Bitdefender ANTIVIRUS PLUS

MANUAL DE UTILIZARE

Bitdefender Antivirus Plus
Manual de utilizare

Publicat 09.12.2019

Termeni legali

Bitdefender

Cuprins

INSTALARE

1. PREGĂTIREA PENTRU INSTALARE

Pentru a instala Bitdefender Antivirus Plus fără probleme, parcurgeți 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, consultă *„Cerințe de sistem”* (p. 3).
- 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.
- 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.

2. CERINȚE DE SISTEM

Poți instala Bitdefender Antivirus Plus 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.

2.1. Cerințe software

Pentru a putea utiliza Bitdefender și toate funcțiile sale, computerul tău trebuie să întrunească 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

3. INSTALAREA PRODUSULUI TĂU BITDEFENDER

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

Dacă achiziționezi protecții pentru mai mult de un calculator (de exemplu, ai achiziționat Bitdefender Antivirus Plus pentru 3 calculatoare), reia procedura de instalare și activați produsul pe fiecare calculator folosind același cont. Contul pe care trebuie să-l folosești este cel care conține abonamentul tău activ pentru Bitdefender.

3.1. Instalează din Bitdefender Central

Din Bitdefender Central poți descărca kitul de instalare corespunzător abonamentului achiziționat. Odată ce procesul de instalare s-a finalizat, Bitdefender Antivirus Plus este dezactivat.

Pentru a descărca Bitdefender Antivirus Plus din Bitdefender Central:

1. Accesează Bitdefender Central.
2. Selectează fereastra **Dispozitivele mele**și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA**.
3. Alege una dintre cele doua 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 detectată o soluție antivirus necompatibilă sau o versiune mai veche a Bitdefender, ți se va cere să o ștergi de pe sistemul tău. Te rugăm să urmezi instrucțiunile pentru a șterge software-ul din sistemul tău, evitând astfel apariția problemelor pe viitor. Este posibil să fie nevoie să pornești calculatorul pentru a finaliza dezinstalarea soluțiilor antivirus detectate.

Pachetul de instalare Bitdefender Antivirus Plus 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 Antivirus Plus.

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 Antivirus Plus.

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 dezinstalată 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.

Efectuează clic pe **FINALIZARE** pentru a accesa interfața Bitdefender Antivirus Plus.

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 detectată o soluție antivirus necompatibilă sau o versiune mai veche a Bitdefender, ți se va cere să o ștergi de pe sistemul tău. Te rugăm să urmezi instrucțiunile pentru a șterge software-ul din sistemul tău, evitând astfel apariția problemelor pe viitor. Este posibil să fie nevoie să pornești 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. Urmați pașii pentru instalarea Bitdefender Antivirus Plus.

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 Antivirus Plus.

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 dezinstalată 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, consultă 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 ți-ai uitat parola, este necesar să accesezi https://my.bitdefender.com pentru a o reseta. Apoi, utilizezi 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. Selectează serviciul pe care dorești să îl utilizezi. Vei fi redirecționat către pagina de autentificare a acelui serviciu.

2. Urmează instrucțiunile oferite de serviciul selectat pentru a face legătura dintre contul tău 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 - Activează-ți 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.

Procedează în funcție de situația ta:

- 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, poți 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.

Efectuează clic pe **FINALIZARE** pentru a accesa interfața Bitdefender Antivirus Plus.

PRIMII PAȘI

4. INFORMAȚII DE BAZĂ

Odată ce ai instalat Bitdefender Antivirus Plus, calculatorul tău este protejat împotriva tuturor tipurilor de amenințări (cum ar fi programele periculoase, programele spion, ransomware, exploits, botnets și troienii).

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 tău pentru a ști ce anume și când să scaneze, reducând astfel la minimum impactul asupra performanțelor sistemului tău.

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 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. 124).

Poți menține evidența parolelor și a conturilor tale online salvându-le cu *„Protecția datelor de autentificare cu Password Manager"* (p. 114) într-un portofel. Cu o singură parolă generală îți poți proteja confidențialitatea de intrușii care ar putea încerca să te lase fără bani.

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, consultă secțiunea *„Evaluare securitate rețele Wi-Fi"* (p. 104).

Fișierele tale personale stocate local, cum ar fi documente, fotografii 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, consultă *„Protecție fișiere"* (p. 108).

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. 111).

În timp ce lucrezi, te joci sau vizionezi filme, Bitdefender îți poate oferi o experiență neîntreruptă a utilizatorului prin amânarea sarcinilor de întreținere, eliminarea întreruperilor și ajustarea efectelor vizuale ale sistemului. Poți beneficia de toate acestea activând și configurând opțiunea *„Profiluri"* (p. 137).

Bitdefender va lua majoritatea deciziilor legate de securitate în locul tău 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, consultă capitolul *„Notificări"* (p. 15).

Din când în când, trebuie să deschizi Bitdefender și să remediezi oricare din problemele existente. Este posibil să fie nevoie să configurezi anumite componente ale Bitdefender sau să iei măsuri preventive pentru a-ți proteja calculatorul și datele.

Pentru a folosi caracteristicile online ale Bitdefender Antivirus Plus și pentru administrarea abonamentelor și dispozitivelor tale, accesează-ți contul Bitdefender. Pentru mai multe informații, consultă capitolul *„Bitdefender Central"* (p. 30).

În secțiunea „Cum să" (p. 42) vei găsi instrucțiuni pas cu pas de efectuare a sarcinilor obișnuite. Dacă te confrunți cu probleme în utilizarea Bitdefender, accesează secțiunea *„Soluționarea problemelor frecvente"* (p. 145) pentru soluții posibile la cele mai frecvente probleme.

4.1. Deschiderea ferestrei Bitdefender

Pentru a accesa interfața principală a Bitdefender Antivirus Plus, urmează pașii de mai jos:

- În **Windows 7**:
  1. Efectuează clic pe **Start** și mergi la **Toate programele**.
  2. Efectuează clic pe **Bitdefender**.
  3. Efectuează clic pe **Bitdefender Antivirus Plus** sau, mai rapid, efectuează 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, deschide aplicația pentru desktop și efectuează dublu clic pe pictograma Bitdefender din bara de sistem.

- În **Windows 10**:

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

Pentru mai multe informații despre fereastra și pictograma Bitdefender de pe bara de sistem, consultă *„Interfața Bitdefender"* (p. 19).

4.2. Notificări

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

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, poți lua măsuri suplimentare dacă este cazul sau poți 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 verifici și să le remediezi atunci când ai 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 te ajuta să gestionezi cu ușurință evenimentele înregistrate, ferestra Notificări oferă opțiuni de ștergere sau marcare ca citite a tuturor evenimentelor din secțiunea respectivă.

4.3. 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 tău se alimentează de la baterie, este recomandat să amâni 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 tale este redus la minimum.

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

Profil Lucru
: Optimizează eficiența activității tale prin identificarea și ajustarea setărilor produsului și ale sistemului.

Profil Film
: Sporește efectele vizuale și elimină întreruperile în timpul vizionării filmelor.

Profil Joc
: Sporește 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.

4.3.1. 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. Selectează secțiunea **Profiluri**.
3. Folosește butonul corespunzător pentru a activa funcția **Activează profilurile automat**.

Dacă nu dorești activarea automată a Profilurilor, oprește 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. 137)

4.4. Protecție cu parolă pentru setările Bitdefender

Dacă nu ești singura persoană cu drepturi administrative care folosește acest calculator, este recomandat să îți protejezi 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**
>
> Te sfătuim să reții parola sau să o notezi și să o păstrezi într-un loc sigur. Dacă ai uitat parola, trebuie să reinstalezi programul sau să contactezi 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, introdu noua parolă pe care dorești să o utilizezi de acum înainte pentru a restricționa accesul la setările produsului tău Bitdefender.

4.5. 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. Selectează secțiunea **Avansat**.
3. Dezactivează opțiunea **Rapoarte produs**.

4.6. Notificări privind ofertele speciale

Atunci când sunt disponibile oferte promoționale, produsul Bitdefender este configurat să te notifice prin intermediul unei ferestre de tip pop-up. Aceasta îți oferă oportunitatea de a beneficia de prețuri avantajoase și de a-ți 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.

5. INTERFAȚA BITDEFENDER

Bitdefender Antivirus Plus 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 dorești să monitorizezi în permanență informațiile de securitate esențiale și să ai acces rapid la principalele setări, adaugă Widget-ul de securitate pe desktop.

5.1. Pictograma barei de sistem

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

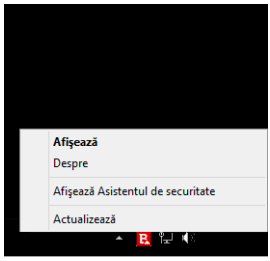
Notă
Este posibil ca pictograma Bitdefender să nu fie vizibilă întotdeauna. Pentru afișarea permanentă a pictogramei:

- În **Windows 7, Windows 8 și Windows 8.1**:
  1. Efectuează clic pe săgeata din colțul din dreapta jos al ecranului.

2. Efectuează clic pe **Personalizare...** pentru a deschide fereastra Pictogramelor din zona notificărilor.
3. Selectează 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. Activează butonul de lângă **Agent Bitdefender**.

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



Pictogramă în bară

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

Iconița Bitdefender din bara de sistem te informează despre problemele care îți 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 tău. Acestea necesită atenția ta imediat și trebuie remediate în cel mai scurt timp.

Dacă Bitdefender nu funcționează, pictograma din bara de sistem apare pe un fundal gri: . 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.

5.2. 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 și poți realiza acțiuni rapide.
- **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 împotriva privirilor iscoditoare, poți efectua plăți online într-un mediu sigur și poți deschide aplicația VPN.
- **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 Antivirus Plus, poți contacta departamentul de Asistență Tehnică Bitdefender.

5.3. 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.

Poți 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 diferite sarcini pentru a menține sistemul protejat.

5.3.1. 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 tale. 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 mutați 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.

5.3.2. 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**.

5.3.3. Acțiuni rapide

Utilizând acțiuni rapide poți lansa rapid sarcini pe care le consideri importante pentru păstrarea protecției sistemului tău și îmbunătățirea modului în care lucrezi.

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 îndepărtezi.
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**. Scanează calculatorul pentru identificarea vulnerabilităților, pentru a te 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**. Deschide Bitdefender Safepay™ pentru a-ți 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.
-

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 ta, se vor instala următoarele produse Bitdefender:

- Bitdefender Antivirus Plus 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.

5.4. Secțiunile Bitdefender

Produsul Bitdefender este livrat cu 2 secțiuni împărțite în caracteristici utile pentru a te ajuta să te protejezi în timp ce lucrezi, navighezi pe internet, te joci jocuri sau dorești să faci plăți online.

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

5.4.1. **Protecție**

În secțiunea Securitate poți configura setările tale avansate de securitate, poți configura caracteristicile Protecție fișiere și Online Threat Prevention, poți verifica și remedia eventualele vulnerabilități ale sistemului 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 tale. 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, consultă *„Protecție antivirus”* (p. 72).

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-ți proteja activitatea online, consultă *„Online Threat Prevention”* (p. 97).

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 îți poți menține sistemul protejat împotriva amenințărilor, consultă *„Advanced Threat Defense”* (p. 94).

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.

Efectuează 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, consultă *„Vulnerabilități"* (p. 100).

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. 108).

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. 111).

5.4.2. Confidențialitate

În secțiunea Confidențialitate, poți deschide aplicația Bitdefender VPN, îți poți proteja tranzacțiile online și îți poți securiza experiența de navigare.

Caracteristicile pe care le poți 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. 124).

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. 114).

SAFEPAY

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

Pentru mai multe informații despre Bitdefender Safepay™, consultă *„Securitate Safepay pentru tranzacțiile online"* (p. 128).

DATA PROTECTION

Caracteristica Data Protection îți permite să ștergi definitiv fișiere. Efectuează 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. 133).

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.

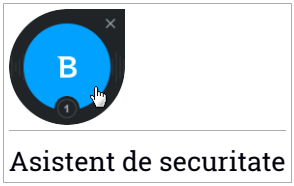
Pentru mai multe informații despre această funcție, consultă *„Anti-tracker"* (p. 121).

5.5. Asistent de securitate

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

- deschide fereastra principală a Bitdefender.
- monitorizarea activității de scanare în timp real
- monitorizarea stării de securitate a sistemului tău și remedierea problemelor existente
- vezi 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 tău 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 tău.

Acestea necesită atenția ta imediat și trebuie remediate în cel mai scurt timp. Efectuează clic pe pictograma de stare pentru a începe remedierea problemelor raportate.

Probleme care nu sunt critice afectează securitatea sistemului tău. Ar trebui să verifici și să le remediezi atunci când ai timp. Efectuează clic pe pictograma de stare pentru a începe remedierea problemelor raportate.

Sistemul tău este protejat.

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

Atunci când se raportează erori, efectuează 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). Efectuează clic pe contorul de evenimente, de exemplu pentru un eveniment necitit, pentru a deschide fereastra Notificări. Pentru mai multe informații, consultă capitolul *„Notificări”* (p. 15).

5.5.1. Scanarea fișierelor și directoarelor

Poți utiliza Widget-ul de securitate pentru a scana rapid fișiere și directoare. Trage și fixează orice fișier sau director pe care dorești să-l scanezi direct în **Widget-ul de securitate**.

Va apărea Asistentul de scanare care te 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 îți va permite să specifici alte acțiuni pentru a fi aplicate în cazul fișierelor infectate.

5.5.2. Ascundere / afișare Widget de securitate

Dacă nu mai dorești ca widget-ul să fie vizibil, efectuează clic pe .

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

- Din bara de sistem:
  1. Clic dreapta pe pictograma Bitdefender din bara de sistem.
  2. Efectuează 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.

5.6. 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.

6. 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:

- Descarcă și instalează Bitdefender pe sistemele de operare Windows, macOS, iOS și Android. Produsele disponibile pentru descărcare sunt:
  - Bitdefender Antivirus Plus
  - Bitdefender Antivirus pentru Mac
  - Bitdefender Mobile Security pentru Android
  - Bitdefender Mobile Security for iOS
- Administrează și reînnoiește abonamentele Bitdefender.
- Adaugă dispozitive noi la rețeaua ta și administrează-le oriunde te-ai afla.

6.1. Accesare Bitdefender Central

Există mai multe moduri de accesare aBitdefender Central:

- Din interfața principală Bitdefender:
  1. Efectuează 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. Mergi 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.

6.2. 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. Accesează Bitdefender Central.
2. Efectuează 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.

     Efectuează 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.

6.2.1. 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. Accesează Bitdefender Central.
2. Efectuează 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.

6.3. Abonamentele mele

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

6.3.1. Verifică abonamentele disponibile

Pentru a verifica abonamentele disponibile:

1. Accesează Bitdefender Central.
2. Selectează fereastra **Abonamentele mele**.

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

Poți adăuga dispozitive unui abonament sau îl poți reînnoi selectând un card de abonament.

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

6.3.2. Adaugă dispozitiv nou

Dacă abonamentul tău acoperă mai multe dispozitive, poți adăuga un dispozitiv nou și poți instala Bitdefender Antivirus Plus pe acesta, după cum urmează:

1. Accesează Bitdefender Central.
2. Selectează fereastra **Dispozitivele mele** și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA**.
3. Alege una dintre cele doua 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.

6.3.3. Reînnoire abonament

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

1. Accesează Bitdefender Central.

2. Selectează fereastra **Abonamentele mele**.
3. Selectează cardul de abonare dorit.
4. Efectuează clic pe **Reînnoire** pentru a continua.

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

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

Pentru a activa un abonament folosind un cod de activare:

1. Accesează Bitdefender Central.
2. Selectează fereastra **Abonamentele mele**.
3. Apasă pe butonul **COD DE ACTIVARE**, apoi introdu 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.

6.4. Dispozitivele mele

Zona **Dispozitivele mele** din Bitdefender Central îți 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 te identifica ușor dispozitivele, poți personaliza denumirea acestora:

1. Accesează Bitdefender Central.
2. Selectează 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**.

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

1. Accesează Bitdefender Central.
2. Selectează 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. Efectuează clic pe **ADAUGĂ** pentru a salva profilul.
7. Selectează deținătorul dorit din lista **Deținător dispozitiv**, apoi efectuează clic pe **ALOCARE**.

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

1. Accesează Bitdefender Central.
2. Selectează 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, poți remedia manual problemele care afectează securitatea dispozitivelor.
- **Securitate**. Din această fereastră, poți executa de la distanță o Scanare rapidă sau de sistem pe dispozitive. Efectuează clic pe butonul **SCANARE** pentru a începe procesul. De asemenea, poți afla data ultimei scanări a dispozitivului și poți primi un raport cu privire la cea mai recentă scanară, cu cele mai importante informații disponibile.Pentru mai multe informații referitoare la aceste două proceduri de scanare, consultă *„Executarea unei scanări a sistemului”* (p. 79) și *„Rularea unei scanări rapide”* (p. 78).
- **Vulnerabilități**. Pentru a verifica existența unor vulnerabilități pe un dispozitiv, cum ar fi lipsa actualizărilor Windows, aplicații expirate sau parole slabe, efectuează 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 execuți o nouă scanare pe dispozitivul respectiv și apoi să întreprinzi acțiunile recomandate. Efectuează clic pe **Mai multe detalii** pentru a accesa un raport detaliat despre problemele identificate. Pentru detalii despre această funcție, consultă *„Vulnerabilități”* (p. 100).

6.5. Notificări

Pentru a te ajuta să fii la curent cu ceea ce se întâmplă pe dispozitivele asociate contului tău, ai la dispoziție pictograma 🔔. Odată ce efectuezi clic pe aceasta, vei avea o imagine de ansamblu ce constă în informații despre activitatea produselor Bitdefender instalate pe dispozitivele tale.

7. 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 ești 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 tău.

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

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

- Dacă computerul tău este conectat la internet printr-un server proxy, trebuie să configurezi setările proxy, după cum se specifică în *„Cum pot configura Bitdefender să utilizeze o conexiune la internet de tip proxy?”* (p. 65).
- Dacă te conectezi la internet prin dial-up, atunci este recomandat să actualizezi manual Bitdefender în mod regulat. Pentru mai multe informații, consultă capitolul *„Efectuarea unei actualizări”* (p. 39).

7.1. Cum verifici 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.

Poți 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, repornește sistemul cât mai curând posibil.

7.2. Efectuarea unei actualizări

Pentru efectuarea actualizărilor este necesară existența unei conexiuni la internet.

Pentru a porni o actualizare, efectuează clic dreapta pe pictograma Bitdefender 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, ți se va cere fie să confirmi actualizarea, fie aceasta va fi realizată automat.

Important
Poate fi necesar ca după realizarea unei actualizări să repornești calculatorul. Îți recomandăm să faci acest lucru cât mai repede cu putință.

De asemenea, poți efectua actualizări ale dispozitivelor tale 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. Accesează Bitdefender Central.
2. Selectează secțiunea **Dispozitivele mele**.
3. Efectuează clic pe fila dispozitivului dorit și apoi pe pictograma din colțul din dreapta sus al ecranului.
4. Selectează **Actualizare**.

7.3. Activarea sau dezactivarea actualizării automate

Pentru activa sau dezactiva actualizarea automată:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței Bitdefender.
2. Selectează secțiunea **Actualizare**.
3. Activează sau dezactivează butonul corespunzător.

4. Se deschide o fereastră de avertizare. Trebuie să confirmi alegerea prin selectarea din meniu a duratei dezactivării actualizarii 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. Îți recomandăm să dezactivezi actualizarea automată pentru cât mai puțin timp posibil. Dacă nu este actualizat în mod regulat, Bitdefender nu va putea să te protejeze împotriva ultimelor amenințări apărute.

7.4. 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 te mai avertiza.

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

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, trage 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**.

7.5. Actualizări permanente

Pentru a te asigura că folosești 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 îți va solicita să repornești sistemul. Dacă ratezi această notificare, poți fie să efectuezi clic pe **REPORNEȘTE ACUM** în fereastra Notificări unde este menționată cea mai recentă actualizare, fie să repornești manual sistemul.

Notă

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

CUM SĂ

8. INSTALARE

8.1. Cum instalez Bitdefender pe un al doilea calculator?

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

Pentru a instala Bitdefender pe un al doilea calculator:

1. Efectuează 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-ai instalat pe produsul Bitdefender va apărea în panoul de control Bitdefender Central.

8.2. Cum reinstalez Bitdefender?

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

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

În cazul în care te aflii într-una dintre situațiile menționate mai sus, urmează acești pași:

- În **Windows 7**:
  1. Efectuează clic pe **Start** și mergi la **Toate programele**.
  2. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
  3. Efectuează 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, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control” direct în ecranul de Start) și efectuează click pe pictograma acestuia.
2. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
4. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.
5. După finalizarea procesului, va fi necesară repornirea calculatorului.

- În **Windows 10**:

1. Efectuează clic pe **Start**, apoi pe Setări.
2. Efectuează clic pe pictograma **Sistem** din zona Setări și selectează **Aplicații & funcții**.
3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
4. Efectuează clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Efectuează 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.

8.3. De unde se poate descărca produsul Bitdefender?

Poți instala Bitdefender folosind CD-ul de instalare sau aplicația de instalare web pe care o poți descărca pe calculatorul tău din platforma Bitdefender Central.

Notă
Înainte de a rula aplicația de instalare, îți recomandăm să dezinstalezi orice soluție de securitate de pe sistemul tău. Atunci când utilizezi mai multe soluții de securitate pe același calculator, sistemul devine instabil.

Pentru a instala Bitdefender din Bitdefender Central:

1. Accesează Bitdefender Central.

2. Selectează fereastra **Dispozitivele mele** și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA**.
3. Alege una dintre cele doua 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. Rulează produsul Bitdefender descărcat.

8.4. 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.

8.5. Cum folosesc abonamentul Bitdefender după un upgrade Windows?

Această situație apare atunci când faci un upgrade al sistemului de operare și dorești să utilizezi în continuare abonamentul Bitdefender.

Dacă folosești o versiune anterioară a Bitdefender, poți 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 Bitdefender Internet Security până la cea mai recentă versiune de Bitdefender Internet Security 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:

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

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

  - În **Windows 7**:

    1. Efectuează clic pe **Start**, mergi la **Control Panel** și efectuează clic pe **Programe și Caracteristici**.
    2. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
    3. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.
    4. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

       Deschide 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, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control” direct în ecranul de Start) și efectuează click pe pictograma acestuia.
    2. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
    3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
    4. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.
    5. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

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

- În **Windows 10**:

  1. Efectuează clic pe **Start**, apoi pe Setări.
  2. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează **Aplicații** .
  3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
  4. Efectuează clic din nou pe **Dezinstalare** pentru a confirma selecția.
  5. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.
  6. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

     Deschide 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.

- Ți-ai modificat sistemul și dorești să utilizezi în continuare protecția Bitdefender. Prin urmare, trebuie să reinstalezi produsul folosind cea mai recentă versiune.

  Pentru a rezolva această problemă:

  1. Descarcă fișierul de instalare:
     a. Accesează Bitdefender Central.
     b. Selectează fereastra **Dispozitivele mele**și apoi efectuează clic pe **INSTALEAZĂ PROTECȚIA**.
     c. Alege una dintre cele doua 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. Rulează produsul Bitdefender descărcat.

Pentru mai multe informații cu privire la procesul de instalare Bitdefender, consultă *„Instalarea produsului tău Bitdefender”* (p. 4).

8.6. 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 ai 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. Efectuează clic pe **REPORNEȘTE ACUM** în fereastra de notificare în care sunt afișate informațiile privind actualizarea. Dacă ai ratat-o, accesează fereastra Notificări, identifica cea mai recentă actualizare și apoi efectuează clic pe butonul **REPORNEȘTE ACUM**. Așteaptă repornirea calculatorului.

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

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

3. Închide 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.

9. BITDEFENDER CENTRAL

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

Ai creat un nou cont Bitdefender și dorești să începi să-l folosești.

Pentru a vă autentifica cu alt cont Bitdefender:

1. Efectuează 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 tău trece automat la abonamentul asociat noului cont Bitdefender.
Dacă nu există niciun abonament disponibil asociat noului cont Bitdefender sau dacă dorești să îl transferi pe contul anterior, poți contacta Bitdefender pentru asistență, în modul descris în secțiunea *„Solicitarea ajutorului”* (p. 171).

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

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

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

- Din interfața Bitdefender:
  1. Efectuează 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. Introdu 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. Mergi la: https://central.bitdefender.com.
  2. Selectează **AUTENTIFICARE**.
  3. Introdu 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, introdu adresa e-mail și noua parolă setată.

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

În contul tău Bitdefender, ai posibilitatea de a vizualiza cele mai recente sesiuni de autentificare active și inactive de pe dispozitivele asociate contului tău. În plus, te poți deconecta de la distanță urmând acești pași:

1. Accesează Bitdefender Central.
2. Efectuează clic pe icoana din partea dreapta de sus al ecranului.
3. Efectuează clic pe **Contul meu** în meniul derulant.
4. Selectează **Administrare sesiuni** din meniul glisant.
5. În secțiunea **Sesiuni active**, selectează opțiunea **Deconectare** din dreptul dispozitivului pe care dorești să închei sesiunea.

10. SCANAREA CU BITDEFENDER

10.1. 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 dorești să-l scanezi, alege Bitdefender și selectează **Scanează cu Bitdefender** din meniu.

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

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

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

- Suspectezi un anumit fișier sau director că este infectat.
- Atunci când descarci fișiere de pe internet considerate că ar putea fi periculoase.
- Scanează un director comun din rețea înainte de a copia fișiere din acesta pe calculatorul tău.

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

   Dacă rămân amenințări nesoluționate, ți se va cere să selectezi acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultă capitolul *„Asistentul de scanare antivirus”* (p. 83).

10.3. Cum programez o scanare?

Poți configura Bitdefender să activeze scanarea locațiilor importante de sistem când nu te aflii 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 oe 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**.

   Selectează 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.

10.4. Cum creez o activitate de scanare personalizată?

Dacă dorești să scanezi anumite locații de pe computer sau pentru a configura opțiunile de scanare, poți configura și rula o sarcină de scanare personalizată.

Pentru a crea o activitate de scanare personalizată, procedează 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, mărind 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, ți se va solicita să alegi acțiunile care trebuie întreprinse în cazul fișierelor detectate.

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

10.5. 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:

- Ai un director mare pe sistemul tău în care există filme și muzică
- Ai o arhivă mare pe sistemul tău în care păstrezi diferite date.
- Păstrează un director în care să instalezi 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.

10.6. 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. Dezactivează 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 confirmi alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real. Poți dezactiva protecția în timp real pentru 5, 15 sau 30 de minute, pentru o oră, permanent sau doar până la repornirea sistemului.
2. Afișează elementele ascunse din Windows. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot afișa elementele ascunse din Windows?"* (p. 67).
3. Restaurează fișierul din zona de carantină:
   a. Efectuează clic pe **Securitate** din meniul de navigare al interfeței Bitdefender.
   b. În secțiunea **ANTIVIRUS**, efectuează clic pe **Carantină**.
   c. Selectează fișierul și efectuează clic pe **RESTABILIRE**.
4. Adaugă 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. 56).
5. Activează protecția antivirus în timp real a Bitdefender.
6. Contactează un reprezentant al echipei noastre de asistență tehnică și solicită eliminarea actualizării informațiilor privind amenințările. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Solicitarea ajutorului"* (p. 171).

10.7. 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 poți 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 poți verifica ce operațiuni de scanare au fost realizate recent. Efectuează clic pe o notificare pentru a vizualiza detaliile acesteia.
4. Pentru a deschide un jurnal de scanare, efectuează clic pe **Vizualizare jurnal**.

11. PROTECȚIE CONFIDENȚIALITATE

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

Pentru a asigura confidențialitatea operațiunilor pe care le efectuezi online, poți folosi browserul furnizat de Bitdefender, care îți protejează tranzacțiile și aplicațiile de home banking.

Bitdefender Safepay™ este un browser securizat proiectat pentru a-ți proteja informațiile referitoare la cardul de credit, numărul de cont sau orice alte date sensibile pe care le introduci când accesezi 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. Efectuează clic pe butonul pentru a accesa **Tastatura virtuală**.

   Folosește **Tastatura virtuală** atunci când introduci informații confidențiale, cum ar fi parolele.

11.2. Cum șterg definitiv un fișier cu ajutorul Bitdefender?

Dacă dorești să ștergi definitiv un fișier din sistemul tău, este necesar să ștergi fizic datele de pe hard disk.

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

1. Efectuează clic dreapta pe fișierul sau directorul pe care dorești să-l ștergi definitiv, alege Bitdefender și selectează**Ștergere definitivă fișiere**.
2. Efectuează clic pe **ȘTERGE DEFINITIV** și apoi confirmă că dorești să continui procesul.

   Așteaptă ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.

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

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

În cazul în care fișierele criptat 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;

12. INFORMAȚII UTILE

12.1. Cum îmi testez soluția de securitate?

Pentru a te asigura că produsul Bitdefender funcționează corespunzător, îți recomandăm să utilizezi testul Eicar.

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

Pentru a testa soluția de securitate:

1. Descarcă testul din pagina oficială a organizației EICAR http://www.eicar.org/.
2. Efectuează clic pe fila **Fișier de testare anti-malware**.
3. Efectuează clic pe **Descărcare** în meniul din stânga.
4. Din zona de Download **folosind protocolul standard http** efectuează clic pe fișierul de testare **eicar.com**.
5. Vei primi notificarea că pagina pe care încerci să o accesezi conține fișierul de testare EICAR (și nu o amenințare).

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

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

Dacă nu primești nicio alertă Bitdefender, îți recomandăm să contactezi Bitdefender pentru asistență, așa cum este indicat la secțiunea *„Solicitarea ajutorului”* (p. 171).

12.2. Cum dezinstalez Bitdefender?

Dacă dorești să dezinstalezi Bitdefender Antivirus Plus:

- În **Windows 7**:
  1. Efectuează clic pe **Start**, mergi la **Control Panel** și efectuează clic pe **Programe și Caracteristici**.
  2. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
  3. Efectuează clic pe **ȘTERGE** în fereastra care se deschide.

4. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

- În **Windows 8 și Windows 8.1**:

1. Din ecranul de Start al Windows, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control” direct în ecranul de Start) și efectuează click pe pictograma acestuia.
2. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
4. Efectuează clic pe **ȘTERGE** în fereastra care se deschide.
5. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

- În **Windows 10**:

1. Efectuează clic pe **Start**, apoi pe Setări.
2. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează **Aplicații** .
3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
4. Efectuează clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Efectuează clic pe **ȘTERGE** în fereastra care se deschide.
6. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

Notă
Această procedură de reinstalare va șterge definitiv setările personalizate.

12.3. 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. Efectuează clic pe **Start**, mergi la **Control Panel** și efectuează clic pe **Programe și Caracteristici**.
2. Găsește **Bitdefender VPN** și selectează **Dezinstalare**.

   Așteaptă până când procesul de dezinstalare este finalizat.

- În **Windows 8 și Windows 8.1**:
  1. Din ecranul de Start al Windows, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control” direct în ecranul de Start) și efectuează click pe pictograma acestuia.
  2. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
  3. Găsește **Bitdefender VPN** și selectează **Dezinstalare**.

     Așteaptă până când procesul de dezinstalare este finalizat.
- În **Windows 10**:
  1. Efectuează clic pe **Start**, apoi pe Setări.
  2. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează**Aplicații instalate**.
  3. Găsește **Bitdefender VPN** și selectează **Dezinstalare**.
  4. Efectuează clic din nou pe **Dezinstalare** pentru a confirma selecția.

     Așteaptă până când procesul de dezinstalare este finalizat.

12.4. 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.

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

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

Din acest motiv, Bitdefender îți permite să îți configurezi produsul să închidă sistemul imediat după finalizarea scanării.

Spre exemplu: ți-ai terminat lucrul la calculator și vrei să mergi la culcare. Dorești să efectuezi o verificare integrală a sistemului tău în vederea detectării amenințărilor cu ajutorulBitdefender.

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, ți se va cere să selectezi acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultă capitolul *„Asistentul de scanare antivirus"* (p. 83).

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

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

Important
Conexiune de internet de acasă nu sunt folosite, în mod normal, ca server proxy. Ca regulă de bază, verifică și configurează 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. Selectează 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 specifici 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 poți configura cum dorești. Următoarele setări trebuie specificate:
  - **Adresă** - introdu adresa IP a serverului proxy.
  - **Port** - introdu portul folosit Bitdefender pentru a se conecta la serverul proxy.
  - **Utilizator** - introdu un nume de utilizator recunoscut de proxy.
  - **Parolă** - introdu o parolă validă pentru numele de utilizator introdus.

6. Efectuează 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.

12.7. 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. Efectuează clic pe **Start**.
  2. Localizează **Computer** din meniul **Start**.
  3. Efectuează clic-dreapta pe **Computer** și selectează **Properties**.
  4. Sub **System** vei găsi informații referitoare la sistemul tău .
- Pentru **Windows 8**:
  1. 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**.
  2. Selectează **Proprietăți** din meniul din partea de jos.

3. Mergi la secțiunea Sistem pentru a vedea tipul sistemului.

- În **Windows 10**:

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

12.8. Cum pot afișa elementele ascunse din Windows?

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

Urmează acești pași pentru a afișa obiectele ascunse din Windows:

1. Efectuează clic pe **Start** și mergi la **Panoul de control**.

   În **Windows 8 și Windows 8.1**: Din ecranul de Start al Windows, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control” direct în ecranul de Start) și efectuează clic pe pictograma acestuia.
2. Selectează **Opțiunile dosarului**:
3. Mergi la fila **View**.
4. Selectează **Show hidden files and folders**.
5. Debifează **Hide extensions for known file types**.
6. Debifează**Hide protected operating system files**.
7. Efectuează clic pe **Aplică** și apoi pe **OK**.

În **Windows 10**:

1. Introdu "Show hidden files and folders" în caseta de căutare din bara de sarcini și efectuează clic pe pictogramă.
2. Selectează **Show hidden files, folders, and drives**.
3. Debifează **Hide extensions for known file types**.
4. Debifează**Hide protected operating system files**.
5. Efectuează clic pe **Aplică** și apoi pe **OK**.

12.9. Cum elimin celelalte soluții de securitate?

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

Atunci când utilizezi mai multe soluții de securitate pe același calculator, sistemul devine instabil. Programul de instalare a Bitdefender Antivirus Plus detectează în mod automat alte programe de securitate și îți oferă opțiunea de a le dezinstala.

Dacă nu ai dezinstalat celelalte soluții de securitate în timpul instalării inițiale:

- În **Windows 7**:
  1. Efectuează clic pe **Start**, mergi la **Control Panel** și efectuează clic pe **Programe și Caracteristici**.
  2. Așteaptă câteva momente până când este afișată lista programelor instalate.
  3. Găsește numele programului pe care dorești să-l dezinstalezi și selectează **Dezinstalare**.
  4. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.
- În **Windows 8 și Windows 8.1**:
  1. Din ecranul de Start al Windows, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control” direct în ecranul de Start) și efectuează click pe pictograma acestuia.
  2. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
  3. Așteaptă câteva momente până când este afișată lista programelor instalate.
  4. Găsește numele programului pe care dorești să-l dezinstalezi și selectează **Dezinstalare**.
  5. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.
- În **Windows 10**:
  1. Efectuează clic pe **Start**, apoi pe Setări.

2. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează **Aplicații** .
3. Găsește numele programului pe care dorești să-l dezinstalezi și selectează **Dezinstalare**.
4. Efectuează clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

Dacă nu reușești să elimini cealaltă soluție de securitate, descarcă instrumentul de dezinstalare de pe site-ul furnizorului sau contactează-l direct pentru a-ți oferi instrucțiuni cu privire la dezinstalare.

12.10. 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 inactive 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. Repornește calculatorul.
  2. Apasă tasta **F8** de mai multe ori înainte ca Windows să pornească pentru a avea acces la meniul de pornire.
  3. Selectează **Safe Mode** din meniul de pornire sau **Safe mode with Networking** dacă dorești să ai acces la internet.
  4. Apasă **Enter** și așteaptă până când Windows se încarcă în Safe Mode.
  5. Acest proces se finalizează cu un mesaj de confirmare. Efectuează clic pe **OK** pentru a confirma.
  6. Pentru a porni Windows în mod normal, repornește 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. Selectează secțiunea **Boot**.
  4. În secțiunea **Opțiuni pornire**, bifează caseta **Pornire sigură**.
  5. Efectuează clic pe **Rețea** și apoi pe **OK**.
  6. Fă clic pe **OK** în fereastra **Configurare sistem (System Configuration)** care te 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**x. Fă clic pe **OK** și apoi pe **Repornire**. Așteaptă aplicarea noilor setări.

ADMINISTRAREA SECURITĂȚII TALE

13. PROTECȚIE ANTIVIRUS

Bitdefender îți 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 tău. Bitdefender va scana, de exemplu, un document Word atunci când îl deschizi și un mesaj e-mail atunci când îl primești.

  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, păstrează activată funcția de **scanare la accesare**.

- Scanarea la cerere - permite detectarea și eliminarea amenințărilor care există deja în sistemul tău. Acesta este modul clasic de scanare, inițiată de utilizator – tu alegi 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 te asigura că este sigur să îl accesezi. Pentru mai multe informații, consultă capitolul *„Scanarea automată a suporturilor media amovibile"* (p. 87).

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, consultă capitolul *„Configurarea excepțiilor de scanare"* (p. 89).

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, consultă capitolul *„Gestionarea fișierelor aflate în carantină"* (p. 92).

În cazul în care calculatorul tău a fost infectat cu amenințări, consultă *„Eliminarea amenințărilor din sistemul tău"* (p. 159). Pentru a te ajuta să îți cureți computerul de amenințările care nu pot fi eliminate din sistemul de operare

Windows, Bitdefender îți pune la dispoziție*„Bitdefender Modul de recuperare (Mediul de recuperare în Windows 10)"* (p. 159). Acesta este un mediu sigur, creat în special pentru eliminarea amenințărilor, care îți permite să pornești 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.

13.1. 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.

13.1.1. 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 dorești să dezactivezi protecția în timp real, se afișează o fereastră de avertizare. Trebuie să confirmi alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real. Poți 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. Îți recomandăm să dezactivezi protecția în timp real pentru cât mai puțin timp posibil. Dacă protecția în timp real este dezactivată, nu vei mai fi protejat împotriva amenințărilor.

13.1.2. Configurarea setărilor avansate de protecție în timp real

Utilizatorii avansați pot beneficia în urma ofertelor Bitdefender în ceea ce privește setările de scanare. Poți 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 îți 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 tău. Amenințările îți 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.** Poți seta Bitdefender să scaneze sectoarele de boot ale hard-discului. 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 poți 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.** Selectează această opțiune pentru a scana sistemul în vederea identificării aplicațiilor de tip keylogger. Aplicațiile keyloggers înregistrează ceea ce introduci 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.** Selectează 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 tău.

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. Configurează 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, dispare riscul de a fi infectat. Pentru mai multe informații, consultă capitolul *„Gestionarea fișierelor aflate în carantină”* (p. 92).

  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 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, vei 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, consultă capitolul *„Gestionarea fișierelor aflate în carantină”* (p. 92).

Interzice accesul

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

13.1.3. 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**. Selectează această opțiune pentru a reseta setările antivirus la valorile implicite.

13.2. Scanare la cerere

Principalul obiectiv Bitdefender este protejarea calculatorului tău 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 îți scanezi calculatorul de amenințări după instalarea Bitdefender. Și este, de asemenea, recomandat să îți scanezi 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. Poți scana computerul oricând dorești prin rularea sarcinilor implicite sau a propriilor sarcini de scanare (sarcini definite de utilizator). Dacă dorești să scanezi anumite locații de pe computerul tău sau să configurezi opțiunile de scanare, poți configura și rula o scanare personalizată.

13.2.1. Scanarea unui fișier sau a unui director pentru detectarea amenințărilor

Trebuie să scanezi fișierele și directoarele ori de câte ori consideri că acestea pot fi infectate. Efectuează clic dreapta pe fișierul sau directorul pe care dorești să îl scanezi, indică **Bitdefender** și selectează **Scanează cu Bitdefender**. Va apărea Asistentul de scanare care te va ghida de-a lungul procesului de scanare. După finalizarea scanării, ți se va cere să selectezi acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.

13.2.2. Rularea unei scanări rapide

Scanarea rapidă utilizează o tehnologie de scanare "in-the-cloud" (online) pentru a detecta amenințările ce rulează pe sistemul tău. 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**, efectuează clic pe **Scanare rapidă**.
3. Urmează programul asistent de scanare antivirus pentru a finaliza scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate. Dacă rămân amenințări nesoluționate, ți se va cere să selectezi acțiunile ce vor fi aplicate în cazul acestora.

13.2.3. 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 execuți această activitate într-un moment când nu utilizezi computerul.

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

- Asigură-te 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, consultă capitolul *„Actualizarea permanentă a Bitdefender"* (p. 38).
- Închide toate programele deschise.

Dacă dorești să scanezi anumite locații de pe computer sau pentru a configura opțiunile de scanare, poți configura și rula o sarcină de scanare personalizată. Pentru mai multe informații, consultă capitolul *„Configurarea unei scanări personalizate"* (p. 80).

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

13.2.4. 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, mărind 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, ți se va solicita să alegi acțiunile care trebuie întreprinse în cazul fișierelor detectate.

Informații cu privire la opțiunile de scanare

Aceste informații îți pot fi de folos:

- Dacă nu ești familiarizat cu anumiți termeni, verifică-i în glosar. De asemenea, poți 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 tău. Amenințările îți 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 utilizezi 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 (megaocteți).

  > **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.** Poți seta Bitdefender să scaneze sectoarele de boot ale hard-discului. 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 poți porni sistemul și accesa datele.

- **Scanează memoria.** Selectează această opțiune pentru a scana programele ce rulează în memoria sistemului tău.
- **Scanează regiștrii.** Selectează 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.** Selectează această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe computerul tău.
- **Scanare după keyloggers.** Selectează această opțiune pentru a scana sistemul în vederea identificării aplicațiilor de tip keylogger. Aplicațiile keyloggers înregistrează ceea ce introduci 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.

13.2.5. Asistentul de scanare antivirus

Ori de câte ori inițiezi o scanare la cerere (de exemplu, faci clic pe un director, evidențiezi Bitdefender și selectezi **Scanează cu Bitdefender**), se inițiază asistentul de Scanare antivirus Bitdefender. Urmează 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. Caută iconița de scanare în curs în bara de sistem. Poți 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. Poți 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).

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

Oprirea sau întreruperea temporară a scanării. Poți opri scanarea oricând dorești făcând clic pe **STOP**. Vei trece direct la ultimul pas al asistentului de

scanare. Pentru a opri temporar procesul de scanare, efectuează clic pe **ÎNTRERUPE**. Va trebui să efectuezi 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 fii rugat să introduci parola. Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizezi parola. Sunt disponibile următoarele opțiuni:

- **Parolă.** Dacă dorești ca Bitdefender să scaneze arhiva, selectează această opțiune și introdu parola. Dacă nu cunoști parola, selectează 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.** Selectează această opțiune dacă dorești să nu ți 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.

Alege opțiunea dorită și efectuează clic pe **OK** pentru a continua scanarea.

Pasul 2 - Selectarea acțiunilor

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

Notă

Atunci când execuți 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, ți se va cere să selectezi acțiunile ce vor fi aplicate în cazul acestora.

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

Poți alege o acțiune globală care să fie aplicată pentru rezolvarea tuturor problemelor găsite, sau poți 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, consultă capitolul *„Gestionarea fișierelor aflate în carantină"* (p. 92).

  > **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, vei 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, vei 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, poți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.

Efectuează 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 dorești informații complete cu privire la procesul de scanare, efectuează clic pe **AFIȘEAZĂ JURNAL** pentru a vizualiza jurnalul de scanare.

Important

În majoritatea cazurilor, Bitdefender va dezinfecta fișierele infectate detectate sau le va izola. Cu toate acestea, există anumite probleme care nu pot fi rezolvate automat. Dacă este necesar, repornește sistemul pentru a finaliza procesul de curățare. Pentru mai multe informații și instrucțiuni privind modul de eliminare a amenințărilor în mod manual, consultă *„Eliminarea amenințărilor din sistemul tău”* (p. 159).

13.2.6. Examinarea jurnalelor de scanare

De fiecare dată când efectuezi 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 poți 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 poți verifica ce operațiuni de scanare au fost realizate recent. Efectuează clic pe o notificare pentru a vizualiza detaliile acesteia.

4. Pentru a deschide un jurnal de scanare, efectuează clic pe **Vizualizare jurnal**.

13.3. 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)

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

13.3.1. 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). Vei 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 se va afișa în tăvița de sistem. Poți 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 te va informa dacă poți 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, ți va cere să selectezi acțiunile ce vor fi aplicate în cazul acestora.

Notă
Ia 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 îți pot fi de folos:

- Te rugăm să acorzi atenție maximă atunci când folosești un CD/DVD infectat cu amenințări, deoarece o amenințare nu poate fi ștearsă de pe CD/DVD (suportul media este de tip read-only). Asigură-te că protecția în timp real este activată pentru a preveni răspândirea amenințărilor în cadrul sistemului tău. Cea mai bună metodă este să copiezi datele inmportante de pe CD pe sistemul tău și apoi să arunci 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 tău”* (p. 159).

13.3.2. 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 dezinfecteze (să elimine codul malițios) sau să le mute în carantină. Dacă ambele acțiuni eșuează, asistentul de scanare Antivirus îți va permite să specifici alte acțiuni pentru a fi aplicate în cazul fișierelor infectate. Opțiunile de scanare sunt standard și nu le poți modifica.

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

13.4. 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. Selectează secțiunea **Avansat**.
3. Activează sau dezactivează opțiunea **Scanare fișier de configurare a gazdelor**.

13.5. 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 ta 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: efectuează clic-dreapta pe fișierul sau directorul pe care dorești să-l scanezi și selectează **Scanează cu Bitdefender**.

13.5.1. 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 directoarelor excluse de la scanare**. În fereastra care va apărea, poți administra fișierele și directoarele excluse de la scanare.
5. Pentru a adăuga excepții, urmează pașii de mai jos:
   a. Efectuează clic pe **Add**.
   b. Efectuează clic pe **RĂSFOIRE**, selectează fișierul sau directorul care dorești să fie exclus de la scanare și apoi dă clic pe **ADĂUGARE**. Ca o alternativă, poți 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. Efectuează clic pe **Add**.

13.5.2. 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
Acționează 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. Accesează 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. Efectuează 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**.

13.5.3. 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. Procedează astfel:
   - Pentru a șterge un element de pe listă, selectează-l și efectuează clic pe **Ștergere**.
   - Pentru a edita o înregistrare din tabel, dă dublu clic pe aceasta (sau selecteaz-o și efectuează 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**.

13.6. 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**, efectuează 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**.

Efectuează clic pe comutatoare pentru a activa sau dezactiva:

Scanează din nou carantina după actualizarea informațiilor despre amenințări
Menține 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.

Șterge conținutul mai vechi de 30 de zile
Fișirele 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, selectează-l și efectuează clic pe butonul **ȘTERGE**. Dacă doriți să restaurați un fișier aflat în carantină în locația sa originală, selectează-l și efectuează clic pe **RESTAUREAZĂ**.

14. 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 tău, 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.

14.1. 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.

14.2. 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.

14.3. 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.

14.4. Detecție exploit-uri

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.

15. 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 vizitezi această pagină web.

  Această pagină web poate avea conținut periculos. Vizitează 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, selecteaz-o și apoi clic pe **Șterge**.

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

15.1. Alertele Bitdefender sunt afișate în browser

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

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

Trebuie să decizi ce vei 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.

16. VULNERABILITĂȚI

Un pas important în protejarea calculatorului tău împotriva acțiunilor și aplicațiilor periculoase este de a menține actualizat sistemul de operare și aplicațiile pe care le utilizezi 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 tău și te 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 tău prin oricare dintre cele două metode de mai jos:

- Poți scana sistemul pentru a identifica vulnerabilitățile acestuia și le poți remedia pas cu pas folosind opțiunea **Scanare vulnerabilitate**.
- Prin intermediul monitorizării automate a vulnerabilităților, poți verifica și remedia vulnerabilitățile detectate, în fereastra Notificări.

Ar trebui să verifici și să remediezi vulnerabilitățile sistemului săptămânal sau o dată la două săptămâni.

16.1. 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**

  Poti vedea lista conturilor de utilizator Windows configurate pe calculatorul tău și nivelul de protecție asigurat de parola acestora.

  Poți să soliciți utilizatorului să schimbe parola la următoarea autentificare sau poți schimba ta 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.

16.2. 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. Poți vizualiza informații detaliate cu privire la vulnerabilitățile sistemului detectate. În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedează după cum urmează:
   - Dacă sunt disponibile actualizări Windows, efectuează clic pe **Instalare**.
   - Dacă actualizarea automată Windows este dezactivată, efectuează 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, efectuează clic pe **Modificare parolă** pentru a forța utilizatorul să modifice parola la următoarea conectare sau schimb-o chiar tu. Pentru a crea o parolă puternică, utilizează o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).
   - Dacă funcția de executare automată Windows este activată, efectuează 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 informări automate cu privire la vulnearibilitățile sistemului sau aplicației, menține opțiunea **Vulnerabilitate** activată.

3. Selectează vulnerabilitățile sistemului care dorești să fie verificate în mod regulat, cu ajutorul comutatoarelor corespunzătoare.

Actualizări Windows
Verifică dacă sistemul de operare Windows are instalate cele mai recente actualizări de securitate importante de la Microsoft.

Actualizări aplicații
Verifică dacă aplicațiile instalate pe sistemul tău sunt actualizate. Aplicațiile neactualizate pot fi exploatate de software-uri periculoase, expunându-ți 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 tău. Pentru a crea o parolă puternică, utilizează o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

Redare automată
Verifică 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 dezactivezi 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 dezactivezi monitorizarea pentru o anumită vulnerabilitate, posibilele probleme aferente nu vor mai fi înregistrate în fereastra Notificări.

16.3. 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

16.3.1. 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**.

16.3.2. 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**.

16.3.3. 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**.

16.3.4. 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 Antivirus Plus este configurat pentru a pune în aplicare automat următoarele setări:

- Funcția Advanced Threat Defense este activă
- 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.

16.3.5. Verifică 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 efectuezi clic pe link-ul **Vizualizare detalii** din dreptul fiecărei rețele, se afișează următoarele detalii:

- **Securizate** - aici poți 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.

17. 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 împrăștia 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:

- Criptează fișierele sensibile și personale și nu permite descriptarea 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, fotografii 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.

17.1. 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.

17.2. Protejează 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.

17.3. 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 aplicație 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**.

17.4. 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, înaite 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.

18. REMEDIERE RANSOMWARE

Funcția Remediere ransomware Bitdefender face un backup al fișierelor tale, precum documente, fotografii, 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.

18.1. 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.

18.2. 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**.

18.3. 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.

18.4. 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;

18.5. 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**.

19. 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 îți reamintești fiecare parolă setată pentru conturile tale 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 tale, 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

19.1. Creare bază de date nouă pentru Portofel

Portofelul Bitdefender este locația în care îți poți păstra datele personale. Pentru o experiență de navigare mai ușoară, este necesar să creezi 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 - introdu o denumire unică pentru baza de date Portofel.
   - Parola principală - introdu o parolă pentru Portofel.
   - Reintroducere parolă - reintrodu parola configurată
   - Indiciu - introdu un indiciu pentru a-ți aminti mai ușor parola.
5. Efectuează clic pe **CONTINUĂ**.
6. În acest punct, poți opta pentru stocarea informațiilor în cloud. Dacă selectezi da, datele bancare vor rămâne stocate local pe dispozitiv. Selectează opțiunea dorită, apoi efectuează clic pe **CONTINUĂ**.
7. Selectează browser-ul web din care dorești să importi datele.
8. Efectuează clic pe **FINALIZARE**.

19.2. 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. Efectuează clic pe **Deschide**.

6. Introdu o denumire pentru Portofelul tău 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**.

19.3. Exportă 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. Efectuează clic pe pictograma ⋮ din portofelul dorit și apoi selectează **Export**.
4. Caută locația bazei de date a portofelului tău și selecteaz-o (fișierul .db).
5. Efectuează clic pe **Save**.

Notă
Portofelul trebuie să fie deschis pentru ca opțiunea **Exportă** să fie disponibilă. Dacă portofelul pe care trebuie să-l exporți este blocat, efectuează clic pe **ACTIVEAZĂ PORTOFEL** și apoi introdu parola atribuită atunci când acesta a fost creat.

19.4. Sincronizează 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. Efectuează clic pe pictograma ⋮ din portofelul dorit și apoi selectează **Setări**.
4. Selectează opțiunea dorită din fereastra afișată și efectuează 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.

19.5. Gestionează 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. Introdu parola generală și efectuează clic pe **OK**.

Se afișează o nouă fereastră. Selectează 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, selectează categoria dorită din partea de sus, efectuează clic pe **+ Adăugare**, introdu informațiile în câmpurile corespunzătoare și efectuează clic pe butonul de Salvare.
- Pentru a edita un obiect din listă, selectează-l și efectuează clic pe butonul **Editează**.
- Pentru a șterge o înregistrare, selecteaz-o și efectuează clic pe butonul **Ștergere**.

19.6. 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.

19.7. 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. Selectează 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** - ți se va solicita să introduci parola master atunci când accesezi 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**
> Te sfătuim să reții parola master sau să o notezi și să o păstrezi într-un loc sigur. Dacă ai uitat parola, trebuie să reinstalezi programul sau să contactezi Bitdefender pentru asistență.

Îmbunătățește-ti 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. Selectează 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. Selectează secțiunea **Setări completare automată**.
4. Configurează 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** - ți se va solicita de fiecare dată să confirmi dacă dorești să adăugi datele tale 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 tale 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 dorești să efectuezi o plată online sau să te autentifici.

Administrarea informațiilor referitoare la Password Manager din browser

Poți administra cu ușurință modulul Password Manager direct din browser, pentru a avea toate datele importante la îndemână. Aplicația 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, deschide browser-ul, permite instalarea aplicației suplimentare și efectuează 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. Efectuează clic pe **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, poți adăuga date noi în Portofel.
- Generator parolă - enables îți permite să generezi parole aleatorii pe care le poți utiliza pentru conturile noi sau existente. Efectuează 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.

20. 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.

20.1. 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 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.

20.2. 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.

20.3. 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  .

21. 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 redirecționat prin intermediul unui server separat, ceea ce face ca dispozitivul tău să fie imposibil de identificat între multitudinea de alte dispozitive care folosesc serviciile noastre. Mai mult decât atât, în timp ce ești conectat la internet prin intermediul aplicației Bitdefender VPN, poți accesa conținut care în mod normal este restricționat în anumite zone.

Notă

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

21.1. 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.

21.2. 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**.

21.3. 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. 126).

Pentru conectare sau deconectare, pur și simplu efectuează click 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 ai 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 redirecționat către platforma noastră Support Center unde poți citi un articol util despre cum sa folosești Bitdefender VPN.
- **Despre** – sunt afișate informații despre versiunea instalată.

21.4. 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 Plus, 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 Antivirus Plus, 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.

22. 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 îți poți 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 poți fi niciodată suficient de precaut cu privire la securizarea tranzacțiilor online.

Bitdefender Safepay™ este, în primul rând, un browser protejat, un mediu proiectat pentru a ca tranzacțiile tale 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, consultă capitolul *„Protecția datelor de autentificare cu Password Manager”* (p. 114).

Bitdefender Safepay™ îți oferă următoarele funcții:

- Blochează accesul la calculatorul tău și orice încercări de a realiza capturi ale ecranului tău.
- 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 introduci de pe aceasta.
- Este complet idependentă de celelalte browsere ale tale.
- Include protecție pentru punctele wireless de acces la Internet încorporată pe care o poți utiliza în cazul conectării la rețele Wi-fi nesecurizate.
- Acceptă marcajele și îți permite să navighezi pe site-urile tale preferate de tranzacții bancare/cumpărături.
- Nu se limitează la tranzacții bancare și cumpărături online. Orice site poate fi deschis în Bitdefender Safepay™.

22.1. Utilizarea Bitdefender Safepay™

În mod implicit, Bitdefender detectează dacă navighezi către un site de tranzacții online sau de cumpărături online în orice browser de pe calculatorul tău și îți solicită să îl lansezi în Bitdefender Safepay™.

Pentru a accesa interfața Bitdefender Safepay™ principală, folosește 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. Efectuează clic pe **Start** și mergi la **Toate programele**.
    2. Efectuează clic pe **Bitdefender**.
    3. Efectuează clic pe **Bitdefender Safepay™**.
  - În **Windows 8 și Windows 8.1**:

    Localizează Bitdefender Safepay™ din ecranul de Start Windows (de exemplu, poți tasta "Bitdefender Safepay™" direct pe ecranul de Start) și apoi efectuează clic pe pictograma.
  - În **Windows 10**:

    Introdu "Bitdefender Safepay™" în caseta de căutare din bara de sarcini și efectuează clic pe pictogramă.

Dacă ești obișnuit cu browserele Internet, nu vei avea probleme în utilizarea Bitdefender Safepay™ - arată și se comportă ca un browser obișnuit:

- introdu URL-urile pe care dorești să le accesezi în bara de adrese.
- adaugă secțiuni pentru a vizita mai multe site-uri în fereastra Bitdefender Safepay™ făcând clic pe  .
- revino la navigarea anterioară, mergi către o altă pagină și reîmprospătează pagini folosind  .

- accesează setările Bitdefender Safepay™ făcând clic pe ••• și selectând **Setări**.
- protejează-ți parolele cu Password Manager dând clic pe .
- administrează marcajele făcând clic pe ☆ de lângă bara de adrese.
- activează tastatura virtuală făcând clic pe .
- mărește sau micșorează dimensiunea browser-ului apăsând simultan tastele **Ctrl** și **+/-** de pe tastatura numerica.
- vizualizează informațiile despre produsul tău 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, apasă tastele **Alt+Tab** sau efectuează clic pe opțiunea **Comută pe Desktop** din colțul din stânga sus al ferestrei.

22.2. Configurarea setărilor

Efectuează clic pe ••• și alege **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 automat cu Bitdefender Safepay™ a unui site web din listă, clic pe × din dreptul înregistrării dorite din coloana **Ștergere**.

Blocare pop-up-uri
Poți opta pentru blocarea pop-up-urilor făcând clic pe comutatorul corespunzător.

De asemenea, poți crea o listă a site-urilor pe care permiți afișarea pop-up-urilor. Este recomandat ca lista să conțină doar site-uri web în care ai 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
Activează această opțiune dacă dorești să confirmi înainte ca procesul de tipărire să înceapă.

22.3. Administrarea marcajelor

Dacă ai 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, poți adăuga marchează în Bitdefender Safepay™ pentru a putea lansa cu ușurință site-urile Internet în viitor.

Urmează pașii de mai jos pentru a adăuga un URL la marcajele Bitdefender Safepay™:

1. Efectuează 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. Efectuează clic pe butonul **+** pentru a adăuga un marcaj nou.
3. Introduceți URL-ul și titlul marcajului și apoi faceți clic pe **CREEAZĂ**. Efectuează clic pe opțiunea **Deschide automat în Safepay** dacă dorești ca pagina marcată să se deschidă cu Bitdefender Safepay™ de fiecare dată când o accesezi. URL-ul este și el adăugat la lista Domeniilor de pe pagina setări.

22.4. 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**.

22.5. 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**.

23. DATA PROTECTION

23.1. Ștergerea permanentă a fișierelor

Atunci când ștergi 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 îți permite să ștergi definitiv date prin eliminarea fizică a acestora de pe hard disk.

Poți șterge definitiv și rapid fișiere și directoare din computerul tău cu ajutorul meniul contextual Windows urmând pașii de mai jos:

1. Efectuează clic dreapta pe un fișier sau director pe care dorești să-l ștergi definitiv.
2. Selectează **Bitdefender** > **Ștergere definitivă fișiere** din meniul contextual afișat.
3. Efectuează clic pe **ȘTERGE DEFINITIV** și apoi confirmă că dorești să continui procesul.

   Așteaptă ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.
4. Sunt afișate rezultatele. Efectuează clic pe **Finalizare** pentru a părăsi asistentul.

Ca alternativă, poți 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. Urmează pașii asistentului de ștergere definitivă a fișierelor:
   a. Efectuează clic pe butonul **ADAUGĂ FIȘIERE** pentru a adăuga fișierele sau directoarele pe care dorești să le ștergi definitiv.

      Ca alternativă, glisează aceste fișiere sau foldere în această fereastră.
   b. Efectuează clic pe **ȘTERGE DEFINITIV** și apoi confirmă că dorești să continui procesul.

      Așteaptă ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.

c. **Sumar**

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

24. 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 introduci un CD în unitatea optică.

Din nefericire, această funcție poate fi utilizată și de amenințări pentru lansarea automată și infiltrarea în calculatorul tău 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, poți împiedica orice unități flash formatate 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. Conectează unitatea flash la calculatorul tău.
2. Navighează în calculator pentru a localiza dispozitivul amovibil de stocare și efectuează clic dreapta pe această pictogramă.
3. În meniul contextual, evidențiază **Bitdefender** și selectează **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 tău de pe dispozitive USB neimunizate, dezactivează funcția de rulare automată a mediilor. Pentru mai multe informații, consultă capitolul *„Cu ajutorul monitorizării automate a vulnerabilităților”* (p. 102).

OPTIMIZARE DE SISTEM

25. 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, poți 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 decizi să nu utilizezi **Profiluri**, se activează un profil implicit numit **Standard**, care nu îți optimizează sistemul.

În funcție de activitatea ta, 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 ta, se aplică următoarele setări ale sistemului la activarea unui profil Lucru, Film sau Joc:

- Actualizările automate Windows sunt amânate.
- Alertele 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 Antivirus Plus este configurat pentru a pune în aplicare automat următoarele setări:

- Funcția Advanced Threat Defense este activă
- Următoarele setări din Online Threat Prevention sunt activate:
  - Scanare web criptată
  - Protecție împotriva fraudelor
  - Protecție împotriva tentativelor de phishing

25.1. 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, îți pot afecta performanțele sistemului. Profilul de serviciu a fost proiectat pentru a te ajuta să îți îmbunătățești 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. Selectează secțiunea **Profiluri**.
3. Efectuează clic pe butonul **CONFIGUREAZĂ** din zona Profil Lucru.
4. Selectează ajustările sistemului care dorești 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. Selectează secțiunea **Profiluri**.
3. Efectuează 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. Mergi la locația unde se găsește fișierul executabil, selectează-l și efectuează clic pe **OK** pentru a-l adăuga în listă.

25.2. 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 te poți 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. Selectează secțiunea **Profiluri**.
3. Efectuează clic pe butonul **CONFIGUREAZĂ** din zona Profil film.
4. Selectează ajustările sistemului care dorești 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 lansezi o anumită aplicație pentru redarea video clipurilor, poți 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. Selectează secțiunea **Profiluri**.
3. Efectuează 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. Mergi la locația unde se găsește fișierul executabil, selectează-l și efectuează clic pe **OK** pentru a-l adăuga în listă.

25.3. 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 tu să te poți 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. Selectează secțiunea **Profiluri**.
3. Efectuează clic pe butonul **CONFIGUREAZĂ** din zona Profil Joc.

4. Selectează ajustările sistemului care dorești 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 ai lansat un anumit joc sau o aplicație, ai posibilitatea să adaugi 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. Selectează secțiunea **Profiluri**.
3. Efectuează 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. Mergi la locația unde se găsește fișierul executabil al jocului, selectează-l și efectuează clic pe **OK** pentru a-l adăuga în listă.

25.4. Profil Wi-Fi public

Trimiterea de e-mailuri, introducerea unor date de autentificare sensibile sau cumpărăturile online în timp ce ești conectat la rețele wireless nesigure pot expune la riscuri datele tale personale. Profilul Wi-Fi public ajustează setările produsului pentru a-ți 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. Selectează secțiunea **Profiluri**.
3. Efectuează clic pe butonul **CONFIGUREAZĂ** din zona Profil Wi-Fi public.
4. Permite **să ajusteze setările produsului pentru a optimiza protecția atunci când ești conectat la o rețea Wi-Fi publică nesigură căsuța** bifată.
5. Efectuează clic pe **Save**.

25.5. Profil mod baterie

Modul Baterie se adresează utilizatorilor de laptop si 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 tine.

Configurarea Modului Baterie

Pentru a configura profilul Mod baterie:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței Bitdefender.
2. Selectează secțiunea **Profiluri**.
3. Fă clic pe butonul **CONFIGUREAZĂ** din zona Mod Baterie.
4. Selectează ajustările sistemului care vor fi aplicate, prin bifarea opțiunilor de mai jos:
   - Optimizează setările de produs pentru Profilul Baterie.
   - Amână programele de fundal și activitățile de întreținere.
   - Amânare actualizare Windows automată.
   - Ajustează configurările planului de energie pentru Modul Baterie.
   - Dezactivează 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.

25.6. Optimizare în timp real

Optimizarea în timp real Bitdefender este un plugin care îmbunătățește silențios performanțele sistemului tău, în fundal, asigurându-se că nu ești întrerupt când te afli 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 tale.

Pentru a activa sau dezactiva optimizarea în timp real:

1. Efectuează clic pe **Setări** din meniul de navigare al interfeței Bitdefender.
2. Selectează secțiunea **Profiluri**.
3. Derulează în jos până când observi opțiunea de optimizare în timp real și apoi folosește butonul corespunzător pentru a o activa sau dezactiva.

REMEDIEREA PROBLEMELOR

26. SOLUȚIONAREA PROBLEMELOR FRECVENTE

Acest capitol prezintă anumite probleme cu care te poți confrunta la utilizarea Bitdefender și îți oferă soluții posibile la aceste probleme. Majoritatea acestor probleme pot fi soluționate prin configurarea adecvată a setărilor produsului.

- *„Sistemul meu funcționează lent"* (p. 145)
- *„Nu începe scanarea"* (p. 146)
- *„Nu mai pot utiliza o aplicație"* (p. 149)
- *„Ce trebuie făcut atunci când Bitdefender blochează un site web, un domeniu, o adresă IP sau o aplicație online care sunt sigure"* (p. 150)
- *„Ce trebuie să faci dacă Bitdefender detectează ca ransomware o aplicație sigură"* (p. 151)
- *„Cum să actualizezi Bitdefender în cazul unei conexiuni lente la internet"* (p. 151)
- *„Serviciile Bitdefender nu răspund"* (p. 152)
- *„Funcția Completare automată din Portofel nu funcționează"* (p. 153)
- *„Nu s-a reușit dezinstalarea Bitdefender"* (p. 154)
- *„Sistemul meu nu pornește după ce am instalat Bitdefender"* (p. 155)

Dacă problema ta nu este prezentată aici sau dacă soluțiile oferite nu îți sunt de ajutor, poți contacta echipa de suport tehnic a Bitdefender folosind informațiile din capitolul *„Solicitarea ajutorului"* (p. 171).

26.1. 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 observi 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 îndepărtezi orice alte soluții de securitate pe care le-ai utilizat înainte de a iniția instalarea Bitdefender.

Pentru mai multe informații, consultă capitolul *„Cum elimin celelalte soluții de securitate?"* (p. 68).

- **Cerințele de sistem pentru rularea Bitdefender nu sunt îndeplinite.**

  Dacă dispozitivul tău nu îndeplinește cerințele de sistem, computerul va fi fi afectat de încetiniri, mai ales atunci când mai multe aplicații rulează în același timp. Pentru mai multe informații, consultă capitolul *„Cerințe de sistem"* (p. 3).

- **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 folosești un program, dezinstalează-l. Acest lucru este valabil și pentru orice alte programe software sau aplicații de evaluare pe care omiți să le ștergi.

  Important
  Dacă suspectezi că un program sau o aplicație este o parte esențială a sistemului tău de operare, nu le șterge, ci contactează Serviciul de asistență clienți al Bitdefender.

- **Sistemul tău poate fi infectat**.

  Amenințările pot afecta, de asemenea, viteza sistemului tău , precum și comportamentul general al acestuia. Programele periculoase de tip spyware, malware, troieni și adware afectează performanța calculatorului tău. Scanează sistemul periodic, cel puțin o dată pe săptămână. Este recomandat să utilizezi funcția de Scanare sistem a Bitdefender deoarece aceasta scanează toate tipurile de amenințări care pun în pericol securitatea sistemului tău.

  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. Urmează pașii asistentului.

26.2. 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, reinstalează Bitdefender:

  - În **Windows 7**:
    1. Efectuează clic pe **Start**, mergi la **Control Panel** și efectuează clic pe **Programe și Caracteristici**.
    2. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
    3. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.
    4. Așteaptă finalizarea procesului de reinstalare și apoi repornește sistemul.
  - În **Windows 8 și Windows 8.1**:
    1. Din ecranul de Start al Windows, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control” direct în ecranul de Start) și efectuează click pe pictograma acestuia.
    2. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
    3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
    4. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.
    5. Așteaptă finalizarea procesului de reinstalare și apoi repornește sistemul.
  - În **Windows 10**:
    1. Efectuează clic pe **Start**, apoi pe Setări.
    2. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează**Aplicații instalate**.
    3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
    4. Efectuează clic din nou pe **Dezinstalare** pentru a confirma selecția.
    5. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.
    6. Așteaptă finalizarea procesului de reinstalare și apoi repornește 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 tău**
.

  În acest caz:

  1. Dezinstalează cealaltă soluție de securitate. Pentru mai multe informații, consultă capitolul *„Cum elimin celelalte soluții de securitate?"* (p. 68).
  2. Reinstalează Bitdefender:
     - În **Windows 7**:
       a. Efectuează clic pe **Start**, mergi la **Control Panel** și efectuează clic pe **Programe și Caracteristici**.
       b. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
       c. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.
       d. Așteaptă finalizarea procesului de reinstalare și apoi repornește sistemul.
     - În **Windows 8 și Windows 8.1**:
       a. Din ecranul de Start al Windows, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control" direct în ecranul de Start) și efectuează click pe pictograma acestuia.
       b. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
       c. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
       d. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.
       e. Așteaptă finalizarea procesului de reinstalare și apoi repornește sistemul.
     - În **Windows 10**:
       a. Efectuează clic pe **Start**, apoi pe Setări.
       b. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează**Aplicații instalate**.

c. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.

d. Efectuează clic din nou pe **Dezinstalare** pentru a confirma selecția.

e. Efectuează clic pe **REINSTALEAZĂ** în fereastra afișată.

f. Așteaptă finalizarea procesului de reinstalare și apoi repornește 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 ți-au fost de folos, te rugăm să contactezi Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 171).

26.3. Nu mai pot utiliza o aplicație

Această problemă apare când încerci să utilizezi un program care a funcționat normal înainte de instalarea Bitdefender.

După instalarea Bitdefender ar putea apărea următoarele situații:

- Este posibil să primești 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 încerci să-l utilizezi.

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 tău 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, poți 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 ți-au fost de folos, te rugăm să contactezi Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 171).

26.4. 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 ți-au fost de folos, te rugăm să contactezi Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 171).

26.5. 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.

26.6. Cum să actualizezi Bitdefender în cazul unei conexiuni lente la internet

Dacă dispui de o conexiune lentă la internet (cum ar fi cea de tip dial-up), în timpul procesului de actualizare pot apărea erori.

Pentru a-ți 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. Selectează 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.

26.7. Serviciile Bitdefender nu răspund

Acest articol te ajută să remediezi problema **Serviciile Bitdefender nu răspund**. Această problemă poate apărea în următoarele situații:

- Pictograma Bitdefender din bara de sistem este afișată în culoarea gri și vei 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 tău, în același timp cu Bitdefender.

Pentru a remedia această problemă, încearcă următoarele soluții:

1. Așteaptă câteva momente pentru a vedea dacă apar schimbări. Eroarea poate fi temporară.
2. Repornește calculatorul și așteaptă câteva momente până când se încarcă Bitdefender. Deschide Bitdefender pentru a vedea dacă eroarea persistă. De obicei, repornirea calculatorului rezolvă problema.
3. Îți recomandăm să dezinstalezi toate celelalte soluții de securitate și apoi să reinstalezi Bitdefender. Îți recomandăm să dezinstalezi toate celelalte soluții de securitate și apoi să reinstalezi Bitdefender.

   Pentru mai multe informații, consultă capitolul *„Cum elimin celelalte soluții de securitate?”* (p. 68).

Dacă eroarea persistă, te rugăm să contactezi reprezentanții serviciului de asistență, după cum este specificat în secțiunea *„Solicitarea ajutorului”* (p. 171).

26.8. Funcția Completare automată din Portofel nu funcționează

Ai 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 tău.

Pentru a remedia această problemă, urmează pașii de mai jos:

- În **Internet Explorer:**
  1. Deschide Internet Explorer.
  2. Efectuează clic pe Instrumente.
  3. Efectuează clic pe Gestionare programe de completare.
  4. Efectuează clic pe Bare de instrumente și extensii.
  5. Poziționează cursorul pe **Portofel Bitdefender** și efectuează clic pe **Activare**.
- În **Mozilla Firefox:**
  1. Deschide Mozilla Firefox.
  2. Efectuează clic pe Instrumente.
  3. Efectuează clic pe Programe de completare.
  4. Efectuează clic pe Extensii.
  5. Poziționează cursorul pe **Portofel Bitdefender** și efectuează clic pe **Activare**.
- În **Google Chrome:**
  1. Deschide Google Chrome.
  2. Mergi la pictograma Meniului.
  3. Efectuează clic pe Mai multe instrumente.
  4. Efectuează clic pe Extensii.
  5. Poziționează cursorul pe **Portofel Bitdefender** și efectuează clic pe **Activare**.

Notă
Programul de completare se va activa după repornirea browserului.

Apoi verifică dacă funcția de completare automată din Portofel funcționează pentru conturile tale online.

Dacă aceste informații nu ți-au fost de folos, te rugăm să contactezi Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului"* (p. 171).

26.9. Nu s-a reușit dezinstalarea Bitdefender

Dacă dorești să ștergi produsul Bitdefender și observi că procesul este suspendat sau sistemul se blochează, efectuează clic pe **Anulare** pentru a abandona acțiunea. Dacă anularea nu este posibilă, repornește sistemul.

Dacă dezinstalarea eșuează, în sistemul tău pot rămâne unele chei de regiștri și fișiere Bitdefender. Aceste rămășite 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. Efectuează clic pe **Start**, mergi la **Control Panel** și efectuează clic pe **Programe și Caracteristici**.
  2. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
  3. Efectuează clic pe **ȘTERGE** în fereastra care se deschide.
  4. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.
- În **Windows 8 și Windows 8.1**:
  1. Din ecranul de Start al Windows, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control" direct în ecranul de Start) și efectuează click pe pictograma acestuia.
  2. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
  3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
  4. Efectuează clic pe **ȘTERGE** în fereastra care se deschide.

5. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

- În **Windows 10**:

1. Efectuează clic pe **Start**, apoi pe Setări.
2. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează**Aplicații instalate**.
3. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.
4. Efectuează clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Efectuează clic pe **ȘTERGE** în fereastra care se deschide.
6. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

26.10. Sistemul meu nu pornește după ce am instalat Bitdefender

Dacă se întâmplă ca, după ce tocmai ai instalat Bitdefender,să nu poți 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 acționezi pentru fiecare situație:

- **Ai avut Bitdefender instalat anterior și acesta nu a fost dezinstalat corespunzător.**

  Pentru a remedia această problemă:

1. Repornește sistemul în Safe Mode. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot să repornesc sistemul în Safe Mode?"* (p. 69).
2. Șterge Bitdefender din sistemul tău:
   - În **Windows 7**:
     a. Efectuează clic pe **Start**, mergi la **Control Panel** și efectuează clic pe **Programe și Caracteristici**.
     b. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.

c. Efectuează clic pe **ȘTERGE** în fereastra care se deschide.

d. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

e. Repornește sistemul în modul normal.

- În **Windows 8 și Windows 8.1**:

  a. Din ecranul de Start al Windows, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control" direct în ecranul de Start) și efectuează click pe pictograma acestuia.

  b. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.

  c. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.

  d. Efectuează clic pe **ȘTERGE** în fereastra care se deschide.

  e. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

  f. Repornește sistemul în modul normal.

- În **Windows 10**:

  a. Efectuează clic pe **Start**, apoi pe Setări.

  b. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează**Aplicații instalate**.

  c. Găsește **Bitdefender Antivirus Plus** și selectează **Dezinstalare**.

  d. Efectuează clic din nou pe **Dezinstalare** pentru a confirma selecția.

  e. Efectuează clic pe **ȘTERGE** în fereastra care se deschide.

  f. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

  g. Repornește sistemul în modul normal.

3. Reinstalează produsul tău Bitdefender.

- **Ai avut instalată o altă soluție de securitate înainte, iar aceasta nu a fost dezinstalată corespunzător.**

  Pentru a remedia această problemă:

1. Repornește sistemul în Safe Mode. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot să repornesc sistemul în Safe Mode?"* (p. 69).
2. Șterge cealaltă soluție de securitate din sistem:
   - În **Windows 7**:
     a. Efectuează clic pe **Start**, mergi la **Control Panel** și efectuează clic pe **Programe și Caracteristici**.
     b. Găsește numele programului pe care dorești să-l dezinstalezi și selectează **Ștergere**.
     c. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.
   - În **Windows 8 și Windows 8.1**:
     a. Din ecranul de Start al Windows, localizează **Panoul de control** (de exemplu, poți începe să tastezi „Panou de control" direct în ecranul de Start) și efectuează click pe pictograma acestuia.
     b. Efectuează clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
     c. Găsește numele programului pe care dorești să-l dezinstalezi și selectează **Ștergere**.
     d. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.
   - În **Windows 10**:
     a. Efectuează clic pe **Start**, apoi pe Setări.
     b. Efectuează clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează**Aplicații instalate**.
     c. Găsește numele programului pe care dorești să-l dezinstalezi și selectează **Dezinstalare**.
     d. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.

   Pentru a dezinstala celălalt software în mod corect, mergi pe site-ul web al producătorului și lansează instrumentul de dezinstalare sau contactează direct producătorul, solicitând instrucțiunile de dezinstalare.
3. Repornește sistemul în modul normal și reinstalează Bitdefender.

Situația nu s-a rezolvat deși ai urmat toți pașii de mai sus.

Pentru a remedia această problemă:

1. Repornește sistemul în Safe Mode. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot să repornesc sistemul în Safe Mode?”* (p. 69).
2. Cu ajutorul funcției System Restore din Windows poți restabili computerul la o dată anterioară instalării produsului Bitdefender.
3. Repornește sistemul în modul normal și contactează reprezentanții serviciului de asistență, după cum este specificat în secțiunea *„Solicitarea ajutorului”* (p. 171).

27. ELIMINAREA AMENINȚĂRILOR DIN SISTEMUL TĂU

Amenințările îți 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 tău. În astfel de cazuri, este necesară intervenția ta.

- *„Bitdefender Modul de recuperare (Mediul de recuperare în Windows 10)"* (p. 159)
- *„Ce trebuie să faci atunci când Bitdefender detectează amenințări pe computerul tău?"* (p. 163)
- *„Cum elimin o amenințare dintr-o arhivă?"* (p. 165)
- *„Cum elimin o amenințare dintr-o arhivă de e-mail?"* (p. 166)
- *„Ce trebuie să fac dacă suspectez că un fișier este periculos?"* (p. 167)
- *„Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?"* (p. 167)
- *„Ce reprezintă elementele omise din jurnalul de scanare?"* (p. 168)
- *„Ce reprezintă fișierele supracomprimate din jurnalul de scanare?"* (p. 168)
- *„De ce Bitdefender a șters în mod automat un fișier infectat?"* (p. 168)

Dacă problema ta nu este prezentată aici sau dacă soluțiile oferite nu îți sunt de ajutor, poți contacta echipa de suport tehnic a Bitdefender folosind informațiile din capitolul *„Solicitarea ajutorului"* (p. 171).

27.1. Bitdefender Modul de recuperare (Mediul de recuperare în Windows 10)

Mediu de recuperare este o caracteristică a Bitdefender care îți permite să scanezi și să dezinfectezi toate partițiile hard discului din/ de pe sistemul de operare.

Odată ce Bitdefender Antivirus Plus este instalat pe on **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 poți 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 Modului de recuperare pe acest sistem de operare.

Descărcarea imaginii Modului 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 Modului de recuperare Bitdefender de pe serverele Bitdefender. Calculatorul va fi repornit imediat ce se finalizează descărcarea,

   Se va afișa un meniu prin care ți se va solicita să selectezi sistemul de operare. În această fază, poți alege să pornești 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 Modului de recuperare pe acest sistem de operare.

Pornirea sistemului tău în Modul de recuperare în Windows 7, Windows 8 și Windows 8.1

Poți 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 îți va solicita să selectezi un sistem de operare. Selectează **Mediul de recuperare Bitdefender** pentru a porni într-un mediu Bitdefender din care poți elibera partiția Windows.
5. În cazul în care ți se solicită, apasă **Enter** și ajustează rezoluția ecranului la valoarea cea mai apropiată de cea pe care o folosești de obicei. Apoi apasă din nou pe **Enter**.

   Mediul de recuperare Bitdefender se încarcă în câteva momente.

Pornește computerul direct în Mediul de recuperare

În cazul în care nu mai pornește Windows, poți 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 Modului de recuperare după cum este descris în „Descărcarea imaginii Modului de recuperare Bitdefender” (p. 160).

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. Accesează Mediul de recuperare, conform descrierii din „Pornirea sistemului tău în Modul de recuperare în Windows 7, Windows 8 și Windows 8.1” (p. 160).
  2. Va apărea logo-ul Bitdefender și motoarele soluției de securitate vor începe să fie copiate.
  3. Va fi afișată o fereastră de întâmpinare. Efectuează clic pe **Continue**.
  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. Efectuează clic pe **Scanează acum**, selectează locația de scanat din fereastra care apare și efectuează clic pe **Deschidere** pentru a începe scanarea.

     Este recomandat scanarea întregii partiții Windows.

     Notă
     Atunci când lucrezi în Mediul de recuperare, vei 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. Așteaptă finalizarea procesului de scanare. Dacă este detectată o amenințare, urmează instrucțiunile pentru îndepărtarea acesteia.
8. Pentru a ieși din Mediul de recuperare, efectuează clic dreapta în secțiunea liberă de pe desktop, selectează **Ieșire** din meniul care apare și apoi selectează dacă dorești să repornești sau să închizi computerul.

- În **Windows 10**:

1. Accesează Mediul de recuperare, conform descrierii din „Pornirea sistemului în Mediul de recuperare în Windows 10” (p. 162).
2. Procesul de scanare Bitdefender începe automat imediat ce sistemul este încărcat în Mediul de recuperare.
3. Așteaptă 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.

27.2. 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:

- Ți-ai 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, selectează acțiunea dorită pentru elementele infectate (dezinfectare, ștergere, mutare în carantină).

Avertisment
În cazul în care consideri că fișierul face parte din sistemul de operare Windows sau că nu este un fișier infectat, nu urma acești pași și contactează 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 ștergi fișierul/fișierele manual:

Prima metodă poate fi utilizată în modul normal:

1. Dezactivează 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. Afișează elementele ascunse din Windows. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot afișa elementele ascunse din Windows?"* (p. 67).
3. Mergi la locația unde se găsește fișierul infectat (verifică jurnalul de scanare) și șterge-l.
4. Activează protecția antivirus în timp real a Bitdefender.

În cazul în care prima metodă nu a reușit să elimine infecția:

1. Repornește sistemul în Safe Mode. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot să repornesc sistemul în Safe Mode?"* (p. 69).
2. Afișează elementele ascunse din Windows. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum pot afișa elementele ascunse din Windows?"* (p. 67).
3. Mergi la locația unde se găsește fișierul infectat (verifică jurnalul de scanare) și șterge-l.
4. Repornește sistemul în mod normal.

Dacă aceste informații nu ți-au fost de folos, te rugăm să contactezi Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului"* (p. 171).

27.3. 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. Dezactivează 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. Accesează locația arhivei și dezarhiveaz-o utilizând o aplicație de arhivare, cum ar fi WinZip.
4. Identifica fișierul infectat și șterge-l.
5. Șterge arhiva inițială pentru a te asigura că fișierul infectat este eliminat în totalitate.
6. Recomprimă fișierele într-o nouă arhivă utilizând o aplicație de arhivare, cum ar fi WinZip.
7. Activează protecția antivirus în timp real a Bitdefender și execută o scanare a sistemului pentru a te 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 ți-au fost de folos, te rugăm să contactezi Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 171).

27.4. 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. Scanează baza de date de e-mail folosind Bitdefender.
2. Dezactivează 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. Deschide raportul de scanare și utilizeaza informațiile de identificare (Subiect, De la, Către) aferente mesajelor infectate pentru a le localiza în clientul de e-mail.
4. Șterge mesajele infectate. Majoritatea clienților de e-mail mută mesajul șters într-un director de recuperare, de unde acesta poate fi recuperat. Trebuie să te asiguri că mesajul este șters și din acest director de recuperare.
5. Arhivează directorul în care se află mesajul infectat.
   - În Microsoft Outlook 2007: În meniul File, efectuează clic pe Data File Management. Selectează fișierele din directoarele personale (.pst) pe care intenționezi să le compactezi și efectuează clic pe Settings. Efectuează clic pe Compactare acum.

- În Microsoft Outlook 2010 / 2013 / 2016: Din meniul Fișier, selectează Detalii și apoi Setări cont (Adăugare sau eliminare conturi sau modificare setări de conectare existente) Apoi efectuează clic pe Fișier de date, selectează fișierele din directoarele personale (.pst) pe care intenționezi să le compactezi și efectuează clic pe Setări. Efectuează clic pe Compactare acum.

6. Activează protecția antivirus în timp real a Bitdefender.

Dacă aceste informații nu ți-au fost de folos, te rugăm să contactezi Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 171).

27.5. Ce trebuie să fac dacă suspectez că un fișier este periculos?

Există posibilitatea să consideri că un anumit fișier din sistemul tău este periculos chiar dacă Bitdefender nu l-a detectat.

Pentru a te asigura că sistemul tău este protejat:

1. Execută o **scanare a sistemului** cu Bitdefender. Pentru a afla cum poți face acest lucru, consultă secțiunea *„Cum îmi scanez sistemul?”* (p. 53).
2. Dacă procesul de scanare nu a detectat nimic, dar încă ai dubii cu privire la fișier, contactează reprezentanții serviciul de asistență pentru ajutor.

   Pentru a afla cum poți face acest lucru, consultă secțiunea *„Solicitarea ajutorului”* (p. 171).

27.6. 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-ti proteja calculatorul. Dacă dorești să scanezi acele fișiere folosind Bitdefender, trebuie să contactezi producătorul produsului pentru a obține mai multe detalii despre respectivele fișiere.

Noi îți recomandăm să ignori acele fișiere deoarece acestea nu reprezintă o amenințare pentru sistemul tău.

27.7. Ce reprezintă elementele omise din jurnalul de scanare?

Toate fișierele care apar ca fiind omise în raportul de scanare nu conțin niciun fel de viruși.

Pentru performanțe sporite, Bitdefender nu scanează fișiere care nu au fost modificate de la ultima scanare.

27.8. 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.

27.9. 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, 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.

Acesta este cazul fișierelor de instalare care sunt descărcate de pe site-uri web nesigure. Dacă te afli într-o astfel de situație, descarcă fișierul de instalare de pe site-ul web al producătorului sau de pe un alt site web sigur.

CONTACTEAZĂ-NE

28. SOLICITAREA AJUTORULUI

Bitdefender oferă clienților săi un nivel neegalat în ceea ce privește rapiditatea și acuratețea suportului tehnic. Dacă te confrunți cu o problemă sau ai o întrebare referitoare la produsul Bitdefender deținut, poți utiliza mai multe resurse online pentru a găsi o soluție sau un răspuns. În același timp, poți contacta echipa de Servicii clienți a Bitdefender. Reprezentanții noștri pentru suport tehnic îți vor răspunde la întrebări la timp și îți vor oferi asistența de care ai nevoie.

Secțiunea *„Soluționarea problemelor frecvente"* (p. 145) îți oferă informațiile necesare referitoare la cele mai frecvent întâlnite probleme atunci când utilizezi acest produs.

Dacă nu găsești un răspuns la întrebarea ta printre resursele puse la dispoziție, ne poți contacta direct:

- „Contactează-ne direct din Bitdefender Antivirus Plus" (p. 171)
- „Contactează-ne prin intermediul Centrului nostru de asistență online" (p. 172)

Contactează-ne direct din Bitdefender Antivirus Plus

Dacă dispui de o conexiune la internet funcțională, poți contacta Bitdefender pentru asistență direct din interfața produsului tău.

Urmează acești pași:

1. Dă clic pe **Asistență** din meniul de navigare al interfeței Bitdefender.
2. Ai la dispoziție următoarele opțiuni:
   - **GHIDUL UTILIZATORULUI**

     Accesează baza noastră de date și caută 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. Completează 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. Introdu 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 ta.

c. Efectuează clic pe **ÎNCHIDE** pentru a părăsi asistentul. Vei fi contactat cât mai curând posibil de către unul dintre reprezentanții noștri.

Contactează-ne prin intermediul Centrului nostru de asistență online

Dacă nu poți accesa informațiile necesare utilizând produsul Bitdefender, consultă Centrul nostru online de asistență:

1. Mergi la https://www.bitdefender.ro/support/consumer.html.

   Centrul de asistență Bitdefender include numeroase articole care cuprind soluții la problemele asociate Bitdefender.

2. Folosește bara de căutare din partea de sus a ferestrei pentru a găsi articole care ți-ar putea oferi o soluție la problema ta. Pentru a efectua o căutare, introdu un cuvânt în bara de căutare și efectuează clic pe **Căutare**.

3. Citește articolele sau documentele relevante și încearcă soluțiile propuse.

4. Dacă soluția propusă nu te ajută să rezolvi problema, mergi la

   https://www.bitdefender.ro/support/contact-us.htmlși ia legătura cu reprezentanții serviciului de asistență.

29. RESURSE ONLINE

Sunt disponibile mai multe resurse online pentru a te 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, poți folosi motorul de căutare preferat pentru a afla informații suplimentare privind securitatea calculatoarelor, produsele și compania Bitdefender.

29.1. 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.

29.2. 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 tău Bitdefender nu funcționează bine, nu poate înlătura anumite amenințări de pe calculator sau dacă ai întrebări referitoare la modul de funcționare, postează problema sau întrebarea pe forum.

Tehnicienii suport ai Bitdefender monitorizează forumul pentru a verifica noile postări cu scopul de a te ajuta. De asemenea, poți 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. Efectuează clic pe linkul **Home & Home Office Protection** pentru a accesa secțiunea dedicată produselor pentru consumatori individuali.

29.3. Portalul HOTforSecurity

HOTforSecurity reprezintă o sursă bogată de informații referitoare la securitatea calculatoarelor. Aici poți afla informații despre diverse pericole la care se expune computerul tău atunci când este conectat la internet (malware, phishing, spam, infracțiuni cibernetice).

Se postează în mod regulat noi articole pentru a te ține la curent cu cele mai recente pericole descoperite, tendințele actuale din domeniul securității și alte informații din domeniul securității calculatoarelor.

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

30. 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 ezita să ne contactezi indiferent ce problemă sau întrebare ai avea.

30.1. 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
Pagină web:https://www.bitdefender.ro

30.2. 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 ta:

1. Mergi la https://www.bitdefender.ro/partners/partner-locator.html.
2. Selectează țara și orașul folosind opțiunile corespunzătoare.
3. În cazul în care nu găsești un distribuitor Bitdefender în țara ta, nu ezita să ne contactezi 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.

30.3. 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
Pagină web: https://www.bitdefender.es

România

BITDEFENDER SRL
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 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
Pagină 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
Pagină 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 tău o altă versiune mai veche; dacă nu, nu poți 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 ta și rulează independent de voința ta. 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. Aceeași 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 responsabilii 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. Efectuează 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 comunicare între două computere.

Client de mail

Un client de mail este o aplicație care îți permite să trimiți și să recepționezi 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-ți 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 tale. Această facilitate are avantaje și dezavantaje pentru mulți deoarece, pe de o parte, este eficientă și pertinentă din moment ce vizualizezi doar acele anunțuri despre subiecte care te 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.

Exploit-uri
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 acționare 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.

Keyloggerele nu au o natură malițioasă. 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 euristică

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-euristică

Această metodă de scanare se bazează pe baze de date cu informații specifice despre amenințări. Avantajul metodelor ne-euristice 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, neitruzivă, proiectată pentru minimizarea impactului soluției tale de securitate asupra performanțelor. Prin monitorizarea activității calculatorului tău în fundal, creează șabloane care ajută la optimizarea proceselor de pornire și 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 îți dau posibilitatea de a arhiva un fișier astfel încât să ocupe mai putină memorie. De exemplu, să presupunem că ai 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 utilizatorul 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 de natură malițioasa. 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 să faca acest lucru, 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 vei 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 au un tipar binar consistent, astfel de amenințări sunt greu de identificat.