele personalizate pot fi protejate doar pentru utilizatorii curenți. Fișierele de sistem și de aplicații nu pot fi adăugate la excepții.

4.8.3. Configurarea accesului la aplicații

Aceste aplicații 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 are un comportament normal, îi poți permite accesul urmând acești pași:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **PROTECȚIE FIȘIERE**, dă clic pe **Acces aplicație**.
3. Vor apărea aici aplicațiile care au solicitat modificarea unor fișiere din directoarele tale protejate. Activează butonul din dreptul aplicației despre care ești convins că este sigură.



În aceeași fereastră, poți dezactiva protecția ransomware pentru anumite aplicații dezactivând butonul corespunzător.

Dacă dorești să adaugi noi aplicații în listă, efectuează clic pe linkul **Adăugă în listă o aplicație nouă**.

4.8.4. Protecție la pornire

Nu este un secret că multe aplicații periculoase sunt configurate pentru a rula la pornirea sistemului, fapt care poate afecta grav aparatul. Protecția Bitdefender pentru timpul de pornire scanează toate zonele critice ale sistemului, înainte de încărcarea tuturor fișierelor, cu zero impact asupra sistemului.

Pentru a dezactiva protecția la pornirea sistemului:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **PROTECȚIE FIȘIERE**, dă clic pe **Setări**.
3. Dezactivează **Protecție la pornire**.



Notă

Aplicațiile adăugate în lista de excepții vor fi scanate și tratate în mod corespunzător.

4.9. Remediere ransomware

Funcția Remediere ransomware Bitdefender face un backup al fișierelor tale, precum documente, fotografiile, clipuri video sau muzică, pentru a se asigura că acestea sunt protejate împotriva deteriorării sau a pierderii în cazul unei criptări ransomware. De fiecare dată când este detectat un atac ransomware, Bitdefender va bloca toate procesele implicate în atac și va începe procesul de remediere. Astfel, vei putea recupera întregul conținut al fișierelor tale fără să plătești vreo răscumpărare.

Activarea sau dezactivarea funcției Remediere ransomware

Pentru a activa sau dezactiva funcția Remediere ransomware:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.



2. În secțiunea **REMEDIERE RANSOMWARE**, activează sau dezactivează opțiunea.



Notă

Pentru a te asigura că fișierele tale sunt protejate împotriva atacurilor ransomware, îți recomandăm să păstrezi activă opțiunea Remediere ransomware.

Activarea sau dezactivarea restabilirii automate

Restabilirea automată se asigură că fișierele tale sunt restabilite automat în eventualitatea unei criptări ransomware.

Pentru a activa sau dezactiva restabilirea automată:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **REMEDIERE RANSOMWARE**, selectează **Setări**.
3. Activează sau dezactivează funcția **Restabilire automată**.

Vizualizarea fișierelor restabilite automat

Atunci când opțiunea **Restabilire automată** este activată, Bitdefender va restabili automat fișierele criptate de ransomware. Astfel, te poți bucura de o experiență fără griji de utilizare a computerului știind că fișierele tale sunt în siguranță.

Pentru a vizualiza fișierele care au fost restabilite automat:

1. Efectuează clic pe **Notificări** din meniul de navigare al interfeței **Bitdefender**.
2. În fila **Toate**, selectează notificarea privind cel mai recent comportament ransomware remediat, apoi apasă pe **Fișiere restabilite**.

Este afișată lista fișierelor restabilite. Tot aici poți vedea și locația în care au fost restabilite fișierele tale.

Restabilirea manuală a fișierelor criptate

În cazul în care trebuie să restabilești manual fișierele criptate de ransomware, urmează acești pași:



1. Efectuează clic pe **Notificări** din meniul de navigare al interfeței **Bitdefender**.
2. În fila **Toate**, selectează notificarea privind cel mai recent comportament ransomware detectat, apoi apasă pe **Fișiere criptate**.
3. Este afișată lista fișierelor criptate.

Pentru a continua, selectează **RECUPERARE FIȘIERE**.

4. În cazul în care procesul de restabilire eșuează, fie complet, fie parțial, trebuie să selectezi locația în care să fie salvate fișierele decriptate. Apasă pe **LOCAȚIE RESTAURARE** și apoi selectează o locație de pe PC-ul tău.
5. Va apărea o fereastră de confirmare.

Selectează **FINALIZARE** pentru a încheia procesul de restabilire.

Fișierele cu următoarele extensii pot fi restabilite în cazul în care sunt criptate:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb; .doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html; .ico; .jar; .java; .jpeg; .jpg; .js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp; .odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

Adăugarea aplicațiilor în lista de excepții

Poți configura reguli de exceptare pentru aplicațiile sigure astfel încât funcția Remediere ransomware să nu le blocheze dacă efectuează acțiuni specifice programelor ransomware.

Pentru a adăuga aplicații în lista de excepții a funcției Remediere ransomware:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **REMEDIERE RANSOMWARE**, selectează **Excepții**.
3. Pentru a adăuga noi aplicații în listă, selectează **Adăugă în listă o aplicație nouă**.



4.10. File Encryption

Funcția Bitdefender File Encryption îți permite să crezi pe computerul tău partiții logice criptate și protejate prin parolă (seifuri), unde poți stoca în deplină siguranță documentele tale confidențiale. Datele stocate în seifuri pot fi accesate doar de către utilizatorii care cunosc parola.

Parola vă permite să deschideți un seif, să stocați date în acesta și să îl închideți pentru a-i proteja conținutul. Când seiful este deschis, puteți adăuga fișiere noi și puteți accesa sau modifica fișierele existente.

La nivel fizic, seiful este de fapt un fișier criptat de pe hard discul dumneavoastră, având extensia `bvd`. Deși fișierele fizice reprezentând seifurile pot fi accesate prin intermediul altor sisteme de operare (cum ar fi Linux), informația stocată pe acestea nu poate fi citită deoarece acestea sunt criptate.

Seifurile pentru fișiere pot fi administrate din **fereastra Bitdefender** sau prin utilizarea meniului contextual Windows și a partiției logice asociate seifului.

Administrarea seifurilor pentru fișiere

Pentru a administra seifurile tale de fișiere din Bitdefender:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **FILE ENCRYPTION**, dă clic pe **Setări**.

Seifurile pentru fișiere existente se afișează în această fereastră.

Crearea seifurilor pentru fișiere

Pentru a crea un seif nou:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **FILE ENCRYPTION**, efectuează clic pe **Creează un seif nou**.
3. Specificați locația și numele seifului pentru fișiere.
 - Tastați numele seifului în câmpul corespunzător.
 - Efectuează clic pe **CAUȚĂ**, selectează locația seifului și memorează fișierul seif cu denumirea dorită.



4. Selectați litera unei unități din meniul corespunzător. Atunci când deschideți seiful, puteți vedea în My Computer o partiție virtuală denumită cu litera selectată.
5. Dacă dorești să modifice dimensiunea implicită (100 MB) a seifului, folosește săgețile sus/jos din caseta **Mărime seif (MB)**.
6. Introduceți noua parolă a seifului în câmpurile **Parolă nouă** și **Confirmare parolă**. Parola trebuie să conțină minim 8 caractere. Oricine va încerca să deschidă seiful și să acceseze fișierele acestuia va trebui să furnizeze parola.
7. Efectuează clic pe **CREEAZĂ**.

Bitdefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana.

Pentru a crea mai rapid un nou seif, clic dreapta pe desktop sau într-un director de pe computer, selectează **Bitdefender > Bitdefender Criptare fișiere** și apoi **Creează un seif nou**.



Notă

Poate fi convenabil să salvați toate seifurile de fișiere în același loc. Astfel, le veți găsi mai ușor.

Importul unui seif de fișiere

Pentru a importa un seif de fișier salvat local:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **FILE ENCRYPTION**, efectuează clic pe **Importă seif**.
3. Căutați locația seifului dumneavoastră și selectați-o (fișierul .bvd).
4. Faceți clic pe **Deschide**.

Deschiderea seifurilor pentru fișiere

Pentru a accesa și a lucra cu fișierele stocate într-un seif, trebuie mai întâi să deschideți seiful. Atunci când deschideți seiful, puteți vedea o partiție virtuală în My Computer. Partiția este denumită cu litera atribuită seifului.

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.



2. În secțiunea **FILE ENCRYPTION**, dă clic pe **Setări**.
3. Selectează seiful pe care dorești să îl deschizi și apoi efectuează clic pe **DEBLOCARE**.
4. Introdu parola solicitată și apoi efectuează clic pe **OK**.
5. Efectuează clic pe **DESCHIDE** pentru a deschide seiful tău.

Bitdefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana.

Pentru a deschide mai rapid un seif, localizați pe calculator, fișierul .bvd care reprezintă seiful pe care doriți să-l deschideți. Efectuează clic dreapta pe fișier, mută cursorul pe **Bitdefender > Seif fișier Bitdefender** și selectează **Deblocare**. Introduceți parola necesară și faceți clic pe **OK**.

Adăugarea fișierelor în seifuri

Înainte de a putea adăuga fișiere sau directoare într-un seif, trebuie să deschideți seiful.

Pentru a adăuga noi fișiere în seif:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **FILE ENCRYPTION**, dă clic pe **Setări**.
3. Selectează seiful în care dorești să adaugi fișiere și apoi efectuează clic pe **DEBLOCARE**.
4. Introdu parola solicitată și apoi efectuează clic pe **OK**.
5. Efectuează clic pe **DESCHIDE** pentru a deschide seiful tău.
6. Adaugă fișiere sau directoare așa cum faci în mod normal în Windows (de exemplu, poți utiliza metoda copiere-inserare).

Pentru a adăuga mai rapid fișiere în seiful tău, efectuează clic dreapta pe fișierul sau directorul pe care dorești să îl copiezi într-un seif, mută cursorul deasupra **Bitdefender > Seif Fișiere Bitdefender** și selectează **Adăugare la Seif Fișiere**.

- Dacă un singur seif este deschis, fișierul sau directorul este copiat direct în acel seif.



- Dacă mai multe seifuri sunt deschise, vi se va solicita să alegeți seiful în care să fie copiat obiectul. Selectați din meniu litera corespunzătoare seifului dorit și faceți clic pe **OK** pentru a copia obiectul.

Închiderea seifurilor

Atunci când ați terminat de lucrat într-un seif pentru fișiere, trebuie să îl închideți pentru a vă proteja datele. Prin închiderea seifului, partiția virtuală corespunzătoare dispare din My Computer. Ca urmare, este complet blocat accesul la datele stocate în seif.

Pentru a bloca un seif:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **FILE ENCRYPTION**, dă clic pe **Setări**.
3. Selectează seiful pe care dorești să îl blochezi și apoi efectuează clic pe **BLOCARE**.

Bitdefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana.

Pentru a bloca mai rapid un seif, efectuează clic dreapta pe fișierul **.bvd** care reprezintă seiful, mută cursorul pe **Bitdefender > Seif fișiere Bitdefender** și selectează **Blocare**.

Ștergerea fișierelor din seifuri

Pentru a elimina fișiere sau directoare dintr-un seif, trebuie ca seiful să fie deschis. Pentru a șterge fișiere sau directoare dintr-un seif:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **FILE ENCRYPTION**, dă clic pe **Setări**.
3. Selectează seiful din care dorești să ștergi fișiere și apoi efectuează clic pe **DEBLOCARE** în cazul în care este blocat.
4. Efectuează clic pe **DESCHIDE**.

Ștergeți fișierele sau directoarele așa cum faceți în mod normal în Windows (de exemplu, faceți clic-dreapta pe un fișier pe care doriți să îl ștergeți și selectați **Delete (Șterge)**).



Modificarea parolei seifului

Parola protejează conținutul unui seif împotriva accesului neautorizat. Numai utilizatorii care cunosc parola pot deschide seiful și pot accesa documentele și datele stocate în acesta.

Un seif trebuie să fie închis pentru a-i putea schimba parola. Pentru a modifica parola unui seif:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **FILE ENCRYPTION**, dă clic pe **Setări**.
3. Selectează seiful pentru care dorești să modifice parola și apoi efectuează clic pe **SETĂRI**.
4. Introduceți parola curentă a seifului în câmpul **Parolă veche**.
5. Introduceți noua parolă a seifului în câmpurile **Parolă nouă** și **Confirmați noua parolă**.



Notă

Parola trebuie să conțină minim 8 caractere. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, \$ sau @).

Bitdefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana.

Pentru a schimba mai rapid parola unui seif, localizați pe calculator fișierul .bvd care reprezintă seiful. Efectuează clic dreapta pe fișier, mută cursorul deasupra opțiunii **Bitdefender > Seif Bitdefender pentru fișiere** și selectează **Modifică parola seifului**.

4.11. Protecția datelor de autentificare cu Password Manager

Folosim calculatorul pentru a face cumpărături online sau pentru a ne plăti facturile, pentru a ne conecta la platformele de socializare sau pentru a ne autentifica în aplicațiile de mesagerie instant.

Dar toată lumea știe că nu este ușor să-ți reamintești parolele.



Iar dacă nu suntem atenți atunci când navigăm pe internet, datele noastre confidențiale, precum adresa de e-mail, ID-ul de mesagerie instant sau datele cardului de credit pot fi compromise.

Păstrarea parolelor sau a datelor personale scrise pe hârtie sau în calculator poate fi periculoasă datorită faptului că acestea ar putea fi accesate și folosite de persoane care vor să fure sau să utilizeze aceste informații. Și nu este un lucru ușor să vă reamintiți fiecare parolă setată pentru conturile dumneavoastră sau pentru site-urile preferate.

Prin urmare, există oare vreo modalitate prin care să ne asigurăm că ne găsim parolele atunci când avem nevoie de ele? Și putem fi siguri că parolele noastre sunt în deplină siguranță întotdeauna?

Modulul Password Manager îți permite să gestionezi parolele, îți protejează confidențialitatea și îți oferă o experiență de navigare sigură.

Folosind o singură parolă master pentru a accesa datele dumneavoastră, Password Manager te ajută să îți păstrezi parolele în deplină siguranță într-un Portofel.

Pentru a asigura cea mai bună protecție pentru activitățile tale online, Password Manager este integrat cu Bitdefender Safepay™, oferindu-ți o soluție unică pentru diversele modalități în care îți pot fi compromise datele.

Password Manager protejează următoarele date personale:

- Informații personale, precum adresa de e-mail sau numărul de telefon
- Date de autentificare pentru site-uri web
- Informații privind contul bancar sau numărul cardului de credit
- Date de acces la conturile de e-mail
- Parole pentru aplicații
- Parole pentru rețelele Wi-Fi

Creare bază de date nouă pentru Portofel

Portofelul Bitdefender este locația în care vă puteți păstra datele personale. Pentru o experiență de navigare mai ușoară, este necesar să creați o bază de date a Portofelului, după cum urmează:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.



2. În secțiunea **PASSWORD MANAGER**, efectuează clic pe **Creează Portofel nou**.
3. Efectuează clic pe **Creare nou**.
4. Introduceți informațiile solicitate în câmpurile corespunzătoare.
 - Eticheta Portofel - introduceți o denumire unică pentru baza de date Portofel.
 - Parola principală - introduceți o parolă pentru Portofel.
 - Reintroducere parolă - reintroduceți parola configurată
 - Indiciu - introduceți un indiciu pentru a vă aminti mai ușor parola.
5. Faceți clic pe **CONTINUĂ**.
6. În acest punct, puteți opta pentru stocarea informațiilor în cloud. Dacă selectați da, datele bancare vor rămâne stocate local pe dispozitiv. Selectează opțiunea dorită, apoi efectuează clic pe **CONTINUĂ**.
7. Selectați browser-ul web din care doriți să importați datele.
8. Efectuează clic pe **FINALIZARE**.

Import bază de date existentă


Pentru a importa o bază de date pentru portofel salvată local:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PASSWORD MANAGER**, efectuează clic pe **Creează Portofel nou**.
3. Efectuează clic pe **DE LA ȚINTĂ**.
4. Navighează la locația de pe dispozitivul tău unde dorești să salvezi baza de date a portofelului și apoi alege un nume pentru aceasta.
5. Faceți clic pe **Deschide**.
6. Introduceți o denumire pentru Portofelul dumneavoastră și parola atribuită la crearea acestuia.
7. Efectuează clic pe **IMPORT**.
8. Selectează programele din care dorești ca Portofelul să importe datele de autentificare și apoi butonul **FINALIZARE**.



Exportați baza de date a Portofelului

Pentru a exporta baza de date a Portofelului:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PASSWORD MANAGER**, efectuează clic pe **Portofelele mele**.
3. Efectuați clic pe pictograma  din portofelul dorit și apoi selectați **Export**.
4. Căutați locația bazei de date a portofelului dumneavoastră și selectați-o (fișierul .db).
5. Faceți clic pe **Save**.




Notă

Portofelul trebuie să fie deschis pentru ca opțiunea **Exportă** să fie disponibilă. Dacă portofelul pe care trebuie să-l exportați este blocat, efectuează clic pe **ACTIVEAZĂ PORTOFEL** și apoi introdu parola atribuită atunci când acesta a fost creat.

Sincronizați portofelele în cloud

Pentru a activa sau dezactiva sincronizarea portofelelor în cloud:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PASSWORD MANAGER**, efectuează clic pe **Portofelele mele**.
3. Efectuați clic pe pictograma  din portofelul dorit și apoi selectați **Setări**.
4. Selectați opțiunea dorită din fereastra afișată și faceți clic pe **Salvare**.



Notă

Portofelul trebuie să fie deschis pentru ca opțiunea **Exportă** să fie disponibilă. Dacă portofelul pe care trebuie să-l sincronizezi este blocat, efectuează clic pe **ACTIVEAZĂ PORTOFEL** și apoi introdu parola atribuită atunci când acesta a fost creat.

Gestionați datele de autentificare pentru Portofel

Pentru a administra parolele tale:



1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PASSWORD MANAGER**, efectuează clic pe **Portofelele mele**.
3. Selectează baza de date dorită pentru Portofel și apoi efectuează clic pe **ACTIVARE PORTOFEL**.
4. Introduceți parola generală și faceți clic pe **OK**.

Se afișează o nouă fereastră. Selectați categoria dorită din partea de sus a ferestrei:

- Identitate
- Site-uri web
- Banking online
- Adrese e-mail
- Aplicații
- Rețele Wi-Fi

Adăugarea/ modificarea datelor de autentificare

- Pentru a adăuga o nouă parolă, selectați categoria dorită din partea de sus, faceți clic pe **+ Adăugare**, introduceți informațiile în câmpurile corespunzătoare și faceți clic pe butonul de Salvare.
- Pentru a edita un obiect din listă, selectați-l și faceți clic pe butonul **Editează**.
- Pentru a șterge o înregistrare, selectați-o și efectuați clic pe butonul **Ștergere**.

Activarea sau dezactivarea protecției Password Manager

Pentru a activa sau dezactiva protecția Password Manager:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PASSWORD MANAGER**, activează sau dezactivează butonul.

Administrarea setărilor Password Manager

Pentru a configura în detaliu parola principală:



1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PASSWORD MANAGER**, efectuează clic pe **Setări**.
3. Selectați secțiunea **Setări securitate**.

Sunt disponibile următoarele opțiuni:

- **Solicită parola principală la conectarea la dispozitivul meu** - ți se va solicita să introduci parola master atunci când accesezi dispozitivul tău.
- **Solicită parola master la deschiderea browserului sau a aplicațiilor** - vi se va solicita să introduceți parola master atunci când accesați un browser sau o aplicație.
- **Nu îmi mai cere parola principală** - nu ți se va solicita să introduci parola principală la accesarea calculatorului, a unui browser sau a unei aplicații.
- **Blochează automat Portofelul atunci când dispozitivul e lăsat nesupravegheat** - ți se va solicita să introduci parola master atunci când revii la dispozitiv după 15 minute.



Important

Vă sfătuim să rețineți parola master sau să o notați și să o păstrați într-un loc sigur. Dacă ați uitat parola, trebuie să reinstalați programul sau să contactați Bitdefender pentru asistență.

Îmbunătățiți-vă experiența în utilizare

Pentru a selecta browserele sau aplicațiile în care dorești să integrezi modulul Password Manager:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PASSWORD MANAGER**, efectuează clic pe **Setări**.
3. Selectați secțiunea **Plugins**.

Bifează o aplicație pentru a utiliza modulul Password Manager și îmbunătățește-ți experiența de utilizare:

- Internet Explorer
- Mozilla Firefox
- Google Chrome



- Safepay

Configurarea funcției de Completare automată

Funcția de Completare automată îți permite să te conectezi mai ușor la site-urile web preferate sau să te autentifici în conturile tale online. La prima introducere a datelor de autentificare și a informațiilor personale în browser-ul web, acestea sunt securizate automat în Portofel.

Pentru a configura setările de **completare automată**:


1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **PASSWORD MANAGER**, efectuează clic pe **Setări**.
3. Selectați secțiunea **Setări completare automată**.
4. Configurați următoarele opțiuni:
 - **Configurează modul în care Password Manager îți securizează datele de autentificare:**
 - **Salvează datele automat în Portofel** - datele de autentificare și alte informații care pot fi identificate, cum ar fi datele personale și cele ale cardului de credit, sunt salvate și actualizate automat în Portofel.
 - **Întreabă-mă de fiecare dată** - vi se va solicita de fiecare dată să confirmați dacă doriți să adăugați datele dumneavoastră în Portofel.
 - **Nu permite salvarea datelor, voi actualiza informațiile manual** - datele pot fi adăugate doar manual în Portofel.
 - **Completare automată a datelor de autentificare:**
 - **Datele de autentificare se completează automat de fiecare dată** - informațiile dumneavoastră sunt introduse automat în browser.
 - **Formulare de completare automată:**
 - **Solicită opțiunile mele de completare când accesez o pagină cu formulare** - se va afișa o fereastră cu opțiunile de completare de fiecare dată când Bitdefender detectează că doriți să efectuați o plată online sau să vă autentificați.



Administrarea informațiilor referitoare la Password Manager din browser

Puteți administra cu ușurință modulul Password Manager direct din browser, pentru a avea toate datele importante la îndemână. Aplicați suplimentară Portofel Bitdefender este acceptată de următoarele browsere: Google Chrome, Internet Explorer și Mozilla Firefox și este, de asemenea, integrată cu Safepay.

Pentru a accesa extensia Portofel Bitdefender, deschideți browser-ul,

permiteți instalarea aplicației suplimentare și faceți clic pe pictograma  de pe bara de instrumente.

Extensia Portofel Bitdefender include următoarele opțiuni:

- Deschide Portofelul - deschide aplicația Portofel.
- Blochează Portofelul - blochează portofelul.
- Pagini web - deschide un submeniu cu toate autentificările la site-uri Internet stocate în Portofel. Apasă **Adaugă pagină web** pentru a adăuga site-uri noi în listă.
- Completează formularele - deschide un submeniu cu informațiile adăugate de tine pentru o anumită categorie. De aici, puteți adăuga date noi în Portofel.
- Generator parolă - enables vă permite să generați parole aleatorii pe care le puteți utiliza pentru conturile noi sau existente. Faceți clic pe **Afișare setări avansate** pentru a seta complexitatea parolei.
- Setări - deschide fereastra de setări a modulului Password Manager.
- Raportează problema - raportează orice problemă întâmpinată în legătură cu Bitdefender Password Manager.

4.12. Anti-tracker

Multe dintre site-urile web pe care le accesezi utilizează instrumente de urmărire de tip tracker pentru a colecta informații despre comportamentul tău, fie pentru a le distribui unor companii terțe, fie pentru a afișa anunțuri mai relevante pentru tine. Astfel, proprietarii site-urilor web fac bani pentru a putea oferi conținut gratuit sau pentru a continua să funcționeze. Pe lângă colectarea de informații, tracker-ele pot încetini experiența ta de navigare sau îți pot afecta lățimea de bandă.



Odată ce extensia Bitdefender Anti-tracker a fost activată în browserul web, eviți urmărirea astfel încât datele tale rămân confidențiale în timp ce navighezi online și reduci timpul necesar pentru încărcarea site-urilor web.


Extensia Bitdefender este compatibilă cu următoarele browsere web:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Tracker-ele pe care le detectăm sunt grupate în următoarele categorii:

- **Publicitate** - se utilizează pentru a analiza traficul de pe site-urile web, comportamentul utilizatorilor sau tiparele de trafic generat de utilizatori.
- **Interacțiunea cu clienții** - se utilizează pentru a măsura interacțiunea utilizatorilor cu diferite forme de introducere de informații, cum ar fi chat sau suport.
- **Esențiale** - se utilizează pentru a monitoriza funcționalitățile de importanță critică ale paginilor web.
- **Date de analiză site** - se utilizează pentru a colecta date referitoare la utilizarea paginilor web.
- **Rețele de socializare** - se utilizează pentru a monitoriza audiența pe rețelele de socializare, activitatea și implicarea utilizatorilor pentru diferite platforme de socializare.

Interfața Anti-tracker

Atunci când extensia Bitdefender Anti-tracker este activată, se afișează pictograma  în dreptul barei de căutare a browserului web. De fiecare dată când accesezi un site web, vei observa un contor pe pictogramă, care arată numărul de trackere detectate și blocate. Pentru a vedea mai multe detalii despre tracker-ele blocate, accesează pictograma respectivă pentru a deschide interfața. În afară de numărul de trackere blocate, poți vedea timpul necesar încărcării paginii și categoriile de care aparțin tracker-ele detectate. Pentru a vedea lista site-urilor care practică activități de urmărire, selectează categoria dorită.

Pentru a dezactiva funcția Bitdefender de blocare a tracker-elor pe site-ul pe care îl accesați în momentul respectiv, selectează opțiunea **Întrerupeți protecția pe acest site**. Această setare se aplică numai atâta timp cât site-ul





este deschis și va reveni automat la starea inițială după ce părăsești site-ul web.

Pentru a permite tracker-elor dintr-o anumită categorie să îți monitorizeze activitatea, selectează activitatea dorită și apoi clic pe butonul corespunzător. Dacă te răzgândești, apasă din nou pe același buton.

Dezactivarea Bitdefender Anti-tracker

Pentru a dezactiva Bitdefender Anti-tracker:

● Din browser-ul web:

1. Deschideți browser-ul web.
2. Accesează pictograma  din dreptul barei de adresă a browserului.
3. Accesează pictograma  din colțul din dreapta sus.
4. Utilizează butonul corespunzător pentru dezactivare.



Pictograma Bitdefender devine gri.

● Din interfața Bitdefender:


1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În panoul **ANTI-TRACKER**, selectează **Setări**.
3. Dezactivează butonul corespunzător din dreptul browserului web pentru care dorești să dezactivezi extensia.

Permiterea urmăririi unui site web

Dacă dorești ca activitatea ta să fie urmărită în timp ce accesezi un anumit site web, poți adăuga adresa acestuia în lista de excepții, după cum urmează:

1. Deschideți browser-ul web.
2. Accesează pictograma  din dreptul barei de căutare.
3. Accesează pictograma  din colțul din dreapta sus.
4. Dacă te afli pe site-ul web pe care dorești să-l adaugi la excepții, selectează opțiunea **Adaugă în listă acest site web**.



Dacă dorești să adaugi un alt site web, introdu adresa acestuia în câmpul corespunzător și apoi selectează .

4.13. VPN

Aplicația VPN poate fi instalată din produsul Bitdefender și utilizată ori de câte ori dorești să adaugi un strat suplimentar de protecție conexiunii tale. 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 redirectionat 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, confirmați că ai cunoștință de reglementările aplicabile țării respective și riscurile la care te-ai putea expune.

Instalarea VPN

Aplicația VPN poate fi instalată din interfața Bitdefender, astfel:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **VPN**, efectuează clic pe **Instalare VPN**.
3. În fereastra cu descrierea aplicației VPN, citește **Contractul de abonament** și apoi efectuează clic pe **INSTALARE BITDEFENDER VPN**.

Așteaptă câteva momente până ce fișierele sunt descărcate și instalate.

Dacă este detectată o altă aplicație VPN, îți recomandăm să o dezinstalezi. Dacă instalezi mai multe soluții VPN, este posibil să experimentezi încetiniri ale sistemului sau alte probleme de funcționalitate.

4. Efectuează clic pe **DESCHIDE BITDEFENDER VPN** pentru a finaliza procesul de instalare.



Notă

Bitdefender VPN necesită .Net Framework 4.5.2 sau o versiune ulterioară. În cazul în care nu ai instalat acest pachet, se va afișa o fereastră de notificare. Efectuează clic pe **Instalează .Net Framework** pentru a fi redirecționat către o pagină de unde poți descărca cea mai nouă versiune a acestui software.

Deschiderea conexiunii VPN

Pentru a accesa interfața Bitdefender VPN principală, folosește una dintre metodele următoare:

- Din bara de sistem

1. Efectuează clic pe pictograma  din bara de sistem și apoi pe **Afișare**.

- Din interfața Bitdefender:


1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În panoul **VPN**, efectuează clic pe **Deschidere VPN**.

Interfața VPN

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 adecvat server, în timp ce utilizatorii premium au posibilitatea de a schimba locația serverului la care doresc să se conecteze. Pentru mai multe informații despre abonamentele VPN, accesează „**Abonamente**” (p. 155).

Pentru conectare sau deconectare, pur și simplu efectuează clic pe starea afișată în partea de sus a ecranului sau efectuează click dreapta pe pictograma din bara de sistem. Pictograma din bara de sistem afișează o bifă de culoare verde atunci când aplicația VPN este conectată și o bifă de culoare roșie atunci când aceasta este deconectată.

Când ești conectat, timpul scurs și lățimea de bandă utilizată sunt afișate în partea de jos a interfeței.

Pentru a obține acces la mai multe opțiuni, accesează secțiunea **Meniu** efectuând clic pe  pictograma din stânga sus. Aici aveți la dispoziție următoarele opțiuni:



- **Contul meu** – sunt afișate detalii despre contul tău Bitdefender și abonamentul VPN. Efectuează clic pe **Schimbă contul** dacă dorești să te conectezi cu un alt cont.
- **Setări** – în funcție de nevoile tale, poți personaliza comportamentul produsului tău:
 - poți primi notificări atunci când funcția VPN se conectează sau se deconectează automat
 - lansează automat aplicația VPN la pornirea Windows-ului
 - lansează automat aplicația VPN atunci când dispozitivul tău se conectează la rețele wireless nesecurizate
- **Upgrade la Premium** - dacă folosești versiunea gratuită, poți efectua upgrade la planul premium de aici.
- **Suport** - ești redirectionat către platforma noastră Support Center unde poți citi un articol util despre cum să folosești Bitdefender VPN.
- **Despre** – sunt afișate informații despre versiunea instalată.

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 Family Pack, ceea ce înseamnă că îl vei putea folosi pe toată durata de valabilitate, indiferent de starea abonamentului soluției de securitate. În cazul în care abonamentul Bitdefender Premium VPN expiră, dar există în continuare un abonament activ pentru Bitdefender Family Pack, vei reveni la planul gratuit.

Bitdefender VPN este un produs pentru toate tipurile de platforme, disponibil în cadrul produselor Bitdefender compatibile cu Windows, macOS, Android și iOS. Odată ce faci upgrade la planul Premium, îți vei putea folosi



abonamentul pentru toate produsele, cu condiția să te conectezi cu același cont Bitdefender.

4.14. Securitate Safepay pentru tranzacțiile online

Calculatorul a început să devină principalul instrument pentru cumpărături și tranzacții bancare. Achitarea facturilor, transferul de bani, achiziționarea a cam tot ce vă puteți imagina nu au fost niciodată mai rapide sau mai ușoare.

Aceasta implică transmiterea de informații personale, date de cont și credit, parole și alte tipuri de informații personale prin Internet, cu alte cuvinte, exact tipul de informații pe care infractorii cibernetici sunt foarte interesați să le obțină. Hackerii se străduiesc în permanență să sustragă aceste informații, deci, nu puteți fi niciodată suficient de precauți cu privire la securizarea tranzacțiilor online.

Bitdefender Safepay™ este, în primul rând, un browser protejat, un mediu proiectat pentru a ca tranzacțiile dvs. online să rămână confidențiale și securizate.

Pentru cea mai bună protecție a confidențialității, Bitdefender Password Manager a fost integrat în Bitdefender Safepay™ pentru a te proteja datele ori de câte ori dorești să accesezi locații private online. Pentru mai multe informații, consultați capitolul „*Protecția datelor de autentificare cu Password Manager*” (p. 143).

Bitdefender Safepay™ vă oferă următoarele funcții:

- Blochează accesul la calculatorul dumneavoastră și orice încercări de a realiza capturi ale ecranului dumneavoastră.
- Aceasta îți protejează parolele când navighezi pe internet, cu ajutorul modulului Password Manager.
- Include o tastatură virtuală care, dacă este utilizată, nu permite hackerilor să citească ceea ce introduceți de pe aceasta.
- Este complet independentă de celelalte browsere ale dumneavoastră.
- Include protecție pentru punctele wireless de acces la Internet încorporată pe care o puteți utiliza în cazul conectării la rețele Wi-fi nesecurizate.
- Acceptă marcajele și vă permite să navigați pe site-urile dumneavoastră preferate de tranzacții bancare/cumpărături.



- Nu se limitează la tranzacții bancare și cumpărături online. Orice site poate fi deschis în Bitdefender Safepay™.

Utilizarea Bitdefender Safepay™

În mod implicit, Bitdefender detectează dacă navigați către un site de tranzacții online sau de cumpărături online în orice browser de pe calculatorul dumneavoastră și vă solicită să îl lansați în Bitdefender Safepay™.

Pentru a accesa interfața Bitdefender Safepay™ principală, folosiți una dintre metodele următoare:

- Din **interfața Bitdefender**:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **SAFEPLAY**, selectează **Deschide Safeplay**.

- Din Windows:

- În **Windows 7**:

1. Faceți clic pe **Start** și mergeți la **Toate programele**.
2. Faceți clic pe **Bitdefender**.
3. Faceți clic pe **Bitdefender Safepay™**.

- În **Windows 8 și Windows 8.1**:

Localizați Bitdefender Safepay™ din ecranul de Start Windows (de exemplu, puteți tasta "Bitdefender Safepay™" direct pe ecranul de Start) și apoi faceți clic pe pictograma.

- În **Windows 10**:








Introduceți "Bitdefender Safepay™" în caseta de căutare din bara de sarcini și faceți clic pe pictogramă.

Dacă sunteți obișnuiți cu browserele Internet, nu veți avea probleme în utilizarea Bitdefender Safepay™ - arată și se comportă ca un browser obișnuit:

- introduceți URL-urile pe care doriți să le accesați în bara de adrese.
- adăugați secțiuni pentru a vizita mai multe site-uri în fereastra Bitdefender

Safepay™ făcând clic pe .



- reveniți la navigarea anterioară, mergeți către o altă pagină și reîmprospătați pagini folosind .
- accesați **setările** Bitdefender Safepay™ făcând clic pe  și selectând **Setări**.
- protejează-ți parolele cu **Password Manager** dând clic pe .
- administrați **marcajele** făcând clic pe  de lângă bara de adrese.
- activați tastatura virtuală făcând clic pe .
- măriți sau micșorați dimensiunea browser-ului apăsând simultan tastele **Ctrl** și **+/-** de pe tastatura numerică.
- vizualizați informațiile despre produsul dvs. Bitdefender făcând clic pe  și selectând **Despre**.
- tipăriți informațiile importate printr-un clic pe  și selectați **Tipărire**.



Notă

Pentru a comuta între Bitdefender Safepay™ și ecranul Windows, apăsați tastele **Alt+Tab** sau efectuați clic pe opțiunea **Comută pe Desktop** din colțul din stânga sus al ferestrei.

Configurarea setărilor

Faceți clic pe  și alegeți **Setări** pentru a configura Bitdefender Safepay™:

Aplicați regulile Safepay Bitdefender pentru domeniile accesate

Aici vor apărea site-urile web pe care le-ai adăugat la **Bookmarks** cu opțiunea **Deschidere automată în Safepay** activată. Dacă dorești să dezactivezi deschiderea automată cu Bitdefender Safepay™ a unui site web din listă, clic pe **x** din dreptul înregistrării dorite din coloana **Ștergere**.



Blocare pop-up-uri

Puteți opta pentru blocarea pop-up-urilor făcând clic pe comutatorul corespunzător.

De asemenea, puteți crea o listă a site-urilor pe care permiteți afișarea pop-up-urilor. Este recomandat ca lista să conțină doar site-uri web în care aveți deplină încredere.

Pentru a adăuga un site în listă, introdu adresa acestuia în câmpul corespunzător și efectuează clic pe **Adaugă domeniu**.

Pentru a șterge un site web din listă, selectează x-ul corespunzător înregistrării dorite.

Administrare plugin-uri

Poți opta pentru activarea sau dezactivarea anumitor plugin-uri din Bitdefender Safepay™.

Gestionare certificate

Poți importa certificate din sistemul tău într-un magazin de certificate.

Faceți clic pe **IMPORT CERTIFICATE** și urmați instrucțiunile asistentului pentru a utiliza certificatele în Bitdefender Safepay™.

Utilizați Tastatura Virtuală

Tastatura virtuală va apărea automat atunci când este selectat un câmp de parolă.

Folosește butonul corespunzător pentru a activa sau dezactiva această funcție.

Confirmare imprimare


Activați această opțiune dacă doriți să confirmați înainte ca procesul de tipărire să înceapă.

Administrarea marcajelor

Dacă ați dezactivat detectarea automată a unei părți dintre site-uri sau a tuturor site-urilor sau dacă Bitdefender pur și simplu nu detectează anumite site-uri internet, puteți adăuga marcați în Bitdefender Safepay™ pentru a putea lansa cu ușurință site-urile Internet în viitor.

Urmați pașii de mai jos pentru a adăuga un URL la marcajele Bitdefender Safepay™:



1. Faceți clic pe pictograma  de lângă bara de adrese pentru a deschide pagina Marcaje.



Notă

Pagina Marcaje se deschide în mod implicit la lansarea Bitdefender Safepay™.

2. Faceți clic pe butonul **+** pentru a adăuga un marcaj nou.
3. Introduceți URL-ul și titlul marcajului și apoi faceți clic pe **CREEAZĂ**. Faceți clic pe opțiunea **Deschide automat în Safepay** dacă doriți ca pagina marcată să se deschidă cu Bitdefender Safepay™ de fiecare dată când o accesați. URL-ul este și el adăugat la lista Domeniilor de pe pagina **setări**.

Dezactivarea notificărilor Safepay

Când este detectat un site bancar, produsul Bitdefender este setat să te notifice prin intermediul unei ferestre pop-up.

Pentru a dezactiva notificările Safepay:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În panoul **SAFEPAY**, selectează **Setări**.
3. Dezactivează **Notificările Safepay**.

Utilizarea VPN cu Safepay

Pentru a efectua plăți online într-un mediu sigur în timp ce ești conectat la rețele nesecurizate, produsul Bitdefender poate fi setat să lanseze automat aplicația VPN în același timp cu Safepay.

Pentru a începe utilizarea aplicației VPN împreună cu Safepay:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În panoul **SAFEPAY**, selectează **Setări**.
3. Activează opțiunea **Folosește funcția VPN cu Safepay**.



4.15. Data Protection

Ștergerea permanentă a fișierelor

Atunci când ștergeți un fișier, acesta nu mai poate fi accesat prin mijloace normale. Cu toate acestea, fișierul continuă să existe pe hard disc până ce este suprascris prin copierea altor fișiere.

Opțiunea de ștergere definitivă a fișierelor Bitdefender vă permite să ștergeți definitiv date prin eliminarea fizică a acestora de pe hard disk.

Puteți șterge definitiv și rapid fișiere și directoare din computerul dumneavoastră cu ajutorul meniului contextual Windows urmând pașii de mai jos:

1. Faceți clic dreapta pe un fișier sau director pe care doriți să-l ștergeți definitiv.
2. Selectați **Bitdefender** > **Ștergere definitivă fișiere** din meniul contextual afișat.
3. Efectuează clic pe **ȘTERGE DEFINITIV** și apoi confirmă că dorești să continui procesul.

Așteptați ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.

4. Sunt afișate rezultatele. Efectuați clic pe **Finalizare** pentru a părăsi asistentul.

Ca alternativă, puteți șterge definitiv fișierele din interfața Bitdefender, după cum urmează:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În panoul **DATA PROTECTION**, efectuează clic pe **Ștergere definitivă**.
3. Urmați pașii asistentului de ștergere definitivă a fișierelor:

- a. Efectuați clic pe butonul **ADAUGĂ FIȘIERE** pentru a adăuga fișierele sau directoarele pe care doriți să le ștergeți definitiv.

Ca alternativă, glisați aceste fișiere sau foldere în această fereastră.

- b. Efectuează clic pe **ȘTERGE DEFINITIV** și apoi confirmă că dorești să continui procesul.

Așteptați ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.



c. Sumar

Sunt afișate rezultatele. Efectuați clic pe **Finalizare** pentru a părăsi asistentul.

4.16. Control Parental

Bitdefender Parental Control îți permite să gestionezi și să protejezi activitățile online ale copiilor tăi. De îndată ce ai configurat Bitdefender Parental Control, poți afla cu ușurință ce fac copiii tăi pe dispozitivele pe care le folosesc și unde au fost în ultimele 24 de ore. În plus, pentru a te ajuta să afli mai multe despre ceea ce fac copiii tăi, această caracteristică îți oferă și statistici cu privire la activitățile și interesele lor.

Abonamentul tău Bitdefender include următoarele caracteristici:

- Pe dispozitivele Windows, macOS și Android:
 - Blocarea paginilor web neadecvate.
 - Blocarea unor aplicații, precum jocuri, aplicații de chat, programe de partajare de fișiere și altele.
 - Blocarea utilizării dispozitivului monitorizat.
 - Blocarea accesului la internet pentru anumite intervale de timp (de exemplu în timpul rezervat lecțiilor).
 - Setarea unor restricții de timp pentru utilizarea dispozitivelor.
 - Vizualizarea timpului mediu petrecut în fața ecranului de către copiii tăi pe un anumit dispozitiv.
 - Vizualizarea unui raport cu aplicațiile utilizate pe dispozitivul monitorizat în ultimele 30 de zile.
 - Setează zonele restricționate.
 - Identificarea locației dispozitivului Android al copilului tău.
- Pe dispozitivele iOS:
 - Blocarea apelurilor primite din lista de contacte.
 - Setează zonele restricționate.
 - Identificarea locației dispozitivului iOS al copilului tău.



Dacă dorești să ai acces la mai multe funcții, poți face upgrade la versiunea Premium a Bitdefender Parental Control. Caracteristicile incluse în versiunea Premium sunt:

- Poți vedea dacă copiii tăi au devenit victime ale unui comportament agresiv.
- Poți vedea dacă au avut loc tentative de hărțuire cibernetică de către colegi sau persoane străine în timpul petrecut online.

Funcțiile incluse în versiunea Premium sunt disponibile pentru dispozitivele Windows, macOS, Android și iOS.

Pentru a verifica activitățile online ale copiilor tăi, pentru a gestiona dispozitivele pe care le utilizează aceștia sau pentru a schimba setările de Control parental, este necesar să accesezi contul tău Bitdefender.

Există două posibilități de accesare a contului Bitdefender: fie dintr-un browser web, accesând <https://central.bitdefender.com>, fie din aplicația Bitdefender Central, care poate fi instalată pe dispozitivele Android și iOS.

Pentru a instala aplicația Bitdefender Central pe dispozitivele tale:

- **Pe Android** - caută Bitdefender Central în Google Play și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.
- **Pe iOS** - caută Bitdefender Central în App Store și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.



Notă

În acest material sunt prezentate opțiunile disponibile în platforma web și instrucțiunile aferente.

4.16.1. Accesarea funcției Control parental - Copiii mei

După accesarea secțiunii Control parental, se afișează fereastra **Copiii mei**. Aici poți începe să creezi profiluri pentru copiii tăi, pe care le poți vizualiza și edita ulterior. Odată create, profilurile sunt afișate sub forma unor casete de profil, permițându-ți să le administrezi și să verifici rapid status-ul acestora.

De îndată ce ai creat un profil, poți începe să configurezi setări personalizate mai detaliate pentru a monitoriza și controla accesul copiilor dumneavoastră la internet și la anumite aplicații.

Poți accesa setările funcției Control Parental din Bitdefender Central de pe orice computer sau dispozitiv mobil conectat la internet.



Accesați-vă contul Bitdefender:

- Pe orice dispozitiv cu acces la internet:
 1. Accesați **Bitdefender Central**.
 2. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
 3. Selectează secțiunea **Control parental**.
 4. În fereastra **Copiii mei**, poți gestiona și configura profilurile de Control parental pentru fiecare dispozitiv.
- Din interfața Bitdefender:
 1. Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
 2. În secțiunea **CONTROL PARENTAL**, selectează **Configurare**.

Sunteți redirecționat(ă) la pagina web a contului Bitdefender. Asigură-te că ești conectat(ă) cu datele tale de autentificare.
 3. Selectează funcția **Control parental**.
 4. În fereastra **Copiii mei**, poți gestiona și configura profilurile de Control parental pentru fiecare dispozitiv.



Notă

Asigurați-vă că sunteți conectat la calculator pe contul de administrator. Doar utilizatorii cu drepturi administrative pe sistem (administratorii de sistem) pot accesa și configura Controlul parental.


4.16.2. Creează profiluri pentru copiii tăi

Pentru a începe monitorizarea activităților online ale copiilor tăi, este necesar să configurezi profilurile și să instalezi aplicația Bitdefender Parental Control pe dispozitivele utilizate de aceștia.

Pentru a crea un profil de copil:

1. Accesați **Bitdefender Central**.
2. Selectează secțiunea **Control parental**.
3. Selectează opțiunea **CREAZĂ UN PROFIL DE COPIL** din fereastra **Copiii mei**.



4. Introdu informații specifice, cum ar fi numele, data nașterii sau sexul. Pentru a adăuga o imagine la profilul copilului tău, accesează pictograma  din colțul din dreapta jos al opțiunii **Fotografie de profil**. Selectează **SALVEAZĂ** pentru a continua.

În baza standardelor de dezvoltare a copilului, setarea datei nașterii copilului încarcă automat setările de căutare web considerate corespunzătoare pentru categoria sa de vârstă.

5. Selectează opțiunea **SĂ ADĂUGĂM UN DISPOZITIV**.
6. Dacă dispozitivul copilului tău are deja instalat un produs Bitdefender, selectează dispozitivul acestuia din lista disponibilă și apoi contul pe care dorești să-l monitorizezi. Selectează opțiunea **TRIBUIE**.

În cazul în care copilul tău nu are instalat niciun produs Bitdefender pe dispozitivul pe care îl folosește, selectează **Instalează pe un dispozitiv nou** și apoi **TRIMITE LINKUL PENTRU DESCĂRCARE**. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.


Pe dispozitivul pe care dorești să instalezi Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.



Important

Pe dispozitivele Windows și macOS pe care nu este instalat niciun produs Bitdefender, se va instala tracker-ul de monitorizare Bitdefender Parental Control astfel încât să poți monitoriza activitățile online ale copiilor tăi.

Pe dispozitivele Android și iOS, se va descărca și instala aplicația Bitdefender Parental Control.

Pentru a atribui alte dispozitive, accesează pictograma  din profilul copilului și apoi selectează **Dispozitive**. Urmează instrucțiunile de la pasul 6 din acest capitol.

Instalarea aplicației Bitdefender Parental Control pe dispozitivele Android și iOS

Pentru a monitoriza activitățile online ale copiilor tăi pe dispozitive Android sau iOS, este necesar să instalezi aplicația Parental Control dedicată și apoi să conectezi dispozitivele lor la contul tău Bitdefender. În funcție de dispozitivele deținute de copiii tăi, urmează acești pași:



● Pe Android:

1. Deschide Google Play Store, caută Bitdefender Parental Control și apoi selectează opțiunea ce instalare.
2. Selectează opțiunea **ACCEPTĂ** atunci când ți se va solicita să permiți drepturile de acces. Bitdefender necesită drepturi de acces pentru a te menține la curent cu activitatea copilului tău, iar dacă acestea nu sunt acordate, aplicația nu se va instala.
3. Deschide aplicația Control parental.
4. Când deschizi pentru prima dată aplicația, va fi afișat un program asistent introductiv conținând detalii despre caracteristicile produsului. Selectează **ÎNAINTE** pentru a continua să primești indicații sau apasă pe **OMITERE** pentru a închide asistentul.
5. Pentru a continua instalarea, Bitdefender necesită de aprobarea ta pentru a colecta date cu caracter personal care aparțin copilului tău, care vor fi folosite numai pentru a-ți oferi informații despre activitatea copilului tău. Pentru detalii suplimentare, accesează **Politica de confidențialitate**. Apăsând pe **CONTINUĂ**, îți exprimi acordul pentru colectarea de date cu caracter personal de pe dispozitivul respectiv.
6. Conectează-te la contul tău Bitdefender. Dacă nu ai cont Bitdefender, creează-ți unul folosind opțiunea corespunzătoare. Alternativ, te poți autentifica utilizând un cont Facebook, Google sau Microsoft.
7. Selectează **ACTIVEAZĂ** pentru a fi redirecționat către ecranul din care poți activa opțiunea Accesibilitate pentru această aplicație. Urmează instrucțiunile de pe ecran pentru a configura aplicația în mod corespunzător.
8. Selectează **PERMITE** pentru a fi redirecționat către ecranul din care poți activa opțiunea Activarea accesului la datele privind utilizarea pentru această aplicație. Urmează instrucțiunile de pe ecran pentru a configura aplicația în mod corespunzător.
9. Selectează **ACTIVEAZĂ** pentru a fi redirecționat către ecranul din care poți activa opțiunea Activarea drepturilor de administrator dispozitiv pentru această aplicație. Urmează instrucțiunile de pe ecran pentru a configura aplicația în mod corespunzător.

Aceasta va împiedica deinstalarea de către copilul tău a aplicației Control parental.



10. Asociază dispozitivul cu profilul copilului tău.

● Pe iOS:

1. Deschide App Store, caută Bitdefender Parental Control și apoi selectează opțiunea ce instalare.
2. Pentru a continua instalarea, Bitdefender necesită de aprobarea ta pentru a colecta date cu caracter personal care aparțin copilului tău, care vor fi folosite numai pentru a-ți oferi informații despre activitatea copilului tău. Pentru detalii suplimentare, accesează **Politica de confidențialitate**. Apăsând pe **Continuă**, îți exprimi acordul pentru colectarea de date cu caracter personal de pe dispozitivul respectiv.
3. Conectează-te la contul tău Bitdefender. Dacă nu ai cont Bitdefender, creează-ți unul folosind opțiunea corespunzătoare. Alternativ, te poți autentifica utilizând un cont Facebook, Google sau Microsoft.
4. Ți se va solicita să permiți toate drepturile de acces necesare pentru această aplicație. Selectează **Permite**.
5. Permite accesul la locația dispozitivului astfel încât Bitdefender să o poată accesa.
6. Permite aplicației să trimită notificări. Pentru administrarea notificărilor Bitdefender, accesează Setări > Notificări > Parental.
7. Pentru a putea monitoriza contactele copilului tău, este necesar să activezi opțiunea **Blocarea și identificarea apelurilor**. Urmează pașii necesari astfel încât să poți utiliza Bitdefender Parental Control pentru restricționarea apelurilor primite.
8. Asociază dispozitivul cu profilul copilului tău.

Monitorizarea activității online a copiilor tăi

Bitdefender Parental Control te ajută să urmărești exact ce face copilul tău în mediul online. Astfel, poți afla întotdeauna cu precizie în ce activități au fost implicați copiii tăi în timpul utilizării dispozitivelor atribuite.

În funcție de setările făcute, Bitdefender generează rapoarte care pot conține informații detaliate despre fiecare eveniment, cum ar fi:

- Starea evenimentului.
- Severitatea de notificare.
- Numele dispozitivului.



- Data și ora producerii evenimentului.

Pentru a monitoriza traficul pe internet, aplicațiile accesate sau activitatea online a copiilor tăi:

1. Accesați **Bitdefender Central**.
2. Selectează secțiunea **Control parental**.
3. Selectează fila dispozitivului dorit.

În fereastra **Activitate**, puteți vizualiza informațiile care vă interesează. Ca alternativă, selectează link-ul **Vizualizează activitatea de azi** din fila dispozitivului monitorizat pentru a fi redirecționat către fereastra **Activitate**.



Notă

Secțiunea Activitate va conține doar detalii furnizate de dispozitivele Windows, macOS și Android.

Configurarea setărilor rapoartelor

În mod implicit, atunci când funcția de Control parental este activată, activitățile online ale copiilor tăi sunt înregistrate în fișiere jurnal.

Pentru a primi notificări prin e-mail în legătură cu activitățile online ale copiilor tăi:

1. Accesați **Bitdefender Central**.
2. Selectează secțiunea **Control parental**.
3. Selectează secțiunea **Setări rapoarte**.
4. Activați opțiunea corespunzătoare pentru a primi rapoarte de activitate.
5. Introduceți adresa de e-mail la care vor fi trimise notificările prin e-mail.
6. Setează frecvența selectând: săptămânal sau lunar, apoi clic pe **SALVEAZĂ**.

De asemenea, poți alege să primești notificări în contul tău Bitdefender în următoarele situații:


- De fiecare dată când copiii tăi încearcă să acceseze aplicații blocate (pe Windows, macOS și Android).
- De fiecare dată când copiii tăi primesc apeluri de la numere de telefon blocate/necunoscute (pe iOS).



- De fiecare dată când copilul tău părăsește zonele sigure sau intră în zonele restricționate.
- De fiecare dată când copiii tău raportează că au ajuns în siguranță la destinație.


Editarea profilului

Pentru a edita un profil existent:

1. Accesați **Bitdefender Central**.
2. Selectează secțiunea **Control parental**.
3. Faceți clic pe pictograma  de pe cardul de profil dorit și apoi selectați **Editare**.
4. După personalizarea setărilor dorite, selectați **Salvează**.

Ștergerea unui profil

Pentru a șterge un profil existent:

1. Accesați **Bitdefender Central**.
2. Selectează secțiunea **Control parental**.
3. Faceți clic pe pictograma  de pe cardul de profil dorit și apoi selectați **Ștergere**.
4. Confirmă alegerea.

4.16.3. Configurarea profilurilor de Control parental

Pentru a începe monitorizarea copiilor tău, trebuie alocat un profil dispozitivelor pe care este instalată caracteristica sau aplicația Bitdefender Parental Control.

După crearea unui profil, poți personaliza în detaliu setările de monitorizare și control privind accesul la internet și la anumite aplicații.

Pentru a începe configurarea unui profil, selectați cardul de profil dorit din fereastra **Copiii mei**.

Selectează o filă pentru a configura funcția corespunzătoare de Control parental pentru dispozitivul respectiv:



- **Activitate** - aici poți vizualiza toate activitățile, interesele, locațiile și interacțiunile cu prietenii din ziua curentă.
- **Aplicații** - de aici poți bloca accesul la anumite aplicații, precum jocuri, programe de mesagerie, filme etc.
- **Site-uri web** - de aici poți filtra navigarea pe internet.
- **Contacte telefon** - aici poți menționa care dintre contactele din listele copiilor tăi pot intra în contact cu acesta prin intermediul telefonului.
- **Locație copil** - aici poți stabili locațiile care sunt sigure sau nesigure pentru copiii tăi.
- **Rețele de socializare** - aici poți vedea activitatea copiilor tăi pe platformele de rețele sociale din ultimele 30 de zile. Aceste informații sunt disponibile numai pentru utilizatorii care au făcut upgrade la **Bitdefender Parental Control Premium**.
- **Timpul petrecut în fața ecranului** - de aici poți bloca accesul la dispozitivele asociate profilurilor copiilor tăi. Accesul poate fi restricționat atât la un anumit interval de timp, cât și pentru limite zilnice cumulate.
- **Dispozitive** - aici poți vizualiza starea dispozitivelor monitorizate, poți atribui un nou dispozitiv profilului copilului tău sau poți elimina un dispozitiv atribuit.

Activitate

Fereastra Activitate îți oferă informații detaliate despre activitățile online ale copiilor tăi în ultimele 24 de ore, în interiorul și exteriorul casei tale. Pentru a vizualiza activitățile din zilele anterioare, efectuați clic pe pictograma calendarului din colțul din stânga sus al ferestrei.

În funcție de activitate, această fereastră poate include informații despre:

- **Locații** - aici poți vizualiza locațiile vizitate de copiii tăi în cursul zilei.
- **Interese** - aici poți vizualiza informații despre categoriile de site-uri web accesate de copiii tăi. Dați clic pe linkul **Revizuire conținut necorespunzător** pentru a permite sau interzice accesul la anumite interese.
- **Interacțiuni sociale** - aici poți vizualiza contactele cu care au comunicat copiii tăi. Accesează opțiunea **Administrare contacte** pentru a selecta contactele cu care copiii tăi ar trebui să mențină sau nu legătura.



- **Aplicații** - aici poți vizualiza aplicațiile pe care le-au utilizat copiii tăi. Fă clic pe linkul **Verificare restricții aplicații** pentru a bloca sau permite accesul la anumite aplicații.
- **Activitate zilnică** - aici poți vedea timpul petrecut online pe toate dispozitivele atribuite copiilor tăi și locul unde aceștia au fost activi. Informațiile colectate sunt din ziua curentă.

Aplicații

Fereastra Aplicații îți permite să blochezi executarea anumitor aplicații pe dispozitivele Windows, macOS și Android. Astfel poți bloca jocurile, fișierele media și aplicațiile de mesagerie, precum și alte categorii de aplicații.

Aici poți vedea și topul aplicațiilor utilizate în ultimele 30 de zile, alături de timpul de utilizare a acestora de către copiii tăi. Informațiile despre timpul de utilizare a aplicațiilor pot fi obținute numai în cazul dispozitivelor Windows, macOS și Android.

Pentru a configura controlul aplicațiilor pentru un anumit cont de utilizator:

1. Este afișată lista dispozitivelor asociate.
Selectează panoul dispozitivului pentru care dorești să restricționezi accesul la aplicații.
2. Apasă pe **Administrare aplicații utilizate de...**
Se afișează o listă a aplicațiilor instalate.
3. Selectează **Blocat** din dreptul aplicațiilor care dorești să nu mai fie folosite de copilul tău.
4. Selectează **SALVEAZĂ** pentru a aplica noile setări.

Poți opri monitorizarea aplicațiilor instalate dezactivând opțiunea **Monitorizare aplicații utilizate** din colțul din dreapta sus al ferestrei.


Site-uri web

Fereastra Site-uri web te ajută să blochezi site-urile cu conținut necorespunzător pe dispozitivele Windows, MacOS și Android. Astfel poți bloca site-urile web care găzduiesc clipuri video, jocuri, fișiere media și aplicații de mesagerie, precum și alte categorii de conținuturi negative.

Caracteristica poate fi activată sau dezactivată utilizând butonul corespunzător.



În funcție de vârsta setată pentru copiii tăi, lista de Interese include implicit o selecție de categorii activate. Pentru a permite sau bloca accesul la o anumită categorie, faceți clic pe aceasta.

Pictograma  indică faptul că un anumit conținut dintr-o anumită categorie nu poate fi accesat de copilul tău.

Acceptarea sau blocarea unui site web

Pentru a permite sau restricționa accesul la anumite pagini web, trebuie să le adaugi în lista de Excepții, după cum urmează:

1. Faceți clic pe butonul **ADMINISTRARE**.
2. Introduceți pagina web a cărei accesare doriți să o permiteți sau să o blocați în câmpul corespunzător.
3. Selectați **Permite** sau **Blocare**.
4. Faceți clic pe **Finalizare** pentru a salva modificările.




Notă

Restricțiile de acces la anumite site-uri web pot fi configurate numai pentru dispozitivele Windows, Android și macOS adăugate în profilul copilului tău.

Contacte telefon

Fereastra Contacte telefon îți dă posibilitatea de a specifica prietenii din lista copilului tău care pot sau nu pot intra în contact cu acesta prin intermediul telefonului. Pe dispozitivele iOS poți bloca apelurile primite, în timp ce pe dispozitivele Android poți vizualiza lista de contacte.

Pentru a restricționa apelurile primite de la un anumit număr de telefon al unui contact, mai întâi trebuie să adăugi dispozitivul iOS al copilului tău în profilul său:

1. Accesați **Bitdefender Central**.
2. Selectează secțiunea **Control parental**.
3. Accesează pictograma  din profilul copilului și apoi selectează **Dispozitive**.
4. Selectează dispozitivul iOS pe care dorești să-l atribui și apoi selectează opțiunea **ATRIBUIE**. Dacă dispozitivul iOS pe care dorești să-l atribui




profilului copilului tău nu apare în listă, selectează **Instalare pe un dispozitiv nou** și apoi **TRIMITE LINKUL PENTRU DESCĂRCARE**. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.

Pe dispozitivul pe care dorești să instalezi Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

5. Selectează fila **Contacte telefon** din Bitdefender Central.

Se afișează o listă cu carduri. Cardurile reprezintă contactele din smartphone-ul Android al copilului tău.

6. Selectați cardul cu numărul de telefon pe care doriți să îl blocați.

Pictograma  indică faptul că numărul de telefon selectat nu poate lua legătura cu copilul tău.



Notă

Nu vor fi blocate apelurile efectuate și nici mesajele SMS primite sau trimise.

Locație copil

Vizualizați locația curentă a dispozitivului pe Google Maps. Locația este actualizată la fiecare 5 secunde, așadar îl puteți localiza dacă este în mișcare.

Precizia locației depinde de cum poate Bitdefender să o stabilească:

- Dacă funcția GPS este activată pe dispozitiv, locația sa poate fi indicată cu precizie pe o rază de câțiva metri atâta timp cât se află în raza sateliților GPS (mai exact, nu într-o clădire).
- Dacă dispozitivul este înăuntru, locația sa poate fi stabilită la intervale de zeci de metri dacă funcția Wi-Fi este activată și există pe raza sa rețele wireless.
- Altfel, locația va fi stabilită utilizând numai informațiile rețelei mobile, care nu poate oferi o precizie mai mare de câteva sute de metri.

Configurarea locației & Raportare siguranță

Pentru a fi sigur(ă) că numai anumite locații sunt accesate de copilul dumneavoastră, puteți face o listă cu locurile sigure și nesigure. De fiecare



dată când acesta intră singur într-o zonă predefinită, se va afișa o notificare în aplicația Control parental, prin care i se va solicita să confirme că este în siguranță. La selectarea opțiunii **AM AJUNS ÎN SIGURANȚĂ**, vei fi informat prin intermediul unei notificări în contul tău Bitdefender ca acesta a ajuns la destinația finală.

În cazul în care nu primești nicio confirmare de la copilul tău, poți vedea istoricul locației sale pe parcursul zilei verificând profilul acestuia în contul tău Bitdefender.

Pentru a configura o locație:

1. Efectuați clic pe **Dispozitive** în cadrul disponibil în fereastra **Locație copil**.
2. Faceți clic pe **SELECTARE DISPOZITIVE** și apoi selectați dispozitivul pe care doriți să îl configurați.
3. În fereastra **Zone**, faceți clic pe butonul **ADĂUGARE ZONĂ**.
4. Selectați tipul locației **SIGURĂ** sau **RESTRIȚIONATĂ**.
5. Introduceți o denumire validă pentru zona pe care copilul tău o poate sau nu accesa.
6. Stabiliți raza care urmează a fi aplicată pentru monitorizare din bara glisantă **Rază**.
7. Faceți clic pe **ADĂUGARE ZONĂ** pentru a salva setările. Ți se solicită să precizezi dacă copilul tău va călători singur sau nu. Confirmă cu Da sau Nu.



Notă

Dispozitivul de urmărire a locației poate fi folosit pentru monitorizarea dispozitivelor Android și iOS pe care nu este instalată aplicația Control parental Bitdefender.

Rețele de socializare - Hărțuire cibernetică și agresori online

Fereastra Rețele de socializare îți oferă informații despre activitățile online ale copiilor tăi din ultimele 30 de zile în aplicațiile de rețele sociale, cum ar fi WhatsApp, Facebook Messenger sau Instagram. Pentru a te ghida către posibilele capcane online în care ar putea cădea copiii tăi, încercările de hărțuire cibernetică și comportament de agresor sunt detectate și afișate în această zonă. Acest lucru este posibil datorită tehnologiilor de inteligență artificială pe care le folosim pentru a detecta pericolele, cum ar fi:



- Fotografii ce conțin nuditate.
- Mesaje text răutăcioase.
- Divulgarea datelor cu caracter personal (adresa de domiciliu, parole, numerele cardurilor de credit, codurile numerice personale etc.).
- Solicitări de întâlnire primite din partea unor persoane străine.

În special, Bitdefender Parental Control Premium analizează:

- Mesajele text trimise numai în limba engleză prin WhatsApp (Android, Windows și macOS), Facebook Messenger (Windows și Mac) și Instagram (Android).
- Imaginile trimise sau primite prin WhatsApp (Android, Windows și macOS), Facebook Messenger (Android, Windows și macOS) și Instagram (Android).
- Imaginile trimise sau primite prin intermediul oricărei aplicații (iOS).

Notă

Mesajele pe care le analizăm pe WhatsApp provin atât din aplicația pentru mobil, cât și din versiunea web pe Google Chrome. Pentru a putea analiza mesajele din WhatsApp Web de pe Google Chrome pe dispozitivele Android, este necesară activarea opțiunii Accesibilitate pentru Bitdefender Parental Control. Pentru a activa opțiunea Accesibilitate: accesează secțiunea Setări > Accesibilitate > Parental Control.

Mesajele din Facebook Messenger pe care le analizăm provin din aplicația pentru mobil, din <https://www.facebook.com/> și din <https://www.messenger.com/> din Google Chrome, Mozilla Firefox și Microsoft Edge.

Important

Fila Rețele de socializare devine disponibilă numai pentru utilizatorii care au făcut upgrade la versiunea premium. Pentru a face upgrade la Bitdefender Parental Control Premium, consultați „*Abonamente Bitdefender Parental Control*” (p. 177).

Pentru a putea detecta hărțuirile cibernetice și comportamentele de agresor, este necesar să întreprinzi următoarele acțiuni:

1. Creează un profil de copil și atribuie dispozitive profilului copilului tău așa cum este descris în „*Creează profiluri pentru copiii tăi*” (p. 164).
2. Acordă drepturile de acces solicitate în timpul instalării aplicației Bitdefender Parental Control pe dispozitivele Android și iOS.



3. Activează opțiunea **Hărțuire & Agresori**, astfel:

- a. Accesați **Bitdefender Central**.
- b. Selectează secțiunea **Control parental**.
- c. Accesează **Setări rapoarte**.
- d. Activează butonul corespunzător.

După configurare, informațiile sunt preluate automat de la dispozitivele Windows, macOS și iOS. Pentru a permite Bitdefender să colecteze informații din aplicațiile Facebook Messenger și Instagram de pe dispozitivele Android, este necesar să activezi câteva setări, după cum urmează:

● Aplicația Facebook Messenger:

1. Atinge fotografia de profil
2. Accesează **Fotografii & Media**.
3. Activează opțiunile **Salvare fotografii** și **Salvare pe captură**.

● Aplicația Instagram:

1. Atinge fotografia de profil.
2. Accesează **Fotografii & Media**.
3. Accesează "" și apoi **Fotografii originale**
4. Activează opțiunea **Salvare pe captură**.
5. Activează opțiunile **Salvare fotografii originale** și **Salvare fotografii postate**.

Restricționare acces

În secțiunea „Timpul petrecut în fața ecranului”, găsești informații despre timpul de utilizare a dispozitivelor asociate pentru ziua curentă, timpul rămas din limita zilnică pe care ai configurat-o și statusul profilului selectat (activ sau blocat temporar). Din această fereastră poți seta și restricțiile de timp pentru diverse intervale orare, cum ar fi ora de culcare, timpul pentru lecții sau meditații.


Restricții de timp


Pentru a începe configurarea restricțiilor de timp:

1. Selectează **Verificare restricții de timp**.



2. În secțiunea **Setare restricții de timp**, selectează **Adăugare restricție nouă**.
3. Introdu o denumire pentru restricția pe care dorești să o configurezi (de exemplu, ora de culcare, teme, lecții de tenis etc.).
4. Setează intervalul orar și zilele pentru care se vor aplica restricțiile, apoi selectează **ADĂUGARE** pentru a salva setările.

Pentru a modifica o restricție, accesează fereastra Timpul petrecut în fața ecranului, selectează restricția pe care dorești să o modifici și apasă pe pictograma  afișată.

Pentru a șterge o restricție, accesează fereastra Timpul petrecut în fața ecranului, selectează restricția pe care dorești să o modifici și apoi apasă pe pictograma  afișată.

Limita zilnică

Limita de utilizare zilnică poate fi aplicată dispozitivelor Windows, macOS și Android. Dacă configurezi profilul astfel încât să fie blocat temporar după atingerea limitei, atunci această setare se va aplica tuturor dispozitivelor asociate, indiferent dacă acestea sunt pe Windows, MacOS, Android sau iOS.

Pentru a seta limita zilnică de utilizare:

1. Selectează **Verificare restricții de timp**.
2. În secțiunea **Setare limită de utilizare zilnică**, selectează **Adăugare limită zilnică nouă**.
3. Setează intervalul orar și zilele pentru care se vor aplica restricțiile, apoi selectează **SALVARE** pentru a salva setările.

4.16.4. Abonamente Bitdefender Parental Control

Pe lângă funcțiile de control parental incluse în abonamentul tău Bitdefender (**Aplicații**, **Site-uri web**, **Contacte telefon**, **Locație copil** și **Timp petrecut în fața ecranului**), ai posibilitatea de a fi informat în timp real în legătură cu amenințările la care sunt expuși copiii tăi în timp ce utilizează rețelele de socializare. Astfel, poți lua măsuri și începe să îți protejezi copiii împotriva hărțuirii lor de către colegi sau persoane străine. Pentru a primi informații despre activitățile copiilor tăi în timp ce utilizează rețelele de socializare, poți face upgrade la versiunea premium.

Pentru a face upgrade la Bitdefender Parental Control Premium:



1. Accesați **Bitdefender Central**.
2. Selectează secțiunea **Control parental**.
3. Accesează link-ul **AFLĂ MAI MULTE** din banner-ul de sus.
4. Selectează **CUMPĂRĂ VERSIUNEA PREMIUM**.

Vei fi redirecționat către site-ul nostru de pe care poți cumpăra produsul.

Abonamentul Bitdefender Parental Control Premium este independent de abonamentul Bitdefender Family Pack, ceea ce înseamnă că îl vei putea folosi pe toată durata de valabilitate, indiferent de starea abonamentului pentru soluția de securitate utilizată. În cazul în care abonamentul Bitdefender Parental Control Premium expiră, dar cel pentru Bitdefender Family Pack este încă activ, vei avea în continuare acces la caracteristicile produsului, cu excepția funcțiilor de monitorizare a hărțuirii cibernetice și a agresorilor online, care sunt incluse în caracteristica **Rețele de socializare**. Odată ce faci upgrade la planul Premium, îți vei putea folosi abonamentul pentru toate dispozitivele deținute de copiii tăi, cu condiția să te conectezi cu același cont Bitdefender.



Notă

Poți face upgrade la Bitdefender Parental Control Premium numai dacă te afli într-una din următoarele țări: SUA, Canada, Regatul Unit, Irlanda, Africa de Sud, Australia sau Noua Zeelandă. Această listă de țări va fi actualizată de îndată ce produsul va fi disponibil pentru utilizare în noi regiuni.

4.17. Antifurt

Furtul laptop-urilor este o problemă majoră ce afectează atât persoanele fizice, cât și organizațiile. Dincolo de pierderea aparatului în sine, datele pierdute cu acesta pot provoca prejudicii semnificative, atât de natură financiară, cât și personală.

Cu toate acestea, puține persoane iau măsurile corespunzătoare pentru a-și proteja datele personale, comerciale și financiare importante în cazul pierderii sau furtului.

Bitdefender Anti-Theft te ajută să fii mai pregătit pentru astfel de situații, permițându-ți să localizezi de la distanță sau să blochezi laptop-ul și chiar să ștergi toate datele de pe acesta, în cazul în care laptop-ul îți este sustras.

Pentru a utiliza funcțiile Anti-Theft, trebuie să îndepliniți următoarele cerințe preliminare:



- Comenzile pot fi trimise doar din contul Bitdefender.
- Laptop-ul trebuie să fie conectat la internet pentru a primi comenzile.

Funcțiile Anti-Theft funcționează după cum urmează:

Localizează

Vizualizați locația dispozitivului dumneavoastră pe Google Maps.

Precizia locației depinde de modul în care o poate identifica Bitdefender. Locația este determinată în zeci de metri dacă funcția Wi-Fi este activată pe laptopul dumneavoastră și există rețele wireless în zona dumneavoastră.

În cazul în care laptopul este conectat la o rețea LAN cu cablu fără locație Wi-fi disponibilă, locația va fi stabilită în baza adresei IP, care are o precizie considerabil redusă.

Alertă

Transmiteți o alertă de la distanță pe dispozitiv.

Funcția este disponibilă doar pe dispozitivele mobile.

Blochează

Blochează laptopul și setează un cod de 4 cifre pentru deblocare. Când transmiți comanda de **Blocare**, sistemul este repornit și reconectarea la Windows este posibilă numai după introducerea codului setat.

Dacă dorești ca Bitdefender să fotografieze persoanele care încearcă să obțină acces la laptopul tău, bifează caseta corespunzătoare. Fotografiiile sunt realizate cu ajutorul camerei frontale și sunt afișate împreună cu amprenta de timp în panoul de bord Anti-Theft. Doar cele mai recente două fotografii sunt salvate.

Această acțiune este disponibilă numai pentru laptopurile prevăzute cu cameră frontală.

Ștergere

Șterge toate datele din sistemul tău. Când transmiți o comandă de **Ștergere**, laptopul este repornit și datele de pe toate partițiile sunt șterse.

Afișează IP

Afișează ultima adresă IP pentru dispozitivul selectat. Fă clic pe **Afișează IP** pentru ca acesta să devină vizibil.



Serviciul Anti-Theft este activat după instalare și poate fi oprit numai prin intermediul contului dumneavoastră Bitdefender de pe orice dispozitiv conectat la internet, de oriunde.

Utilizarea Funcțiilor Antifurt

Pentru a accesa funcția Antifurt, folosiți una dintre următoarele posibilități:

● Din interfața principală Bitdefender:

1. Efectuează clic pe **Instrumente** din meniul de navigare al interfeței **Bitdefender**.
2. Selectează **ACCESEAZĂ CENTRAL**.
Vei fi redirecționat către pagina Bitdefender Central. Asigură-te că ești conectat(ă) cu datele tale de autentificare.
3. În fereastra Bitdefender Central care se deschide, efectuează clic pe fila dispozitivului dorit și selectează **Antifurt**.

● Pe orice dispozitiv cu acces la internet:

1. Deschideți un browser web și mergeți la: <https://central.bitdefender.com>.
2. Conectează-te la contul tău Bitdefender folosind adresa ta de e-mail și parola.
3. Selectați secțiunea **Dispozitivele mele**.
4. Efectuează clic pe fila dispozitivului dorit și selectează **Antifurt**.
5. Selectați funcția pe care doriți să o folosiți:

Afișează IP - afișează ultima adresă IP a dispozitivului tău.

Localizare - afișează locația dispozitivului dumneavoastră pe Google Maps.



Alertă - trimiterea unei alerte pe dispozitiv.



Blocare - blochează laptopul și setează un cod PIN de deblocare.



Ștergere - șterge toate datele de pe laptopul tău.



Important

După ce ștergeți un dispozitiv, este oprită funcționarea tuturor funcțiilor Anti-Theft.



4.18. Bitdefender USB Immunizer

Funcția Autorun încorporată în sistemele de operare Windows este un instrument foarte util care permite calculatoarelor să execute automat un fișier de pe un suport conectat la acestea. De exemplu, instalările aplicațiilor pot începe automat când introduceți un CD în unitatea optică.

Din nefericire, această funcție poate fi utilizată și de amenințări pentru lansarea automată și infiltrarea în calculatorul dumneavoastră de pe medii reinscriptibile, cum ar fi unitățile USB și cardurile de memorie conectate prin cititoare de carduri. În ultimii ani au fost create numeroase atacuri bazate pe Autorun.

Cu USB Immunizer, puteți împiedica orice unități flash formate NTFS, FAT32 sau FAT să mai execute amenințări. După ce un dispozitiv USB a fost imunizat, amenințările nu îl mai pot configura să ruleze o anumită aplicație când dispozitivul este conectat la un calculator pe care rulează Windows.

Pentru a imuniza un dispozitiv USB:

1. Conectați unitatea flash la calculatorul dumneavoastră.
2. Navigați în calculator pentru a localiza dispozitivul amovibil de stocare și faceți clic dreapta pe această pictogramă.
3. În meniul contextual, evidențiați **Bitdefender** și selectați **Imunizează această unitate**.



Notă

Dacă dispozitivul a fost deja imunizat, în locul opțiunii Imunizare va apărea mesajul **Dispozitivul USB este protejat împotriva amenințărilor cu executare automată**

Pentru a preveni lansarea amenințărilor de către calculatorul dumneavoastră de pe dispozitive USB neimunizate, dezactivați funcția de rulare automată a mediilor. Pentru mai multe informații, consultați capitolul *„Cu ajutorul monitorizării automate a vulnerabilităților”* (p. 123).



5. OPTIMIZARE DE SISTEM

5.1. Instrumente

Bitdefender este livrat cu o secțiune Instrumente care te ajută să menții integritatea sistemului. Utilitățile oferite sunt critice pentru îmbunătățirea performanței sistemului dumneavoastră și gestionarea eficientă a spațiului pe hard disc.

Bitdefender oferă următoarele funcții de optimizare a calculatorului:

- **OneClick Optimizer** analizează și îmbunătățește viteza sistemului prin executarea mai multor sarcini cu un singur clic pe un buton.
- Opțiunea **Startup Optimizer** reduce timpul de pornire al sistemului, oprind aplicațiile care nu sunt necesare la pornirea calculatorului.
- **Disk Cleanup** identifică acele fișiere care pot fi vinovate pentru spațiul redus de pe discul tău, oferindu-ți posibilitatea de a decide dacă dorești să le păstrezi sau nu.

5.1.1. Optimizați viteza sistemului cu un singur clic

Probleme cum ar fi defectarea unității hard, fișierele registru rămase și istoricul browser-ului pot reduce viteza de lucru a sistemului, ceea ce ar putea deveni o problemă pentru dvs. Toate acestea pot fi acum remediate cu un singur clic pe un buton.

OneClick Optimizer vă permite să identificați și să eliminați fișierele inutile prin executarea mai multor sarcini de eliminare în același timp.

Pentru a lansa procesul Oneclick Optimizer:

1. Efectuează clic pe **Instrumente** din meniul de navigare al interfeței **Bitdefender**.
2. Efectuează clic pe **OPTIMIZEAZĂ-MI DISPOZITIVUL**.
 - a. **Analiză în curs**

Așteptați ca Bitdefender să finalizeze problemele legate de sistem.

- **Disk Cleanup** - identifică fișierele și directoarele care nu mai sunt necesare.



- Curățare regiștri - identifică referirile nevalabile sau depășite din regiștrii Windows.
- Ștergere confidențialitate - identifică fișierele internet temporare și fișierele cookie, memoria cache a browser-ului și istoricul.

Se afișează numărul problemelor identificate. Fă clic pe linkul **Vizualizare detalii** pentru a face o verificare înainte de a continua procesul de curățare. Faceți clic pe **Optimizează** pentru a continua.

b. Optimizare în curs

Așteptați până ce Bitdefender finalizează optimizarea sistemului dvs.

c. Probleme

Aici puteți vedea rezultatul operației.

Dacă doriți informații detaliate despre procesul de optimizare, faceți clic pe butonul **Vizualizare raport detaliat**.

5.1.2. Optimizarea timpului de pornire al calculatorului dvs.

Timpul prelungit de pornire a sistemului reprezintă o problemă, din cauza aplicațiilor care sunt setate să ruleze fără ca acest lucru să fie necesar. Minutele de așteptare până la pornirea sistemului pot însemna timp și productivitate prețioase.

Fereastra Startup Optimizer afișează aplicațiile care rulează la pornirea sistemului și vă permite să le administrați comportamentul în această etapă.

Pentru a lansa procesul Startup Optimizer:

1. Efectuează clic pe **Instrumente** din meniul de navigare al interfeței **Bitdefender**.
2. Efectuează clic pe **OPTIMIZEAZĂ BOOT DISPOZITIV**.
 - a. **Selectați aplicațiile**

Puteți vedea o listă a aplicațiilor care rulează la pornirea sistemului. Selectați-le pe cele pe care doriți să le dezactivați sau amânați la pornire.
 - b. **Selecția comunității**

Vedeți cum au decis alți utilizatori din cadrul Bitdefender să procedeze cu aplicația selectată de dvs.



c. Timp de încărcare rețea

Verificați bara glisantă din partea de sus a ferestrei pentru a vedea timpul necesar sistemului dvs. și aplicațiilor selectate pentru executarea la pornire.

Pentru a putea prelua informațiile referitoare la timpul necesar sistemului și aplicațiilor trebuie să reporniți sistemul.

d. Starea la pornire

- **Pornește.** Selectați această opțiune dacă doriți ca o aplicație să înceapă să ruleze la pornirea sistemului. Această opțiune este activată în mod implicit.
- **Întârzie.** Selectați această opțiune pentru a amâna rularea unui program la pornirea sistemului. Aceasta înseamnă că aplicațiile selectate vor porni cu un decalaj de cinci minute după ce utilizatorul s-a autentificat la sistem. Funcția de **Amânare** este predefinită și nu poate fi configurată de utilizator.
- **Dezactivează.** Selectați această opțiune pentru a dezactiva executarea unui program la pornirea sistemului.

e. Rezultate

Se afișează informații cum ar fi timpul estimat pentru pornirea sistemului după amânarea sau dezactivarea programelor.

Pentru a putea vedea toate aceste informații, este posibil să fie necesară o repornire a sistemului.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.



Notă

Dacă abonamentul dvs. expiră sau decideți să dezinstalați Bitdefender, aplicațiile pe care le-ați programat să nu ruleze la pornire vor fi readuse la setările de instalare implicite.

5.1.3. Se optimizează discul

Fișierele și directoarele nenesare, care utilizează spațiu pe disc, pot cauza încetinirea sistemului. Prin urmare, îți recomandăm să optimizezi viteza sistemului curățându-l la intervale regulate.

Bitdefender Disk Cleanup te ajută să optimizezi spațiul de pe discul tău cu ușurință prin identificarea acelor fișiere care pot reprezenta principalul motiv



pentru spațiu redus de pe disc. În plus, ai posibilitatea de a decide ce dorești să faci cu fișierele identificate.

Pentru a începe curățarea sistemului tău:

1. Efectuează clic pe **Instrumente** din meniul de navigare al interfeței **Bitdefender**.
2. Efectuează clic pe **CURĂȚĂ-MI DISPOZITIVUL**.
3. La prima accesare a funcției Disk Cleanup, ți se prezintă această funcție. Efectuează clic pe **OK, AM ÎNȚELES** pentru a continua.

a. Partiții și dispozitive

Poți vizualiza lista unităților de disc disponibile. În afara unităților de disc Windows, sunt scanate și afișate în listă și hard disk-urile externe și dispozitivele USB. Efectuează clic pe **ANALIZARE DISC** din dreptul discului pentru care dorești să realizezi curățarea.

b. Se analizează unitatea de disc


Driverul selectat este în curs de analiză. Așteaptă ca Bitdefender să finalizeze căutarea de fișiere și directoare mari.

c. Probleme

Aici poți vedea rezultatele operației. Pentru a selecta ordinea de afișare a rezultatelor, utilizează săgeata derulantă **SORTEAZĂ DUPĂ** localizată în partea stângă a ferestrei. Poți sorta rezultatele în funcție de dimensiune (de la 10 MB până la mai mult de 5 GB) sau în funcție de tip (fișierele sunt sortate în directoare separate în funcție de extensiile lor).

Selectează fișierele pe care dorești să le ștergi și apoi efectuează clic pe **CONFIRMĂ SELECȚIA** pentru a demara procesul de ștergere.

Fișierele protejate și impotante responsabile pentru funcționarea sistemului tău sunt de asemenea identificate, dar nu pot fi selectate sau șterse.

Efectuează clic pe pictograma  pentru a avea acces la directoarele care corespund fișierelor selectate.

d. Confirmă selecția

Este afișată lista cu fișierele selectate. Aruncă o privire și verifică din nou dacă chiar nu mai ai nevoie de aceste fișiere, pentru că o dată ce



mergi mai departe, acestea nu mai pot fi extrase din Coșul de gunoi. Confirmă alegerea efectuând clic pe **ȘTERGERE**.

e. Sumar

Starea procesului este afișată după cum urmează:

- ✔ Toate fișierele selectate au fost șterse.
- ⚠ Unul sau mai multe dintre fișierele selectate nu au putut fi șterse **sau** niciunul dintre fișierele selectate nu a putut fi șters.

Faceți clic pe **FINALIZARE** pentru a închide fereastra.

5.2. Profiluri

Activitățile de serviciu zilnice, vizionarea filmelor sau jocurile pot încetini performanțele sistemului, cu precădere dacă rulează simultan cu procesele de actualizare Windows și sarcinile de actualizare. Cu Bitdefender, puteți acum alege și aplica profilul dorit, care efectuează ajustările sistemului adecvate pentru îmbunătățirea performanțelor aplicațiilor specifice instalate.

Bitdefender oferă următoarele profiluri:

- Profil Lucru
- Profil Film
- Profil Joc
- Profil Wi-Fi public
- Profil mod baterie

Dacă decideți să nu utilizați **Profiluri**, se activează un profil implicit numit **Standard**, care nu vă optimizează sistemul.

În funcție de activitatea dvs., se aplică următoarele setări ale produsului la activarea unui profil Lucru, Film sau Joc:

- Toate alertele și pop-upurile Bitdefender sunt dezactivate.
- Actualizarea automată este amânată.
- Scanările programate sunt amânate.
- Modulul **Asistență pentru căutare** este dezactivat.
- Notificările privind ofertele speciale sunt dezactivate.



În funcție de activitatea dvs., se aplică următoarele setări ale sistemului la activarea unui profil Lucru, Film sau Joc:

- Actualizările automate Windows sunt amânate.
- Alerțele și pop-up-urile Windows sunt dezactivate.
- Programele inutile care rulează în fundal sunt suspendate.
- Efectele vizuale sunt adaptate pentru performanțe superioare.
- Sarcinile de întreținere sunt amânate.
- Setările planului de alimentare sunt ajustate.

Cât timp Profilul Wi-Fi este activ, Bitdefender Total Security este configurat pentru a pune în aplicare automat următoarele setări:

- Funcția Advanced Threat Defense este activă
- Firewall-ul Bitdefender este pornit și următoarele setări sunt aplicate pentru adaptorul tău wireless:
 - Mod ascuns - PORNIT
 - Tipul rețelei - Public
- Următoarele setări din Online Threat Prevention sunt activate:
 - Scanare web criptată
 - Protecție împotriva fraudelor
 - Protecție împotriva tentativelor de phishing

5.2.1. Profil Lucru

Rularea mai multor sarcini la serviciu, cum ar fi trimiterea de e-mail-uri, comunicarea video cu colegi aflați la distanță sau lucrul cu aplicații de proiectare, vă pot afecta performanțele sistemului. Profilul de serviciu a fost proiectat pentru a vă ajuta să vă îmbunătățiți eficiența la lucru, prin dezactivarea unora dintre serviciile și sarcinile care rulează în fundal.

Configurarea profilului Serviciu.

Pentru a configura măsurile implementate în Profilul Lucru:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.



3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil Lucru.
4. Selectați ajustările sistemului care doriți să fie aplicate, prin bifarea opțiunilor de mai jos:
 - Crește performanța aplicațiilor de lucru
 - Optimizează setările de produs pentru Profilul Lucru
 - Amână programele de fundal și activitățile de întreținere
 - Amânare actualizare Windows automată
5. Efectuează clic pe **SALVEAZĂ** pentru a memora schimbările și a închide fereastra.

Adăugarea manuală a aplicațiilor la lista Profil Serviciu

Dacă Bitdefender nu intră automat în Profilul Serviciu când lansezi o anumită aplicație de serviciu, poți adăuga manual aplicația la **Lista aplicațiilor de lucru**.

Pentru a adăuga manual aplicații în Lista de aplicații de lucru din Profilul Serviciu:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil Lucru.
4. În fereastra **Setări profil de lucru**, efectuează clic pe **Listă aplicații**.
5. Efectuează clic pe **ADĂUGARE**.

Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.

5.2.2. Profil Film

Afișarea videoclipurilor de calitate superioară, cum ar fi filmele de înaltă definiție, necesită resurse semnificative de sistem. Profilul Film adaptează setările sistemului și ale produsului, astfel încât să vă puteți bucura de o experiență plăcută și fără întreruperi.

Configurarea Profilului Film

Pentru a configura măsurile implementate în Profilul Film:



1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil film.
4. Selectați ajustările sistemului care doriți să fie aplicate, prin bifarea opțiunilor de mai jos:
 - Crește performanța aplicațiilor media
 - Optimizează setările de produs pentru Profilul Film
 - Amână programele de fundal și activitățile de întreținere
 - Amânare actualizare Windows automată
 - Ajustează configurările planului de energie pentru filme
5. Efectuează clic pe **SALVEAZĂ** pentru a memora schimbările și a închide fereastra.

Adăugarea manuală a dispozitivelor de redare video în lista Profil Film

Dacă Bitdefender nu intră automat în Profilul Film când lansați o anumită aplicație pentru redarea video clipurilor, puteți adăuga manual aplicația în **Lista aplicațiilor de film**.

Pentru a adăuga manual jucători video în lista Aplicațiilor de film din Profilul Film:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil film.
4. În fereastra **Setări profil film**, efectuează clic pe **Listă jucători**.
5. Efectuează clic pe **ADĂUGARE**.

Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.

5.2.3. Profil Joc

Pentru o experiență plăcută a jocului trebuie reduse încărcările de sistem și încetinirile. Folosind metoda euristică comportamentală, alături de o listă de jocuri cunoscute, Bitdefender poate detecta automat jocurile active și



poate optimiza resursele sistemului pentru ca dvs. să vă puteți bucura de pauza de joc.

Configurarea Profilului Joc

Pentru a configura măsurile implementate în Profilul Joc:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil Joc.
4. Selectați ajustările sistemului care doriți să fie aplicate, prin bifarea opțiunilor de mai jos:
 - Crește performanța jocurilor
 - Optimizează setările de produs pentru Profilul Joc
 - Amână programele de fundal și activitățile de întreținere
 - Amânare actualizare Windows automată
 - Ajustează configurările planului de energie pentru jocuri
5. Efectuează clic pe **SALVEAZĂ** pentru a memora schimbările și a închide fereastra.

Adăugare manuală de jocuri la lista de jocuri

În cazul în care Bitdefender nu intră automat în Profilul Joc atunci când ați lansat un anumit joc sau o aplicație, aveți posibilitatea să adăugați aplicația manual la **Lista de aplicații de jocuri**.

Pentru a adăuga manual jocuri în Lista de aplicații de jocuri în Profilul Joc:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil Joc.
4. În fereastra **Setări profil joc**, efectuează clic pe **Listă jocuri**.
5. Efectuează clic pe **ADĂUGARE**.

Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil al jocului, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.



5.2.4. Profil Wi-Fi public

Trimiterea de e-mailuri, introducerea unor date de autentificare sensibile sau cumpărăturile online în timp ce sunteți conectat la rețele wireless nesigure pot expune la riscuri datele dumneavoastră personale. Profilul Wi-Fi public ajustează setările produsului pentru a vă da posibilitatea de a face plăți online și de a utiliza informații sensibile într-un mediu protejat.

Configurarea profilului Wi-Fi public

Pentru a configura Bitdefender să aplice setările produsului în timpul conectării la o rețea wireless nesigură:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil Wi-Fi public.
4. Permiteți **să ajusteze setările produsului pentru a optimiza protecția atunci când sunteți conectat la o rețea Wi-Fi publică nesigură** căsuța bifată.
5. Faceți clic pe **Save**.

5.2.5. Profil mod baterie

Modul Baterie se adresează utilizatorilor de laptop și tablete. Scopul este acela de a reduce impactul sistemului și al Bitdefender asupra consumului de electricitate dacă nivelul bateriei este inferior celui implicit sau celui selectat de dumneavoastră.

Configurarea Modulului Baterie

Pentru a configura profilul Mod baterie:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.
3. Fă clic pe butonul **CONFIGUREAZĂ** din zona Mod Baterie.
4. Selectați ajustările sistemului care vor fi aplicate, prin bifarea opțiunilor de mai jos:
 - Optimizați setările de produs pentru Profilul Baterie.
 - Amânați programele de fundal și activitățile de întreținere.



- Amânare actualizare Windows automată.
- Ajustați configurările planului de energie pentru Modul Baterie.
- Dezactivați dispozitivele externe și porturile de rețea.

5. Efectuează clic pe **SALVEAZĂ** pentru a memora schimbările și a închide fereastra.

Introdu o valoare validă în casetă sau selectează una folosind săgețile sus/jos pentru a specifica când să intre sistemul în Modul Baterie. Implicit, modul este activat când nivelul de încărcare a bateriei scade sub 30%.

Când Bitdefender operează în Modul Baterie, se aplică următoarele setări:

- Actualizarea automată Bitdefender este amânată.
- Scanările programate sunt amânate.
- **Widget securitate** dezactivat.

Bitdefender detectează dacă laptopul a fost trecut pe alimentarea cu baterie și, în funcție de nivelul de încărcare al bateriei, intră automat în Modul Baterie. De asemenea, Bitdefender iese automat din modul pentru baterie, atunci când detectează că laptopul nu mai funcționează pe baterie.

5.2.6. Optimizare în timp real

Optimizarea în timp real Bitdefender este un plugin care îmbunătățește silențios performanțele sistemului dvs., în fundal, asigurându-se că nu sunteți întrerupt când vă aflați în modul profil. În funcție de solicitarea CPU, plugin-ul monitorizează toate procesele, concentrându-se pe cele care necesită mai multe resurse, pentru a le adapta necesităților dvs.

Pentru a activa sau dezactiva optimizarea în timp real:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Profiluri**.
3. Derulați în jos până când observați opțiunea de optimizare în timp real și apoi folosiți butonul corespunzător pentru a o activa sau dezactiva.



6. REMEDIEREA PROBLEMELOR

6.1. Soluționarea problemelor frecvente

Acest capitol prezintă anumite probleme cu care vă puteți confrunta la utilizarea Bitdefender și vă oferă soluții posibile la aceste probleme. Majoritatea acestor probleme pot fi soluționate prin configurarea adecvată a setărilor produsului.

- *„Sistemul meu funcționează lent”* (p. 193)
- *„Nu începe scanarea”* (p. 195)
- *„Nu mai pot utiliza o aplicație”* (p. 197)
- *„Ce trebuie făcut atunci când Bitdefender blochează un site web, un domeniu, o adresă IP sau o aplicație online care sunt sigure”* (p. 198)
- *„Ce trebuie să faci dacă Bitdefender detectează ca ransomware o aplicație sigură”* (p. 199)
- *„Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet”* (p. 203)
- *„Serviciile Bitdefender nu răspund”* (p. 204)
- *„Filtrul Antispam nu funcționează corespunzător”* (p. 204)
- *„Funcția Completare automată din Portofel nu funcționează”* (p. 209)
- *„Nu s-a reușit deinstalarea Bitdefender”* (p. 210)
- *„Sistemul meu nu pornește după ce am instalat Bitdefender”* (p. 211)

Dacă problema dumneavoastră nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic a Bitdefender folosind informațiile din capitolul *„Solicitarea ajutorului”* (p. 333).

6.1.1. Sistemul meu funcționează lent

De obicei, după instalarea unui program de securitate, este posibil să se producă o ușoară încetinire a funcționării sistemului, fapt ce este normal într-o anumită măsură.

În cazul în care observați o încetinire semnificativă, această problemă poate apărea din următoarele motive:



- **Bitdefender nu este singurul program de securitate instalat în sistem.**

Deși Bitdefender caută și dezinstalează programele de securitate detectate în timpul instalării, se recomandă să îndepărtați orice alte soluții de securitate pe care le-ați utilizat înainte de a iniția instalarea Bitdefender. Pentru mai multe informații, consultați capitolul „*Cum elimin celelalte soluții de securitate?*” (p. 77).

- **Cerințele de sistem pentru rularea Bitdefender nu sunt îndeplinite.**

Dacă dispozitivul tău nu îndeplinește cerințele de sistem, computerul va fi afectat de încetiniri, mai ales atunci când mai multe aplicații rulează în același timp. Pentru mai multe informații, consultați capitolul „*Cerințe de sistem*” (p. 2).

- **Ai instalat aplicații pe care nu le utilizezi.**

Orice calculator are programe sau aplicații pe care nu le utilizezi. Și multe programe nedorite rulează în fundal, ocupând spațiu pe disc și încărcând memoria calculatorului. Dacă nu folosiți un program, dezinstalați-l. Acest lucru este valabil și pentru orice alte programe software sau aplicații de evaluare pe care omiteți să le ștergeți.



Important

Dacă suspectați că un program sau o aplicație este o parte esențială a sistemului dumneavoastră de operare, nu le ștergeți, ci contactați Serviciul de asistență clienți al Bitdefender.

- **Sistemul dumneavoastră poate fi infectat.**

Amenințările pot afecta, de asemenea, viteza sistemului dumneavoastră, precum și comportamentul general al acestuia. Programele periculoase de tip spyware, malware, troieni și adware afectează performanța calculatorului dumneavoastră. Scanați sistemul periodic, cel puțin o dată pe săptămână. Este recomandat să utilizați funcția de Scanare sistem a Bitdefender deoarece aceasta scanează toate tipurile de amenințări care pun în pericol securitatea sistemului dumneavoastră.

Pentru a porni Scanarea sistemului:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTIVIRUS**, efectuează clic pe **Scanare sistem**.
3. Urmați pașii asistentului.



6.1.2. Nu începe scanarea

Acest tip de problemă poate avea două cauze principale:

- **O instalare anterioară a Bitdefender care nu a fost complet eliminată sau o instalare necorespunzătoare a Bitdefender.**

În acest caz, reinstalați Bitdefender:

- **În Windows 7:**

1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
2. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
3. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
4. Așteptați finalizarea procesului de reinstalare și apoi reporniți sistemul.

- **În Windows 8 și Windows 8.1:**

1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
5. Așteptați finalizarea procesului de reinstalare și apoi reporniți sistemul.

- **În Windows 10:**

1. Faceți clic pe **Start**, apoi pe **Setări**.
2. Faceți clic pe pictograma **Sistem** din secțiunea **Setări**, apoi selectați **Aplicații instalate**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
6. Așteptați finalizarea procesului de reinstalare și apoi reporniți sistemul.



Notă

Urmând această procedură de reinstalare, setările personalizate sunt salvate și vor fi disponibile în noul produs instalat. Celelalte setări pot fi restabilite la configurația implicită.

● Bitdefender nu este singura soluție de securitate instalată în sistemul dumneavoastră.

În acest caz:

1. Dezinstalați cealaltă soluție de securitate. Pentru mai multe informații, consultați capitolul „*Cum elimin celelalte soluții de securitate?*” (p. 77).

2. Reinstalați Bitdefender:

● În Windows 7:

- Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
- Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
- Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
- Așteptați finalizarea procesului de reinstalare și apoi reporniți sistemul.

● În Windows 8 și Windows 8.1:

- Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
- Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
- Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
- Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
- Așteptați finalizarea procesului de reinstalare și apoi reporniți sistemul.

● În Windows 10:

- Faceți clic pe **Start**, apoi pe **Setări**.
- Faceți clic pe pictograma **Sistem** din secțiunea **Setări**, apoi selectați **Aplicații instalate**.
- Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.



- d. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
- e. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
- f. Așteptați finalizarea procesului de reinstalare și apoi reporniți sistemul.



Notă

Urmând această procedură de reinstalare, setările personalizate sunt salvate și vor fi disponibile în noul produs instalat. Celelalte setări pot fi restabilite la configurația implicită.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea „*Solicitarea ajutorului*” (p. 333).

6.1.3. Nu mai pot utiliza o aplicație

Această problemă apare când încercați să utilizați un program care a funcționat normal înainte de instalarea Bitdefender.

După instalarea Bitdefender ar putea apărea următoarele situații:

- Este posibil să primiți un mesaj din partea Bitdefender referitor la faptul că programul încearcă să efectueze o modificare asupra sistemului.
- Este posibil să primiți un mesaj de eroare din partea programului pe care încercați să-l utilizați.

Acest tip de situație apare când Advanced Threat Defense detectează din greșeală anumite aplicații ca fiind rău intenționate.

Advanced Threat Defense este un modul Bitdefender care monitorizează în mod constant aplicațiile care rulează pe sistemul dumneavoastră și raportează acele aplicații care sunt posibil rău intenționate. Deoarece această opțiune se bazează pe un sistem euristic, pot exista situații în care aplicații legitime să fie raportate de Advanced Threat Defense.

Atunci când se întâmplă aceasta, puteți exclude aplicația respectivă de la monitorizarea efectuată de Advanced Threat Defense.

Pentru a adăuga programul în lista de excepții:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ADVANCED THREAT DEFENSE**, efectuează clic pe **Setări**.



3. În secțiunea **Excepții**, selectează **Adăugare aplicații în lista de excepții**.
4. Găsește și selectează aplicația care dorești să fie exceptată și dă clic pe **OK**.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea „*Solicitarea ajutorului*” (p. 333).

6.1.4. Ce trebuie făcut atunci când Bitdefender blochează un site web, un domeniu, o adresă IP sau o aplicație online care sunt sigure

Bitdefender oferă o experiență sigură de navigare pe internet prin filtrarea întregului trafic web și blocarea oricărui conținut periculos. Cu toate acestea, este posibil ca Bitdefender să considere periculoase un site web, un domeniu, o adresă IP sau o aplicație online care sunt sigure, ceea ce va cauza blocarea acestora în mod incorect de către funcția de scanare a traficului HTTP din cadrul Bitdefender.

În cazul în care aceleași pagini, domenii, adrese IP sau aplicații online sunt blocate în mod repetat, acestea pot fi adăugate în lista de excepții astfel încât să nu fi scanate de motoarele Bitdefender, asigurând o experiență de navigare pe internet fără probleme.

Pentru a adăuga un site web la **Excepții**:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ONLINE THREAT PREVENTION**, dă clic pe **Excepții**.
3. Introdu în câmpul corespunzător adresa site-ului web, numele domeniului, adresa IP sau aplicația online blocată și selectează opțiunea **ADAUGĂ**.
4. Efectuează clic pe **SALVEAZĂ** pentru a memora schimbările și a închide fereastra.

Numai site-urile, domeniile, adresele IP și aplicațiile în care ai deplină încredere ar trebui adăugate în această listă. Acestea vor fi excluse din procesul de scanare de către motoarele contra amenințărilor, a tentativelor de phishing și fraudelor.



Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea „*Solicitarea ajutorului*” (p. 333).

6.1.5. Ce trebuie să faci dacă Bitdefender detectează ca ransomware o aplicație sigură

Ransomware este un program periculos care încearcă să obțină bani de la utilizatori prin blocarea sistemelor vulnerabile. Pentru a-ți proteja sistemul de situații neplăcute, Bitdefender îți oferă posibilitatea de asigurare a fișierelor personale.

Atunci când o aplicație încearcă să modifice sau să șteargă unul dintre fișierele tale protejate, aceasta va fi considerată nesigură și Bitdefender o va bloca.

În cazul în care o aplicație este adăugată în lista aplicațiilor nesigure și ești sigur că utilizarea acesteia este sigură, respectă următorii pași:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **PROTECȚIE FIȘIERE**, dă clic pe **Acces aplicație**.
3. Vor apărea aici aplicațiile care au solicitat modificarea unor fișiere din directoarele tale protejate. Efectuează clic pe butonul **Permite** din dreptul aplicației pe care o consideri sigură.

6.1.6. Nu mă pot conecta la internet

Este posibil să observați că un program sau un browser de internet nu se mai poate conecta la internet sau accesa serviciile de rețea după instalarea Bitdefender.

În acest caz, cea mai bună soluție este să configurați Bitdefender să permită în mod automat conexiunile către și de la aplicația software respectivă.

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **FIREWALL**, efectuează clic pe **Setări**.
3. În fereastra **Reguli**, efectuează clic pe **Adăugare regulă**.



4. Va apărea o nouă fereastră în care puteți adăuga detaliile. Asigurați-vă că ați selectat toate tipurile de rețea disponibile și în secțiunea **Permisivune** selectați **Permite**.

Închideți Bitdefender, deschideți aplicația software și încercați din nou să vă conectați la internet.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea „*Solicitarea ajutorului*” (p. 333).

6.1.7. Nu pot accesa un dispozitiv din rețeaua mea

În funcție de rețeaua la care sunteți conectat, firewallul Bitdefender poate bloca conexiunea dintre sistemul dumneavoastră și un alt dispozitiv (cum ar fi un alt computer sau o imprimantă). În consecință, nu mai puteți partaja sau imprima fișiere.

În acest caz, cea mai bună soluție este să configurezi Bitdefender să permită în mod automat conexiunile către și de la dispozitivul respectiv, după cum urmează:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **FIREWALL**, efectuează clic pe **Setări**.
3. În fereastra **Reguli**, efectuează clic pe **Adăugare regulă**.
4. În fereastra **Setări**, activează opțiunea **Aplică această regulă tuturor aplicațiilor**.
5. Dă clic pe fila **Avansat**.
6. În caseta **Adresă remote personalizată**, introdu adresa IP a calculatorului sau imprimantei la care dorești să ai acces nerestricționat.

Dacă tot nu vă puteți conecta la dispozitiv, este posibil ca problema să nu fie cauzată de Bitdefender.

Verificați alte cauze posibile, cum ar fi:

- Firewallul de pe celălalt calculator poate bloca partajarea de fișiere și imprimante cu calculatorul dumneavoastră.
- Dacă se folosește Windows Firewall, acesta poate fi configurat să permită partajarea de fișiere, după cum urmează:



● În **Windows 7**:

1. Faceți clic pe **Start**, mergeți la **Control Panel** și selectați **System and Security**.
2. Mergeți la **Windows Firewall** și faceți clic pe **Permite aplicației să comunice prin firewall-ul de protecție Windows**.
3. Selectați căsuța **File and Printer Sharing**.

● În **Windows 8 și Windows 8.1**:

1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.
2. Faceți clic pe **Sistem și securitate**, mergeți la **Windows Firewall** și selectați **Permite aplicației să comunice prin Paravanul de protecție Windows**.
3. Selectați căsuța **File and Printer Sharing** și faceți clic pe **OK**.

● În **Windows 10**:

1. Introduceți "Allow an app through Windows Firewall" în caseta de căutare din bara de sarcini și faceți clic pe pictogramă.
2. Faceți clic pe **Modificare setări**.
3. Din lista **Aplicații și funcții permise**, bifați caseta **Partajare fișiere și imprimată** și faceți clic pe **OK**.

● Dacă se folosește un alt program firewall, consultați documentația sau fișierul de ajutor ale acestuia.

● Cauze generale care pot împiedica folosirea sau conectarea la imprimanta partajată:

● Poate fi necesar să vă conectați la un cont Windows de administrator pentru a avea acces la imprimanta partajată.

● Numai anumite calculatoare și anumiți utilizatori pot accesa imprimanta partajată. Dacă partajați imprimanta dumneavoastră, verificați restricțiile de acces stabilite pentru aceasta pentru a vedea dacă utilizatorul de pe celălalt calculator o poate accesa. Dacă încercați să vă conectați la o imprimantă partajată, întrebați utilizatorul de pe celălalt calculator dacă vi se permite accesul la imprimantă.



- Imprimanta conectată la calculatorul dumneavoastră sau la celălalt calculator nu este partajată.
- Imprimanta partajată nu este adăugată pe calculator.



Notă

Pentru a afla cum să administrați imprimantele partajate (partajarea unei imprimante, stabilirea sau eliminarea permisiunilor de acces la o imprimantă, conectarea la o imprimantă de rețea sau partajată), mergeți la Centrul de Asistență și Suport al Windows (în meniul Start, faceți clic pe **Help and Support**).

- Accesul la o imprimantă din rețea poate fi restricționat pentru anumite computere sau pentru anumiți utilizatori. Este recomandat să consultați administratorul rețelei pentru a afla dacă vă puteți conecta la imprimanta în cauză.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea „*Solicitarea ajutorului*” (p. 333).

6.1.8. Conexiunea mea la internet este lentă

Această situație poate apărea după instalarea Bitdefender. Problema poate fi cauzată de erori de configurare a firewallului Bitdefender.

Pentru a remedia această problemă:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
 2. În secțiunea **FIREWALL**, dezactivează butonul pentru a dezactiva această caracteristică.
 3. Verificați dacă, după ce ați dezactivat firewallul Bitdefender, conexiunea dumneavoastră la internet s-a îmbunătățit.
- Dacă nu se remediază problema cu viteza redusă a conexiunii la internet, este posibil ca problema să nu fie cauzată de Bitdefender. Trebuie să contactați furnizorul dumneavoastră de servicii de internet pentru a verifica dacă conexiunea este funcțională la nivelul acestuia.

În cazul în care primiți o confirmare din partea furnizorului dumneavoastră de servicii de internet că respectiva conexiune este funcțională la nivelul său, iar problema încă persistă, contactați



Bitdefender conform descrierii din secțiunea „*Solicitarea ajutorului*” (p. 333).

- În cazul în care conexiunea la internet s-a îmbunătățit după dezactivarea firewallului Bitdefender:
 - a. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
 - b. În panoul **FIREWALL**, efectuează clic pe **Setări**.
 - c. Accesează fila **Adaptoare rețea** și setează conexiunea la internet pe **Acasă/Birou**.
 - d. În fila **Setări**, dezactivează opțiunea **Protecție împotriva scanării porturilor**.
În secțiunea **Mod ascuns**, dă clic pe **Modifică setările de vizibilitate**. Activează Modul ascuns pentru adaptorul de rețea la care ești conectat.
 - e. Închideți Bitdefender, reporniți sistemul și verificați viteza conexiunii la internet.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea „*Solicitarea ajutorului*” (p. 333).

6.1.9. Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet

Dacă dispuneți de o conexiune lentă la internet (cum ar fi cea de tip dial-up), în timpul procesului de actualizare pot apărea erori.

Pentru a îți păstra sistemul actualizat cu cea mai recentă bază de date cu informațiile privind amenințările a Bitdefender:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței **Bitdefender**.
2. Selectați secțiunea **Actualizare**.
3. Dezactivează butonul **Actualizare discretă**.
4. Data viitoare când va fi disponibilă o actualizare, ți se va solicita să selectezi actualizarea pe care dorești să o descarci. Selectează numai opțiunea **Actualizare semnături**.



5. Bitdefender va descărca și instala numai baza de date cu informații privind amenințările.

6.1.10. Serviciile Bitdefender nu răspund

Acest articol vă ajută să remediați problema **Serviciile Bitdefender nu răspund**. Această problemă poate apărea în următoarele situații:

- Pictograma Bitdefender din **bara de sistem** este afișată în culoarea gri și veți fi notificat de faptul să serviciile Bitdefender nu răspund.
- Fereastra Bitdefender indică faptul că serviciile Bitdefender nu răspund.

Problema poate fi cauzată de:

- erori temporare de comunicare între serviciile Bitdefender.
- unele dintre serviciile Bitdefender sunt oprite.
- alte soluții de securitate rulează pe calculatorul dumneavoastră, în același timp cu Bitdefender.

Pentru a remedia această problemă, încercați următoarele soluții:

1. Așteptați câteva momente pentru a vedea dacă apar schimbări. Eroarea poate fi temporară.
2. Reporniți calculatorul și așteptați câteva momente până când se încarcă Bitdefender. Deschideți Bitdefender pentru a vedea dacă eroarea persistă. De obicei, repornirea calculatorului rezolvă problema.
3. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați Bitdefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați Bitdefender.

Pentru mai multe informații, consultați capitolul **„Cum elimin celelalte soluții de securitate?”** (p. 77).

Dacă eroarea persistă, vă rugăm să contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea **„Solicitarea ajutorului”** (p. 333).

6.1.11. Filtrul Antispam nu funcționează corespunzător

Acest articol vă ajută să remediați următoarele probleme legate de funcționarea filtrului antispam al Bitdefender:

- **Mai multe mesaje e-mail legitime sunt marcate ca [spam].**



- Multe mesaje spam nu sunt marcate corespunzător de filtrul antispam.
- Filtrul antispam nu detectează niciun mesaj spam.

Mesaje legitime sunt marcate ca [spam]

Mesaje legitime sunt marcate ca [spam] pentru că filtrul antispam Bitdefender le percepe ca atare. În mod normal, puteți rezolva această problemă printr-o configurare adecvată a filtrului Antispam.

Bitdefender adaugă automat într-o Listă de prieteni destinatarii mesajelor e-mail trimise de dumneavoastră. Mesajele e-mail primite de la persoanele de pe Lista de prieteni sunt considerate a fi legitime. Ele nu sunt verificate de filtrul antispam și, astfel, nu sunt marcate niciodată ca [spam].

Configurarea automată a Listei de prieteni nu previne erorile de detecție care pot apărea în următoarele situații:

- Primiți multe mesaje comerciale nesolicitate, ca urmare a înscrierii pe diferite site-uri web. În acest caz, soluția este să adăugați adresele de e-mail de la care primiți astfel de mesaje în Lista de prieteni.
- O parte semnificativă a mesajelor e-mail pe care le primiți sunt trimise de oameni cărora nu le-ați scris niciodată pe e-mail, cum ar fi: clienți, potențiali parteneri de afaceri și alții. În acest caz, sunt necesare alte soluții.

Dacă folosiți unul dintre clienții de e-mail în care se integrează Bitdefender, **indicați erorile de detecție.**




Notă

Bitdefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, consultați „*Clienți și protocoale de e-mail compatibile*” (p. 108).

Adăugați-vă contactele pe Lista de prieteni

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje legitime pe Lista de prieteni. Urmați acești pași:

1. În clientul dumneavoastră de mail, selectați un mesaj e-mail al expeditorului pe care doriți să-l adăugați pe Lista de prieteni.
2. Faceți clic pe butonul  **Adaugă prieten** din bara de instrumente antispam Bitdefender.



3. Vi se poate cere să confirmați adresa adăugată pe Lista de prieteni. Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.



Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.

Dacă folosiți un alt client de mail, puteți adăuga contacte pe Lista de prieteni din interfața Bitdefender. Urmați acești pași:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTISPAM**, efectuează clic pe **Administrare prieteni**.
Va apărea o fereastră de configurare.
3. Introdu adresa de e-mail de la care dorești să primești mereu mesaje și apoi dă clic pe **ADĂUGARE**. Puteți adăuga oricâte adrese de e-mail doriți.
4. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Indicați erorile de detecție

Dacă folosiți un client de e-mail compatibil, puteți corecta cu ușurință filtrul antispam (indicând ce mesaje e-mail nu ar fi trebuit marcate ca fiind de tip [spam]). Astfel, veți îmbunătăți eficiența filtrului antispam. Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele legitime pe care Bitdefender le-a marcat incorect ca [spam].
4. Faceți clic pe butonul  **Adaugă prieten** din bara de instrumente antispam Bitdefender, pentru a adăuga expeditorul pe Lista de prieteni. Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare. Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.
5. Faceți clic pe butonul  **Nu este spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail). Mesajul e-mail va fi mutat în directorul Mesaje primite.

Numeroase mesaje spam nu sunt detectate

Dacă primiți multe mesaje spam care nu sunt marcate [spam], trebuie să configurați filtrul antispam Bitdefender, pentru a-i îmbunătăți eficiența.



Încercați următoarele soluții:

1. Dacă folosiți unul dintre clienții de e-mail în care se integrează Bitdefender, **indicați mesajele spam nedetectate.**


Notă

Bitdefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, consultați *„Clienți și protocoale de e-mail compatibile”* (p. 108).

2. **Adăugați spammerii pe Lista de spammeri.** Mesajele e-mail primite de la adrese de pe Lista de spammeri sunt marcate automat ca [spam].


Indicați mesajele spam nedetectate

Dacă folosiți un client de mail admis, puteți indica cu ușurință care mesaje e-mail ar fi trebuit detectate ca spam. Astfel, veți îmbunătăți eficiența filtrului antispam. Uurmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți la directorul Inbox.
3. Selectați mesajele spam nedetectate.
4. Faceți clic pe butonul  **Spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail). Acestea sunt marcate imediat ca [spam] și mutate în directorul de mesaje nesolicitate (junk).

Adăugați spammeri pe Lista de spammeri

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje spam pe Lista de spammeri. Uurmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele pe care Bitdefender le-a marcat ca [spam].
4. Faceți clic pe butonul  **Adaugă spammer** din bara de instrumente antispam Bitdefender.



5. Vi se poate cere să confirmați adresa adăugată pe Lista de spammeri. Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.

Dacă folosiți un alt client de mail, puteți adăuga manual spammeri în Lista de spammeri din interfața Bitdefender. Este recomandat să procedați astfel numai atunci când ați primit mai multe mesaje spam de la aceeași adresă de e-mail. Urmați acești pași:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În panoul **ANTISPAM**, efectuează clic pe **Administrare spammeri**.
Va apărea o fereastră de configurare.
3. Introdu adresa de e-mail a spammer-ului și apoi dă clic pe **ADĂUGARE**.
Puteți adăuga oricâte adrese de e-mail doriți.
4. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Filtrul antispam nu detectează niciun mesaj spam

Dacă niciun mesaj spam nu este marcat ca [spam], este posibil să existe probleme legate de filtrul Antispam Bitdefender. Înainte de a remedia această problemă, asigurați-vă că ea nu se datorează următoarelor cauze:

- Este posibil ca protecția antispam să fie dezactivată. Pentru a verifica starea protecției antispam, dă clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**. Accesează secțiunea **Antispam** pentru a verifica dacă această caracteristică este activată.

Dacă protecția Antispam este dezactivată, aceasta este cauza problemei dvs. Faceți clic pe selectorul corespunzător pentru a activa protecția antispam.

- Protecția antispam Bitdefender este disponibilă numai pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3. Aceasta înseamnă că:
 - Mesajele e-mail primite prin servicii de e-mail oferite online (cum ar fi Yahoo, Gmail, Hotmail sau altele) nu sunt supuse verificării antispam de către Bitdefender.
 - Dacă aveți un client de e-mail configurat să primească mesaje prin alt protocol decât POP3 (de exemplu IMAP4), Bitdefender nu supune aceste mesaje unei verificări antispam.



Notă

POP3 este unul dintre cele mai des folosite protocoale de descărcare a mesajelor e-mail de pe un server de mail. Dacă nu știți ce protocol folosește clientul dumneavoastră de e-mail pentru a descărca mesajele, întrebați persoana care l-a configurat.

- Bitdefender Total Security nu scanează traficul POP3 generat de Lotus Notes.

O soluție posibilă este repararea sau reinstalarea produsului. Dacă doriți, puteți contacta Bitdefender pentru suport, folosind informațiile din secțiunea „*Solicitarea ajutorului*” (p. 333).

6.1.12. Funcția Completare automată din Portofel nu funcționează

Ați salvat datele tale de autentificare în Bitdefender Password Manager și ai observat că funcția de completare automată nu funcționează. De obicei, această problemă apare atunci când extensia Portofelului Bitdefender nu este instalată în browserul dumneavoastră.

Pentru a remedia această problemă, urmați pașii de mai jos:

● În Internet Explorer:

1. Deschideți Internet Explorer.
2. Faceți clic pe Instrumente.
3. Faceți clic pe Gestionare programe de completare.
4. Faceți clic pe Bare de instrumente și extensii.
5. Poziționați cursorul pe **Portofel Bitdefender** și faceți clic pe **Activare**.

● În Mozilla Firefox:

1. Deschideți Mozilla Firefox.
2. Faceți clic pe Instrumente.
3. Faceți clic pe Programe de completare.
4. Faceți clic pe Extensii.
5. Poziționați cursorul pe **Portofel Bitdefender** și faceți clic pe **Activare**.

● În Google Chrome:



1. Deschideți Google Chrome.
2. Mergeți la pictograma Meniului.
3. Efectuează clic pe Mai multe instrumente.
4. Faceți clic pe Extensii.
5. Poziționați cursorul pe **Portofel Bitdefender** și faceți clic pe **Activare**.



Notă

Programul de completare se va activa după repornirea browserului.

Apoi verificați dacă funcția de completare automată din Portofel funcționează pentru conturile dumneavoastră online.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea „*Solicitarea ajutorului*” (p. 333).

6.1.13. Nu s-a reușit dezinstalarea Bitdefender

Dacă doriți să ștergeți produsul Bitdefender și observați că procesul este suspendat sau sistemul se blochează, faceți clic pe **Anulare** pentru a abandona acțiunea. Dacă anularea nu este posibilă, reporniți sistemul.

Dacă dezinstalarea eșuează, în sistemul dumneavoastră pot rămâne unele chei de regiștri și fișiere Bitdefender. Aceste rămășițe pot împiedica instalarea ulterioară a Bitdefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului.

Pentru a șterge definitiv Bitdefender de pe sistemul tău:

● În Windows 7:

1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
2. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
3. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
4. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

● În Windows 8 și Windows 8.1:



1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
5. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

● În **Windows 10**:

1. Faceți clic pe **Start**, apoi pe Setări.
2. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.
3. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
6. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

6.1.14. Sistemul meu nu pornește după ce am instalat Bitdefender

Dacă se întâmplă ca, după ce tocmai ați instalat Bitdefender, să nu puteți reporni sistemul în modul normal, pot exista mai multe motive pentru această problemă.

Cel mai probabil această problemă este cauzată fie de o instalare anterioară a Bitdefender care nu a fost dezinstalată corespunzător fie de o altă soluție de securitate care este instalată pe sistem.

Mai jos sunt prezentate modurile în care să acționați pentru fiecare situație:

● **Ați avut Bitdefender instalat anterior și acesta nu a fost dezinstalat corespunzător.**

Pentru a remedia această problemă:

1. Reporniți sistemul în Safe Mode. Pentru a afla cum poți face acest lucru, consultă secțiunea **„Cum pot să repornesc sistemul în Safe Mode?”** (p. 79).
2. Ștergeți Bitdefender din sistemul dumneavoastră:



- În **Windows 7**:
 - a. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
 - b. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
 - c. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
 - d. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.
 - e. Reporniți sistemul în modul normal.
 - În **Windows 8 și Windows 8.1**:
 - a. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.
 - b. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
 - c. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
 - d. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
 - e. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.
 - f. Reporniți sistemul în modul normal.
 - În **Windows 10**:
 - a. Faceți clic pe **Start**, apoi pe **Setări**.
 - b. Faceți clic pe pictograma **Sistem** din secțiunea **Setări**, apoi selectați **Aplicații instalate**.
 - c. Găsiți **Bitdefender Total Security** și selectați **Dezinstalare**.
 - d. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
 - e. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
 - f. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.
 - g. Reporniți sistemul în modul normal.
3. Reinstalați produsul dumneavoastră Bitdefender.



- **Ați avut instalată o altă soluție de securitate înainte, iar aceasta nu a fost dezinstalată corespunzător.**

Pentru a remedia această problemă:

1. Reporniți sistemul în Safe Mode. Pentru a afla cum poți face acest lucru, consultă secțiunea „*Cum pot să repornesc sistemul în Safe Mode?*” (p. 79).
2. Ștergeți cealaltă soluție de securitate din sistem:

- **În Windows 7:**

- a. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
- b. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Ștergere**.
- c. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

- **În Windows 8 și Windows 8.1:**

- a. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.
- b. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
- c. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Ștergere**.
- d. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.

- **În Windows 10:**

- a. Faceți clic pe **Start**, apoi pe Setări.
- b. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.
- c. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Dezinstalare**.
- d. Așteptați finalizarea procesului de dezinstalare și apoi reporniți sistemul.



Pentru a dezinstala celălalt software în mod corect, mergeți pe site-ul web al producătorului și lansați instrumentul de dezinstalare sau contactați direct producătorul, solicitând instrucțiunile de dezinstalare.

3. Reporniți sistemul în modul normal și reinstalați Bitdefender.

Situația nu s-a rezolvat deși ați urmat toți pașii de mai sus.

Pentru a remedia această problemă:

1. Reporniți sistemul în Safe Mode. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot să repornesc sistemul în Safe Mode?”* (p. 79).
2. Cu ajutorul funcției System Restore din Windows puteți restabili computerul la o dată anterioară instalării produsului Bitdefender.
3. Reporniți sistemul în modul normal și contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea *„Solicitarea ajutorului”* (p. 333).

6.2. Eliminarea amenințărilor din sistemul dumneavoastră

Amenințările vă pot afecta sistemul în moduri diferite, iar modul de acțiune al Bitdefender depinde de tipul de atac al amenințării. Deoarece amenințările își schimbă comportamentul în mod frecvent, este dificil de stabilit un model privind comportamentul și acțiunile acestora.

Există cazuri când Bitdefender nu poate elimina în mod automat amenințarea din sistemul dumneavoastră. În astfel de cazuri, este necesară intervenția dumneavoastră.

- *„Bitdefender Modul de recuperare (Mediul de recuperare în Windows 10)”* (p. 215)
- *„Ce trebuie să faci atunci când Bitdefender detectează amenințări pe computerul tău?”* (p. 218)
- *„Cum elimin o amenințare dintr-o arhivă?”* (p. 220)
- *„Cum elimin o amenințare dintr-o arhivă de e-mail?”* (p. 221)
- *„Ce trebuie să fac dacă suspectez că un fișier este periculos?”* (p. 222)
- *„Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?”* (p. 223)



- „Ce reprezintă elementele omise din jurnalul de scanare?” (p. 223)
- „Ce reprezintă fișierele supracomprimate din jurnalul de scanare?” (p. 223)
- „De ce Bitdefender a șters în mod automat un fișier infectat?” (p. 224)

Dacă problema dumneavoastră nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic a Bitdefender folosind informațiile din capitolul „*Solicitarea ajutorului*” (p. 333).

6.2.1. Bitdefender Modul de recuperare (Mediul de recuperare în Windows 10)

Mediu de recuperare este o caracteristică a Bitdefender care vă permite să scanați și să dezinfectați toate partițiile hard discului din/ de pe sistemul de operare.

Odată ce Bitdefender Total Security este instalat pe un **Windows 7, Windows 8 și Windows 8.1** și fișierul de imagine de salvare Bitdefender este descărcat, Mediul de recuperare poate fi folosit chiar și atunci când nu puteți porni sistemul în Windows.

În Windows 10, Modul de recuperare Bitdefender este integrat în Windows RE, ceea ce înseamnă că nu este necesară descărcarea unei imagini a Modulului de recuperare pe acest sistem de operare.

Descărcarea imaginii Modulului de recuperare Bitdefender

Pentru a putea utiliza Modul de recuperare în **Windows 7, Windows 8 și Windows 8.1**, mai întâi trebuie să descarci fișierul de imagine, după cum urmează:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, efectuează clic pe **Modul de recuperare**.
3. Dă clic pe **Da** în fereastra de confirmare afișată pentru a reporni computerul.

Așteaptă până când se descarcă fișierul de imagine al Modulului de recuperare Bitdefender de pe serverele Bitdefender. Calculatorul va fi repornit imediat ce se finalizează descărcarea,



Se va afișa un meniu prin care vi se va solicita să selectați sistemul de operare. În această fază, puteți alege să porniți sistemul în Mediul de recuperare sau în modul normal.



Notă

Datorită integrării cu Mediul de recuperare Windows în **Windows 10**, nu este necesară descărcarea unei imagini a Modulului de recuperare pe acest sistem de operare.

Pornirea sistemului tău în Modul de recuperare în Windows 7, Windows 8 și Windows 8.1

Puteți accesa Mediul de recuperare în unul dintre următoarele două moduri:

Din **interfața Bitdefender**

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, efectuează clic pe **Modul de recuperare**.
3. Dă clic pe **Da** în fereastra de confirmare afișată pentru a reporni computerul.
4. După ce este repornit computerul, apare un meniu care vă va solicita să selectați un sistem de operare. Selectați **Mediul de recuperare Bitdefender** pentru a porni într-un mediu Bitdefender din care puteți elibera partiția Windows.
5. În cazul în care vi se solicită, apăsați **Enter** și ajustați rezoluția ecranului la valoarea cea mai apropiată de cea pe care o folosiți de obicei. Apoi apăsați din nou pe **Enter**.

Mediul de recuperare Bitdefender se încarcă în câteva momente.

Porniți computerul direct în Mediul de recuperare

În cazul în care nu mai pornește Windows, puteți porni computerul direct în Mediul de recuperare al Bitdefender, urmând pașii de mai jos:

● În **Windows 7**:

1. Apasă tasta **F8** până când apare fereastra **Opțiuni avansate de pornire**.
2. Utilizează săgețile pentru a selecta Modul de recuperare Bitdefender și apoi apasă tasta **Enter**.



Mediul de recuperare pentru Bitdefender se va încărca în câteva momente.

● În **Windows 8 și Windows 8.1:**

1. Apasă tasta **Shift** până când apare fereastra **Opțiuni avansate la startup**.
2. Selectează opțiunea **Utilizează un alt sistem de operare** și apoi Modul de recuperare Bitdefender.

Mediul de recuperare pentru Bitdefender se va încărca în câteva momente.

 **Notă**

Este posibilă pornirea calculatorului în Mediul de recuperare numai dacă a fost descărcat anterior fișierul de imagine al Modulului de recuperare după cum este descris în „[Descărcarea imaginii Modulului de recuperare Bitdefender](#)” (p. 215).

Pornirea sistemului în Mediul de recuperare în Windows 10

Poți intra în Modul de recuperare numai din produsul tău Bitdefender, după cum urmează:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. În secțiunea **ANTIVIRUS**, efectuează clic pe **Mediul de recuperare**.
3. Efectuează clic pe **Repornire** în fereastra care se deschide.

Mediul de recuperare Bitdefender se încarcă în câteva momente.

Scanarea sistemului tău în Modul de recuperare (Mediul de recuperare în Windows 10)

Pentru a scana sistemul în Modul de recuperare (Mediul de recuperare):

● În **Windows 7, Windows 8 și Windows 8.1:**

1. Accesați Mediul de recuperare, conform descrierii din „[Pornirea sistemului tău în Modul de recuperare în Windows 7, Windows 8 și Windows 8.1](#)” (p. 216).
2. Va apărea logo-ul Bitdefender și motoarele soluției de securitate vor începe să fie copiate.



3. Va fi afișată o fereastră de întâmpinare. Faceți clic pe **Continuare**.
4. Este demarată procedura de actualizare a bazei de date cu informații privind amenințările.
5. După ce s-a finalizat actualizarea, va apărea fereastra pentru scanarea antivirus la cerere a Bitdefender.
6. Faceți clic pe **Scanează acum**, selectați locația de scanat din fereastra care apare și faceți clic pe **Deschidere** pentru a începe scanarea.

Este recomandat scanarea întregii partiții Windows.



Notă

Atunci când lucrați în Mediul de recuperare, veți întâlni denumiri de partiții de tip Linux. Partițiile discului vor fi afișate ca sda1 corespunzând probabil (C:) partiție de tip Windows, sda2 corespunzând (D:) și așa mai departe..

7. Așteptați finalizarea procesului de scanare. Dacă este detectată o amenințare, urmează instrucțiunile pentru îndepărtarea acesteia.
8. Pentru a ieși din Mediul de recuperare, faceți clic dreapta în secțiunea liberă de pe desktop, selectați **Ieșire** din meniul care apare și apoi selectați dacă doriți să reporniți sau să închideți computerul.

● În Windows 10:

1. Accesează Mediul de recuperare, conform descrierii din „**Pornirea sistemului în Mediul de recuperare în Windows 10**” (p. 217).
2. Procesul de scanare Bitdefender începe automat imediat ce sistemul este încărcat în Mediul de recuperare.
3. Așteptați finalizarea procesului de scanare. Dacă este detectată o amenințare, urmează instrucțiunile pentru îndepărtarea acesteia.
4. Pentru a ieși din Mediul de recuperare, efectuează clic pe butonul **ÎNCHIDERE** din fereastra cu rezultatele scanării.

6.2.2. Ce trebuie să faci atunci când Bitdefender detectează amenințări pe computerul tău?

Poți descoperi că există o amenințare pe calculatorul tău prin una din următoarele metode:



- V-ați scanat calculatorul și Bitdefender a găsit elemente infectate pe acesta.
- O alertă de amenințări te informează că Bitdefender a blocat una sau mai multe amenințări pe calculatorul tău.

În astfel de situații, actualizează Bitdefender pentru a te asigura că ai cele mai recente baze de date cu informații privind amenințările și efectuează o scanare a sistemului pentru analizarea acestuia.

După finalizarea scanării sistemului, selectați acțiunea dorită pentru elementele infectate (dezinfectare, ștergere, mutare în carantină).

Avertisment

În cazul în care considerați că fișierul face parte din sistemul de operare Windows sau că nu este un fișier infectat, nu urmați acești pași și contactați serviciul de asistență clienți Bitdefender cât mai curând posibil.

Dacă acțiunea selectată nu a putut fi efectuată, iar jurnalul de scanare indică o infectare care nu a putut fi eliminată, trebuie să ștergeți fișierul/fișierele manual:

Prima metodă poate fi utilizată în modul normal:

1. Dezactivați protecția antivirus în timp real a Bitdefender:
 - a. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
 - b. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
 - c. În fereastra **Shield**, dezactivează opțiunea **Bitdefender Shield**.
2. Afișați elementele ascunse din Windows. Pentru a afla cum poți face acest lucru, consultă secțiunea „*Cum pot afișa elementele ascunse din Windows?*” (p. 77).
3. Mergeți la locația unde se găsește fișierul infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Activați protecția antivirus în timp real a Bitdefender.

În cazul în care prima metodă nu a reușit să elimine infecția:

1. Reporniți sistemul în Safe Mode. Pentru a afla cum poți face acest lucru, consultă secțiunea „*Cum pot să repornesc sistemul în Safe Mode?*” (p. 79).



2. Afișați elementele ascunse din Windows. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot afișa elementele ascunse din Windows?”* (p. 77).
3. Mergeți la locația unde se găsește fișierul infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Reporniți sistemul în mod normal.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 333).

6.2.3. Cum elimin o amenințare dintr-o arhivă?

O arhivă este un fișier sau o colecție de fișiere comprimate într-un format special, în scopul reducerii spațiului de pe hard-disc necesar stocării fișierelor.

Unele dintre aceste formate sunt formate deschise, ceea ce permite Bitdefender să scaneze în interiorul acestora și apoi să ia măsurile corespunzătoare pentru eliminarea infecțiilor.

Alte formate de arhivă sunt închise complet sau parțial, iar Bitdefender poate identifica numai prezența amenințărilor din acestea însă nu poate lua niciun fel de măsură în acest sens.

Dacă Bitdefender anunță că a fost detectată o amenințare într-o arhivă și nu este disponibilă nicio acțiune, aceasta înseamnă că eliminarea amenințării nu este posibilă din cauza restricțiilor legate de setările referitoare la permisiunile arhivelor.

Iată cum poți elimina o amenințare stocată într-o arhivă:

1. Identifică arhiva care conține amenințarea în urma unei scanări a sistemului.
2. Dezactivați protecția antivirus în timp real a Bitdefender:
 - a. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
 - b. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
 - c. În fereastra **Shield**, dezactivează opțiunea **Bitdefender Shield**.
3. Accesați locația arhivei și dezarhivați-o utilizând o aplicație de arhivare, cum ar fi WinZip.



4. Identificați fișierul infectat și ștergeți-l.
5. Ștergeți arhiva inițială pentru a vă asigura că fișierul infectat este eliminat în totalitate.
6. Recomprimați fișierele într-o nouă arhivă utilizând o aplicație de arhivare, cum ar fi WinZip.
7. Activați protecția antivirus în timp real a Bitdefender și executați o scanare a sistemului pentru a vă asigura că sistemul nu este infectat.



Notă

Este important de reținut faptul că o amenințare aflată într-o arhivă nu reprezintă o amenințare imediată la adresa sistemului tău deoarece trebuie să fie dezarhivată și executată pentru a putea infecta calculatorul.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea „*Solicitarea ajutorului*” (p. 333).

6.2.4. Cum elimin o amenințare dintr-o arhivă de e-mail?

Bitdefender poate de asemenea să identifice amenințări din bazele de date de e-mail și arhivele de e-mail stocate pe disc.

Uneori este necesară identificarea mesajului infectat utilizând informațiile puse la dispoziție în raportul de scanare și ștergerea acestuia în mod manual.

Iată cum poți elimina o amenințare stocată într-o arhivă de e-mail:

1. Scațați baza de date de e-mail folosind Bitdefender.
2. Dezactivați protecția antivirus în timp real a Bitdefender:
 - a. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
 - b. În secțiunea **ANTIVIRUS**, dă clic pe **Setări**.
 - c. În fereastra **Shield**, dezactivează opțiunea **Bitdefender Shield**.
3. Deschideți raportul de scanare și utilizați informațiile de identificare (Subiect, De la, Către) aferente mesajelor infectate pentru a le localiza în clientul de e-mail.
4. Ștergeți mesajele infectate. Majoritatea clienților de e-mail mută mesajul șters într-un director de recuperare, de unde acesta poate fi recuperat.



Trebuie să vă asigurați că mesajul este șters și din acest director de recuperare.

5. Arhivați directorul în care se află mesajul infectat.

- În Microsoft Outlook 2007: În meniul File, faceți clic pe Data File Management. Selectați fișierele din directoarele personale (.pst) pe care intenționați să le compactați și faceți clic pe Settings. Faceți clic pe Compactare acum.
- În Microsoft Outlook 2010 / 2013 / 2016: Din meniul Fișier, selectați Detalii și apoi Setări cont (Adăugare sau eliminare conturi sau modificare setări de conectare existente) Apoi faceți clic pe Fișier de date, selectați fișierele din directoarele personale (.pst) pe care intenționați să le compactați și faceți clic pe Setări. Faceți clic pe Compactare acum.

6. Activați protecția antivirus în timp real a Bitdefender.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea „*Solicitarea ajutorului*” (p. 333).

6.2.5. Ce trebuie să fac dacă suspectez că un fișier este periculos?

Există posibilitatea să considerați că un anumit fișier din sistemul dumneavoastră este periculos chiar dacă Bitdefender nu l-a detectat.

Pentru a te asigura că sistemul tău este protejat:

1. Executați o **scanare a sistemului** cu Bitdefender. Pentru a afla cum poți face acest lucru, consultă secțiunea „*Cum îmi scanez sistemul?*” (p. 52).
2. Dacă procesul de scanare nu a detectat nimic, dar încă aveți dubii cu privire la fișier, contactați reprezentanții serviciului de asistență pentru ajutor.

Pentru a afla cum poți face acest lucru, consultă secțiunea „*Solicitarea ajutorului*” (p. 333).



6.2.6. Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?

Aceasta reprezintă doar o notificare referitoare la faptul că Bitdefender a detectat aceste fișiere ca fiind protejate fie prin parolă, fie cu o anumită formă de criptare.

Cel mai frecvent, elementele protejate prin parolă sunt următoarele:

- Fișiere care aparțin unei alte soluții de securitate.
- Fișiere care aparțin sistemului de operare.

Pentru a putea scana conținutul, aceste fișiere trebuie să fie extrase sau decriptate.

În cazul în care conținutul respectiv este extras, Bitdefender va scana automat conținutul pentru a vă proteja calculatorul. Dacă doriți să scanați acele fișiere folosind Bitdefender, trebuie să contactați producătorul produsului pentru a obține mai multe detalii despre respectivele fișiere.

Noi vă recomandăm să ignorați acele fișiere deoarece acestea nu reprezintă o amenințare pentru sistemul dumneavoastră.

6.2.7. Ce reprezintă elementele omise din jurnalul de scanare?

Toate fișierele care apar ca fiind omise în raportul de scanare nu conțin niciun fel de virusi.

Pentru performanțe sporite, Bitdefender nu scanează fișiere care nu au fost modificate de la ultima scanare.

6.2.8. Ce reprezintă fișierele supracomprimate din jurnalul de scanare?

Elementele supracomprimate sunt elemente care nu au putut fi extrase de către motorul de scanare sau elemente pentru care timpul necesar decriptării ar fi fost prea lung ducând la instabilitatea sistemului.

Comprimarea în exces se referă la faptul că Bitdefender a sărit peste scanarea respectivei arhive deoarece dezarhivarea acesteia s-a dovedit a consuma prea mult din resursele sistemului. Conținutul va fi scanat pe baza accesului în timp real, dacă este cazul.



6.2.9. De ce Bitdefender a șters în mod automat un fișier infectat?

În cazul în care este detectat un fișier infectat, Bitdefender va încerca în mod automat să-l dezinfecteze. Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

Pentru anumite tipuri de amenințări, dezinfectarea nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

Acesta este cazul fișierelor de instalare care sunt descărcate de pe site-uri web nesigure. Dacă vă aflați într-o astfel de situație, descărcați fișierul de instalare de pe site-ul web al producătorului sau de pe un alt site web sigur.



ANTIVIRUS PENTRU MAC



7. INSTALARE ȘI DEZINSTALARE

Acest capitol acoperă următoarele subiecte:

- „Cerințe de sistem” (p. 226)
- „Instalarea Bitdefender Antivirus for Mac” (p. 226)
- „Eliminare Bitdefender Antivirus for Mac” (p. 231)

7.1. Cerințe de sistem

Poți instala Bitdefender Antivirus for Mac pe calculatoare Macintosh cu sistem de operare OS X Yosemite (10.10.5), OS X El Capitan (10.11.6), macOS Sierra (10.12.6), macOS High Sierra (10.13.6) sau macOS Mojave (10.14 sau mai recent).

Mac-ul tău trebuie să aibă minimum 1 GB de spațiu disponibil pe hard disk.

Este necesar să fii conectat 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. Selectează **Raport de sistem** pentru informații detaliate despre hardware.

7.2. 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**.
5. Alegeți una dintre cele două opțiuni disponibile:



● Protejează acest dispozitiv

- a. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
- b. Salvează fișierul de instalare.

● Protejează alte dispozitive

- a. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
- b. Selectează **TRIMITE LINKUL PENTRU DESCĂRCARE**.

- c. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**.

Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.

- d. Pe dispozitivul pe care dorești să instalezi produsul Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

6. Rulați produsul Bitdefender descărcat.

7. Urmează pașii de instalare.

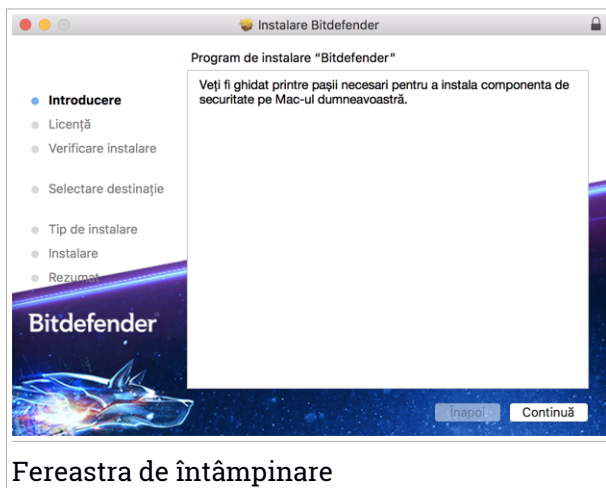
7.2.1. Proces de instalare

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. Urmăți programul asistent de instalare.



Pasul 1 - Fereastra de întâmpinare



Fereastra de întâmpinare

Faceți clic pe **Continuă**.

Pasul 2 - Citește Contractul de abonament



Citește Contractul de abonament

Înainte de a continua instalarea, este necesar să îți exprimi acordul cu privire la clauzele Contractului de abonament. Rezervă-ți câteva momente



pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Antivirus for Mac.

Din această fereastră poți selecta și limba în care dorești să instalezi produsul.

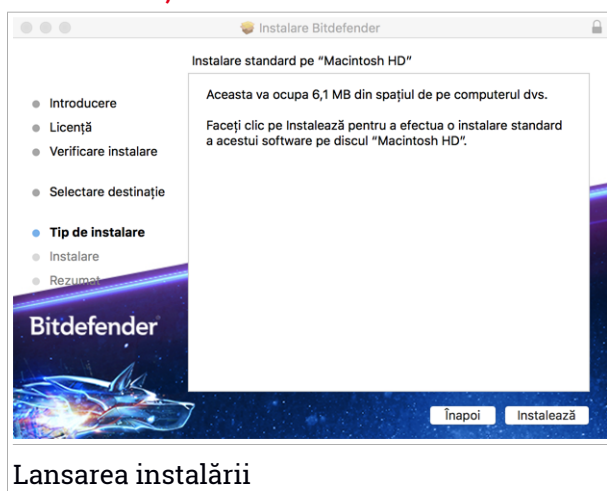
Faceți clic pe **Continuă** și apoi pe **Sunt de acord**.



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



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.



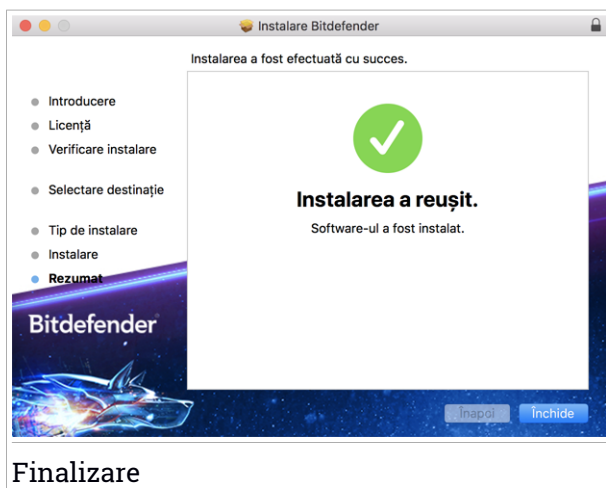
Pasul 4 - Instalare Bitdefender Antivirus for Mac



Instalarea Bitdefender Antivirus for Mac

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

Pasul 5 - Finalizare



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 10.13.0 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 afișată, efectuează clic pe linkul **Securitate & Confidențialitate**. Selectează **Permite** din partea de jos a ferestrei sau selectează Bitdefender SRL din listă și apoi **OK**.
- Dacă instalezi Bitdefender Antivirus for Mac pe macOS Mojave 10.14 sau o versiune mai nouă, se va afișa o notificare. Această notificare te informează că este necesar să permiți în mod manual Bitdefender Antivirus for Mac să-și încarce fișierele pe sistemul tău. Pentru a continua, accesează linkul **Securitate și confidențialitate** și apoi selectează **OK**. Selectează **Permite** în dreptul Bitdefender SRL.

7.3. Eliminarea Bitdefender Antivirus for Mac

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

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

1. Deschide o fereastră **Finder**, apoi accesează directorul Aplicații.
2. Deschide directorul Bitdefender și fă dublu-clic pe BitdefenderUninstaller.
3. Fă clic pe **Dezinstalare** și așteaptă finalizarea procesului.
4. Faceți clic pe **Închide** pentru a finaliza.



Important

În cazul apariției unei erori, puteți contacta serviciul Bitdefender Customer Care, așa cum se descrie în *„Solicitarea ajutorului”* (p. 333).



8. INTRODUCERE

Acest capitol acoperă următoarele subiecte:

- „Despre Bitdefender Antivirus for Mac” (p. 232)
- „Deschiderea Bitdefender Antivirus for Mac” (p. 232)
- „Fereastră principală aplicație” (p. 233)
- „Pictogramă aplicație în Dock” (p. 234)
- „Meniu de navigare” (p. 234)
- „Mod întunecat” (p. 235)

8.1. Despre Bitdefender Antivirus for Mac


Bitdefender Antivirus for Mac este un scanner antivirus puternic, care poate detecta și elimina toate tipurile de programe periculoase („amenințări”), incluzând:

- ransomware
- adware
- viruși
- spyware
- Troieni
- keylogger
- viermi

Această aplicație detectează și elimină nu numai amenințările pentru Mac, ci și amenințările pentru Windows, împiedicându-te astfel să transmiți fișiere infectate familiei, prietenilor și colegilor care utilizează calculatoare.

8.2. 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.



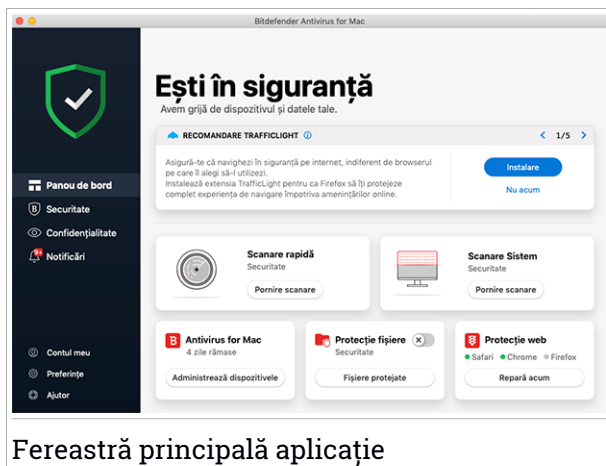
Important

Prima dată când deschizi Bitdefender Antivirus for Mac pe macOS Mojave 10.14 sau o versiune mai nouă, se va afișa o recomandare de protecție. Această recomandare apare deoarece avem nevoie de anumite drepturi de acces pentru a scana întregul sistem în vederea identificării amenințărilor. Pentru a ne acorda aceste drepturi, este necesar să fii autentificat ca administrator și să parcurgi pașii următori:

1. Accesează linkul **Preferințe sistem**.
2. Accesează pictograma  și apoi introdu datele tale de autentificare ca administrator.
3. Se afișează o nouă fereastră. Trage fișierul **BDLDaemon** în lista aplicațiilor permise.

8.3. Fereastră principală aplicație

Bitdefender Antivirus for Mac îndeplinește deopotrivă cerințele persoanelor experimentate și pe cele ale începătorilor în utilizarea calculatorului. Interfața sa grafică este proiectată pentru a se potrivi fiecărei categorii de utilizatori.



Fereastră principală aplicație

Pentru a parcurge interfața Bitdefender, în partea din stânga sus este afișat un asistent de introducere care conține detalii despre cum să interacționezi cu produsul și cum să îl configurezi. Selectează săgeata dreapta pentru a continua să primești indicații sau **Renunță la tur** pentru a închide asistentul.



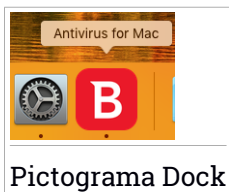
Bara de stare din partea de sus a ferestrei vă oferă informații privind starea de securitate a sistemului prin utilizarea unor mesaje explicite și a unor culori sugestive. În cazul în care nu există avertizări din partea Bitdefender Antivirus for Mac, bara de stare este de culoare verde. Atunci când este detectată o problemă de securitate, bara de stare își schimbă culoarea în roșu. Pentru informații detaliate referitoare la probleme și la modalitățile de soluționare a acestora, consultați capitolul „*Remedierea problemelor*” (p. 248).

Pentru a îți oferi o funcționare eficientă și protecție sporită în timp ce realizezi diferite activități, **Bitdefender Autopilot** va acționa ca un consultant personal de securitate. În funcție de activitatea pe care o desfășori, fie că lucrezi, fie că faci plăți online, Bitdefender Autopilot îți va oferi recomandări contextuale în funcție de modul de utilizare a dispozitivului tău și nevoile tale. Acest lucru te va ajuta să descoperi și să beneficiezi de avantajele furnizate de caracteristicile incluse în aplicația Bitdefender Antivirus for Mac.

Din meniul de navigare din partea stângă poți accesa secțiunile Bitdefender pentru o configurare detaliată și sarcini administrative avansate (filele **Protecție** și **Confidențialitate**), notificări, **contul tău Bitdefender** și secțiunea **Preferințe**. De asemenea, ne puteți contacta (fila **Ajutor**) pentru asistență în cazul în care aveți întrebări sau intervine ceva neprevăzut.

8.4. Pictogramă aplicație în Dock

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










8.5. Meniu de navigare

În partea stângă a interfeței Bitdefender se regăsește meniul de navigare, care îți permite să accesezi rapid caracteristicile Bitdefender de care ai nevoie



pentru gestionarea produsului tău. Secțiunile disponibile în această zonă sunt:

-  **Panou de bord.** De aici, poți rezolva rapid problemele de securitate, poți vizualiza recomandări în funcție de nevoile și tiparele de utilizare ale sistemului tău, poți efectua acțiuni rapide și accesa contul tău Bitdefender pentru a gestiona dispozitivele pe care le-ai adăugat la abonamentul tău Bitdefender.
-  **Securitate.** De aici, poți lansa sarcini de scanare antivirus, poți adăuga fișiere în lista de excepții, poți proteja fișiere și aplicații împotriva atacurilor de tip ransomware, îți poți securiza backup-urile Time Machine și îți poți configura protecția în timp ce navighezi pe Internet.
-  **Confidențialitate.** De aici, poți deschide aplicația Bitdefender VPN și extensia Anti-tracker în browserul web.
-  **Notificări.** De aici, poți vedea detalii despre acțiunile întreprinse asupra fișierelor scanate.
-  **Contul meu.** De aici, îți poți accesa contul tău Bitdefender pentru a verifica abonamentele și a efectua sarcinile de securitate pe dispozitivele pe care le administrezi. Sunt de asemenea disponibile detalii despre contul Bitdefender și despre abonamentul în curs.
-  **Confidențialitate.** De aici, poți configura setările Bitdefender.
-  **Ajutor.** De aici, ori de câte ori ai nevoie de asistență pentru a rezolva o situație în legătură cu produsul Bitdefender, poți contacta departamentul de Asistență tehnică. De asemenea, ne poți trimite feedback pentru a ne ajuta să îmbunătățim produsul.

8.6. Mod întunecat

Pentru a-ți feri ochii de lumina puternică atunci când lucrezi noaptea sau într-un mediu fără lumină, Bitdefender Antivirus for Mac acceptă Modul întunecat pentru Mojave 10.14 sau mai recent. Culoarele interfeței au fost optimizate astfel încât să poți utiliza Mac-ul fără a-ți obosi ochii. Interfața Bitdefender Antivirus for Mac se ajustează singură în funcție de setările de aspect ale dispozitivului tău.



9. PROTECȚIA ÎMPOTRIVA SOFTURILOR PERICULOASE

Acest capitol acoperă următoarele subiecte:

- „*Recomandări de utilizare*” (p. 236)
- „*Scanarea Mac-ului dumneavoastră*” (p. 237)
- „*Asistent scanare*” (p. 238)
- „*Carantină*” (p. 239)
- „*Bitdefender Shield (protecție în timp real)*” (p. 240)
- „*Excepții scanare*” (p. 241)
- „*Protecție web*” (p. 242)
- „*Anti-tracker*” (p. 243)
- „*Protecție Fișiere*” (p. 246)
- „*Protecție Time Machine*” (p. 248)
- „*Remediarea problemelor*” (p. 248)
- „*Notificări*” (p. 250)
- „*Actualizări*” (p. 251)

9.1. Recomandări de utilizare

Pentru a îți proteja sistemul împotriva amenințărilor și pentru a preveni infectarea accidentală a altor sisteme, respectă aceste bune practici:

- Menține activat **Bitdefender Shield** pentru a permite fișierelor de sistem să fie scanate automat de către Bitdefender Antivirus for Mac.
- Actualizează-ți produsul Bitdefender Antivirus for Mac pentru a avea acces la cele mai recente informații despre amenințări și actualizări de produse.
- Verificați și soluționați în mod regulat problemele raportate de Bitdefender Antivirus for Mac. Pentru informații detaliate, consultați capitolul „*Remediarea problemelor*” (p. 248).
- 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



tale, se adaugă un nou mesaj în secțiunea de Notificări Bitdefender. Pentru mai multe informații, accesați „*Notificări*” (p. 250).

- 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 fișier DMG, instalați-l și apoi scanați conținutul acestuia (fișierele 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 nicio altă configurație 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. 253).

9.2. Scanarea Mac-ului dumneavoastră

În afara caracteristicii **Bitdefender Shield**, care monitorizează cu regularitate aplicațiile instalate în vederea identificării acțiunilor de tip amenințare și împiedicării pătrunderii noilor amenințări 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. Efectuează clic pe **Securitate** din meniul de navigare al interfeței Bitdefender.
2. Selectează fila **Antivirus**.
3. Faceți clic pe unul dintre cele trei butoane de scanare pentru a începe scanarea dorită.
 - **Quick Scan (Scanare rapidă)** - verifică dacă există amenințări în cele mai vulnerabile locații din sistemul tău (de exemplu, directoarele care



conțin documentele, fișierele descărcate de pe internet sau din e-mail și fișierele temporare ale fiecărui utilizator).

- **Full Scan (Scanare completă)** - efectuează o verificare completă a întregului sistem pentru identificarea amenințărilor. 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).

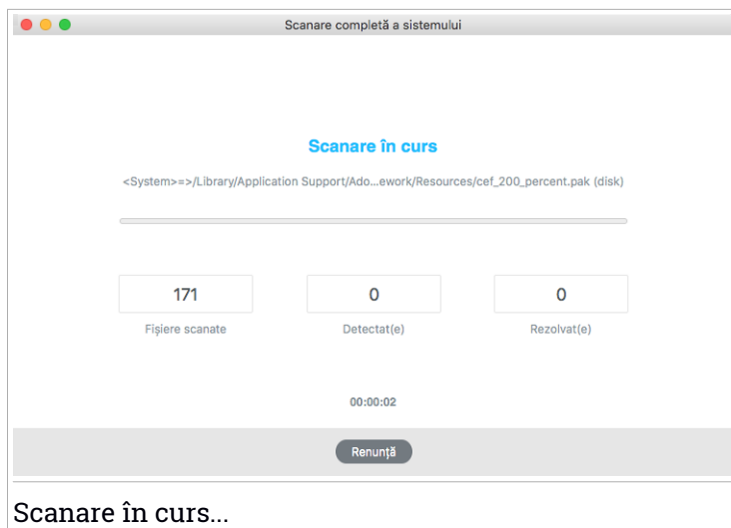
În funcție de preferințele tale, poți alege să nu scanezi anumite volume instalate prin adăugarea acestora în lista de **Excepții** din fereastra Protecție.

- **Custom Scan (Scanare personalizată)** - te ajută să verifici anumite fișiere, foldere sau volume pentru a identifica amenințările.

De asemenea, poți porni o Scanare de sistem sau o Scanare rapidă din Panoul de control.

9.3. Asistent scanare

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



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.

9.4. Carantină

Bitdefender Antivirus for Mac permite izolarea fișierelor infectate sau suspecte într-o zonă sigură, numită carantină. Atunci când sunt în carantină, amenințările sunt inofensive, pentru că nu pot fi executate sau citite.



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**.

Pentru a vizualiza lista tuturor obiectelor adăugate în carantină:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței Bitdefender.
2. Se deschide fereastra **Antivirus**.
Selectează **Deschide** din fereastra **Carantină**.

9.5. Bitdefender Shield (protecție în timp real)

Bitdefender oferă protecție în timp real împotriva unei game largi de amenințări prin scanarea tuturor aplicațiilor instalate, a versiunilor actualizate a acestora, precum și a fișierelor noi și modificate.

Pentru dezactivarea protecției în timp real:

1. Selectează **Preferințe** din meniul de navigare al interfeței Bitdefender.
2. Dezactivați **Bitdefender Shield** din fereastra **Protecție**.



Avertisment

Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați protecția în timp real pentru cât mai puțin timp posibil. Dacă protecția în timp real este dezactivată, nu veți mai fi protejat împotriva amenințărilor.

9.6. 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



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

Pentru a accesa lista de excepții:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței Bitdefender.
2. Se deschide fereastra **Antivirus**.
Selectează **Deschide** din fereastra **Excepții**.



Există două modalități de a crea o excepție de la scanare:

- Trage un fișier, director sau partiție în lista de excepții prin drag&drop.
- Apasă pe butonul marcat cu semnul plus (+), situat sub lista excepțiilor. Apoi alege fișierul, directorul sau volumul care urmează a fi exclus din operațiunea de scanare.

Pentru a șterge o excepție de la scanare, selectează-o din listă și apasă pe butonul marcat cu semnul minus (-), situat sub lista excepțiilor.

9.7. Protecție web

Bitdefender Antivirus for Mac folosește extensiile 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:

1. Selectează **Remediază acum** din secțiunea **Protecție web** a Panoului de control.
2. Se deschide fereastra **Protecție web**.

Se va afișa browser-ul web instalat pe sistemul tău. Pentru a instala extensia TrafficLight în browser-ul dumneavoastră, faceți clic pe **Descarcă extensia**.

3. Se face redirecționarea către:

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

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

Administrarea setărilor extensiilor

Sunt disponibile mai multe funcții pentru protecția dumneavoastră împotriva tuturor tipurilor de amenințări pe care le puteți întâlni în timpul browsing-ului



web. 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 - avertizează în avans cu privire la site-urile web periculoase din cadrul rezultatelor căutării tale.

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

● Lista de excepții

Site-urile web pot fi excluse de la scanarea cu motoarele Bitdefender. În câmpul corespunzător, introdu denumirea site-ului web pe care dorești să îl adaugi în lista de excepții și apoi selectează **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.
- ⚠ Această pagină web poate avea conținut periculos. Vizitați cu atenție această pagină.
- ✗ Îți recomandăm să părăsești pagina web imediat, deoarece conține programe periculoase sau alte amenințări.

În Safari, fundalul pictogramelor Semaforului este negru.

9.8. Anti-tracker

Multe dintre site-urile web pe care le accesezi utilizează instrumente de urmărire de tip tracker pentru a colecta informații despre comportamentul tău, fie pentru a le distribui unor companii terțe, fie pentru a afișa anunțuri



mai relevante pentru tine. Astfel, proprietarii site-urilor web fac bani pentru a putea oferi conținut gratuit sau pentru a continua să funcționeze. Pe lângă colectarea de informații, tracker-ele pot încetini experiența ta de navigare sau îți pot afecta lățimea de bandă.

Odată ce extensia Bitdefender Anti-tracker a fost activată în browserul web, eviți urmărirea astfel încât datele tale rămân confidențiale în timp ce navighezi online și reduci timpul necesar pentru încărcarea site-urilor web.

Extensia Bitdefender este compatibilă cu următoarele browsere web:

- Google Chrome
- Mozilla Firefox
- Safari

Tracker-ele pe care le detectăm sunt grupate în următoarele categorii:

- **Publicitate** - se utilizează pentru a analiza traficul de pe site-urile web, comportamentul utilizatorilor sau tiparele de trafic generat de utilizatori.
- **Interacțiunea cu clienții** - se utilizează pentru a măsura interacțiunea utilizatorilor cu diferite forme de introducere de informații, cum ar fi chat sau suport.
- **Esențiale** - se utilizează pentru a monitoriza funcționalitățile de importanță critică ale paginilor web.
- **Date de analiză site** - se utilizează pentru a colecta date referitoare la utilizarea paginilor web.
- **Rețele de socializare** - se utilizează pentru a monitoriza audiența pe rețelele de socializare, activitatea și implicarea utilizatorilor pentru diferite platforme de socializare.


Activarea Bitdefender Anti-tracker

Pentru a activa extensia Bitdefender Anti-tracker în browserul web:

1. Efectuează clic pe **Confidențialitate** din meniul de navigare al interfeței Bitdefender.
2. Selectează fila **Anti-tracker**.
3. Selectează opțiunea **Activare extensie** din dreptul browserului web pentru care dorești să activezi extensia.



9.8.1. Interfața Anti-tracker



Atunci când extensia Bitdefender Anti-tracker este activată, se afișează pictograma  în dreptul barei de căutare a browserului web. De fiecare dată când accesezi un site web, vei observa un contor pe pictogramă, care arată numărul de trackere detectate și blocate. Pentru a vedea mai multe detalii despre tracker-ele blocate, accesează pictograma respectivă pentru a deschide interfața. În afară de numărul de trackere blocate, poți vedea timpul necesar încărcării paginii și categoriile de care aparțin tracker-ele detectate. Pentru a vedea lista site-urilor care practică activități de urmărire, selectează categoria dorită.

Pentru a dezactiva funcția Bitdefender de blocare a tracker-elor pe site-ul pe care îl accesezi în momentul respectiv, selectează opțiunea **Înterupeți protecția pe acest site**. Această setare se aplică numai atâta timp cât site-ul este deschis și va reveni automat la starea inițială după ce părăsești site-ul web.

Pentru a permite tracker-elor dintr-o anumită categorie să îți monitorizeze activitatea, selectează activitatea dorită și apoi clic pe butonul corespunzător. Dacă te răzgândești, apasă din nou pe același buton.

9.8.2. Dezactivarea Bitdefender Anti-tracker


Pentru a dezactiva Bitdefender Anti-tracker în browserul web:

1. Deschideți browser-ul web.
2. Accesează pictograma  din dreptul barei de adresă a browserului.
3. Accesează pictograma  din colțul din dreapta sus.
4. Utilizează butonul corespunzător pentru dezactivare.



Pictograma Bitdefender devine gri.

9.8.3. Permitearea urmăririi unui site web

Dacă dorești ca activitatea ta să fie urmărită în timp ce accesezi un anumit site web, poți adăuga adresa acestuia în lista de excepții, după cum urmează:

1. Deschideți browser-ul web.
2. Accesează pictograma  din dreptul barei de căutare.



3. Accesează pictograma  din colțul din dreapta sus.
4. Dacă te afli pe site-ul web pe care dorești să-l adaugi la excepții, selectează opțiunea **Adaugă în listă acest site web**.
Dacă dorești să adaugi un alt site web, introdu adresa acestuia în câmpul corespunzător și apoi selectează .

9.9. Protecție Fișiere

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. În 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 PROTECȚIE FIȘIERE, 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.

Pentru a adăuga ulterior fișiere în mediul protejat:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței Bitdefender.
2. Selectează fila **Anti-Ransomware**.
3. Selectează **Fișiere protejate** din secțiunea Protecție fișiere.
4. 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.

9.9.1. Administrare aplicații

Aceste aplicații 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 are un comportament normal, îi poți permite accesul urmând acești pași:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței Bitdefender.
2. Selectează fila **Anti-Ransomware**.
3. Selectează **Acces aplicații** din secțiunea Protecție fișiere.
4. Modifică starea aplicației selectând „Permite” în dreptul aplicației blocate.

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.



Acces aplicație

Aplicațiile care au solicitat modificarea fișierelor tale protejate vor apărea aici.

Aplicație	Detalii	Acțiune

Efectuează clic pe Adăugare (+) pentru a administra aplicațiile noi.

Protecție Fișiere

9.10. 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.

În cazul în care trebuie să restabilești fișiere dintr-un backup Time Machine, accesează pagina de asistență Apple pentru instrucțiuni.

Activarea sau dezactivarea protecției Time Machine

Pentru a activa sau dezactiva Protecția Time Machine:

1. Efectuează clic pe **Securitate** din meniul de navigare al interfeței **Bitdefender**.
2. Selectează fila **Anti-Ransomware**.
3. Activează sau dezactivează opțiunea **Protecție Time Machine**.

9.11. 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:

- Noua actualizare a informațiilor despre amenințări nu a fost descărcată de pe serverele noastre.
- Au fost detectate amenințări pe sistemul tău și produsul nu le poate dezinfecta automat.
- Protecția în timp real este dezactivată.

Pentru a verifica și soluționa problemele detectate:

1. 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 schimbă culoarea în roșu.
2. Verificați descrierea acesteia pentru a obține mai multe informații.
3. Atunci când este detectată o problemă, apasă pe butonul corespunzător pentru a întreprinde o acțiune.

Amenințări neeliminate:
1 problemă

Numele infecției	Cale către fișierul infectat	Acțiune inițiată
EICAR-Test-File...	/Users/Tester/Downloads/eicar.com	

Arată în Finder Adaugă la Excepții Rescanare Închide

Fereastra de amenințări nesoluționate

Lista amenințărilor nerezolvate este actualizată după fiecare scanare de sistem, indiferent dacă scanarea se desfășoară automat în fundal sau este inițiată de către tine.



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

- Ștergere manuală. Întreprindeți această acțiune pentru a elimina infecțiile manual.
- **Adaugă la Excepții.** Această acțiune nu este disponibilă pentru amenințări care se regăsesc în arhive.

9.12. Notificări

Bitdefender menține un jurnal detaliat al evenimentelor legate de activitatea sa pe computerul dumneavoastră. Ori de câte ori se întâmplă un lucru important pentru securitatea sistemului sau datelor dumneavoastră, se adaugă un nou mesaj la Notificările Bitdefender, ca și când ați primi un e-mail nou în Inbox-ul dumneavoastră.

Notificările reprezintă un instrument important pentru monitorizarea și gestionarea protecției Bitdefender. De exemplu, poți verifica cu ușurință dacă actualizarea a fost efectuată cu succes, dacă au fost detectate amenințări sau vulnerabilități pe calculatorul tău, etc. În plus, puteți lua măsuri suplimentare dacă este cazul sau puteți modifica măsurile luate prin intermediul Bitdefender.

Pentru a accesa jurnalul de Notificări, efectuează clic pe **Notificări** din meniul de navigare al interfeței Bitdefender. De fiecare dată când se produce un eveniment critic, se poate observa modificarea contorului pe pictograma



În funcție de tip și severitate, notificările sunt grupate în:

- Evenimentele **critice** indică probleme critice. Acestea ar trebui verificate imediat.
- Evenimentele de tip **Avertizare** indică probleme care nu sunt de foarte mare importanță. Ar trebui să verificați și să le remediați atunci când aveți timp.
- Evenimentele de tip **Informații** indică operațiile finalizate cu succes.

Fă clic pe fiecare filă pentru mai multe detalii despre evenimentele generate. Detaliile pe scurt sunt afișate la un singur clic pe titlul fiecărui eveniment, respectiv: o scurtă descriere, acțiunea pe care Bitdefender a întreprins-o atunci când a survenit, precum și data și ora producerii evenimentului. Pot



fi setate diverse opțiuni prin intermediul cărora să fie aplicații și alte acțiuni, dacă este necesar.

Pentru a vă ajuta să gestionați cu ușurință evenimentele înregistrate, fereastra Notificări oferă opțiuni de ștergere sau marcare ca citite a tuturor evenimentelor din secțiunea respectivă.

9.13. Actualizări

Zi de zi sunt descoperite și identificate noi amenințări. De aceea este foarte important să îți păstrezi Bitdefender Antivirus for Mac actualizat cu ultimele actualizări care conțin informații despre amenințări.

Actualizarea informațiilor privind amenințările se efectuează din mers, adică fișierele care trebuie actualizate sunt înlocuite progresiv. Astfel, actualizarea nu va afecta funcționarea produsului și, în același timp, se elimină orice vulnerabilitate.

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

9.13.1. 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. Faceți clic pe butonul **Acțiuni** din bara de meniu.
2. Selectează **Actualizează baza de date cu informații referitoare la amenințări**.

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

Puteți vizualiza progresul actualizării, precum și fișierele descărcate.



9.13.2. Obținerea actualizărilor prin intermediul unui server proxy

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

Dacă te conectezi la internet prin intermediul unui server proxy ce necesită autentificare, trebuie să treci în mod regulat la o conexiune directă la internet pentru a putea obține actualizările cu privire la informațiile despre amenințări.

9.13.3. 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 repornirea sistemului pentru a porni instalarea noilor 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 notificare, puteți fie să faceți clic pe **Repornește pentru upgrade** din bara de meniu sau să reporniți manual sistemul.

9.13.4. Cum găsești informații despre Bitdefender Antivirus for Mac

Pentru a găsi informații despre versiunea Bitdefender Antivirus for Mac pe care ai instalat-o, accesează fereastra **Despre**. Din aceeași fereastră poți accesa și vizualiza Contractul de abonament și Politica de Confidențialitate și poți vizualiza Licențele cu sursă deschisă.

Pentru a accesa fereastra Despre:

1. Deschideți Bitdefender Antivirus for Mac.
2. Efectuează clic pe Bitdefender Antivirus for Mac din bara de meniu și selectează **Despre Antivirus pentru Mac**.



10. CONFIGURAREA PREFERINȚELOR

Acest capitol acoperă următoarele subiecte:

- „Accesarea preferințelor” (p. 253)
- „Preferințe de protecție” (p. 253)
- „Preferințe avansate” (p. 254)
- „Oferte speciale” (p. 254)

10.1. Accesarea preferințelor

Pentru deschiderea ferestrei de preferințe a Bitdefender Antivirus for Mac:

1. Puteți proceda în oricare dintre următoarele modalități:
 - Selectează **Preferințe** din meniul de navigare al interfeței Bitdefender.
 - Faceți clic pe Bitdefender Antivirus for Mac în bara de meniu și selectați **Preferințe**.
 - Apăsăți tastele comandă-virgulă (,).

10.2. 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 Shield.** Bitdefender Shield oferă protecție în timp real împotriva unei game largi de amenințări prin scanarea tuturor aplicațiilor instalate, a versiunilor actualizate a acestora, precum și a fișierelor noi și modificate. Nu recomandă dezactivarea Bitdefender Shield, însă dacă nu poți evita acest lucru, dezactivează-l pentru o perioadă de timp cât mai scurtă. Dacă Bitdefender Shield este dezactivat, nu vei mai fi protejat împotriva amenințărilor.
- **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.

Poți alege să nu aplici această setare în cazul scanării personalizate și prin drag&drop prin debifarea casetei 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.

10.3. Preferințe avansate

Poți selecta o acțiune generală ce urmează a fi întreprinsă pentru toate problemele și obiectele suspecte identificate în timpul procesului de scanare.

Acțiuni pentru obiecte infectate

Încearcă dezinfectarea sau mutarea în carantină - Dacă sunt detectate fișiere infectate, Bitdefender va încerca să le dezinfecteze (să elimine codul periculos) sau să le mute în carantină.

Nu întreprinde nicio acțiune - Nu se va întreprinde nicio acțiune asupra fișierelor detectate.

Acțiuni pentru obiecte suspecte

Mută fișierele în carantină - Dacă sunt detectate fișiere suspecte, Bitdefender le va muta în carantină.

Nu întreprinde nicio acțiune - Nu se va întreprinde nicio acțiune asupra fișierelor detectate.

10.4. Oferte speciale

Atunci când sunt disponibile oferte promoționale, produsul Bitdefender este configurat să vă notifice prin intermediul unei ferestre de tip pop-up. Aceasta vă oferă oportunitatea de a beneficia de prețuri avantajoase și de a vă menține dispozitivele protejate pentru o perioadă mai lungă de timp.

Pentru a activa sau dezactiva notificările privind ofertele speciale:

1. Selectează **Preferințe** din meniul de navigare al interfeței Bitdefender.
2. Selectează fila **Altele**.
3. Activează sau dezactivează opțiunea **Ofertele mele**.

Opțiunea **Ofertele mele** este activată implicit.



11. VPN

Acest capitol acoperă următoarele subiecte:

- „Despre VPN” (p. 255)
- „Deschiderea conexiunii VPN” (p. 255)
- „Interfata” (p. 256)
- „Abonamente” (p. 258)

11.1. 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 redirectionat 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, confirmați că ai cunoștință de reglementările aplicabile țării respective și riscurile la care te-ai putea expune.


11.2. Deschiderea conexiunii VPN

Există trei modalități de deschidere a aplicației VPN Bitdefender:

- Efectuează clic pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.

Selectează **Deschide** din secțiunea VPN Bitdefender.



- Accesează pictograma  din bara de meniu.
- Accesează directorul Aplicații, deschide directorul Bitdefender și apoi dublu clic pe pictograma VPN Bitdefender .

Prima dată când deschizi aplicația, ți se solicită să permiți Bitdefender să adauge configurații. Permițând Bitdefender să adauge configurații, îți exprimi acordul ca întreaga activitate din rețea a dispozitivului tău să poată fi filtrată sau monitorizată atunci când utilizezi aplicația VPN.



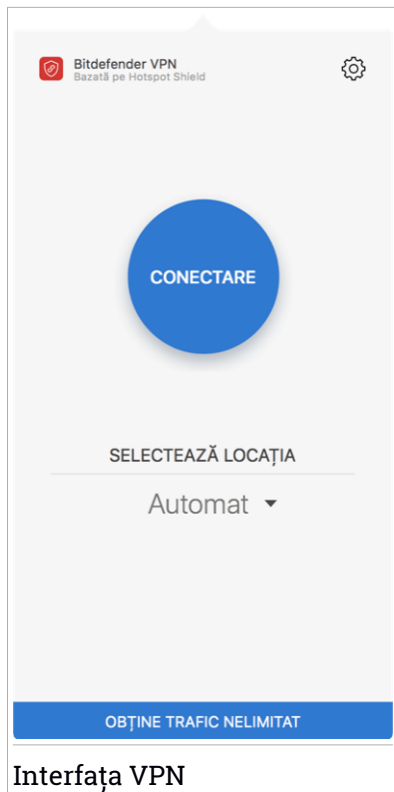
Notă

Aplicația Bitdefender VPN poate fi instalată numai pe macOS Sierra (10.12.6), macOS High Sierra (10.13.6) sau macOS Mojave (10.14 sau mai recent).


11.3. Interfața

Interfața VPN afișează starea aplicației, respectiv dacă este conectată sau deconectată. Locația serverului pentru utilizatorii versiunii gratuite este setată automat de Bitdefender la serverul cel mai adecvat, în timp ce utilizatorii premium au posibilitatea de a schimba locația serverului la care doresc să se conecteze, selectând-o din lista **SELECT LOCATION (ALEGE LOCAȚIA)**. Pentru detalii despre abonamentele VPN, accesează „*Abonamente*” (p. 258).

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.



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 afișate detalii despre contul tău Bitdefender și abonamentul VPN. Efectuează clic pe **Schimbă contul** dacă dorești să te conectezi cu un 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



- **Upgrade la Premium** - dacă folosești versiunea gratuită, poți efectua upgrade la planul premium de aici. Efectuează clic pe **EFACTUEAZĂ UPGRADE ACUM** pentru a fi redirecționat către o pagină web de unde poți cumpăra un abonament.
- **Support** - ești redirecționat către platforma noastră Support Center unde poți citi un articol util despre cum să folosești Bitdefender VPN.
- **Despre** – sunt afișate informații despre versiunea instalată.
- **Renunțare** - ieși din aplicație.

11.4. 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 securității tale. 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.

Bitdefender VPN este un produs pentru toate tipurile de platforme, disponibil în cadrul produselor Bitdefender compatibile cu Windows, macOS, Android și iOS. Odată ce faci upgrade la planul Premium, îți vei putea folosi abonamentul pentru toate produsele, cu condiția să te conectezi cu același cont Bitdefender.



12. BITDEFENDER CENTRAL

Acest capitol acoperă următoarele subiecte:

- „*Despre Bitdefender Central*” (p. 259)
- „*Abonamentele mele*” (p. 262)
- „*Dispozitivele mele*” (p. 263)

12.1. Despre Bitdefender Central

Bitdefender Central este platforma din care ai acces la funcțiile și serviciile online ale produsului și din care poți executa de la distanță sarcini importante pe dispozitivele pe care este instalat Bitdefender. Te poți conecta la contul tău Bitdefender de pe orice computer sau dispozitiv mobil conectat la internet, accesând <https://central.bitdefender.com>, sau direct din aplicația Bitdefender Central de pe dispozitivele Android și iOS.

Pentru a instala aplicația Bitdefender Central pe dispozitivele tale:

- **Pe Android** - caută Bitdefender Central în Google Play și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.
- **Pe iOS** - caută Bitdefender Central în App Store și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.

După autentificare, poți face următoarele:

- Descărcați și instalați 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
- Administrați și reînnoiți abonamentele Bitdefender.
- Adăugați dispozitive noi la rețeaua dvs. și administrați-le oriunde v-ați afla.



12.2. Accesare Bitdefender Central

Există mai multe moduri de accesare a Bitdefender 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. Deschide un browser web pe orice dispozitiv cu acces la internet.
2. Mergeți la: <https://central.bitdefender.com>.
3. Conectează-te la contul tău cu ajutorul adresei de e-mail și parolei.

● De pe dispozitivul tău Android sau iOS:

Deschide aplicația Bitdefender Central pe care ai instalat-o.



Notă

În acest material prezentăm opțiunile pe care le poți găsi în interfața web.


12.3. Autentificare în doi pași

Metoda de autentificare în doi pași adaugă un strat suplimentar de securitate contului tău Bitdefender, solicitând un cod de autentificare suplimentar pe lângă datele tale de conectare. În acest fel, vei evita ca altcineva să preia controlul asupra contului tău și veți ține la distanță atacuri cibernetice precum keyloggere, atacuri de tip „brute-force” sau pe bază de dicționar.

Activați autentificarea de tip „two-factor”

Prin activarea autentificării în doi pași, contul tău Bitdefender devine mult mai sigur. Identitatea ta va fi verificată de fiecare dată când te vei conecta de la diferite dispozitive pentru a instala unul dintre produsele Bitdefender, pentru a verifica starea abonamentului tău sau pentru a executa sarcini de la distanță pe dispozitivele tale.

Pentru a activa autentificarea de tip „two-factor”:

1. Accesați **Bitdefender Central**.
2. Faceți clic pe icoana  din partea dreapta de sus al ecranului.



3. Selectează **Cont Bitdefender** din meniul derulant.
4. Selectează fila **Parolă și securitate**.
5. Selectează **PRIMII PAȘI**.

Selectează una dintre următoarele metode:

- **Aplicație de autentificare** - folosește o aplicație de autentificare pentru a genera un cod de fiecare dată când dorești să te conectezi la contul tău Bitdefender.

Dacă dorești să utilizezi o aplicație de autentificare, dar nu ești sigur ce să alegi, îți punem la dispoziție o listă cu aplicațiile de autentificare pe care le recomandăm.

- a. Selectează **UTILIZEAZĂ O APLICAȚIE DE AUTENTIFICARE** pentru a începe.
- b. Pentru a te autentifica pe un dispozitiv cu sistem de operare Android sau iOS, folosește dispozitivul tău pentru a scana codul QR.

Pentru a te autentifica pe un laptop sau computer, poți adăuga manual codul afișat.

Faceți clic pe **CONTINUĂ**.

- c. Introdu codul furnizat de aplicație sau cel afișat la pasul anterior, apoi selectează **ACTIVARE**.

- **E-mail** - de fiecare dată când te conectezi la contul tău Bitdefender, se va trimite un cod de verificare către căsuța ta de e-mail. Verifică contul de e-mail și introdu codul primit.

- a. Selectează **UTILIZEAZĂ ADRESA DE E-MAIL** pentru a începe.
- b. Verifică-ți contul de e-mail și introdu codul furnizat.
- c. Selectează **ACTIVARE**.

Dacă nu mai dorești să folosești Autentificarea în doi pași:


1. Selectează opțiunea **DEZACTIVEAZĂ AUTENTIFICAREA ÎN DOI PAȘI**.
2. Verifică aplicația sau contul de e-mail și introdu codul primit.
3. Confirmă alegerea.



12.4. Adăugarea dispozitivelor sigure

Pentru a ne asigura că tu ești singura persoană care poate accesa contul tău Bitdefender, este posibil să îți solicităm mai întâi un cod de securitate. Dacă dorești să omiți acest pas de fiecare dată când te conectezi de pe același dispozitiv, îți recomandăm să îl setezi ca dispozitiv sigur.

Pentru a adăuga dispozitive marcate ca fiind sigure:

1. Accesați **Bitdefender Central**.
2. Faceți clic pe icoana  din partea dreapta de sus al ecranului.
3. Selectează **Cont Bitdefender** din meniul derulant.
4. Selectează fila **Parolă și securitate**.
5. Selectează opțiunea **Dispozitive sigure**.
6. Se afișează lista cu dispozitivele pe care este instalat Bitdefender. Selectează dispozitivul dorit.

Poți adăuga oricât de multe dispozitive dorești, cu condiția ca pe acestea să fie instalat Bitdefender și abonamentul tău să fie valid.

12.5. Abonamentele mele

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

12.5.1. 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  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. Efectuează clic pe **ACTIVARE** pentru a continua.

Abonamentul este acum activat.

Pentru a începe instalarea produsului pe dispozitivele tale, consultă „*Instalarea Bitdefender Antivirus for Mac*” (p. 226).

12.5.2. 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.

12.6. Dispozitivele mele

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

12.6.1. 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. Introduceți o nouă denumire în câmpul **Denumire dispozitiv** și apoi selectează **SALVARE**.

Puteți crea și alocă 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**.
5. Efectuează clic pe **Adăugare proprietar** 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**.

12.6.2. 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**.

După ce ai efectuat clic pe fila dispozitivului, sunt disponibile următoarele secțiuni:

- **Panou de bord.** În această fereastră, poți vizualiza detalii despre dispozitivul selectat, poți verifica starea sa de protecție 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. Atunci când există probleme care îți



afectează dispozitivul, efectuează clic pe săgeata din zona de stare din partea de sus pentru a afla mai multe detalii. De aici, puteți remedia manual problemele care afectează securitatea dispozitivelor.

- **Securitate.** Din această fereastră puteți rula de la distanță o operațiune de Scanare rapidă sau completă a dispozitivelor. Faceți clic pe butonul **SCANARE** pentru a începe procesul. De asemenea, puteți afla data ultimei scanări a dispozitivului și puteți primi un raport cu privire la cea mai recentă scanare, cu cele mai importante informații disponibile. Pentru mai multe informații referitoare la aceste două proceduri de scanare, consultați *„Scanarea Mac-ului dumneavoastră”* (p. 237).



13. 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:
 - a. Mergeți la: <https://central.bitdefender.com>.
 - b. Introduceți informațiile solicitate în câmpurile corespunzătoare. Informațiile furnizate aici vor rămâne confidențiale.
 - c. Înainte de a merge mai departe este necesar să îți exprimi acordul cu privire la Termenii de utilizare. Accesează secțiunea Termenii de utilizare și citește termenii cu atenție întrucât conțin termenii și condițiile care îți permit utilizarea Bitdefender.
Suplimentar, poți accesa și citi Politica de confidențialitate.
 - d. Efectuează clic pe **CREARE CONT**.
2. Descarcă Bitdefender Antivirus for Mac astfel:
 - a. Selectează fereastra **Dispozitivele mele** și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA**.
 - b. Alegeți una dintre cele două opțiuni disponibile:
 - **Protejează acest dispozitiv**
 - i. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
 - ii. Salvează fișierul de instalare.
 - **Protejează alte dispozitive**
 - i. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
 - ii. Selectează **TRIMITE LINKUL PENTRU DESCĂRCARE**.



iii. Introduceți o adresă de e-mail în câmpul corespunzător și apăsați pe **TRIMITE E-MAIL**.

Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.


iv. Pe dispozitivul pe care dorești să instalezi produsul Bitdefender, accesează contul de e-mail introdus și apoi apăsați pe butonul de descărcare corespunzător.

c. Rulați produsul Bitdefender descărcat.

Am un cod 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. Efectuează clic pe **ACTIVARE** pentru a continua.

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, modificărilor de stare și al altor mesaje critice legate de activitatea sa. Pentru a accesa aceste informații, selectați opțiunea **Notificări** din meniul de navigare al interfeței Bitdefender.

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

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

Dacă te conectezi la internet prin intermediul unui server proxy ce necesită autentificare, trebuie să treci în mod regulat la o conexiune directă la internet pentru a putea obține actualizările cu privire la informațiile despre amenințări.

Cum dezinstalez Bitdefender Antivirus for Mac?

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

1. Deschide o fereastră **Finder**, apoi accesează directorul Aplicații.
2. Deschide directorul Bitdefender și fă dublu-clic pe BitdefenderUninstaller.
3. Fă clic pe **Dezinstalare** și așteaptă finalizarea procesului.
4. Faceți clic pe **Închide** pentru a finaliza.





Important

În cazul apariției unei erori, puteți contacta serviciul Bitdefender Customer Care, așa cum se descrie în „*Solicitarea ajutorului*” (p. 333).



Cum șterg extensiile TrafficLight din browser-ul meu web?

- Pentru a șterge extensiile TrafficLight din Mozilla Firefox, urmați pașii de mai jos:
 1. Mergeți la **Instrumente** și selectați **Add-ons**.
 2. Selectați **Extensii** din coloana din partea stângă.
 3. Selectați extensia și faceți clic pe **Ștergere**.
 4. Reporniți browser-ul pentru finalizarea procesului de ștergere.
- Pentru a șterge extensiile TrafficLight din Google Chrome, urmați pașii de mai jos:
 1. În colțul din dreapta sus, efectuează clic pe **Mai mult** .
 2. Mergi la **Mai multe instrumente** și selectează **Extensii**.
 3. Selectează pictograma **Eliminare.....**  din dreptul extensiei pe care dorești să o elimini.
 4. Efectuează clic pe **Dezinstalare** pentru a confirma procesul de ștergere.
- Pentru a șterge Bitdefender TrafficLight din Safari, urmați pașii de mai jos:
 1. Accesează secțiunea **Preferințe** sau apasă pe **Command-Comma(,)**.
 2. Selectează **Extensii**.

Se va afișa o listă cu extensiile instalate.
 3. Selectează extensia Bitdefender TrafficLight, apoi **Dezinstalare**.
 4. Selectează **Dezinstalare** încă o dată pentru a confirma procesul de ștergere.

De ce să folosesc Bitdefender VPN?

Trebuie să procedezi cu atenție atunci când accesezi, descarci sau încarci conținut pe internet. Ca să fii sigur că ești protejat atunci când navighezi pe web, îți recomandăm să folosești Bitdefender VPN când:

- 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?

Bitdefender VPN este conceput să îți protejeze datele personale, să îți ascundă adresa IP în timp ce ești conectat la rețele wireless nesecurizate și la conținutul cu acces restricționat din 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?

Bitdefender VPN este conceput să îți ofere o navigare ușoară pe web; totuși, conexiunea ta la internet sau distanța față de serverul la care te conectezi pot cauza o încetinire. În acest caz, dacă nu trebuie neapărat să te conectezi din locația ta la un server îndepărtat (de ex. din SUA sau China), îți recomandăm să permiți Bitdefender VPN să te conecteze automat la cel mai apropiat server, sau să găsești un server mai apropiat de locația ta curentă.



MOBILE SECURITY PENTRU IOS



14. CE ESTE BITDEFENDER MOBILE SECURITY FOR IOS

Activitățile online, cum ar fi plata facturilor, rezervări pentru vacanță sau achiziționarea de produse și servicii se realizează comod, fără complicații. Însă, la fel ca în cazul multor altor activități pe internet, acestea implică și riscuri mari și, dacă detaliile de securitate sunt ignorate, datele personale pot fi accesate neautorizat. Și ce poate fi mai important decât protejarea datelor stocate în conturile online și pe smartphone-ul personal?

Bitdefender Mobile Security for iOS îți permite:

- Protejează-ți datele în timp ce folosești rețele wireless nesecurizate.
- Ferește-te de site-urile și domeniile potențial periculoase atunci când navighezi pe internet.
- Să verifici dacă s-a produs o accesare neautorizată a conturilor online pe care le utilizezi zilnic.

Bitdefender Mobile Security for iOS este livrat gratuit și necesită activare cu un **cont Bitdefender**.



15. INTRODUCERE

Cerințe dispozitiv

Bitdefender Mobile Security for iOS funcționează pe orice dispozitiv cu sistem de operare iOS 11.2 sau mai recent și necesită o conexiune activă la internet pentru a fi activat și pentru a depista dacă s-a produs vreo accesare neautorizată a datelor din conturile tale online.


Instalarea Bitdefender Mobile Security for iOS

● Din Bitdefender Central

● Pe iOS

1. Accesați **Bitdefender Central**.
2. Atinge pictograma  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
3. Selectează **INSTALARE PROTECȚIE** și apoi **Protejează acest dispozitiv**.
4. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, atinge butonul corespunzător.
5. Ești redirecționat către aplicația **App Store**. În ecranul App Store, selectează opțiunea de instalare.

● Pe Windows, macOS, Android

1. Accesați **Bitdefender Central**.
2. Atinge pictograma  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
3. Apasă pe **INSTALARE PROTECȚIE** și apoi pe **Protejează alte dispozitive**.
4. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, apasă pe butonul corespunzător.
5. Selectează **TRIMITE LINKUL PENTRU DESCĂRCARE**.
6. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este



valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.

7. Pe dispozitivul pe care dorești să instalezi Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

● Din App Store

Căutați Bitdefender Mobile Security for iOS pentru a găsi și instala aplicația.

Când deschizi pentru prima dată aplicația, se va afișa o fereastră ce conține detalii despre caracteristicile produsului. Accesează opțiunea **Înainte de a începe** pentru a continua cu următoarea fereastră.

Înainte de a trece prin pașii de validare, este necesar să accepți Contractul de Abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Mobile Security for iOS.

Selectează **Continuă** pentru a trece la fereastra următoare.

Conectați-vă la contul dumneavoastră Bitdefender

Pentru a utiliza Bitdefender Mobile Security for iOS, trebuie să conectați dispozitivul la un cont Bitdefender, Facebook, Google sau Microsoft conectându-te la cont din aplicația pentru mobil. Îți vom cere să te autentifici când vei deschide aplicația pentru prima dată.

Pentru a lega dispozitivul la contul Bitdefender:

1. Introdu în câmpul corespunzător adresa de e-mail asociată contului tău Bitdefender, apoi selectează opțiunea **ÎNAINTE**. Dacă nu ai încă un cont Bitdefender și dorești să-ți creezi unul, accesează linkul corespunzător și apoi urmează instrucțiunile de pe ecran până când contul este activat.

Pentru a te conecta cu un cont de Facebook, Google sau Microsoft, selectează serviciul dorit din secțiunea **SAU CONECTEAZĂ-TE CU**. Vei fi automat redirecționat către pagina de conectare a serviciului selectat. Urmează instrucțiunile pentru a-ți asocia contul cu Bitdefender Mobile Security for iOS.



Notă

Bitdefender nu are acces la informații confidențiale, precum parola contului pe care te autentifici de obicei sau datele personale ale prietenilor și contactelor.

2. Introdu parola și apoi selectează **AUTENTIFICARE**.

De aici, poți accesa și Politica de confidențialitate Bitdefender.

Panou de bord

Atingeți pictograma Bitdefender Mobile Security for iOS din lista de aplicații a dispozitivului dumneavoastră pentru a deschide interfața aplicației.

Prima dată când accesezi aplicația, ți se va solicita să permiți Bitdefender să-ți trimită notificări. Selectează opțiunea **Permite** pentru a rămâne informat de fiecare dată când Bitdefender trebuie să-ți comunice ceva care are legătură cu aplicația ta. Pentru administrarea notificărilor Bitdefender, accesează Setări > Notificări > Mobile Security.

Pentru a avea acces la informațiile de care ai nevoie, accesează pictograma corespunzătoare din partea de jos a ecranului.

VPN


Protejează-ți confidențialitatea indiferent de rețeaua la care te conectezi menținând criptată conexiunea la internet. Pentru mai multe informații, consultați capitolul „*VPN*” (p. 277).

Protecție web

Rămâi în siguranță în timp ce navighezi pe internet și oricând aplicațiile mai puțin securizate încearcă să acceseze domenii nesigure. Pentru mai multe informații, consultați capitolul „*Protecție web*” (p. 280).

Confidențialitate cont

Află dacă au fost sau nu accesate neautorizat conturile tale de e-mail. Pentru mai multe informații, consultați capitolul „*Confidențialitate cont*” (p. 283).

Pentru a vizualiza opțiuni suplimentare, accesează pictograma  de pe dispozitivul tău când te afli pe pagina principală a aplicației. Vor apărea următoarele opțiuni:

- **Restabilire achiziții** - de aici poți restabili abonamentul Premium VPN pe care l-ai achiziționat prin contul tău iTunes



- **Setări** - de aici ai acces la setările VPN, după cum urmează:
 - **Contract** - aici poți citi condițiile conform cărora poți utiliza serviciul Bitdefender VPN. Dacă selectezi **Nu mai sunt de acord**, nu vei putea utiliza Bitdefender VPN cel puțin până când nu selectezi din nou **Sunt de acord**.
 - **Avertisment rețea Wi-Fi deschisă** - poți activa sau dezactiva notificarea produsului care se afișează de fiecare dată când te conectezi la o rețea Wi-Fi nesecurizată. Scopul acestei notificări este de a te ajuta să-ți menții confidențialitatea și securitatea datelor tale folosind Bitdefender VPN.
 - **Feedback** – de aici poți lansa clientul de e-mail implicit pentru a ne trimite feedback privind aplicația.
 - **Detalii App** - de aici poți accesa informațiile privind versiunea instalată și Contractul de abonament, Politica de confidențialitate și conformitatea cu licențele open-source.



16. 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 redirectionat printr-un server separat, astfel încât dispozitivul tău devine aproape imposibil de identificat prin miriadele de alte dispozitive care utilizează 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

China, Irak, Emiratele Arabe Unite, Turcia, Belarus, Oman, Iran și Rusia practică cenzura pe internet și, prin urmare, utilizarea VPN-urilor pe teritoriul lor a fost interzisă prin lege. În consecință, funcționalitatea VPN Bitdefender nu va fi disponibilă pe teritoriul lor.

Pentru a activa Bitdefender VPN:


1. Accesează pictograma  din partea de jos a ecranului.
2. Selectează **Conectare** de fiecare dată când dorești să fii protejat atunci când te conectezi la rețele wireless nesecurizate.

Selectează **Deconectare** atunci când vrei să dezactivezi conexiunea.



Notă

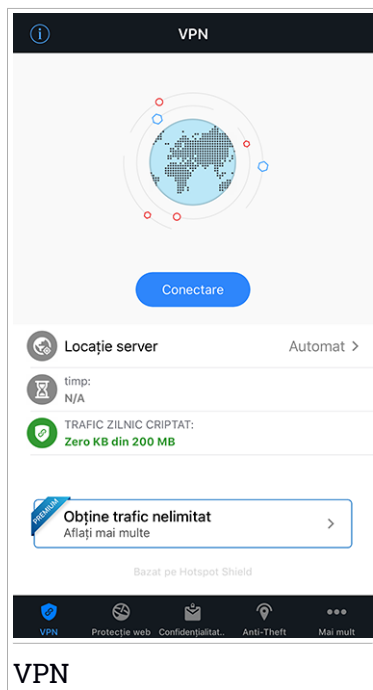
Prima dată când activezi modulul VPN, ți se va solicita să permiți Bitdefender să creeze configurații VPN care să monitorizeze traficul de rețea. Selectează **Permite**, pentru a continua. Dacă a fost setată o metodă de autentificare (prin amprentă sau cod PIN) pentru a-ți proteja smartphone-ul, trebuie să o folosești.

Pictograma  apare în bara de stare atunci când funcția VPN este activă.

Pentru a economisi bateria, îți recomandăm să oprești funcția VPN atunci când nu ai nevoie de ea.



Dacă ai un abonament premium și dorești să te conectezi la un anumit server, selectează **Locație server** în interfața VPN și apoi selectează locația dorită. Pentru detalii despre abonamentele VPN, accesează „**Abonamente**” (p. 278).



16.1. 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 upgrade oricând la versiunea Bitdefender Premium VPN apăsând pe butonul **Obține trafic nelimitat**, disponibil în fereastra VPN. Există două tipuri de abonament dintre care poți alege: anual și lunar.



Abonamentul Bitdefender Premium VPN este independent de abonamentul gratuit Bitdefender Mobile Security for iOS, ceea ce înseamnă că îl vei putea folosi pe toată durata de valabilitate. În cazul în care abonamentul Bitdefender Premium VPN expiră, vei reveni automat la planul gratuit.

Bitdefender VPN este un produs pentru toate tipurile de platforme, disponibil în cadrul produselor Bitdefender compatibile cu Windows, macOS, Android și iOS. Odată ce faci upgrade la planul Premium, îți vei putea folosi abonamentul pentru toate produsele, cu condiția să te conectezi cu același cont Bitdefender.




17. PROTECȚIE WEB

Modulul Protecție web Bitdefender asigură o experiență sigură de navigare trimițându-ți alerte cu privire la paginile web potențial periculoase și încercările de accesare de către aplicațiile instalate mai puțin securizate a unor domenii nesigure.

Atunci când o adresă URL face trimitere la un site web cunoscut pentru conținutul său de tip phishing sau fraudulos sau la conținut periculos, cum ar fi spyware sau virusi, pagina web respectivă este blocată și se afișează o alertă. Același lucru se întâmplă atunci când aplicațiile instalate încearcă să acceseze domenii periculoase.

Pentru a activa Protecția web:

1. Accesează pictograma  din partea de jos a ecranului.
2. Selectează **ÎNCEARCĂ MODULUL PROTECȚIE WEB**.
3. Alege una dintre perioadele de evaluare gratuită puse la dispoziție și apoi confirmă detaliile de plată.
4. Activează butonul Protecție web.



Notă

Prima dată când activezi modulul Protecție web, este posibil să îți se solicite să permiți Bitdefender să creeze configurații VPN care să monitorizeze traficul de rețea. Selectează **Permite**, pentru a continua. Dacă a fost setată o metodă de autentificare (prin amprentă sau cod PIN) pentru a-ți proteja smartphone-ul, trebuie să o folosești. Pentru a putea detecta accesul la domeniile nesigure, modulul Protecție web funcționează împreună cu serviciile VPN.



Important

Dacă te afli într-o zonă în care utilizarea unui serviciu VPN este restricționată prin lege, funcționalitatea Protecție web nu va fi disponibilă.

17.1. Alerte Bitdefender

Ori de câte ori încerci să accesezi un site clasificat ca fiind nesigur, site-ul respectiv este blocat. Pentru a te informa despre acest eveniment, vei primi o notificare din partea Bitdefender în Centrul de notificări, precum și în browser. Pagina conține informații precum URL-ul site-ului web și amenințarea detectată. Trebuie să decideți ce veți face în continuare.

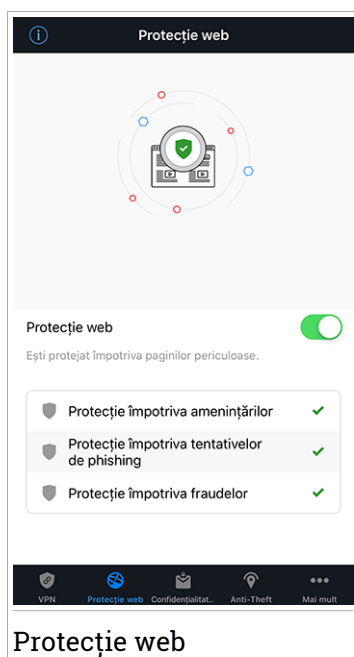


De asemenea, vei primi o notificare în Centrul de notificări ori de câte ori o aplicație mai puțin sigură încearcă să acceseze domenii care nu sunt de încredere. Accesează notificarea respectivă pentru a fi redirecționat către fereastra în care poți decide cum dorești să procedezi în continuare.

Următoarele opțiuni sunt disponibile pentru ambele situații:

- Părăsește site-ul web respectiv selectând **REVENIRE LA O PAGINĂ SIGURĂ**.
- Accesează site-ul, în ciuda avertizării, selectând notificarea respectivă și apoi **Vreau să accesez pagina**.

Confirmă alegerea.



17.2. Abonamente

Modul Protecție web este o caracteristică pe bază de abonament, care oferă posibilitatea evaluării gratuite, astfel încât să poți decide dacă aceasta corespunde cerințelor tale. Există două tipuri de abonament dintre care poți alege: anual și lunar.



Dacă abonamentul Protecție web Bitdefender expiră, nu vei primi nicio alertă în momentul accesării unui conținut periculos.

Dacă ai achiziționat unul dintre pachetele Bitdefender, cum ar fi Bitdefender Total Security, atunci ai acces nelimitat la modulul Protecție web.




18. CONFIDENȚIALITATE CONT

Funcția Confidențialitate cont Bitdefender detectează dacă s-au produs scurgeri de informații din conturile pe care le folosești pentru a efectua plăți și cumpărături online sau pentru a te conecta la diverse aplicații sau site-uri web. Datele care ar putea fi stocate într-un cont includ parole, date privind cardurile de credit sau informații privind contul bancar și, dacă acestea nu sunt securizate în mod corespunzător, se poate produce un furt de identitate sau o încălcare a confidențialității.

Starea de confidențialitate a unui cont este afișată imediat după validare.

Pentru a verifica dacă un cont a fost accesat neautorizat, selectează opțiunea **Scanează pentru depistarea accesărilor neautorizate**.

Pentru a începe să-ți păstrezi în siguranță datele personale:

1. Accesează pictograma  din partea de jos a ecranului.
2. Selectează opțiunea **Adaugă** din partea din dreapta-sus a ecranului.
3. Introdu adresa ta de e-mail în câmpul corespunzător și apoi selectează **Continuă**.

Bitdefender trebuie să valideze acest cont înainte de a afișa informații private. Prin urmare, se va trimite un e-mail conținând un cod de validare către adresa de e-mail furnizată.

4. Verifică-ți inbox-ul și apoi introdu codul primit în secțiunea **Confidențialitate cont** a aplicației. Dacă nu găsești e-mail-ul de validare în Inbox, verifică și directorul Spam.


Se afișează starea de confidențialitate a contului validat.

Dacă se identifică scurgeri de informații pe oricare dintre conturile tale, îți recomandăm să modifici parola acestora cât mai curând posibil. Pentru a crea o parolă puternică și sigură, ia în considerare aceste sfaturi:

- Folosește cel puțin opt caractere.
- Include litere mari și mici.
- Adaugă cel puțin un număr sau simbol, precum #, @, % sau !.

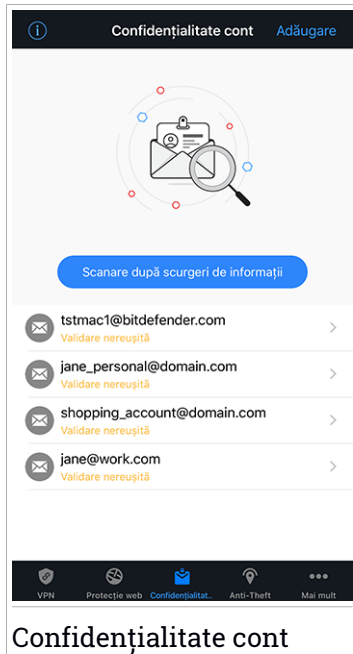
După securizarea unui cont care a fost implicat într-o scurgere de informații, poți confirma modificările marcând căile de acces neautorizat ca fiind **Rezolvat(e)**. Pentru a face acest lucru:



1. Selectează  din dreptul contului pe care tocmai l-ai securizat.
2. Selectează **Marchează ca soluționat**.

Contul va apărea în lista **SOLUȚIONATE**.

După ce toate căile de acces neautorizat sunt marcate ca fiind **Rezolvate**, contul nu va mai apărea ca fiind implicat într-o scurgere de informații, cel puțin până când nu se detectează o nouă scurgere de informații.





19. 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. Te poți conecta la contul tău Bitdefender de pe orice computer sau dispozitiv mobil conectat la internet, accesând <https://central.bitdefender.com>, sau direct din aplicația Bitdefender Central de pe dispozitivele Android și iOS.

Pentru a instala aplicația Bitdefender Central pe dispozitivele tale:

- **Pe Android** - caută Bitdefender Central în Google Play și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.
- **Pe iOS** - caută Bitdefender Central în App Store și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.

După autentificare, puteți face următoarele:

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

Accesarea contului Bitdefender

Există două modalități de accesare a Bitdefender Central

- Din browser-ul web:

1. Deschide un browser web pe orice dispozitiv cu acces la internet.
2. Mergeți la: <https://central.bitdefender.com>.
3. Conectează-te la contul tău cu ajutorul adresei de e-mail și parolei.

- De pe dispozitivul tău Android sau iOS:

Deschide aplicația Bitdefender Central pe care ai instalat-o.



Notă

În acest material sunt prezentate opțiunile disponibile în platforma web și instrucțiunile aferente.


Autentificare în doi pași

Metoda de autentificare în doi pași adaugă un strat suplimentar de securitate contului tău Bitdefender, solicitând un cod de autentificare suplimentar pe lângă datele tale de conectare. În acest fel, vei evita ca altcineva să preia controlul asupra contului tău și vei ține la distanță atacuri cibernetice precum keyloggere, atacuri de tip „brute-force” sau pe bază de dicționar.

Activați autentificarea de tip „two-factor”

Prin activarea autentificării în doi pași, contul tău Bitdefender devine mult mai sigur. Identitatea ta va fi verificată de fiecare dată când te vei conecta de la diferite dispozitive pentru a instala unul dintre produsele Bitdefender, pentru a verifica starea abonamentului tău sau pentru a executa sarcini de la distanță pe dispozitivele tale.

Pentru a activa autentificarea de tip „two-factor”:

1. Accesați **Bitdefender Central**.
2. Selectează pictograma  din partea din dreapta-sus a ecranului.
3. Selectează **Bitdefender Contul** din meniu.
4. Selectează fila **Parolă și securitate**.
5. Selectează **Autentificare în doi pași**.
6. Apasă **PORNEȘTE**.

Selectează una dintre următoarele metode:

- **Aplicație de autentificare** - folosește o aplicație de autentificare pentru a genera un cod de fiecare dată când dorești să te conectezi la contul tău Bitdefender.

Dacă dorești să utilizezi o aplicație de autentificare, dar nu ești sigur ce să alegi, îți punem la dispoziție o listă cu aplicațiile de autentificare pe care le recomandăm.

- a. Selectează **UTILIZEAZĂ O APLICAȚIE DE AUTENTIFICARE** pentru a începe.



- b. Pentru a te autentifica pe un dispozitiv cu sistem de operare Android sau iOS, folosește dispozitivul tău pentru a scana codul QR.

Pentru a te autentifica pe un laptop sau computer, poți adăuga manual codul afișat.

Apasă **Continuă**.

- c. Introdu codul furnizat de aplicație sau cel afișat la pasul anterior, apoi selectează **ACTIVARE**.

- **E-mail** - de fiecare dată când te conectezi la contul tău Bitdefender, se va trimite un cod de verificare către căsuța ta de e-mail. Verifică contul de e-mail și introdu codul primit.

- a. Selectează **UTILIZEAZĂ ADRESA DE E-MAIL** pentru a începe.

- b. Verifică-ți contul de e-mail și introdu codul furnizat.

Reține că ai cinci minute la dispoziție pentru a-ți verifica contul de e-mail și pentru a introduce codul generat. Dacă timpul expiră, trebuie să generezi unul nou urmând aceiași pași.

- c. Apasă **Activare**.

- d. Ai la dispoziție zece coduri de activare. Poți copia, descărca sau tipări lista pentru a o utiliza ulterior în cazul în care îți pierzi adresa de e-mail sau nu te poți conecta. Fiecare cod poate fi folosit o singură dată.

- e. Apasă pe **Finalizare**.

Dacă nu mai dorești să folosești Autentificarea în doi pași:

1. Selectează opțiunea **DEZACTIVEAZĂ AUTENTIFICAREA ÎN DOI PAȘI**.
2. Verifică aplicația sau contul de e-mail și introdu codul primit.

Dacă ai optat pentru a primi codul de autentificare prin e-mail, ai cinci minute la dispoziție pentru a-ți verifica contul de e-mail și pentru a introduce codul generat. Dacă timpul expiră, trebuie să generezi unul nou urmând aceiași pași.

3. Confirmă alegerea.


Adăugarea dispozitivelor sigure

Pentru a ne asigura că tu ești singura persoană care poate accesa contul tău Bitdefender, este posibil să îți solicităm mai întâi un cod de securitate.



Dacă dorești să omiți acest pas de fiecare dată când te conectezi de pe același dispozitiv, îți recomandăm să îl setezi ca dispozitiv sigur.

Pentru a adăuga dispozitive marcate ca fiind sigure:



1. Accesați **Bitdefender Central**.
2. Selectează pictograma  din partea din dreapta-sus a ecranului.
3. Selectează **Bitdefender Contul** din meniu.
4. Selectează fila **Parolă și securitate**.
5. Selectează opțiunea **Dispozitive sigure**.
6. Se afișează lista cu dispozitivele pe care este instalat Bitdefender. Selectează dispozitivul dorit.

Poți adăuga oricât de multe dispozitive dorești, cu condiția ca pe acestea să fie instalat Bitdefender și abonamentul tău să fie valid.

Dispozitivele mele

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

Pentru a-ți identifica și administra cu ușurință dispozitivele, poți să personalizezi numele dispozitivului și să creezi sau să atribui un proprietar fiecăruia dintre ele:


1. Atingeți pictograma  din colțul din stânga sus al ecranului și apoi selectați **Dispozitivele mele**.
2. Selectează cardul dispozitivului dorit și apoi pe pictograma  din colțul din dreapta sus al ecranului. Sunt disponibile următoarele opțiuni:
 - **Setări** - de aici poți schimba numele dispozitivului selectat.
 - **Profil** - de aici poți atribui un profil dispozitivului selectat. Accesează **Adaugă proprietar**, completează câmpurile respective, stabilește un Nume, introdu adresa de e-mail, numărul de telefon, data nașterii și poți chiar adăuga o poză de profil.



- **Eliminare** - de aici se poate elimina din contul tău Bitdefender un profil, împreună cu dispozitivul asociat.

Conectarea cu un alt cont Bitdefender

Pentru a te conecta cu un alt cont Bitdefender:

1. Accesează pictograma  din partea de jos a ecranului.
2. Selectează opțiunea **Deconectare**.
3. Introdu adresa de e-mail și parola asociate contului tău Bitdefender în câmpurile corespunzătoare.
4. Atingeți **AUTENTIFICARE**.



MOBILE SECURITY PENTRU ANDROID



20. FUNCȚII DE PROTECȚIE

Bitdefender Mobile Security vă protejează dispozitivul Android cu ajutorul următoarelor caracteristici:

- Scanare malware
- Protecție web
- VPN
- Antifurt, care include:
 - Localizare de la distanță
 - Blocare dispozitiv de la distanță
 - Ștergere dispozitiv de la distanță
 - Alerte de la distanță
- Confidențialitate cont
- Blocare Aplicații
- Rapoarte
- WearON

Puteți utiliza gratis funcțiile produsului timp de 14 zile. După expirarea perioadei de valabilitate, este necesar să achiziționați versiunea completă pentru a vă proteja dispozitivul mobil.



21. INTRODUCERE


Cerințe dispozitiv

Bitdefender Mobile Security este compatibil cu orice dispozitiv cu sistem de operare Android 4.1 sau mai recent. Este necesară o conexiune activă la internet pentru scanarea in-the-cloud a programelor periculoase.


Instalarea Bitdefender Mobile Security

● Din Bitdefender Central

● Pe Android

1. Mergeți la: <https://central.bitdefender.com>.
2. Conectați-vă la contul dumneavoastră Bitdefender.
3. Atinge  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
4. Selectează **INSTALARE PROTECȚIE** și apoi **Protejează acest dispozitiv**.
5. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, atinge butonul corespunzător.
6. Sunteți redirecționat către aplicația **Google Play**. În ecranul Google Play, selectează opțiunea de instalare.

● Pentru Windows, macOS, iOS

1. Mergeți la: <https://central.bitdefender.com>.
2. Conectați-vă la contul dumneavoastră Bitdefender.
3. Apasă pe  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
4. Apasă pe **INSTALARE PROTECȚIE** și apoi pe **Protejează alte dispozitive**.
5. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, apăsa pe butonul corespunzător.
6. Selectează **TRIMITE LINKUL PENTRU DESCĂRCARE**.



7. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.
8. Pe dispozitivul pe care dorești să instalezi Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

● Din Google Play

Căutați Bitdefender Mobile Security pentru a găsi și instala aplicația.

Alternativ, scanați codul QR:



Înainte de a trece prin pașii de validare, este necesar să acceptți Contractul de Abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Mobile Security.

Apasă **CONTINUĂ** pentru a trece la fereastra următoare.

Conectați-vă la contul dumneavoastră Bitdefender

Pentru a utiliza Bitdefender Mobile Security, trebuie să conectezi dispozitivul la un cont Bitdefender, Facebook, Google sau Microsoft conectându-te la cont din aplicația pentru mobil. Îți vom cere să te autentifici când vei deschide aplicația pentru prima dată.

Dacă ai instalat Bitdefender Mobile Security din contul tău Bitdefender, aplicația va încerca să se conecteze automat la contul respectiv.

Pentru a lega dispozitivul la contul Bitdefender:



1. Introdu adresa de e-mail și parola asociate contului tău Bitdefender în câmpurile corespunzătoare. Dacă nu ai un cont Bitdefender și dorești să îți creezi unul, selectează link-ul corespunzător.

2. Atingeți **AUTENTIFICARE**.

Pentru a te conecta cu un cont de Facebook, Google sau Microsoft, selectează serviciul dorit din secțiunea **SAU CONECTEAZĂ-TE CU**. Vei fi automat redirecționat către pagina de conectare a serviciului selectat. Urmează instrucțiunile pentru a-ți asocia contul cu Bitdefender Mobile Security.



Notă

Bitdefender nu are acces la informații confidențiale, precum parola contului pe care te autentifici de obicei sau datele personale ale prietenilor și contactelor.

Configurare protecție

Odată ce te-ai conectat cu succes la aplicație, se va afișa fereastra **Configurare protecție**. Pentru a îți securiza dispozitivul, îți recomandăm să treci prin următorii pași:

● **Stare abonament.** Pentru a beneficia de protecția Bitdefender Mobile Security, este necesar să activezi produsul cu ajutorul abonamentului, care prevede cât timp puteți utiliza produsul. Imediat ce expiră, aplicația nu mai funcționează și nu vă mai protejează dispozitivul.

Dacă ai un cod de activare, apasă **AM UN COD**, apoi apasă **ACTIVARE**.

Dacă te-ai autentificat cu un cont Bitdefender nou și nu ai un cod de activare, poți utiliza produsul timp de 14 zile, gratuit.

● **Protecție web.** Dacă dispozitivul tău necesită activarea Accesibilității pentru a activa Protecția Web, apasă pe **ACTIVARE**. Vei fi redirecționat la meniul Accesibilitate. Selectează Bitdefender Mobile Security și activează opțiunea corespunzătoare.

● **Scanare malware.** Efectuează o scanare pentru a te asigura că dispozitivul tău nu este vulnerabil la amenințări. Pentru a porni procesul de scanare, apasă pe **SCANEAZĂ ACUM**.

Imediat ce începe procesul de scanare, se afișează panoul de control. Aici, poți vedea starea de securitate a dispozitivului tău.



Panou de bord

Atingeți pictograma Bitdefender Mobile Security din lista de aplicații a dispozitivului dumneavoastră pentru a deschide interfața aplicației.

Panoul de control oferă informații despre starea de securitate a dispozitivului tău și, prin intermediul funcției Autopilot, te ajută să îmbunătățești securitatea dispozitivului tău oferindu-ți recomandări cu privire la caracteristicile disponibile.

Panoul de stare din partea de sus a ferestrei te informează cu privire la starea de securitate a dispozitivului tău folosind mesaje explicite și culori sugestive. Dacă Bitdefender Mobile Security nu prezintă avertismente, panoul de stare este verde. Atunci când a fost detectată o problemă de securitate, culoarea panoului de stare devine roșie.

Pentru a îți oferi o funcționare eficientă și protecție sporită în timp ce realizezi diferite activități, **Bitdefender Autopilot** va acționa ca un consultant personal de securitate. În funcție de activitatea pe care o desfășori, Bitdefender Autopilot îți va oferi recomandări contextuale în funcție de modul de utilizare a dispozitivului tău și nevoile tale. Acest lucru te va ajuta să descoperi și să beneficiezi de avantajele furnizate de caracteristicile incluse în aplicația Bitdefender Mobile Security.

De fiecare dată când un anumit proces este în curs de desfășurare sau o funcție necesită răspunsul dumneavoastră, pe Panoul de bord se afișează un card cu mai multe informații și acțiuni posibile.

Poți accesa funcțiile Bitdefender Mobile Security și poți naviga cu ușurință din bara de navigare din partea de jos:

Scanare malware

Îți permite pornirea unei scanări la cerere și activarea scanării dispozitivelor de stocare. Pentru mai multe informații, consultați capitolul „*Scanare malware*” (p. 297).

Protecție web

Asigură o experiență de navigare sigură informându-te cu privire la paginile web potențial periculoase. Pentru mai multe informații, consultați capitolul „*Protecție web*” (p. 300).



VPN

Criptează comunicațiile prin internet, ajutându-te să-ți păstrezi confidențialitatea indiferent de rețeaua la care ești conectat. Pentru mai multe informații, consultați capitolul „*VPN*” (p. 302).

Antifurt

Vă permite să activați și să dezactivați caracteristicile Anti-Theft, precum și să configurați setările acestei funcții. Pentru mai multe informații, consultați capitolul „*Funcții Antifurt*” (p. 305).

Confidențialitate cont

Verifică dacă s-au produs scurgeri de informații din conturile tale online. Pentru mai multe informații, consultați capitolul „*Confidențialitate cont*” (p. 309).

Blocare Aplicații

Vă permite să protejați aplicațiile instalate prin setarea unui cod de acces PIN. Pentru mai multe informații, consultați capitolul „*Blocare Aplicații*” (p. 311).

Rapoarte

Păstrează un jurnal al tuturor acțiunilor importante, modificărilor de stare și al altor mesaje critice legate de activitatea dispozitivului. Pentru mai multe informații, consultați capitolul „*Rapoarte*” (p. 316).

WearON

Comunică cu smartwatch pentru a te ajuta să îți găsești telefonul dacă îl rătăcești sau uiti unde l-ai lăsat. Pentru mai multe informații, consultați capitolul „*WearON*” (p. 317).



22. SCANARE MALWARE

Bitdefender vă protejează dispozitivul și datele împotriva aplicațiilor rău intenționate, utilizând scanarea la instalare și scanarea la cerere.



Notă

Asigurați-vă că dispozitivul dvs. mobil este conectat la internet. Dacă dispozitivul nu este conectat la internet, procesul de scanare nu va porni.

● Scanare la instalare


De fiecare dată când instalați o aplicație, Bitdefender Mobile Security o scanează automat utilizând tehnologia in-the-cloud. Același proces de scanare este inițiat la fiecare actualizare a aplicațiilor instalate.

Dacă aplicația este depistată a fi rău intenționată, va apărea o alertă care vă va solicita deinstalarea acesteia. Atinge **Dezinstalare** pentru a merge la ecranul de deinstalare a aplicației respective.

● Scanare la cerere

Oricând doriți să vă asigurați că aplicațiile instalate pe dispozitivul dumneavoastră sunt sigure în utilizare, puteți iniția o scanare la cerere.

Pentru a porni o scanare la cerere:

1. Apasă pe  **Scanner programe periculoase** din bara de navigare din partea de jos.
2. Atingeți **INIȚIERE SCANARE**.

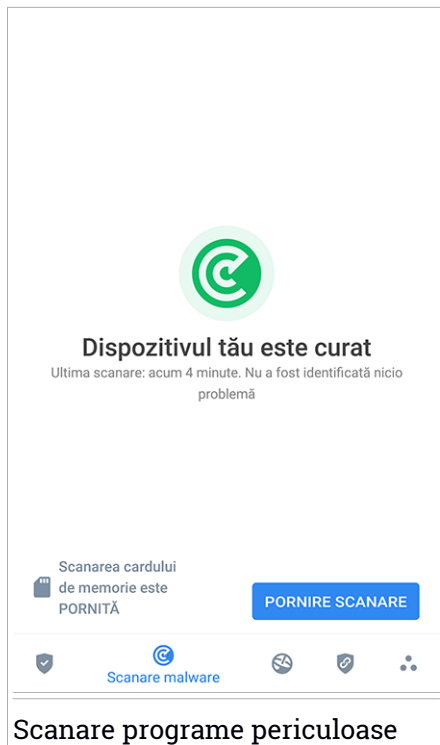


Notă

Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția de Scanare programe periculoase. După ce atingeți **INIȚIERE SCANARE**, selectează **Permite** pentru următoarele:

- Permiteți ca **Antivirus** să efectueze și să gestioneze apelurile telefonice?
- Permiteți ca **Antivirus** să acceseze fotografiile, fișiere media și fișiere stocate pe dispozitivul dumneavoastră?



Este afișată evoluția scanării și poți opri procesul în orice moment.



Scanare programe periculoase

În mod implicit, Bitdefender Mobile Security va scana spațiile de stocare internă ale dispozitivului dumneavoastră, inclusiv orice cartelă SD instalată. În acest fel, orice aplicații periculoase ce se pot afla pe cartelă pot fi detectate înainte de a produce pagube.


Pentru a dezactiva setarea Scanare dispozitive de stocare:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.
3. Dezactivează selectorul **Scanare dispozitive de stocare** din secțiunea Scanner programe periculoase.

Dacă este detectată orice aplicație rău intenționată, informațiile referitoare la aceasta vor fi afișate și o poți șterge apăsând butonul **DEZINSTALARE**.



Cardul de Scanare programe periculoase afișează starea dispozitivului dumneavoastră. Când dispozitivul este în siguranță, cardul este verde. Când este necesară o scanare a dispozitivului sau există vreo acțiune care necesită răspunsul dumneavoastră, cardul este roșu.

Dacă folosești versiunea de Android 7.1 sau o versiune mai recentă, poți accesa o scurtătură la funcția de Scanare malware astfel încât să poți executa scanările mai rapid, fără a deschide interfața Bitdefender Mobile Security. Pentru a face acest lucru, apasă și menține apăsată pictograma Bitdefender din ecranul principal sau bara de aplicații, apoi selectează pictograma .



23. PROTECȚIE WEB

Web Protection verifică, prin intermediul serviciilor în cloud Bitdefender, paginile internet pe care le accesați cu browser-ul Android implicit, Google Chrome, Firefox, Opera, Opera Mini și Dolphin. O listă completă de browsere compatibile este disponibilă în secțiunea Securitate Web.

Dacă o adresă URL indică un site web cunoscut pentru phishing sau fraude sau un conținut rău intenționat cum ar fi programe spion sau viruși, pagina web este blocată temporar și este afișat un mesaj de alertă.

Puteți apoi alege să ignorați alerta și să accesați pagina web sau să vă întoarceți la o pagină sigură.





Notă

Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Securitate web.

Permiteți înregistrarea ca serviciu Accesibilitate și atingeți **PORNIRE** atunci când vi se solicită acest lucru. Atingeți **Antivirus** și activați butonul, apoi confirmați că sunteți de acord cu permisiunea dispozitivului dumneavoastră.

De fiecare dată când accesezi un site bancar, Protecția Web Bitdefender este setată să te notifice să utilizezi Bitdefender VPN. Notificarea apare în bara de stare. Îți recomandăm să utilizezi Bitdefender VPN în timp ce ești înregistrat în contul tău bancar astfel încât să fii protejat de posibilele încălcări ale securității.

Pentru a dezactiva notificarea Protecție Web:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.
3. Dezactivează comutatorul corespunzător din zona Protecție Web.



Funcția Protecție web este activă

Ești protejat împotriva paginilor periculoase

[DEZACTIVARE](#)

Browsere protejate

Utilizează oricare dintre aceste browsere pentru a fi în siguranță



Chrome

Instalat

[DESCHIDE](#)



Dolphin



Firefox



Protecție web



Protecție web



24. 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 redirectionat printr-un server separat, astfel încât dispozitivul tău devine aproape imposibil de identificat prin miriadele de alte dispozitive care utilizează 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 legale, este posibil să apară un mesaj de avertizare atunci când încerci să utilizezi caracteristica Bitdefender VPN pentru prima dată. Prin continuarea utilizării acestei caracteristici, confirmi că îți sunt cunoscute reglementările aplicabile din țara respectivă și riscurile la care ai putea fi expus.

Există două modalități de a activa sau dezactiva Bitdefender VPN:

- Apasă **CONECTARE** în cardul VPN din Panoul de bord.

Se afișează starea funcției Bitdefender VPN.

- Apasă  **VPN** din partea de jos a barei de navigare și apoi apasă **CONECTARE**.

Selectează **CONECTARE** de fiecare dată când dorești să fii protejat atunci când te conectezi la rețele wireless nesecurizate.


Selectează **DECONNECTARE** atunci când vrei să dezactivezi conexiunea.




Notă

Când pornești pentru prima dată VPN-ul ți se cere să permiți Bitdefender să configureze o conexiune VPN care să monitorizeze traficul pe rețea. Selectează **OK** pentru a continua.



Dacă folosești versiunea de Android 7.1 sau o versiune mai recentă, poți accesa o scurtătură la Bitdefender VPN fără a deschide interfața Bitdefender Mobile Security. Pentru a face acest lucru, apasă și menține apăsată pictograma Bitdefender din ecranul principal sau bara de aplicații, apoi selectează pictograma .

Pictograma  apare în bara de stare atunci când funcția Bitdefender VPN este activă.

Pentru a economisi bateria, îți recomandăm să oprești funcția VPN atunci când nu ai nevoie de ea.



Dacă ai un abonament premium și dorești să te conectezi la un anumit server, apasă **Locație Server** din funcția VPN și apoi selectează locația dorită. Pentru detalii despre abonamentele VPN, accesează „**Abonamente**” (p. 304).





Setări VPN

Pentru o configurare avansată a VPN-ului tău:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.

În zona VPN, poți configura următoarele opțiuni:

- **Acces rapid VPN** - în bara de stare a dispozitivului tău va apărea o notificare care îți permite să pornești rapid VPN-ul.
- **Rețea Wi-Fi deschisă** - de fiecare dată când te conectezi la o rețea Wi-Fi deschisă, ești notificat în bara de stare a dispozitivului tău să utilizezi VPN.

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 atingând butonul **ACTIVEAZĂ PREMIUM** disponibil în Panoul de bord sau **Activează versiune Premium** din fereastra VPN.

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

Bitdefender VPN este un produs pentru toate tipurile de platforme, disponibil în cadrul produselor Bitdefender compatibile cu Windows, macOS, Android și iOS. Odată ce faci upgrade la planul Premium, îți vei putea folosi abonamentul pentru toate produsele, cu condiția să te conectezi cu același cont Bitdefender.



25. FUNCȚII ANTIFURT

Bitdefender vă permite să localizați dispozitivul și să preveniți accesul neautorizat la datele dvs.

Tot ce trebuie să faceți este să activați funcția Antifurt pe dispozitiv și, apoi, când este cazul, veți putea accesa **Bitdefender Central** de pe orice browser, de oriunde.

Bitdefender Mobile Security oferă următoarele caracteristici Anti-Theft:

Localizare de la distanță

Vizualizați locația curentă a dispozitivului dumneavoastră pe Google Maps. Locația este actualizată la fiecare 5 secunde, așadar îl puteți localiza dacă este în mișcare.

Precizia locației depinde de cum poate Bitdefender să o stabilească:

- Dacă funcția GPS este activată pe dispozitiv, locația sa poate fi indicată cu precizie pe o rază de câțiva metri atâta timp cât se află în raza sateliților GPS (mai exact, nu într-o clădire).
- Dacă dispozitivul este înăuntru, locația sa poate fi stabilită la intervale de zeci de metri dacă funcția Wi-Fi este activată și există pe raza sa rețele wireless.
- Altfel, locația va fi stabilită utilizând numai informațiile rețelei mobile, care nu poate oferi o precizie mai mare de câteva sute de metri.

Blocare de la distanță

Blocați ecranul dispozitivului dumneavoastră și setați un cod PIN numeric pentru deblocarea acestuia.

Ștergere de la distanță

Șterge toate datele dumneavoastră personale de pe dispozitivul dumneavoastră înstrăinat.

Expedierea unei alerte pe dispozitiv (Alarmă)

Expediați de la distanță un mesaj care va fi afișat pe ecranul dispozitivului sau declanșați un sunet puternic care să fie redat în difuzorul telefonului.

Dacă pierdeți dispozitivul, puteți informa persoana care îl găsește cum vi-l poate returna prin afișarea unui mesaj pe ecranul dispozitivului.

Dacă ați rătăcit dispozitivul și se poate să nu fie foarte departe de dumneavoastră (de exemplu, undeva în casă sau în birou), ce metodă





ar fi mai bună pentru a-l găsi decât ca dispozitivul să emită un sunet puternic? Sunetul va fi redat chiar și când dispozitivul se află în modul silențios.

Activarea funcției Antifurt

Pentru a activa funcțiile Antifurt, urmați procesul de configurare din cardul Antifurt disponibil în Panoul de bord.

Alternativ, puteți activa funcția Antifurt urmând pașii de mai jos:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Atinge  **Antifurt**.
3. Atingeți **PORNIRE**.
4. Se va lansa următoarea procedură, care vă va ajuta să activați această funcție:

Notă

Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Antifurt. Pentru activare, urmați pașii de mai jos:

- a. Atingeți **Activare Antifurt**, apoi atingeți **PORNIRE**.
- b. Permite permisiuni pentru **Antivirus** să acceseze locația dispozitivului tău
- a. **Acordă drepturi de administrator**

Aceste drepturi sunt esențiale pentru operarea modulului Antifurt și este obligatoriu să fie acordate pentru a putea continua.
- b. **Configurează codul de acces pentru aplicație**



Pentru a împiedica accesul neautorizat la dispozitivul tău, este necesară configurarea unui cod PIN. La fiecare accesare a dispozitivului tău, este necesar să se introducă mai întâi acest PIN. Alternativ, pe dispozitivele compatibile cu autentificarea prin amprentă, se poate utiliza această modalitate de confirmare în locul codului PIN configurat.

Același cod PIN este utilizat și de App Lock pentru protejarea aplicațiilor instalate.
- c. **Activați Fotografiere**



De fiecare dată când cineva va încerca să îți deblocheze dispozitivul fără succes, în timp ce funcția Instantanee este activată, Bitdefender îi va face o fotografie.

Mai exact, de fiecare dată când se introduce greșit, de trei ori consecutiv, codul PIN, parola, sau confirmarea pe bază de amprentă, care au fost setate de tine pentru a-ți proteja dispozitivul, se va realiza o fotografie cu camera secundară. Imaginea este salvată împreună cu data și ora, precum și motivul realizării, și poate fi vizualizată atunci când deschizi Bitdefender Mobile Security pentru a accesa fereastra Antifurt. Ca soluție alternativă, poți vizualiza fotografia respectivă din contul tău Bitdefender:

- i. Mergeți la: <https://central.bitdefender.com>.
- ii. Conectați-vă la contul dumneavoastră.
- iii. Atinge  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
- iv. Selectează dispozitivul tău Android și apoi fila **Anti-furt**.
- v. Selectează  din dreptul opțiunii **Accesare instantanee** pentru a vizualiza cele mai recente fotografii realizate.

Sunt salvate doar cele mai recente două fotografii.

Odată ce funcția Anti-Theft este activată, poți activa sau dezactiva comenzile Control web individual din fereastra Anti-Furt prin atingerea opțiunilor corespunzătoare.


Folosirea funcțiilor Anti-Theft din Bitdefender Central




Notă

Toate funcțiile Antifurt solicită ca opțiunea **Date de fundamental** să fie activă în setările Utilizare date ale dispozitivului dumneavoastră.

Pentru a accesa caracteristicile Antifurt din contul Bitdefender:

1. Accesați **Bitdefender Central**.
2. Atinge  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
3. În fereastra **DISPOZITIVELE MELE**, selectați cardul dispozitivului dorit.



4. Selectați secțiunea **Antifurt**.
5. În partea de jos a ferestrei, atinge  și apoi butonul corespunzător funcției pe care dorești să o utilizezi:

Localizare - afișează locația dispozitivului dumneavoastră pe Google Maps.



Alertă - scrieți un mesaj care va fi afișat pe ecranul dispozitivului dumneavoastră și/sau setați dispozitivul să emită un sunet de alarmă.



Blocare - blocați dispozitivul și setați un cod PIN de deblocare.



Ștergere - șterge toate datele de pe dispozitivul dumneavoastră.





Important

După ce ștergeți un dispozitiv, este oprită funcționarea tuturor funcțiilor Anti-Theft.

Afișează IP - afișează ultima adresă IP a dispozitivului selectat.

Setări Antifurt

Dacă dorești să activezi sau să dezactivezi comenzile la distanță:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Atinge  **Antifurt**.
3. Activează sau dezactivează opțiunile dorite.



26. CONFIDENȚIALITATE CONT



Funcția Confidențialitate cont Bitdefender detectează dacă s-au produs scurgeri de informații din conturile pe care le folosești pentru a efectua plăți și cumpărături online sau pentru a te conecta la diverse aplicații sau site-uri web. Datele care ar putea fi stocate într-un cont includ parole, date privind cardurile de credit sau informații privind contul bancar și, dacă acestea nu sunt securizate în mod corespunzător, se poate produce un furt de identitate sau o încălcare a confidențialității.

Starea de confidențialitate a unui cont este afișată imediat după validare.

Reverificările automate sunt setate să ruleze în fundal, însă se pot efectua, de asemenea, scanări manuale zilnic.

Se vor afișa notificări de fiecare dată când se descoperă noi scurgeri de informații care implică oricare dintre conturile de e-mail validate.

Pentru a începe să-ți păstrezi în siguranță datele personale:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Confidențialitate cont**.
3. Apasă **PORNEȘTE**.
4. Apare adresa de e-mail utilizată pentru a îți crea contul tău Bitdefender.

Apasă **ADĂUGARE** pentru a continua.

Bitdefender trebuie să valideze acest cont înainte de a afișa informații private. Prin urmare, se va trimite un e-mail conținând un cod de validare către adresa de e-mail furnizată.

5. Verifică-ți inbox-ul și apoi introdu codul primit în secțiunea **Confidențialitate cont** a aplicației. Dacă nu găsești e-mail-ul de validare în Inbox, verifică directorul Spam.

Se afișează starea de confidențialitate a contului validat.



Pentru a adăuga alte conturi, apasă **ADĂUGARE CONT** în fereastra Confidențialitate cont și apoi urmează pașii necesari.

Dacă se identifică scurgeri de informații pe oricare dintre conturile tale, îți recomandăm să modifici parola acestora cât mai curând posibil. Pentru a crea o parolă puternică și sigură, ia în considerare aceste sfaturi:





- Folosește cel puțin opt caractere.
- Include litere mari și mici.
- Aduagă cel puțin un număr sau simbol, precum #, @, % sau !.

După securizarea unui cont care a fost implicat într-o scurgere de informații, poți confirma modificările marcând încălcările identificate ca fiind **Rezolvat(e)**. Pentru a face acest lucru:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Confidențialitate cont.**
3. Selectează contul pe care tocmai l-ai securizat.
4. Apasă pe încălcarea față de care ți-ai securizat contul.
5. Apasă **REZOLVAT** pentru a confirma securizarea contului.

După ce toate încălcările de securitate sunt marcate ca fiind **Rezolvate**, contul nu va mai apărea ca fiind implicat într-o încălcare de securitate, cel puțin până când nu se detectează o nouă încălcare de securitate.

Pentru a dezactiva opțiunea de notificare la fiecare scanare automată:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări.**
3. Dezactivează butonul corespunzător din zona Confidențialitate cont.



27. BLOCARE APLICAȚII

Aplicațiile instalate, cum ar fi e-mail, fotografiile sau mesaje, pot conține date personale pe care doriți să le mențineți confidențiale prin restricționarea selectivă a accesului la acestea.



App Lock vă ajută să blocați accesul nedorit la aplicații prin setarea unui cod de acces PIN. Codul PIN pe care îl configurați trebuie să aibă cel puțin 4 cifre, însă nu mai mult de 8, și va trebui să îl introduceți de fiecare dată când accesați aplicațiile restricționate selectate.

Alternativ, pe dispozitivele compatibile cu autentificarea prin amprentă, se poate utiliza această modalitate de confirmare în locul codului PIN configurat.

Activarea App Lock

Pentru a restricționa accesul la aplicațiile selectate, configurați funcția Blocare aplicații din cardul afișat în Panoul de bord după activarea funcției Antifurt.

Alternativ, puteți activa funcția Blocare aplicații urmând pașii de mai jos:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Blocare aplicații**.
3. Atingeți **PORNIRE**.
4. Pentru accesul la datele privind utilizarea Bitdefender.

Notă

Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Instantanee.

Pentru a o activa, permiteți ca **Antivirus** să facă fotografiile și să înregistreze clipuri video.

5. Reveniți la aplicație, configurați codul de acces și apoi atingeți **CONFIGURARE PIN**.

Notă

Acest pas este disponibil numai dacă nu ați configurat anterior codul PIN în secțiunea Antifurt.



6. Activați opțiunea Fotografiere pentru a putea identifica orice intrus care încearcă să vă acceseze datele.

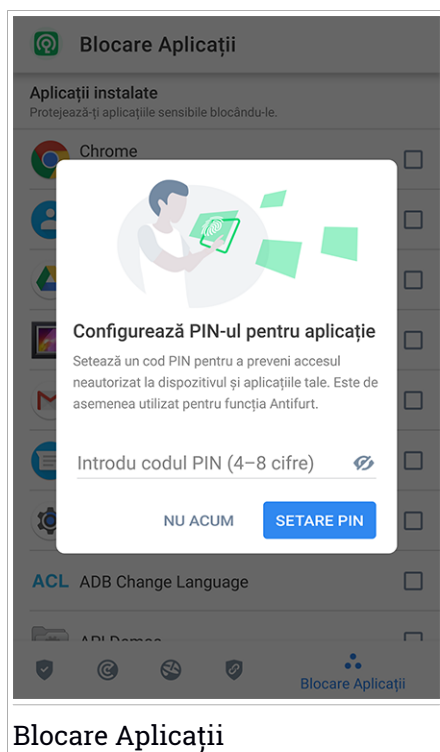
7. Selectează aplicațiile pe care dorești să le protejezi:

Introducerea codului PIN sau aplicarea amprentei greșite de cinci ori consecutiv activează o sesiune de întrerupere a funcționării de 30 de secunde. Astfel, orice încercare de a accesa aplicațiile protejate va fi blocată.



Notă

Același cod PIN este utilizat și de aplicația Antifurt pentru a vă ajuta să vă localizați dispozitivul.



Blocare Aplicații





Mod de blocare

La prima adăugare a unei aplicații la secțiunea Blocare aplicații, apare ecranul Mod blocare aplicații. De aici, puteți selecta dacă funcția Blocare aplicații va proteja sau nu aplicațiile instalate pe dispozitivul dvs.

Puteți selecta una dintre următoarele opțiuni:



- **Solicită deblocare de fiecare dată** - de fiecare dată când sunt accesate aplicațiile blocate, va trebui să utilizezi codul PIN sau amprenta pe care le-ai setat.
- **Păstrează deblocat până la oprirea ecranului** - vei putea accesa la aplicațiile până la oprirea ecranului.
- **Blocare după 30 de secunde** - poți ieși și accesa din nou aplicațiile tale deblocate în interval de 30 de secunde.

Dacă dorești să modifici setarea selectată:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.
3. Atinge **Solicită deblocare de fiecare dată** din secțiunea Blocare aplicații.
4. Alege opțiunea dorită.

Setări Blocare Aplicații

Pentru o configurare avansată a funcției Blocare aplicații:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.

În zona Blocare aplicații, poți configura următoarele opțiuni:

- **Sugestie aplicații sensibile** - vei primi o notificare de blocare de fiecare dată când instalezi o aplicație sensibilă.
- **Solicită deblocare de fiecare dată** - selectează una dintre opțiunile de blocare și deblocare.
- **Deblocare inteligentă** - păstrează aplicațiile deblocate cât timp ești conectat la rețele Wi-Fi sigure.



- **Randomizare taste** - împiedică citirea codului PIN prin randomizarea poziției cifrelor.

Foto Instant

Cu funcția instantaneu Bitdefender vă puteți lua prietenii sau rudele pe nepregătite. Astfel, îi puteți învăța să nu-și mai arunce privirile curioase prin fișierele dumneavoastră personale sau aplicațiile pe care le folosiți.



Această caracteristică funcționează foarte simplu: de fiecare dată când codul PIN sau amprenta setate pentru a vă proteja aplicațiile sunt introduse greșit de trei ori consecutiv, se realizează o fotografie prin camera frontală. Imaginea este salvată împreună cu data și ora, precum și motivul realizării, și poate fi vizualizată atunci când deschideți Bitdefender Mobile Security pentru a accesa caracteristica Blocare aplicații.



Notă


Această caracteristică este disponibilă numai pentru telefoanele prevăzute cu cameră frontală.

Pentru a configura Fotografia instant pentru Blocare aplicații:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.
3. Activează butonul corespunzător din zona Fotografie instant.

Instantaneele făcute atunci când este introdus codul PIN incorect sunt afișate în fereastra Blocare aplicații și pot fi vizualizate pe întregul ecran.



Alternativ, acestea pot fi vizualizate în contul Bitdefender:

1. Mergeți la: <https://central.bitdefender.com>.
2. Conectați-vă la contul dumneavoastră.
3. Atinge  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
4. Selectează dispozitivul tău Android și apoi fila **Anti-furt**.
5. Selectează  din dreptul opțiunii **Accesare instantanee** pentru a vizualiza cele mai recente fotografii realizate.

Sunt salvate doar cele mai recente două fotografii.



Pentru a opri încărcarea instantaneelor în contul tău Bitdefender:



1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.
3. Dezactivează opțiunea **Încărcare fotografii** din secțiunea Fotografie instant.

Deblocare Inteligentă

O metodă ușoară de a evita ca funcția Blocare aplicații să vă solicite să introduceți codul PIN sau amprenta de confirmare pentru aplicațiile protejate de fiecare dată când le accesați este de a activa opțiunea Deblocare inteligentă.

Cu funcția Deblocare inteligentă puteți seta ca fiind sigure rețelele Wi-Fi la care vă conectați de obicei și, atunci când sunteți conectat la acestea, setările funcției Blocare aplicații vor fi dezactivate pentru aplicațiile protejate.

Pentru a configura funcția Deblocare inteligentă:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Blocare aplicații**.
3. Atinge **ADAUGĂ** pentru a configura conexiunea Wi-Fi pe care o utilizezi la momentul actual ca fiind sigură.



Notă

Această setare este disponibilă numai dacă funcția Deblocare inteligentă este activată.

Dacă vă răzgândeți, puteți dezactiva funcția și rețelele Wi-Fi pe care le-ați setat ca fiind sigure vor fi tratate ca fiind nesigure.





28. RAPOARTE

Funcția Rapoarte păstrează un jurnal detaliat al evenimentelor asociate activității de scanare de pe dispozitivul dvs.

La fiecare eveniment relevant pentru securitatea dispozitivului dvs. un nou mesaj este inclus în Reports.

Pentru a accesa secțiunea Rapoarte:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Atinge  **Rapoarte**.

În fereastra Rapoarte, sunt disponibile următoarele secțiuni:



- **RAPOARTE SĂPTĂMÂNNALE** - aici, aveți acces la starea de securitate și la sarcinile efectuate în săptămâna curentă și anterioară. Raportul aferent săptămânii curente este generat în fiecare duminică și veți primi o notificare prin care veți fi informat cu privire la disponibilitatea sa.

Săptămânal va fi afișată o nouă recomandare în această secțiune, astfel că asigurați-vă că reveniți în mod regulat pentru a exploata la maxim aplicația.

Pentru a opri primirea notificărilor de fiecare dată când se generează un raport:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
 2. Apasă  **Setări**.
 3. Dezactivează opțiunea **Notificare raport nou** din zona de Rapoarte.
- **JURNAL ACTIVITATE** - de aici, puteți verifica informațiile referitoare la activitatea aplicației Bitdefender Mobile Security, de la instalarea acesteia pe dispozitivul dvs. Android.

Pentru a șterge jurnalul de activitate disponibil:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.
3. Atinge **Ștergere jurnal de activitate** și apoi atinge **ȘTERGERE**.



29. WEARON

Cu funcția WearONBitdefender, îți poți găsi cu ușurință smartphone-ul, indiferent dacă l-ai lăsat la birou într-o sală de conferință sau sub o pernă pe canapea. Dispozitivul poate fi găsit chiar dacă ai activat modul silențios.

Menține această funcție activată pentru a te asigura că ai întotdeauna smartphone-ul la îndemână.



Notă

Funcția este compatibilă cu Android 4.3 și Android Wear.

Activarea WearON

Pentru a folosi WearON, nu trebuie decât să te conectezi smartwatch-ul la aplicația Bitdefender Mobile Security și să activezi funcția cu următoarea comandă vocală:

Start:<Where is my phone>

Bitdefender WearON are două comenzi:

1. Alertă Telefon

Cu funcția Phone Alert îți poți găsi rapid smartphone-ul, ori de câte ori ești prea departe de el.

Dacă ai smartwatch-ul la tine, acesta detectează automat aplicația de pe telefonul tău și vibrează atunci când ești prea departe de telefon și conexiunea Bluetooth este pierdută.

Pentru a activa această funcție, deschide Bitdefender Mobile Security, atinge **Global Settings** în meniu și selectează butonul corespunzător în secțiunea WearON.



2. Alarmă

Găsirea telefonului nu a fost niciodată mai ușoară. Ori de câte ori uiți unde ți-ai lăsat telefonul, atinge comanda Scream de pe ceas pentru a face telefonul să "țipe".



30. DESPRE

Pentru a găsi informații despre versiunea Bitdefender Mobile Security pe care ai instalat-o, pentru a accesa și citi Contractul de abonament și Politica de confidențialitate, precum și pentru a vizualiza Licențele cu sursă deschisă:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.
3. Atinge opțiunea dorită în secțiunea Despre.



31. 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. Te poți conecta la contul tău Bitdefender de pe orice computer sau dispozitiv mobil conectat la internet, accesând <https://central.bitdefender.com>, sau direct din aplicația Bitdefender Central de pe dispozitivele Android și iOS.

Pentru a instala aplicația Bitdefender Central pe dispozitivele tale:

- **Pe Android** - caută Bitdefender Central în Google Play și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.
- **Pe iOS** - caută Bitdefender Central în App Store și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.

După autentificare, poți face următoarele:

- Descărcați și instalați Bitdefender pe sistemele de operare Windows, macOS, iOS și Android. Produsele disponibile pentru descărcare sunt:
 - Bitdefender Mobile Security
 - Bitdefender Mobile Security for iOS
 - Bitdefender Antivirus pentru Mac
 - Linia de produse Windows Bitdefender
- Administrați și reînnoiți abonamentele Bitdefender.
- Adăugați dispozitive noi la rețeaua dvs. și administrați-le oriunde v-ați afla.
- Protejați-vă dispozitivele din rețea și datele de pe acestea împotriva furtului sau a pierderii cu ajutorul funcției **Anti-Theft**.

Accesarea contului Bitdefender

Există două modalități de accesare a Bitdefender Central

- Din browser-ul web:

1. Deschide un browser web pe orice dispozitiv cu acces la internet.
2. Mergeți la: <https://central.bitdefender.com>.
3. Conectează-te la contul tău cu ajutorul adresei de e-mail și parolei.



- De pe dispozitivul tău Android sau iOS:

Deschide aplicația Bitdefender Central pe care ai instalat-o.



Notă

În acest material sunt prezentate opțiunile disponibile în platforma web și instrucțiunile aferente.


Autentificare în doi pași

Metoda de autentificare în doi pași adaugă un strat suplimentar de securitate contului tău Bitdefender, solicitând un cod de autentificare suplimentar pe lângă datele tale de conectare. În acest fel, vei evita ca altcineva să preia controlul asupra contului tău și veți ține la distanță atacuri cibernetice precum keyloggere, atacuri de tip „brute-force” sau pe bază de dicționar.

Activați autentificarea de tip „two-factor”

Prin activarea autentificării în doi pași, contul tău Bitdefender devine mult mai sigur. Identitatea ta va fi verificată de fiecare dată când te vei conecta de la diferite dispozitive pentru a instala unul dintre produsele Bitdefender, pentru a verifica starea abonamentului tău sau pentru a executa sarcini de la distanță pe dispozitivele tale.

Pentru a activa autentificarea de tip „two-factor”:

1. Accesați **Bitdefender Central**.
2. Selectează pictograma  din partea din dreapta-sus a ecranului.
3. Selectează **Bitdefender Contul** din meniu.
4. Selectează fila **Parolă și securitate**.
5. Selectează **Autentificare în doi pași**.
6. Apasă **PORNEȘTE**.

Selectează una dintre următoarele metode:

- **Aplicație de autentificare** - folosește o aplicație de autentificare pentru a genera un cod de fiecare dată când dorești să te conectezi la contul tău Bitdefender.

Dacă dorești să utilizezi o aplicație de autentificare, dar nu ești sigur ce să alegi, îți punem la dispoziție o listă cu aplicațiile de autentificare pe care le recomandăm.



a. Selectează **UTILIZEAZĂ O APLICAȚIE DE AUTENTIFICARE** pentru a începe.

b. Pentru a te autentifica pe un dispozitiv cu sistem de operare Android sau iOS, folosește dispozitivul tău pentru a scana codul QR.

Pentru a te autentifica pe un laptop sau computer, poți adăuga manual codul afișat.

Apasă **Continuă**.

c. Introdu codul furnizat de aplicație sau cel afișat la pasul anterior, apoi selectează **ACTIVARE**.

● **E-mail** - de fiecare dată când te conectezi la contul tău Bitdefender, se va trimite un cod de verificare către căsuța ta de e-mail. Verifică contul de e-mail și introdu codul primit.

a. Selectează **UTILIZEAZĂ ADRESA DE E-MAIL** pentru a începe.

b. Verifică-ți contul de e-mail și introdu codul furnizat.

Reține că ai cinci minute la dispoziție pentru a-ți verifica contul de e-mail și pentru a introduce codul generat. Dacă timpul expiră, trebuie să generezi unul nou urmând aceiași pași.

c. Apasă **Activare**.

d. Ai la dispoziție zece coduri de activare. Poți copia, descărca sau tipări lista pentru a o utiliza ulterior în cazul în care îți pierzi adresa de e-mail sau nu te poți conecta. Fiecare cod poate fi folosit o singură dată.

e. Apasă pe **Finalizare**.

Dacă nu mai dorești să folosești Autentificarea în doi pași:

1. Selectează opțiunea **DEZACTIVEAZĂ AUTENTIFICAREA ÎN DOI PAȘI**.

2. Verifică aplicația sau contul de e-mail și introdu codul primit.

Dacă ai optat pentru a primi codul de autentificare prin e-mail, ai cinci minute la dispoziție pentru a-ți verifica contul de e-mail și pentru a introduce codul generat. Dacă timpul expiră, trebuie să generezi unul nou urmând aceiași pași.


3. Confirmă alegerea.



Adăugarea dispozitivelor sigure

Pentru a ne asigura că tu ești singura persoană care poate accesa contul tău Bitdefender, este posibil să îți solicităm mai întâi un cod de securitate. Dacă dorești să omiți acest pas de fiecare dată când te conectezi de pe același dispozitiv, îți recomandăm să îl setezi ca dispozitiv sigur.

Pentru a adăuga dispozitive marcate ca fiind sigure:



1. Accesați **Bitdefender Central**.
2. Selectează pictograma  din partea din dreapta-sus a ecranului.
3. Selectează **Bitdefender Contul** din meniu.
4. Selectează fila **Parolă și securitate**.
5. Selectează opțiunea **Dispozitive sigure**.
6. Se afișează lista cu dispozitivele pe care este instalat Bitdefender. Selectează dispozitivul dorit.

Poți adăuga oricât de multe dispozitive dorești, cu condiția ca pe acestea să fie instalat Bitdefender și abonamentul tău să fie valid.

Dispozitivele mele



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

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

1. Accesați **Bitdefender Central**.
2. Atinge  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
3. Atinge cardul dispozitivului dorit și apoi atinge  din colțul din dreapta sus al ecranului.
4. Selectează **Setări**.
5. Introduce o nouă denumire în câmpul **Denumire dispozitiv** și apoi selectează **SALVARE**.



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

1. Accesați **Bitdefender Central**.
2. Atinge  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
3. Atinge cardul dispozitivului dorit și apoi atinge  din colțul din dreapta sus al ecranului.
4. Selectează **Profil**.
5. Atinge **Adăugare proprietar** și completează câmpurile corespunzătoare. Personalizează-ți profilul adăugând o fotografie și selectând data nașterii.
6. Atingeți **ADAUGĂ** pentru a salva profilul.
7. Selectați deținătorul dorit din lista **Deținător dispozitiv**, apoi atingeți **ALOCARE**.

Pentru mai multe operațiuni ce pot fi efectuate de la distanță și informații referitoare la produsul Bitdefender instalat pe un anumit dispozitiv, selectați cardul dispozitivului dorit.

După ce selectați cardul dispozitivului, sunt disponibile următoarele secțiuni:

- **Panou de bord.** În această fereastră, poți vizualiza detalii despre dispozitivul selectat, poți verifica starea sa de protecție, starea funcției VPN Bitdefender 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, apasă pe săgeata jos din zona de stare din partea de sus pentru a afla mai multe detalii. De aici, puteți remedia manual problemele care afectează securitatea dispozitivelor.
- **Securitate.** Din această fereastră puteți rula de la distanță o operațiune de Scanare dispozitiv. Efectuează clic pe butonul **SCANARE** pentru a iniția procesul. De asemenea, puteți afla data ultimei scanări a dispozitivului și puteți primi un raport cu privire la cea mai recentă scanare, cu cele mai importante informații disponibile.
- **Antifurt.** În cazul în care nu vă găsiți telefonul, îl puteți localiza și lua acțiuni de la distanță cu ajutorul funcției Antifurt. Faceți clic pe **LOCALIZARE**




pentru a afla locația dispozitivului. Se va afișa ultima poziție cunoscută, alături de oră și dată. Pentru detalii despre această funcție, consultați *„Funcții Antifurt”* (p. 305).

Abonamentele mele

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

Verificați abonamentele disponibile

Pentru a verifica abonamentele disponibile:

1. Accesați **Bitdefender Central**.
2. Atinge  din colțul din stânga sus al ecranului și apoi selectează **Abonamentele mele**.

Aici aveți informații referitoare la disponibilitatea abonamentelor pe care le dețineți și la numărul de dispozitive care utilizează fiecare dintre aceste abonamente.


Puteți adăuga dispozitive unui abonament sau îl puteți reînnoi selectând un card de abonament.

Adaugă dispozitiv nou

Dacă abonamentul dvs. acoperă mai multe dispozitive, puteți adăuga un dispozitiv nou și puteți instala Bitdefender Mobile Security pe acesta, potrivit celor specificate în *„Instalarea Bitdefender Mobile Security”* (p. 292).

Reînnoire abonament

În cazul în care din abonamentul dumneavoastră mai sunt mai puțin de 30 de zile și ați optat pentru reînnoire automată, puteți reînnoi abonamentul manual urmând pașii de mai jos:

1. Accesați **Bitdefender Central**.
2. Atinge  din colțul din stânga sus al ecranului și apoi selectează **Abonamentele mele**.
3. Selectați cardul de abonare dorit.
4. Faceți clic pe **Reînnoire** pentru a continua.



Se deschide o pagină web în browser-ul dvs., de unde puteți reînnoi abonamentul Bitdefender.



32. ÎNTREBĂRI FRECVENTE

De ce are nevoie Bitdefender Mobile Security de o conexiune la internet?



Aplicația trebuie să comunice cu serverele Bitdefender pentru a determina starea de securitate a aplicațiilor scanate și a paginilor web pe care le vizitați, precum și pentru a primi comenzi de la contul tău Bitdefender, la folosirea funcțiilor Anti-Theft.

Pentru ce are nevoie Bitdefender Mobile Security de fiecare permisiune?

- Acces Internet -> utilizat pentru comunicarea cloud.
- Citire stare și identitate telefon -> utilizată pentru a detecta dacă dispozitivul este conectat la internet și pentru a extrage anumite informații despre dispozitiv necesare pentru a crea o identitate unică pentru comunicarea cu cloud-ul Bitdefender.
- Citiți și scrieți marcaje în browser -> Modulul Securitate web șterge siteurile rău intenționate din istoricul dumneavoastră de navigare.
- Citire date jurnal -> Bitdefender Mobile Security detectează urmele activității programelor periculoase din jurnalele Android.
- Locația -> Necesară pentru localizare la distanță.
- Camera -> necesar pentru Instantanee.
- Storage -> utilizat pentru a permite funcției de Scanare malware să verifice cardul SD.

Cum pot opri trimiterea către Bitdefender a informațiilor despre aplicațiile suspecte?



În mod implicit, Bitdefender Mobile Security trimite rapoarte către serverele Bitdefender cu privire la aplicațiile suspecte pe care le instalezi. Aceste informații sunt esențiale pentru îmbunătățirea detectării amenințărilor și ne poate ajuta să îți oferim o experiență mai bună în viitor. În cazul în care dorești să nu ne mai trimiți informații despre aplicațiile suspecte:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.
3. Dezactivează opțiunea **Detectare în cloud** din zona Scanner programe periculoase.





Unde pot vedea detalii despre activitatea aplicației?

Bitdefender Mobile Security păstrează un jurnal al tuturor acțiunilor importante, modificărilor de stare și al altor mesaje critice legate de activitatea sa. Pentru accesare, vizualizați care este activitatea aplicației:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Atinge  **Rapoarte**.



În fereastra RAPOARTE SĂPTĂMÂNNALE poți accesa rapoartele care sunt generate în fiecare săptămână, iar în fereastra JURNAL ACTIVITATE poți vizualiza informații despre activitatea aplicației tale Bitdefender.

Am uitat codul PIN pe care l-am configurat pentru protejarea aplicației. Ce fac?

1. Accesați **Bitdefender Central**.
2. Atinge  din colțul din stânga sus al ecranului și apoi selectează **Dispozitivele mele**.
3. Atinge cardul dispozitivului dorit și apoi atinge  din colțul din dreapta sus al ecranului.
4. Selectează **Setări**.
5. Recuperați codul PIN din câmpul **PIN aplicație**.

Cum pot schimba codul PIN pe care l-am configurat pentru Blocare aplicații și Antifurt?

Dacă dorești să modifice codul PIN pe care l-ai configurat pentru Blocare aplicații și Antifurt:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Setări**.
3. Atinge **COD PIN** de Securitate în secțiunea Antifurt.
4. Tastează codul PIN actual.
5. Tastează noul cod PIN pe care dorești să îl configurezi.




Cum pot dezactiva funcția Blocare aplicații?



Nu există o opțiune de dezactivare a funcției Blocare aplicații, dar o puteți opri cu ușurință prin debifarea casetelor de lângă aplicațiile selectate după introducerea codului PIN sau amprente de validare configurate.


Cum pot configura o altă rețea wireless ca fiind de încredere?

Mai întâi, trebuie să îți conectezi dispozitivul la rețeaua wireless pe care dorești să o configurezi ca fiind sigură. Urmați acești pași:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Apasă  **Blocare aplicații**.
3. Atinge  din colțul din dreapta sus.
4. Atinge **ADĂUGARE** de lângă rețeaua pe care dorești să o configurezi ca fiind sigură.

Cum pot renunța la afișarea fotografiilor realizate de dispozitivele mele?

Pentru a nu mai afișa fotografiile realizate de dispozitivele tale:

1. Accesați **Bitdefender Central**.
2. Atinge  din partea superioară dreapta a ecranului.
3. Selectează **Contul meu** din meniu.
4. Selectați tabul **Setări**.
5. Dezactivează opțiunea **Afișează/nu mai afișa fotografiile realizate de dispozitivele tale**.

Cum pot efectua cumpărături online în siguranță?

Cumpărăturile online prezintă riscuri mari atunci când sunt ignorate anumite detalii. Pentru a nu deveni victima unei fraude, îți recomandăm următoarele:

- Păstrează securitatea ta actualizată.
- Trimite plăți online numai dacă este asigurată protecția cumpărătorului.
- Folosește un VPN atunci când te conectezi la internet prin intermediul unor rețele wireless publice sau nesecurizate.
- Atenție la parolele atribuite conturilor tale online. Acestea trebuie să fie puternice și să includă litere mari și mici, numere și simboluri (@, !, %, #, etc.).



- Asigură-te că informațiile sunt trimise prin intermediul unor conexiuni sigure. Extensiile site-urilor online trebuie să fie HTTPS://, nu HTTP://.

De ce să folosesc Bitdefender VPN?

Trebuie să procedezi cu atenție atunci când accesezi, descarci sau încarci conținut pe internet. Ca să fii sigur că ești protejat atunci când navighezi pe web, îți recomandăm să folosești Bitdefender VPN când:

- 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?


Bitdefender VPN este conceput să îți protejeze datele personale, să îți ascundă adresa IP în timp ce ești conectat la rețele wireless nesecurizate și la conținutul cu acces restricționat din 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?

Bitdefender VPN este conceput să îți ofere o navigare ușoară pe web; totuși, conexiunea ta la internet sau distanța față de serverul la care te conectezi pot cauza o încetinire. În acest caz, dacă nu trebuie neapărat să te conectezi din locația ta la un server îndepărtat (de ex. din SUA sau China), îți recomandăm să permiți Bitdefender VPN să te conecteze automat la cel mai apropiat server, sau să găsești un server mai apropiat de locația ta curentă.

Pot schimba contul Bitdefender legat la dispozitivul meu?

Da, puteți schimba cu ușurință contul Bitdefender asociat dispozitivului dvs. urmând pașii de mai jos:

1. Apasă  **Mai mult** din bara de navigare din partea de jos.
2. Atinge adresa ta de e-mail.



3. Atinge **Deconectează-te de la contul tău**. Dacă a fost configurat un cod PIN, ți se solicită să îl introduci.
4. Confirmă alegerea.
5. Introdu adresa e-mail și parola contului tău în câmpurile corespunzătoare și selectează **AUTENTIFICARE**.

Ce impact va avea Bitdefender Mobile Security asupra performanței dispozitivului și a autonomiei bateriei?

Impactul este extrem de redus. Aplicația rulează numai atunci când este absolut necesar – inclusiv la instalare și în timpul utilizării interfeței – sau atunci când efectuezi o verificare de siguranță. Bitdefender Mobile Security nu rulează în fundal atunci când efectuați apeluri telefonice, când scrieți mesaje sau vă jucați.

Ce este Administratorul pentru dispozitiv?

Administratorul pentru dispozitiv este o funcție Android care oferă Bitdefender Mobile Security permisiunile necesare pentru realizarea anumitor activități la distanță. Fără aceste privilegii, blocarea la distanță nu ar funcționa, iar ștergerea dispozitivului nu ar putea finaliza ștergerea completă a datelor dumneavoastră. Dacă doriți să ștergeți aplicația, asigurați-vă că revocați aceste privilegii înainte de a efectua deinstalarea din **Setări > Securitate > Selectare administratori dispozitiv**.

Cum se poate remedia eroarea "Token Google inexistent" care apare la autentificarea în Bitdefender Mobile Security.

Această eroare apare atunci când dispozitivul dumneavoastră nu este asociat cu un cont Google sau este asociat cu un cont, dar o problemă temporară împiedică conectarea la Google. Încercați una dintre următoarele soluții:

- Mergeți la **Setări > Aplicații > Gestionati aplicațiile > Bitdefender Mobile Security** și apăsați pe **Ștergeți datele**. Apoi încercați din nou să vă autentificați.
- Asigurați-vă că dispozitivul dumneavoastră este asociat cu un cont Google.
Pentru a verifica, mergeți la **Setări > Conturi și sincronizare** și vedeți dacă apare vreun cont în secțiunea **Gestionati conturile**. Dacă nu apare niciun cont, adăugați contul dumneavoastră, reporniți dispozitivul și încercați să vă autentificați din nou din Bitdefender Mobile Security.
- Reporniți dispozitivul și încercați să vă autentificați din nou.



În ce limbi este disponibil Bitdefender Mobile Security?

În prezent, Bitdefender Mobile Security este disponibil în următoarele limbi:

- Portugheză braziliană
- Cehă
- Olandeză
- Engleză
- Franceză
- Germană
- Greacă
- Maghiară
- Italiană
- Japoneză
- Coreană
- Poloneză
- Portugheză
- Română
- Rusă
- Spaniolă
- Suedeză
- Thailandeză
- Turcă
- Vietnameză

Alte limbi vor fi adăugate în versiunile viitoare. Pentru a modifica limba interfeței Bitdefender Mobile Security, mergeți la setările **Limbă & tastatură** ale dispozitivului dumneavoastră și setați dispozitivul la limba pe care doriți să o utilizați.



CONTACTAȚI-NE



33. SOLICITAREA AJUTORULUI

Bitdefender oferă clienților săi un nivel neegalat în ceea ce privește rapiditatea și acuratețea suportului tehnic. Dacă vă confrunțați cu o problemă sau aveți o întrebare referitoare la produsul Bitdefender deținut, puteți utiliza mai multe resurse online pentru a găsi o soluție sau un răspuns. În același timp, puteți contacta echipa de Servicii clienți a Bitdefender. Reprezentanții noștri pentru suport tehnic vă vor răspunde la întrebări la timp și vă vor oferi asistența de care aveți nevoie.

Secțiunea „*Soluționarea problemelor frecvente*” (p. 193) vă oferă informațiile necesare referitoare la cele mai frecvent întâlnite probleme atunci când utilizați acest produs.

Dacă nu găsiți un răspuns la întrebarea dumneavoastră printre resursele puse la dispoziție, ne puteți contacta direct:

- „Contactează-ne direct din Bitdefender Total Security” (p. 333)
- „Contactați-ne prin intermediul Centrului nostru de asistență online” (p. 334)

Contactează-ne direct din Bitdefender Total Security

Dacă dispuneți de o conexiune la internet funcțională, puteți contacta Bitdefender pentru asistență direct din interfața produsului dumneavoastră.

Urmați acești pași:

1. Dă clic pe **Asistență** din meniul de navigare al **interfeței Bitdefender**.
2. Aveți la dispoziție următoarele opțiuni:

- **GHIDUL UTILIZATORULUI**

Accesați baza noastră de date și căutați informațiile necesare.

- **CENTRUL DE ASISTENȚĂ**

Accesează articolele și tutorialele noastre video online.

- **CONTACTEAZĂ-NE**

Efectuează clic pe **CONTACTARE ASISTENȚĂ** pentru a lansa Instrumentul de asistență Bitdefender și pentru a contacta Departamentul de asistență clienți.

- a. Completați formularul cu datele necesare:



- i. Selectează tipul problemei pe care ai întâlnit-o:
 - ii. Scrie o descriere a problemei întâmpinate.
 - iii. Efectuează clic pe **ÎNCEARCĂ SĂ REPRODUCI ACEASTĂ PROBLEMĂ** în cazul în care te confrunți cu o eroare de produs. Reprodu problema, apoi dă clic pe **FINALIZARE** în panoul Reproducerea problemei.
 - iv. Efectuează clic pe **CONFIRMĂ TICHET**.
- b. Continuă să completezi formularul cu datele necesare:
- i. Scrie numele complet.
 - ii. Introduce adresa ta de e-mail.
 - iii. Bifează caseta prin care îți exprimi acordul.
 - iv. Dă clic pe **Creează un pachet pentru remedierea problemelor**.
Așteaptă câteva minute pentru ca Bitdefender să adune informații referitoare la produs. Aceste informații îi vor ajuta pe inginerii noștri să găsească o soluție la problema dumneavoastră.
- c. Efectuează clic pe **ÎNCHIDE** pentru a părăsi asistentul. Veți fi contactat cât mai curând posibil de către unul dintre reprezentanții noștri.

Contactați-ne prin intermediul Centrului nostru de asistență online

Dacă nu poți accesa informațiile necesare utilizând produsul Bitdefender, consultă Centrul nostru online de asistență:

1. Mergeți la <https://www.bitdefender.ro/support/consumer.html>.

Centrul de asistență Bitdefender include numeroase articole care cuprind soluții la problemele asociate Bitdefender.

2. Folosiți bara de căutare din partea de sus a ferestrei pentru a găsi articole care v-ar putea oferi o soluție la problema dumneavoastră. Pentru a efectua o căutare, introduceți un cuvânt în bara de căutare și faceți clic pe **Căutare**.
3. Citiți articolele sau documentele relevante și încercați soluțiile propuse.
4. Dacă soluția propusă nu vă ajută să rezolvați problema, mergeți la



<https://www.bitdefender.ro/support/contact-us.html> și luați legătura cu reprezentanții serviciului de asistență.



34. 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>

- Forumul de suport al 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.

34.1. 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 amenințărilor, 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 pentru informații sau rapoartele de eroare care vin din partea clienților Bitdefender ajung la Serviciul de asistență Bitdefender sub formă de rapoarte de remediere a erorilor, notițe de evitare a erorilor, articole informaționale pentru a completa fișierele de ajutor ale produsului.

Centrul de asistență Bitdefender este disponibil oricând la

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



34.2. Forumul de suport al Bitdefender

Forumul de suport al Bitdefender le oferă utilizatorilor Bitdefender o modalitate facilă de a obține ajutor și de a-i ajuta pe alții.

În cazul în care produsul dumneavoastră Bitdefender nu funcționează bine, nu poate înlătura anumite amenințări de pe calculator sau dacă aveți întrebări referitoare la modul de funcționare, postați problema sau întrebarea pe forum.

Tehnicienii suport 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, te rugăm să verifici 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.

34.3. Portalul HOTforSecurity

HOTforSecurity reprezintă o sursă bogată de informații referitoare la securitatea calculatoarelor. Aici puteți afla informații despre diverse pericole la care se expune computerul dvs. atunci când este conectat la internet (malware, phishing, spam, infracțiuni cibernetice).

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>.



35. 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 astfel încât să depășească așteptările clienților și partenerilor săi. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

35.1. 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 amenințări: virus_submission@bitdefender.com

Subscrieri spam: spam_submission@bitdefender.com

Raportare abuz: abuse@bitdefender.com

Sit web: <https://www.bitdefender.ro>

35.2. 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/partner-locator.html>.
2. Selectați țara și orașul folosind opțiunile corespunzătoare.
3. În cazul în care nu găsiți un distribuitor Bitdefender în țara dumneavoastră, nu ezitați să ne contactați prin email la adresa sales@bitdefender.com. Te rugăm să scrii mesajul e-mail în limba engleză pentru a ne da posibilitatea să te ajutăm cu promptitudine.

35.3. Filialele Bitdefender

Reprezentanțele Bitdefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât



și 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>

Marea Britanie și Irlanda

BITDEFENDER LTD

C/O Howsons Winton House, Stoke Road, Stoke on Trent

Staffordshire, United Kindon, ST4 2RW

E-mail: info@bitdefender.co.uk

Telefon: (+44) 2036 080 456

Vânzări: sales@bitdefender.co.uk

Suport tehnic: <https://www.bitdefender.co.uk/support/>

Web: <https://www.bitdefender.co.uk>

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>

Danemarca

Bitdefender APS

Agern Alle 24, 2970 Hørsholm, Denmark

Birou: +45 7020 2282



Suport tehnic: <http://bitdefender-antivirus.dk/>

Web: <http://bitdefender-antivirus.dk/>

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

Orhideea Towers, 15A Orhideelor Street, Sector 6

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>

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>



Vocabular

Abonament

Contractul de cumpărare care acordă utilizatorului dreptul de a folosi un anumit produs sau serviciu pe un anumit număr de dispozitive și o anumită perioadă de timp. Un abonament expirat poate fi reînnoit automat folosind informațiile furnizate de utilizator la prima achiziție.

ActiveX

ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe și sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini web interactive care se comportă ca niște aplicații și nu ca niște simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane și să interacționeze și în alte moduri cu pagina web. Controalele ActiveX sunt adesea scrise utilizând limbajul Visual Basic.

Active X este cunoscut pentru lipsa totală de control al securității; experții în securitatea calculatoarelor descurajează utilizarea lui pe internet.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

Bitdefender dispune de o funcție proprie de actualizare care îți permite să verifici manual actualizările sau să permiți actualizarea automată a produsului.

Actualizare informații amenințare

Modelul binar al unei amenințări, utilizat de către soluția de securitate pentru detectarea și eliminarea amenințării.

adware

Aplicația adware este adesea combinată cu o aplicație gazdă care este oferită gratuit dacă utilizatorul acceptă aplicația adware. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere 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 cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licențiere.

Agresori online

Persoanele care caută să atragă minori sau adolescenți în conversații cu scopul de a-i implica în activități sexuale ilegale. Rețelele de socializare sunt locul ideal în care copiii vulnerabili pot fi vânați și seduși cu ușurință să comită activități sexuale, online sau în persoană.

Amenințare

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 amenințărilor se pot și înmulți. Toate amenințările informatice sunt create de om. O simplă amenințare care poate realiza copii ale sale este relativ simplu de produs. Chiar și o asemenea amenințare este periculoasă întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. O amenințare și mai periculoasă este cea care este capabilă să se răspândească în rețea și poate să treacă de sistemele de securitate.

Amenințare persistentă avansată

Amenințările persistente avansate (Advanced persistent threat, APT) exploatează vulnerabilitățile sistemelor pentru a fura informații importante și pentru a le trimite către sursă. Grupurile mari, cum ar fi organizațiile, companiile sau guvernele, sunt vizate de către aceste amenințări.

Obiectivul unei amenințări persistente avansate este de a rămâne nedetectată pentru o perioadă îndelungată de timp, fiind capabilă să monitorizeze și să adune informații importante fără a cauza daune asupra sistemelor vizate. Metoda folosită pentru injectarea amenințării în rețea este prin intermediul unui fișier PDF sau al unui document Office, care par inofensive, astfel încât orice utilizator poate executa fișierele.

Applet-uri Java

Reprezintă un program Java care este proiectat să ruleze doar pe pagini web. Pentru a utiliza un applet pe o pagină web, trebuie specificate numele applet-ului și mărimea acestuia. Când este accesată o pagină



web, browser-ul descarcă applet-ul de pe un server și îl rulează pe mașina utilizatorului (clientul). Applet-urile diferă de aplicații prin aceea că sunt guvernate de un protocol de securitate strict.

Astfel că, deși pot rula pe calculatorul unui utilizator, ele nu pot citi sau scrie date pe aceste calculatoare. Applet-urile sunt restricționate de domeniul de care aparțin în ceea ce privește scrierea și citirea datelor.

Arhivă

Un disc, o casetă sau un director care conține fișiere de rezervă.

Un fișier care conține unul sau mai multe fișiere într-un format comprimat.

Atac pe bază de dicționar

Atacuri prin ghicirea parolei utilizate pentru a accesa un sistem de calculator prin introducerea unei combinații de cuvinte obișnuite pentru a genera posibile parole. Aceași metodă este utilizată pentru a ghici cheile de decriptare ale mesajelor sau documentelor criptate. Atacurile pe bază de dicționar au succes deoarece multe persoane tind să aleagă parole scurte cu cuvinte unice care sunt ușor de ghicit.

Atac prin forță brută

Atac prin ghicirea parolei pentru accesarea unui sistem de calculator prin introducerea combinațiilor posibile de parole, majoritatea începând cu parolele cel mai ușor de ghicit.

Backdoor

Reprezintă o breșă de securitate realizată în mod deliberat. Motivația acestor "găuri" nu este întotdeauna malițioasă: unele sisteme de operare, de exemplu, sunt puse în circulație cu conturi privilegiate pentru tehnicienii din service sau de responsabili cu mentenanța produsului din partea producătorului.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în bara de sarcini Windows (de obicei în partea de jos, lângă ceas) și conține pictograme miniaturale pentru accesul rapid la aplicații de sistem cum ar fi cele legate de fax, imprimantă, modem, volum și altele. Faceți dublu-clic sau clic dreapta cu mouse-ul pe o pictogramă pentru a vizualiza și accesa detaliile și comenzile.



Botnet

Termenul „botnet” este compus din cuvintele „robot” și „network” (rețea). Botnet-urile sunt dispozitive conectate la internet infectate cu amenințări și pot fi utilizate pentru a trimite mesaje spam, pentru a fura date, pentru a controla dispozitivele vulnerabile sau pentru a răspândi programele spion, ransomware și alte tipuri de amenințări. Obiectivul lor este de a infecta cât mai multe dispozitive conectate, precum PC-uri, servere, dispozitive mobile sau IoT aparținând marilor companii sau industrii.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza și încărca pagini de web. Browserele cele mai des folosite includ Microsoft Internet Explorer, Mozilla Firefox și Google Chrome. Acestea sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafice cât și text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet și animație.

Cale fișier

Reprezintă direcția exactă către un fișier de pe un calculator. Această direcție este specificată utilizând sistemul ierarhic de organizare a fișierelor de sus în jos.

Ruta între două puncte, cum ar fi de exemplu canalul de comunicație între două computere.

Client de mail

Un client de mail este o aplicație care vă permite să trimiteți și să recepționați mesaje.

Cod de activare

Este o cheie unică ce poate fi cumpărată de la distribuitorii retail și folosită pentru a activa un anumit produs sau serviciu. Codul de activare permite activarea unui abonament valabil pentru o anumită perioadă de timp și un anumit număr de dispozitive și poate fi, de asemenea, folosit pentru prelungirea unui abonament, cu condiția ca acesta să fie generat pentru același produs sau serviciu.

Cookie

În domeniul internetului, cookie-urile reprezintă mici fișiere ce conțin informații despre fiecare calculator care pot fi analizate și folosite de către cei care publică reclame pentru a vă urmări interesele și preferințele



online. În acest domeniu, tehnologia cookie-urilor este în curs de dezvoltare, iar intenția este de a afișa direct acele anunțuri care corespund intereselor dumneavoastră. Această facilitate are avantaje și dezavantaje pentru mulți deoarece, pe de o parte, este eficientă și pertinentă din moment ce vizualizați doar acele anunțuri despre subiecte care vă interesează. Pe de altă parte, cookie-urile implică de fapt o "monitorizare" și "urmărire" a site-urilor vizitate și a link-urilor accesate. Astfel, în mod logic, părerile sunt împărțite în ceea ce privește confidențialitatea și mulți se simt jigniți de faptul că sunt văzuți ca un simplu "număr SKU" (este vorba de codul de bare de pe spatele ambalajelor care este scanat pe bandă la supermarket). Deși acest punct de vedere poate fi considerat extrem, în anumite cazuri el reprezintă chiar ceea ce se întâmplă în realitate.

Descărcare

Reprezintă copierea (de obicei a unui întreg fișier) de pe o sursă principală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fișier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi și la copierea unui fișier de pe un server de rețea pe un calculator din rețea.

Drive de disc

Este un dispozitiv care citește date de pe un disc și scrie date pe un disc.

Un drive de hard disc citește / scrie date de pe / pe hard disc.

Un drive de floppy accesează dischetele floppy.

Drive-ele de disc pot fi sau interne (incorporate în interiorul unui calculator) sau externe (plasate într-o locație separată care este conectată la calculator).

E-mail

Se referă la poșta electronică. Acesta este un serviciu care transmite mesaje către alte calculatoare prin intermediul rețelei locale sau globale.

Elemente din startup

Orice fișier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, și nu direct fișierul.



Evenimente

O acțiune sau întâmplare detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

Exploatări

O metodă de a profita de diferite erori sau vulnerabilități prezente pe un computer (software sau hardware). Astfel, hackerii pot prelua controlul asupra computerelor sau rețelelor.

Extensie de fișier

Reprezintă porțiunea dintr-un nume de fișier ce urmează după caracterul punct, și care indică tipul de date pe care le stochează fișierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fișiere. De obicei aceasta este formată din una până la trei litere (unele sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: "c" pentru fișierele sursă scrise în limbajul C, "ps" pentru fișiere PostScript sau "txt" pentru fișierele text oarecare.

Fals pozitiv

Apare atunci când un analizator detectează un fișier ca fiind infectat când de fapt acesta nu este infectat.

Fișier de raport

Reprezintă un fișier care listează acțiunile care au avut loc. Bitdefender menține un fișier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fișierelor, numărul de arhive și fișiere scanate, câte fișiere infectate și suspecte au fost găsite.

Hărțuire cibernetică

Atunci când colegii sau persoanele străine comit acte abuzive împotriva copiilor cu scopul de a-i răni fizic. Pentru a produce daune emoționale, agresorii trimit mesaje răutăcioase sau fotografii denigrante, determinându-și victimele să se izoleze de ceilalți sau să se simtă frustrate.

Honeypot

Un sistem capcană configurat în vederea atragerii hackerilor pentru a studia modul lor de acțiune și pentru a identifica metodele eretice pe



care le folosesc pentru a colecta informații de sistem. Companiile și corporațiile sunt mai interesate să implementeze și să folosească așa-numitele „honeypots” pentru a-și îmbunătăți starea generală de securitate.

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât și reasamblarea pachetelor IP.

Keylogger

Un jurnal de chei este o aplicație care înregistrează tot ceea ce tastezi.

Keyloggererele nu au o natură periculoasă. Pot fi folosite în scopuri legitime, cum ar fi monitorizarea activității angajaților sau a companiilor subordonate. Cu toate acestea, utilizarea lor de către infractorii cibernetici în scopuri negative este din ce în ce mai răspândită (de exemplu, pentru colectarea informațiilor cu caracter privat, cum ar fi acreditările de înregistrare și codurile numerice personale).

Linie de comandă

Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Memorie

Reprezintă arii de stocare a datelor din interiorul calculatorului. Termenul de memorie desemnează locul de stocare a datelor pe chipuri și pe cel al cuvintelor pe casete sau cd-uri audio. Fiecare calculator dispune de o anumită capacitate de memorie fizică, referită de obicei prin memorie principală sau RAM.

Metoda euristica

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de amenințări noi. Această metodă de scanare nu se bazează pe baze de date cu informații specifice despre amenințări. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unei amenințări deja existente. Totuși ocazional poate raporta un cod suspicios în programe normale, generând așa-numitul "fals pozitiv".



Metoda ne-uristică

Această metodă de scanare se bazează pe baze de date cu informații specifice despre amenințări. Avantajul metodelor ne-uristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea o amenințare și din acest motiv nu generează fals pozitiv.

Phishing

Reprezintă acțiunea de a trimite un e-mail către un utilizator, pretinzând a fi o companie legitimă, în încercarea de a păcăli utilizatorul să furnizeze informații confidențiale ce vor fi folosite la furtul identității. E-mailul îndreaptă utilizatorul către un site Web unde acesta este rugat să actualizeze informații personale, cum ar fi parole și numere de card de credit, de asigurări sociale și de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals și folosit pentru a fura informațiile despre utilizator.

Photon

Photon este o tehnologie Bitdefender inovatoare, neutruzivă, proiectată pentru minimizarea impactului soluției tale de securitate asupra performanțelor. Prin monitorizarea în fundal a activității PC-ului tău, creează modele de utilizare care vor ajuta la optimizarea pornirii și a proceselor de scanare.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor și tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului, și a altor dispozitive periferice.

În rețelele TCP / IP și UDP acestea reprezintă un punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Programe împachetate

Reprezintă un fișier în format comprimat. Multe dintre sistemele de operare și aplicații conțin comenzi care vă dau posibilitatea de a arhiva un fișier astfel încât să ocupe mai puțină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați.



Totuși, un program care arhivează fișiere va înlocui caracterele de spațiu printr-un caracter special reprezentând spațiu, urmat de un număr care reprezintă numărul de spații înlocuite. În acest caz, cele zece caractere reprezentând spațiu ar necesita doar doi biți. Aceasta este doar un exemplu de comprimare - există multe alte metode în afară de aceasta.

Programe spion

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 o amenințare de tip cal 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 de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere 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.

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.



Rețea virtuală privată (VPN)

Este o tehnologie care permite o conexiune directă temporară și criptată la o anumită rețea prin intermediul unei rețele mai puțin sigure. Astfel, trimiterea și primirea de date este sigură și criptată, dificil de interceptat de către curioși. O dovadă de securitate este autentificarea, care se poate efectua numai folosind un nume de utilizator și o parolă.

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 amenințări sau prezența intrușilor în sistem. În combinație cu amenințările, 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.

Script

Un alt termen pentru fișiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Sector de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului și altele). În cazul discurilor de startup, sectorul de boot conține un program care încarcă sistemul de operare.

Spam

Termen ce acoperă întreaga gamă a mesajelor electronice nesolicitate (junk). În general, acestea sunt cunoscute sub numele de mesaje electronice nesolicitate.



TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul internet și care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware și sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât și convenții folosite în conectarea rețelelor și rutării traficului.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de programele malițioase și viermi, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cele mai mascate tipuri de amenințări de tip cal troian este un program care pretinde că elimină amenințările de pe calculatorul tău, însă, în loc de aceasta, introduce amenințări pe calculatorul 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 de boot

Reprezintă o amenințare care infectează sectorul de boot al unui disc fix sau al unei dischete. Orice încercare de a face boot de pe o dischetă infectată cu un virus de boot va determina amenințarea să devină activă în memorie. Din acest moment de fiecare dată când veți realiza boot-area sistemului, amenințarea va deveni activă în memorie.

Virus de macro

Un tip de amenințare informatică este aceea inclusă ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word și Excel suportă limbaje macro puternice.



Aceste limbaje permit încapsularea de macro-uri în documente și execută aceste macro-uri de fiecare dată când este deschis documentul.

Virus polimorf

O amenințare care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu are un tipar binar consistent, astfel de amenințări sunt greu de identificat.