Bitdefender®

INTERNET SECURITY 2016

MANUAL DE UTILIZARE

Bitdefender Internet Security 2016
Manual de utilizare

Publicat 28.01.2016

Termeni legali

Bitdefender

Cuprins

INSTALARE

1. PREGĂTIREA PENTRU INSTALARE

Pentru a instala Bitdefender Internet Security 2016 fără probleme, parcurgeți acești pași prealabili:

- Asigurați-vă că sistemul pe care doriți să instalați Bitdefender întrunește cerințele minime. În cazul în care calculatorul nu întrunește toate cerințele minime de sistem, Bitdefender nu va fi instalat sau nu va funcționa în mod corespunzător, determinând reducerea vitezei de funcționare și instabilitatea sistemului. Pentru o listă completă a cerințelor de sistem, consultați *„Cerințe de sistem"* (p. 3).
- Autentificați-vă pe calculator cu datele unui cont de administrator.
- Dezinstalați orice alt program similar de pe computer. 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.
- Dezactivați sau dezinstalați orice alt program firewall de pe calculator. Rularea simultană a două programe firewall poate afecta funcționarea lor și poate provoca probleme majore ale sistemului. Windows Firewall va fi dezactivat în timpul instalării.
- Se recomandă ca, în timpul instalării, computerul dumneavoastră să fie conectat la internet, chiar și atunci când realizați instalarea 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

Puteți instala Bitdefender Internet Security 2016 doar pe calculatoare pe care rulează următoarele sisteme de operare:

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

Înainte de instalare, computerul dumneavoastră trebuie să îndeplinească cerințele minime de sistem.

Notă

Pentru a afla pe ce sistem de operare funcționează calculatorul dumneavoastră și informațiile referitoare la hardware, urmați acești pași:

- În **Windows 7**, faceți clic dreapta pe **My Computer** de pe desktop și selectați **Properties** din meniu.
- În **Windows 8 și Windows 8.1**, din ecranul de Start al Windows, localizați Computer (de exemplu, puteți începe să tastați „Computer" direct în ecranul de Start) și faceți clic dreapta pe pictograma acestuia. Selectați Proprietăți din meniul din partea de jos. Căutați în zona System pentru a afla informații referitoare la tipul de sistem.
- În **Windows 10**, introduceți System" în caseta de căutare din bara de sarcini și faceți clic pe pictograma aferentă. Căutați în zona System pentru a afla informații referitoare la tipul de sistem.

2.1. Cerințe minime de sistem

- 1 GB spațiu liber disponibil pe hard disk (cel puțin 800 MB pe unitatea de sistem)
- Procesor de 1.6 GHz
- 1 GB de memorie (RAM)

2.2. Cerințe recomandate de sistem

- 2 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)

2.3. Cerințe software

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

- Internet Explorer 10 sau o versiune mai recentă
- Mozilla Firefox 14 sau o versiune mai recentă
- Google Chrome 20 sau o versiune mai recentă
- Skype 6.3 sau o versiune mai recentă
- Yahoo! Messenger 9 sau o versiune mai recentă
- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express și Windows Mail (pe sisteme de 32 bit)
- Mozilla Thunderbird 14 sau mai recent

3. INSTALAREA PRODUSULUI DUMNEAVOASTRĂ BITDEFENDER

Puteți instala Bitdefender folosind CD-ul de instalare sau aplicația de instalare web descărcată pe calculatorul dumneavoastră din contul Bitdefender Central.

Dacă achiziționați protecții pentru mai mult de un calculator (de exemplu, ați achiziționat Bitdefender Internet Security 2016 pentru 3 calculatoare), reluați procedura de instalare și activați produsul pe fiecare calculator folosind același cont. Contul pe care trebuie să-l folosiți este cel care conține abonamentul dvs. activ pentru Bitdefender.

3.1. Instalați din Bitdefender Central

Din contul Bitdefender Central puteți descărca kitul de instalare corespunzător abonamentului achiziționat. Odată ce procesul de instalare s-a finalizat, Bitdefender Internet Security 2016 este dezactivat.

Pentru a descărca Bitdefender Internet Security 2016 din contul Bitdefender Central, urmați acești pași:

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.
3. În fereastra **Dispozitivele mele**, faceți clic pe **INSTALARE Bitdefender**.
4. Alegeți una dintre cele doua opțiuni disponibile:
   - **DESCARCĂ**

     Dați clic pe buton și salvați fișierul de instalare.
   - **Pe alt dispozitiv**

     Selectați **Windows** pentru a descărca produsul dumneavoastră Bitdefender și apoi dați clic pe **CONTINUARE**. Introduceți adresa de e-mail în câmpul corespunzător și faceți clic pe **TRIMITERE**.
5. Așteptați să se finalizeze descărcare și apoi executați aplicația de instalare.

Validarea instalării

Bitdefender va verifica mai întâi sistemul dvs, pentru a valida instalarea.

Dacă sistemul dumneavoastră nu îndeplinește cerințele minime pentru instalarea Bitdefender, veți fi informat cu privire la zonele ce necesită să fie îmbunătățite înainte să puteți continua.

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

Pachetul de instalare Bitdefender Internet Security 2016 este actualizat constant.

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

După validarea instalării, se va afișa asistentul de configurare. Urmați pașii pentru instalarea Bitdefender Internet Security 2016.

Pasul 1 - Instalarea Bitdefender

Ecranul de instalare a Bitdefender vă permite să alegeți tipul de instalare pe care doriți să o efectuați.

Pentru o experiență de instalare fără probleme, nu trebuie decât să faceți clic pe butonul **Instalare**. Bitdefender va fi instalat în locația implicită cu setări implicite și veți trece direct la Pasul 3 al asistentului.

Dacă doriți să configurați setările de instalare, faceți clic pe **Personalizare**.

În cadrul acestui pas se pot efectua două sarcini suplimentare:

- Vă rugăm să citiți Acordul de licență cu utilizatorul final înainte de a continua cu instalarea. Contractul de licență conține termenii și condițiile conform cărora puteți folosi Bitdefender Internet Security 2016.

  Dacă nu sunteți de acord cu acești termeni, închideți fereastra. Procesul de instalare va fi abandonat și veți ieși din fereastra de instalare.

- Mențineți opțiunea **Trimite rapoarte de utilizare anonime** activă. Prin permiterea acestei opțiuni, sunt trimise rapoarte către serverele Bitdefender, conținând informații despre modul în care utilizați produsul. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot

ajuta să vă oferim produse și mai bune pe viitor. Rapoartele nu conțin date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scopuri comerciale.

Pasul 2 - Setări instalare personalizată

> **Notă**
> Acest pas apare numai dacă ați ales să personalizați instalarea la pasul anterior.

Sunt disponibile următoarele opțiuni:

Calea de instalare

În mod implicit, Bitdefender Internet Security 2016 va fi instalat în C:\Program Files\Bitdefender\Bitdefender 2016\. Dacă doriți să schimbați calea de instalare, faceți clic pe butonul **Modificare** și selectați directorul în care doriți să fie instalat Bitdefender.

Configurare setări proxy

Bitdefender Internet Security 2016 necesită acces la internet pentru activarea produsului, descărcarea actualizărilor produsului și a celor de securitate, a componentelor de detecție in-cloud etc. Dacă folosiți o conexiune proxy în loc de o conexiune directă la internet trebuie să selectați această opțiune și să configurați setările proxy.

Setările pot fi importate din browser-ul implicit sau introduse manual.

Faceți clic pe **Instalare** pentru a confirma preferințele și a începe instalarea. Dacă vă răzgândiți, faceți clic pe butonul **Implicite** corespunzător.

Pasul 3 - Instalare în curs de desfășurare

Așteptați până când instalarea este finalizată. În acest timp sunt afișate informații cu privire la progresul instalării.

Zonele critice ale sistemului dumneavoastră sunt scanate pentru identificarea virușilor, cele mai noi versiuni ale fișierelor aplicațiilor sunt descărcate și instalate, iar serviciile Bitdefender sunt pornite. Această etapă poate dura câteva minute.

Pasul 4 - Instalare finalizată

Produsul dvs. Bitdefender s-a instalat cu succes.

Este afișat rezumatul instalării. Dacă, în timpul instalării, este detectat și dezinstalat un program periculos, poate fi necesară o repornire a sistemului. Faceți clic pe **OK** pentru a continua.

Pasul 5 - Primii pași

În fereastra Primii pași, puteți vizualiza perioada de valabilitate a abonamentului dvs.

În cadrul acestui pas se pot efectua două sarcini suplimentare:

- Achiziționați un nou abonament - acest link vă redirecționează către pagina Bitdefender de unde puteți achiziționa un nou abonament.
- Am un cod de activare - acest link vă redirecționează către contul dvs. Bitdefender Central. Introduceți codul de activare pe care îl aveți, în câmpul corespunzător și faceți clic pe **Trimitere**. În mod alternativ, puteți introduce o cheie de licență valabilă, care va fi transformată într-un abonament cu aceleași atribute: număr de dispozitive și perioada de disponibilitate rămasă.

Faceți clic pe **Finalizare** pentru a accesa interfața Bitdefender Internet Security 2016.

3.2. Instalare de pe CD-ul de instalare

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

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

Notă

Ecranul de instalare oferă opțiunea de a copia pachetul de instalare de pe CD-ul de instalare pe un dispozitiv de stocare USB. Acest lucru este folositor în cazul în care doriți să instalați Bitdefender pe un computer care nu prezintă o unitate disc (de exemplu, pe un notebook). Introduceți dispozitivul de stocare în unitatea USB și apoi faceți clic pe **Copiere pe USB**. Apoi, mergeți la computerul fără unitate de disc, introduceți dispozitivul de stocare în drive-ul USB și faceți dublu-clic pe runsetup.exe din directorul în care ați salvat pachetul de instalare.

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

Validarea instalării

Bitdefender va verifica mai întâi sistemul dvs, pentru a valida instalarea.

Dacă sistemul dumneavoastră nu îndeplinește cerințele minime pentru instalarea Bitdefender, veți fi informat cu privire la zonele ce necesită să fie îmbunătățite înainte să puteți continua.

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

Pachetul de instalare Bitdefender Internet Security 2016 este actualizat constant.

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

După validarea instalării, se va afișa asistentul de configurare. Urmați pașii pentru instalarea Bitdefender Internet Security 2016.

Pasul 1 - Instalarea Bitdefender

Ecranul de instalare a Bitdefender vă permite să alegeți tipul de instalare pe care doriți să o efectuați.

Pentru o experiență de instalare fără probleme, nu trebuie decât să faceți clic pe butonul **Instalare**. Bitdefender va fi instalat în locația implicită cu setări implicite și veți trece direct la Pasul 3 al asistentului.

Dacă doriți să configurați setările de instalare, faceți clic pe **Personalizare**.

În cadrul acestui pas se pot efectua două sarcini suplimentare:

- Citiți Acordul de licență cu utilizatorul final înainte de a continua cu instalarea. Contractul de licență conține termenii și condițiile conform cărora puteți folosi Bitdefender Internet Security 2016.

Dacă nu sunteți de acord cu acești termeni, închideți fereastra. Procesul de instalare va fi abandonat și veți ieși din fereastra de instalare.

- Mențineți opțiunea **Trimite rapoarte de utilizare anonime** activă. Prin permiterea acestei opțiuni, sunt trimise rapoarte către serverele Bitdefender, conținând informații despre modul în care utilizați produsul. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să vă oferim produse și mai bune pe viitor. Rapoartele nu conțin date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scopuri comerciale.

Pasul 2 - Setări instalare personalizată

> **Notă**
> Acest pas apare numai dacă ați ales să personalizați instalarea la pasul anterior.

Sunt disponibile următoarele opțiuni:

Calea de instalare

În mod implicit, Bitdefender Internet Security 2016 va fi instalat în C:\Program Files\Bitdefender\Bitdefender 2016\. Dacă doriți să schimbați calea de instalare, faceți clic pe butonul **Modificare** și selectați directorul în care doriți să fie instalat Bitdefender.

Configurare setări proxy

Bitdefender Internet Security 2016 necesită acces la internet pentru activarea produsului, descărcarea actualizărilor produsului și a celor de securitate, a componentelor de detecție in-cloud etc. Dacă folosiți o conexiune proxy în loc de o conexiune directă la internet trebuie să selectați această opțiune și să configurați setările proxy.

Setările pot fi importate din browser-ul implicit sau introduse manual.

Faceți clic pe **Instalare** pentru a confirma preferințele și a începe instalarea. Dacă vă răzgândiți, faceți clic pe butonul **Implicite** corespunzător.

Pasul 3 - Instalare în curs de desfășurare

Așteptați până când instalarea este finalizată. În acest timp sunt afișate informații cu privire la progresul instalării.

Zonele critice ale sistemului dumneavoastră sunt scanate pentru identificarea virușilor, cele mai noi versiuni ale fișierelor aplicațiilor sunt descărcate și

instalate, iar serviciile Bitdefender sunt pornite. Această etapă poate dura câteva minute.

Pasul 4 - Instalare finalizată

Este afișat rezumatul instalării. Dacă, în timpul instalării, este detectat și dezinstalat un program periculos, poate fi necesară o repornire a sistemului. Faceți clic pe **OK** pentru a continua.

Pasul 5 - Bitdefender Central

După finalizarea instalării inițiale, se va afișa fereastra Bitdefender Central. Este necesar un cont Bitdefender Central pentru a activa produsul și pentru a folosi caracteristicile online ale acestuia. Pentru mai multe informații, consultați *„Bitdefender Central"* (p. 40).

Continuați în funcție de situația dumneavoastră.

Am deja un cont Bitdefender Central

Introduceți adresa de e-mail și parola contului dvs. Bitdefender Central și apoi faceți clic pe **AUTENTIFICARE**.

Dacă ați uitat parola pentru contul dvs. sau pur și simplu doriți să o resetați, faceți clic pe link-ul **Resetare parolă**. Introduceți adresa dvs. de e-mail și apoi faceți clic pe butonul **RESETARE PAROLĂ**.

Doresc să creez un cont Bitdefender Central

Pentru a crea cu succes un cont Bitdefender Central, faceți clic pe link-ul **Creare cont** din partea de jos a ferestrei. Introduceți informațiile solicitate în câmpurile corespunzătoare și apoi faceți clic pe butonul **CREARE CONT**.

Informațiile furnizate aici vor rămâne confidențiale.

Parola trebuie să aibă cel puțin 8 caractere și să includă o cifră.

Notă

După crearea contului, puteți folosi adresa de e-mail și parola furnizate pentru a vă autentifica în cont, la https://central.bitdefender.com.

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

Pentru a vă conecta cu contul de Microsoft, Facebook sau de Google, urmați pașii de mai jos:

1. Selectați serviciul pe care doriți să îl utilizați. Veți fi redirecționat către pagina de autentificare a acelui serviciu.
2. Urmați instrucțiunile oferite de serviciul selectat pentru a face legătura dintre contul dumneavoastră și Bitdefender.

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

Pasul 6 - Primii pași

În fereastra Primii pași, puteți vizualiza perioada de valabilitate a abonamentului dvs.

În cadrul acestui pas se pot efectua două sarcini suplimentare:

- Achiziționați un nou abonament - acest link vă redirecționează către pagina Bitdefender de unde puteți achiziționa un nou abonament.
- Am un cod de activare - acest link vă redirecționează către contul dvs. Bitdefender Central. Introduceți codul de activare pe care îl aveți, în câmpul corespunzător și faceți clic pe **Trimitere**. În mod alternativ, puteți introduce o cheie de licență valabilă, care va fi transformată într-un abonament cu aceleași atribute: număr de dispozitive și perioada de disponibilitate rămasă.

Faceți clic pe **Finalizare** pentru a accesa interfața Bitdefender Internet Security 2016.

INTRO

4. INFORMAȚII DE BAZĂ

Odată ce ați instalat Bitdefender Internet Security 2016, calculatorul dumneavoastră este protejat împotriva tuturor tipurilor de programe periculoase (cum ar fi virușii, programele spion și troienii) și amenințărilor de pe internet (cum ar fi piraților informatici, atacurile de tip phishing și mesajele spam).

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

Puteți activa funcția Autopilot pentru a vă bucura de securitate silențioasă și ca să nu mai fie nevoie de nicio intervenție din partea dumneavoastră pentru configurarea setărilor. Cu toate acestea, puteți profita de setările oferite de Bitdefender pentru a vă ajusta și îmbunătăți protecția.

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

Bitdefender va lua majoritatea deciziilor legate de securitate în locul dumneavoastră și va afișa rareori alerte pop-up. În fereastra Evenimente sunt disponibile detalii privind acțiunile întreprinse și informații cu privire la funcționarea programului. Pentru mai multe informații, consultați *„Evenimente”* (p. 18).

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

Pentru a folosi caracteristicile online ale Bitdefender Internet Security 2016 și pentru administrarea abonamentelor și dispozitivelor dumneavoastră, accesați-vă contul Bitdefender Central. Pentru mai multe informații, consultați *„Bitdefender Central”* (p. 40).

În secțiunea „Cum să” (p. 49) veți găsi instrucțiuni pas cu pas de efectuare a sarcinilor obișnuite. Dacă vă confruntați cu probleme în utilizarea

Bitdefender, accesați secțiunea *„Soluționarea problemelor frecvente”* (p. 171) pentru soluții posibile la cele mai frecvente probleme.

4.1. Deschiderea ferestrei Bitdefender

Pentru a accesa interfața principală a Bitdefender Internet Security 2016, urmați pașii de mai jos:

- În **Windows 7**:
  1. Faceți clic pe **Start** și mergeți la **Toate programele**.
  2. Faceți clic pe **Bitdefender 2016**.
  3. Faceți clic pe **Bitdefender Internet Security 2016** sau, mai rapid, faceți dublu clic pe pictograma Bitdefender din bara de sistem.
- În **Windows 8 și Windows 8.1**:

  Din ecranul de Start al Windows, localizați Bitdefender Internet Security 2016 (de exemplu, puteți începe să tastați „Bitdefender” direct în ecranul de Start) și faceți clic pe pictograma acestuia. În mod alternativ, deschideți aplicația pentru desktop și faceți dublu clic pe pictograma Bitdefender din bara de sistem.
- În **Windows 10**:

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

Pentru mai multe informații despre fereastra și pictograma Bitdefender de pe bara de sistem, consultați *„Interfața Bitdefender”* (p. 26).

4.2. Reparare probleme

Bitdefender utilizează un sistem de monitorizare a problemelor pentru a detecta și pentru a vă informa în legătură cu aspectele care pot afecta securitatea computerului și datelor dumneavoastră. În mod implicit, sunt monitorizate numai problemele considerate a fi foarte importante. Totuși, puteți configura sistemul după cum doriți, prin alegerea problemelor despre care doriți să primiți notificări.

Problemele depistate pot include setări de protecție importante care au fost dezactivate, precum și alte condiții care pot reprezenta un risc de securitate. Acestea sunt grupate în două categorii:

- **Probleme critice** - împiedică Bitdefender să vă protejeze împotriva softurilor periculoase sau reprezintă un risc de securitate major.
- **Probleme minore (necritice)** - vă pot afecta protecția în viitorul apropiat.

Pictograma Bitdefender de pe bara de sistem indică aspectele în curs de soluționare schimbându-și culoarea după cum urmează:

Probleme critice afectează securitatea sistemului dumneavoastră. Acestea necesită atenția dvs imediat și trebuie remediate în cel mai scurt timp.
Probleme care nu sunt critice afectează securitatea sistemului dumneavoastră. Ar trebui să verificați și să le remediați atunci când aveți timp.

De asemenea, dacă plasați cursorul mouse-ului peste iconiță, o fereastră pop-up va confirma existența unor probleme.

Când deschideți interfața Bitdefender, zona de Stare a securității din bara de instrumente superioară va indica tipul de probleme care afectează sistemul dumneavoastră.

4.2.1. Asistentul de remediere a tuturor problemelor

Pentru a remedia problemele detectate, urmați instrucțiunile asistentului **Remediază toate problemele**

1. Pentru a porni asistentul, aveți următoarele alternative:
   - Faceți clic-dreapta pe pictograma Bitdefender din bara de sistem și selectați **Vizualizare probleme de securitate**.
   - Deschideți interfața Bitdefender și faceți clic oriunde în interiorul zonei stării de securitate din partea superioară a barei de instrumente (de exemplu, puteți face clic pe link-ul **Remediere toate problemele!**).
2. Puteți vizualiza problemele care afectează datele și securitatea computerului dumneavoastră. Toate problemele actuale sunt selectate pentru a fi remediate.

   Dacă nu doriți să soluționați o anumită problemă în acest moment, debifați căsuța corespunzătoare. Veți fi rugat să specificați intervalul de amânare pentru soluționarea problemei. Selectați opțiunea dorită din meniu și faceți clic pe **OK**. Pentru a opri monitorizarea respectivei categorii de probleme, selectați **Permanent**.

Starea problemei se va schimba în **Amânată** și nu se va lua nicio măsură pentru remedierea problemei.

3. Pentru a rezolva problemele selectate, faceți clic pe **Reparare**. Unele probleme sunt remediate imediat. Pentru remedierea celorlalte, veți avea la dispoziție programe asistent separate.

Problemele pe care acest program asistent vă permite să le remediați pot fi grupate în următoarele categorii principale:

- **Setări de securitate dezactivate.** Aceste probleme sunt remediate pe loc, prin activarea setărilor de securitate în cauză.
- **Sarcini de securitate preventive pe care trebuie să le efectuați.** Când remediați astfel de probleme, un program asistent vă ajută să finalizați sarcina cu succes.

4.2.2. Configurarea alertelor de stare

Bitdefender vă poate informa când se detectează probleme în funcționarea următoarelor componente de program:

- Antispam
- Antivirus
- Firewall
- Actualizare
- Securitate browser

Puteți configura sistemul de alertare conform preferințelor dumneavoastră selectând problemele specifice despre care doriți să fiți informat. Urmați acești pași:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Avansat**.
3. Faceți clic pe link-ul **Configurare alerte de stare**.
4. Faceți clic pe selectoare pentru a activa sau a dezactiva alertele de stare, în funcție de preferințele dumneavoastră.

4.3. Evenimente

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

Evenimentele reprezintă un instrument extrem de important pentru monitorizarea și gestionarea protecției Bitdefender. De exemplu, puteți verifica rapid dacă produsul a fost actualizat, dacă au fost detectate coduri sau aplicații periculoase pe calculatorul dumneavoastră etc. În plus, puteți lua măsuri suplimentare dacă este cazul sau puteți modifica măsurile luate prin intermediul Bitdefender.

Pentru a accesa jurnalul de Evenimente, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Evenimente** din meniul derulant.

Mesajele sunt grupate conform modulului Bitdefender la a cărui activitate se referă:

- **Actualizare**
- **Antivirus**
- **Protecție web**
- **Vulnerabilități**
- **Firewall**
- **Detecția intruziunilor**
- **Antispam**
- **Protecție Ransomware**

De fiecare dată când survine un eveniment, puteți observa un punct pe pictograma  din partea de sus a interfeței Bitdefender.

Pentru fiecare categorie este disponibilă o listă de evenimente. Pentru a afla informații despre un anumit eveniment din listă, faceți clic pe pictograma  și selectați **Evenimente** din meniul derulant. Detaliile despre eveniment sunt afișate în partea dreaptă a ferestrei. Fiecare eveniment este însoțit de următoarele informații: o scurtă descriere, acțiunea aplicată de Bitdefender în momentul producerii evenimentului și data și ora producerii acestuia. Pot

fi setate diverse opțiuni prin intermediul cărora să fie aplicații și alte acțiuni, dacă este necesar.

Puteți filtra evenimentele în funcție de importanța lor, în ordinea în care s-au produs. Există trei tipuri de evenimente filtrate în funcție de importanța lor, fiecare marcat printr-o anumită pictogramă:

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

Pentru a vizualiza evenimentele petrecute într-o anumită perioadă de timp, selectați perioada dorită folosind câmpul corespunzător.

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

4.4. Autopilot

Pentru toți acei utilizatori care nu-și doresc nimic altceva de la soluția lor de securitate decât să fie protejați fără a fi deranjați, Bitdefender Internet Security 2016 a fost prevăzut cu modul integrat Autopilot.

Atunci când se află în modul Autopilot, Bitdefender aplică o configurație de securitate optimă și ia toate deciziile legate de securitate în locul dumneavoastră. Aceasta înseamnă că nu vor fi afișate ferestre pop-up, alerte și nu va fi necesar să configurați niciun fel de setări.

În modul Autopilot, Bitdefender remediază în mod automat problemele critice și activează și gestionează în mod silențios:

- Protecție antivirus, asigurată de funcția de scanare la accesare și scanare continuă.
- Protecție firewall.
- Protecție web.
- Actualizări automate.

Pentru a activa sau dezactiva funcția Autopilot, dați clic pe butonul **Autopilot** din bara de sus a interfeței Bitdefender.

Atunci când funcția Autopilot este activată, pictograma Bitdefender din bara de sistem va deveni B.

Important
În cazul în care modificați vreo setare administrată de funcția Autopilot atunci când este activată, aceasta se va dezactiva în mod implicit.

Pentru a vizualiza istoricul acțiunilor efectuate de către Bitdefender cât timp a fost activată funcția Autopilot, deschideți fereastra Evenimente.

4.5. Profiluri și Mod Baterie

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

Pentru a se adapta la aceste situații, Bitdefender Internet Security 2016 are două moduri de funcționare speciale:

- Profiluri
- Modul Baterie

4.5.1. Profiluri

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

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

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

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

Profil Joc
: Sporește efectele vizuale și elimină întreruperile în timpul jocurilor.

Activarea și dezactivarea profilurilor

Pentru a activa sau dezactiva profilurile, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.
3. Faceți clic pe modulul **Profiluri**.
4. În fereastra **Profiluri**, selectați secțiunea **Setări Profiluri**.
5. Activați sau dezactivați profilurile făcând clic pe selectorul corespunzător.

Configurați opțiunea Autopilot pentru a monitoriza profilurile

Pentru o experiență ușor de utilizat, puteți configura opțiunea Autopilot pentru gestionarea profilului dumneavoastră de lucru. În acest mod, Bitdefender detectează automat activitatea derulată și aplică setările de optimizare a produsului.

Pentru a permite opțiunii Autopilot să gestioneze profilurile, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.
3. Faceți clic pe modulul **Profiluri**.
4. În fereastra **Profiluri**, selectați secțiunea **Setări Profiluri**.
5. Bifați căsuța corespunzătoare **Permite Autopilot să îmi gestioneze profilurile** .

Dacă nu doriți să permiteți administrarea automată a Profilului dvs., lăsați caseta nebifată și selectați-o manual din lista drop-down a **PROFILULUI** din interfața Bitdefender.

Pentru mai multe informații referitoare la Profiluri, consultați *„Profiluri”* (p. 164)

4.5.2. Modul 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 dumneavoastră.

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 bateire 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.

Pentru a activa sau dezactiva modul baterie, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.
3. Faceți clic pe modulul **Profiluri**, și apoi selectați secțiunea **Mod Baterie**.
4. Activați sau dezactivați modul automat pentru baterie, făcând clic pe selectorul corespunzător.

   Trageți elementul glisant corespunzător de-a lungul scalei pentru a seta dacă sistemul va începe să funcționeze în Modul Baterie. Implicit, modul este activat când nivelul de încărcare a bateriei scade sub 30%.

Notă
Modul Baterie este activat implicit pe laptop-uri și tablete.

Configurarea Modului Baterie

Pentru a configura modul Baterie, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.

3. Faceți clic pe modulul **Profiluri**, și apoi selectați secțiunea **Mod Baterie**.
4. Activați funcția apăsând selectorul corespunzător.
5. Faceți clic pe butonul **Configurează**.
6. Selectați ajustările sistemului care vor fi aplicate, prin bifarea opțiunilor de mai jos:
   - Optimizați setările de produs pentru Profilul Baterie.
   - Amânați programele de fundal și activitățile de întreținere.
   - Amânare actualizare Windows automată.
   - Ajustați configurările planului de energie pentru Modul Baterie.
   - Dezactivați dispozitivele externe și porturile de rețea.
7. Faceți clic pe **Salvează** pentru a salva modificările și închide fereastra.

4.6. Protecție cu parolă pentru setările Bitdefender

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

Pentru a configura protecția prin parolă pentru setările Bitdefender, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Setări generale**.
3. Pentru a activa protecția cu parolă, faceți clic pe butonul corespunzător.
4. Introduceți parola în cele două câmpuri și faceți clic pe **OK**. Parola trebuie să aibă cel puțin 8 caractere.

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

Important

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

Pentru a elimina protecția prin parolă, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Setări generale**.
3. Pentru a dezactiva protecția cu parolă, faceți clic pe butonul corespunzător. Introduceți parola și faceți clic pe **OK**.

Notă
Pentru a modifica parola pentru produsul dumneavoastră, faceți clic pe link-ul **Modificare parolă**.

4.7. Rapoarte anonime privind consumul

În mod implicit, Bitdefender trimite rapoarte care conțin informații referitoare la modul de utilizare a acestuia pe serverele Bitdefender. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să vă oferim produse și mai bune pe viitor. Rapoartele nu conțin date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scopuri comerciale.

În cazul în care nu mai doriți să trimiteți Rapoarte anonime privind consumul, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Avansat**.
3. Faceți clic pe buton pentru a dezactiva rapoartele de utilizare Anonime.

4.8. Oferte speciale și notificări produse

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

În plus, notificările de produse pot apărea atunci când efectuați modificări în produs.

Pentru a activa sau dezactiva ofertele speciale și notificările de produse, urmați acești pași:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Setări generale**.
3. Activați sau dezactivați ofertele speciale și notificările de produse făcând clic pe butonul corespunzător.

Opțiunea de Oferte speciale și notificări de produse este activată implicit.

Notă

După dezactivarea ofertelor speciale și a notificărilor de produse, Bitdefender va continua să vă mențină informat în legătură cu ofertele speciale atunci când utilizați o versiune de evaluare, când licența dumneavoastră urmează să expire sau când utilizați o versiune de produs expirată.

5. INTERFAȚA BITDEFENDER

Bitdefender Internet Security 2016 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 vizualiza starea produsului și pentru a efectua activități esențiale, pictograma barei de sistem a Bitdefender este disponibilă în permanență.

Ecranul principală vă oferă acces la informații importante de produs, la modulele programului și vă permite să efectuați sarcinile obișnuite. Din fereastra principală, puteți accesa modulele Bitdefender pentru configurația avansată și sarcini administrative avansate și puteți administra comportamentul produsului folosind opțiunile Autopilot și Profiluri.

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

5.1. Pictograma barei de sistem

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

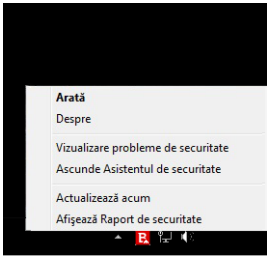
Notă

Este posibil ca pictograma Bitdefender să nu fie vizibilă întotdeauna. Pentru a vă asigura că această pictogramă este afișată permanent, urmați pașii de mai jos:

- În **Windows 7, Windows 8 și Windows 8.1**:
  1. Faceți clic pe săgeata din colțul din dreapta jos al ecranului.
  2. Faceți clic pe **Personalizare...** pentru a deschide fereastra Pictogramelor din zona notificărilor.
  3. Selectați opțiunea **Afișare pictograme și notificări** pentru pictograma **Agent Bitdefender**.
- În **Windows 10**:
  1. Faceți clic pe bara de stare și selectați **Proprietăți**.
  2. Faceți clic pe **Personalizare** în fereastra Barei de sarcini.
  3. Faceți clic pe link-ul **Selectarea pictograme afișate în bara de sarcini** din fereastra **Notificări & acțiuni**.

4. Activați butonul de lângă **Agent Bitdefender**.

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



Pictogramă în SysTray

- **Arată** - deschide fereastra principală a Bitdefender.
- **Despre** - deschide o fereastră în care puteți vedea informații despre Bitdefender și unde puteți solicita asistență profesională în cazul unei probleme.
- **Vizualizare probleme de securitate** - vă ajută să remediați problemele curente de securitate. Dacă opțiunea nu este disponibilă, nu există probleme care trebuie remediate. Pentru mai multe detalii, consultați *„Reparare probleme"* (p. 15).
- **Ascunde/ Afișează asistentul de securitate** - activează / dezactivează widget-ul de securitate.
- **Actualizează** - inițiază o actualizare imediată. Puteți urmări starea actualizării pe panoul de actualizare din fereastra Bitdefender principală.
- **Afișează Raport de securitate** - deschide o fereastră în care puteți vizualiza situația săptămânală și recomandările pentru sistemul dumneavoastră. Puteți urma recomandările pentru a îmbunătăți securitatea sistemului dumneavoastră.

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

Probleme critice afectează securitatea sistemului dumneavoastră. Acestea necesită atenția dvs imediat și trebuie remediate în cel mai scurt timp.
Probleme care nu sunt critice afectează securitatea sistemului dumneavoastră. Ar trebui să verificați și să le remediați atunci când aveți timp.
Funcția Autopilot a Bitdefender este activată.

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. Fereastra principală

Principala fereastră Bitdefender vă permite să realizați sarcini obișnuite, să remediați rapid probleme legate de securitate, să vizualizați informații referitoare funcționarea produsului, să accesați panourile de configurare a produsului și să configurați setările produsului. Puteți accesa orice opțiune prin doar câteva clicuri.

Fereastra este organizată în trei secțiuni principale:

Bara de instrumente din partea superioară
: Aici puteți verifica starea de securitate a calculatorului dumneavoastră, configura comportamentul Bitdefender în situațiile speciale, precum și sarcinile importante de acces.

Zona butoanelor de acțiuni
: Aici, puteți accesa contul panoului de comandă Bitdefender Central și executa diferite sarcini pentru a vă proteja sistemul și a-l menține operațional la viteze optime.

Pictograma  din colțul din stânga jos al interfeței principale vă oferă acces la modulele produsului, pentru a putea începe configurarea setărilor produsului.

 Icoana din partea de sus a interfeței principale vă permite să vă gestionați contul și să accesați funcționalitățile online ale produsului dumneavoastră folosind panoul de control. Aici, puteți accesa și opțiunile Evenimente, Raportul de securitate săptămânal și pagina Ajutor & Asistență.

Conectează	Description
Număr de zile rămase	Se afișează intervalul de timp rămas până la expirarea abonamentului curent. Faceți clic pe link pentru a deschide o fereastră în care veți putea vizualiza mai multe informații despre codul dumneavoastră de licență și vă veți putea înregistra produsul folosind un nou cod de licență.

5.2.1. Bara de instrumente din partea superioară

Bara de instrumente din partea superioară conține următoarele elemente:

- **Zona de stare a securității** din partea stângă a barei de instrumente vă informează dacă există probleme care afectează securitatea computerului dumneavoastră și vă ajută să le soluționați.

  Culoarea secțiunii stării de securitate se schimb în funcție de problemele detectate și, astfel, sunt afișate diferite mesaje:

  - **Secțiunea este colorată cu verde.** Nu există probleme de remediat. Calculatorul și datele dumneavoastră sunt protejate.
  - **Secțiunea este colorată cu galben.** Probleme care nu sunt critice afectează securitatea sistemului dumneavoastră. Ar trebui să verificați și să le remediați atunci când aveți timp.
  - **Secțiunea este colorată cu roșu.** Probleme critice afectează securitatea sistemului dumneavoastră. Ar trebui să vă ocupați de aceste probleme imediat.

  Dacă faceți clic oriunde în interiorul zonei ce indică starea de securitate a sistemului, puteți accesa asistentul care vă va ajuta să eliminați amenințările de pe calculatorul dumneavoastră. Pentru mai multe detalii, consultați *„Reparare probleme”* (p. 15).
- **Pilotul automat** vă permite să activați funcția Pilot automat și să vă bucurați de securitate complet silențioasă. Pentru mai multe detalii, consultați *„Autopilot”* (p. 19).
- **Profiluri** vă permite să lucrați, să vă jucați sau să vizionați filme, economisind timpul necesar pentru configurarea sistemului să amâne sarcinile. Pentru mai multe detalii, consultați *„Profiluri”* (p. 164).

5.2.2. Butoane de acțiuni

Folosind butoanele de acțiuni, puteți accesa rapid contul Bitdefender Central și lansa sarcini importante.

Butoanele de acțiuni disponibile în această zonă sunt:

- **Mergeți la Bitdefender Central**. Accesați contul Bitdefender Central pentru a verifica abonamentele și a efectua sarcinile de securitate pe dispozitivul administrat.

- **Procesul de Scanare Rapidă**. Efectuați o scanare rapidă pentru a vă asigura că în calculatorul dvs. nu există viruși.
- **Scanare Vulnerabilități**. Scanați calculatorul pentru identificarea vulnerabilităților, pentru a vă asigura că toate aplicațiile instalate, precum și Sistemul de operare, sunt actualizate și funcționează corespunzător.
- **Safepay**. Deschideți Bitdefender Safepay™ pentru a vă proteja datele confidențiale, în timpul tranzacțiilor online.
- **Actualizare**. Actualizați Bitdefender pentru a vă asigura că aveți cele mai recente semnături malware.

5.3. Modulele Bitdefender

Produsul Bitdefender este livrat cu o serie de module utile pentru a vă ajuta să vă protejați în timp ce lucrați, navigați pe internet, jucați jocuri sau doriți să faceți plăți online.

Dacă doriți să accesați modulele sau să începeți configurarea produsului, faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.

Modulele sunt separate în trei secțiuni, pe baza funcțiilor pe care le oferă:

- Securitate
- Protecție de date confidențiale
- Instrumente

5.3.1. **Securitate**

În această secțiune, puteți configura nivelul de securitate, gestiona prietenii și spammerii, vizualiza și edita setările de conexiune la rețea și seta vulnerabilitățile sistemului care trebuie remediate.

Modulele pe care le puteți administra în panoul de Protecție sunt:

Antivirus

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

Din modul Antivirus, puteți accesa cu ușurință următoarele sarcini de scanare:

- Procesul de Scanare Rapidă
- Scanare Sistem

- Administrare Scanări
- Mediu de recuperare

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

Protecție web

Protecția web vă ajută să vă protejați contra atacurilor de tip phishing, tentativelor de fraudă și scurgerilor de date personale în timp ce navigați pe Internet.

Pentru mai multe informații referitoare la modul de configurare Bitdefender pentru a vă proteja activitatea online, consultați *„Protecție web"* (p. 117).

Vulnerabilități

Modulul Vulnerabilitate vă ajută să actualizați permanent sistemul și aplicațiile pe care le utilizați regulat.

Faceți clic pe **Scanare vulnerabilități** de sub modulul Vulnerabilități pentru a identifica actualizările Windows critice, actualizările aplicațiilor și parole slabe aferente conturilor Windows.

Pentru informații suplimentare referitoare la configurarea protecției la vulnerabilitate, vă rugăm consultați *„Vulnerabilități"* (p. 122).

Firewall

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

Pentru mai multe informații cu privire la configurarea firewall-ului, consultați *„Firewall"* (p. 126).

Detecția intruziunilor

Modulul de detecție a intruziunilor analizează activitățile din sistem și din rețea pentru a identifica orice comportament neobișnuit și posibilele atacuri.

Pentru mai multe informații referitoare la modul de configurare a Modulului de detecție a intruziunilor pentru a vă proteja activitatea din sistem și din rețea, consultați *„Detecția intruziunilor"* (p. 134).

Antispam

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

Pentru mai multe informații referitoare la protecția antispam, consultați *„Antispam"* (p. 107).

Protecție Ransomware

Modulul Protecție Ransomware asigură protejarea fișierelor personale contra atacurilor infractorilor cibernetici.

Pentru mai multe informații privind configurarea opțiunii Protecție Ransomware pentru a vă proteja sistemul contra atacurilor de tip ransomware, consultați *„Protecție Ransomware"* (p. 135).

5.3.2. Protecție de date confidențiale

În secțiunea Confidențialitate, vă puteți cripta datele personale, proteja tranzacțiile online, securiza experiența de parcurgere și vă puteți proteja copiii prin vizualizarea și restricționarea activității online a acestora.

Modulele pe care le puteți administra în panoul Confidențialitate sunt:

Protecție Date

Modulul Protecție date vă permite să ștergeți permanent fișiere. Faceți clic pe opțiunea **Distrugere fișiere** de sub modulul Protecția datelor pentru a porni un asistent care vă va permite să eliminați complet datele din sistemul dvs.

Pentru informații suplimentare privind configurarea Protecțieid datelor, consultați *„Protecție Date"* (p. 120).

Administrator parolă

Funcția Administrare parolă Bitdefender vă permite să gestionați parolele, vă protejează confidențialitatea și vă oferă o experiență de navigare sigură.

Din modulul Administrator parolă, puteți selecta următoarele sarcini:

- **Deschidere Portofel** - deschide o bază de date existentă pentru Portofel.
- **Blocare Portofel** - blochează baza de date existentă pentru Portofel.
- **Exportă Portofel** - permite salvarea bazei de date actuale într-o locație pe sistemul dvs.
- **Creare Portofel nou** - pornește programul asistent care vă va permite să creați o nouă bază de date tip Portofel.
- **Ștergere** - vă permite să ștergeți baza de date existentă pentru Portofel.

- **Setări** - aici puteți modifica numele bazei de date a Portofelului dumneavoastră și puteți opta sau nu pentru sincronizarea informațiilor existente cu toate dispozitivele dumneavoastră.

Pentru mai multe informații referitoare la configurarea modulului Administrator parolă, consultați *„Protecția datele dumneavoastră cu Administratorul de parolă"* (p. 143).

Safepay

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

Faceți clic pe butonul de acțiuni **Safepay** din interfața Bitdefender pentru a începe să efectuați tranzacții online într-un mediu securizat.

Pentru mai multe informații despre Bitdefender Safepay™, consultați *„Securitate Safepay pentru tranzacțiile online"* (p. 138).

Asistență Parentală

Modulul Asistență Parentală Bitdefender vă permite să monitorizați activitățile copilului dumneavoastră atunci când se află la calculator. În cazul conținutului necorespunzător, puteți decide să restricționați accesul copilului la Internet sau la anumite aplicații.

Faceți clic pe **Configurare** din modulul Asistență Parentală pentru a începe să configurați dispozitivele copiilor dvs. și a le monitoriza activitatea indiferent unde vă aflați.

Pentru mai multe informații referitoare la configurarea modulului Asistență Parentală, consultați *„Asistență Parentală"* (p. 151).

5.3.3. Instrumente

În secțiunea Instrumente, puteți configura profilul de lucru.

Modulele pe care le puteți administra din secțiunea Instrumente sunt:

Profiluri

Profiluri Bitdefender vă oferă o experiență simplificată a utilizatorului în timp ce lucrați, vizionați un film sau jucați un joc, prin monitorizarea pridusului și a instrumentelor de lucru ale sistemului. Faceți clic pe opțiunea **Activează acum** de pe bara de instrumente superioară din interfațaBitdefender pentru a începe să folosiți această funcție.

Bitdefender vă permite să configurați următoarele profiluri:

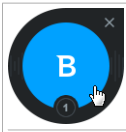
- Profil Lucru
- Profil Film
- Profil Joc

Pentru informații suplimentare privind configurarea modulului de profiluri, consultați *„Profiluri”* (p. 164).

5.4. Asistent de securitate

Widget-ul de securitate reprezintă cea mai rapidă și ușoară metodă pentru monitorizarea și controlul Bitdefender Internet Security 2016. Adăugând acest widget la desktop, veți putea vizualiza informații importante și veți putea efectua sarcini cheie în orice moment:

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



Asistent de securitate

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

 Probleme critice afectează securitatea sistemului dumneavoastră.

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

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

 Sistemul dumneavoastră este protejat.

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

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

În partea de jos a widget-ului se afișează contorul evenimentelor necitite (numărul de evenimente nerezolvate raportate de Bitdefender, dacă există). Faceți clic pe contorul de evenimente, de exemplu 1 pentru un eveniment necitit, pentru a deschide fereastra Evenimente. Pentru mai multe informații, consultați *„Evenimente"* (p. 18).

5.4.1. Scanarea fișierelor și directoarelor

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

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

5.4.2. Ascundere / afișare Widget de securitate

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

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

- Din bara de sistem:
  1. Faceți clic dreapta pe pictograma Bitdefender din bara de sistem.

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

- Din interfața Bitdefender:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Setări generale**.
3. Activați **Afișează Asistentul de securitate** făcând clic pe selectorul corespunzător.

5.5. Raport de securitate

Raportul de securitate oferă un raport săptămânal pentru produsul dumneavoastră și numeroase recomandări pentru îmbunătățirea protecției sistemului dumneavoastră. Aceste recomandări sunt importante pentru gestionarea securității generale și puteți vizualiza cu ușurință acțiunile pe care le puteți întreprinde pe sistemului dumneavoastră.

Raportul este generat o dată pe săptămână și prezintă informații relevante referitoare la activitatea produsului dumneavoastră astfel încât să puteți înțelege cu ușurință ce s-a întâmplat în această perioadă de timp.

Informațiile oferite de Raportul de securitate sunt împărțite în două categorii:

- Zona **Protecție** - vizualizați informații referitoare la protejarea sistemului dvs.
  - **Fișiere scanate**

    Vă permite să vizualizați fișierele scanate de Bitdefender în săptămâna respectivă. Puteți vizualiza detalii, cum ar fi numărul de fișiere scanate și numărul de fișiere curățate de Bitdefender.

    Pentru mai multe informații referitoare la protecția antivirus, consultați *„Protecție antivirus”* (p. 81).

  - **Pagini web scanate**

    Vă permite să verificați numărul de pagini web scanate și blocate de Bitdefender. Bitdefender vă securizează traficul web, protejându-vă informațiile personale în timp ce navigați pe internet.

    Pentru informații suplimentare privind protecția web, consultați *„Protecție web”* (p. 117).

- **Vulnerabilități**

  Vă ajută să identificați și să remediați cu ușurință vulnerabilitățile sistemului pentru a vă proteja calculatorul contra programelor periculoase și hacker-ilor.

  Pentru mai multe informații despre Scanarea vulnerabilităților, consultați secțiunea *„Vulnerabilități"* (p. 122).

- **Cronologia evenimentelor**

  Vă oferă o imagine generală a tuturor proceselor de scanare și problemelor rezolvate de Bitdefender pe parcursul săptămânii. Evenimentele sunt separate pe zile.

  Pentru informații suplimentare cu privire la un jurnal detaliat al evenimentelor asociate activității de pe calculatorul dvs., soncultați Evenimente.

- Zona **Optimizare** - vizualizați informații referitoare la spațiul curățat, aplicațiile optimizate și nivelul bateriei economisite folosind Modul Baterie.

  - **Energie baterie economisită**

    Vă permite să vedeți nivelul de baterie economisit în timpul funcționării sistemului în Modul Baterie.

    Pentru informații suplimentare referitoare la Modul Baterie, consultați *„Modul Baterie"* (p. 22).

  - **Aplicații optimizate**

    Vă permite să vedeți numărul de aplicații pe care le-ați utilizat în Profiluri.

    Pentru mai multe informații referitoare la Profiluri, consultați *„Profiluri"* (p. 164).

5.5.1. Verificarea Raportului de securitate

Raportul de securitate utilizează un sistem de monitorizare a problemelor pentru a detecta și pentru a vă informa în legătură cu aspectele care pot afecta securitatea computerului și datelor dumneavoastră. Problemele depistate pot include setări de protecție importante care au fost dezactivate, precum și alte condiții care pot reprezenta un risc de securitate. Folosind acest raport, puteți să configurați anumite componente ale Bitdefender sau să luați măsuri preventive pentru a vă proteja calculatorul și datele confidențiale.

Pentru a verifica Raportul de securitate, urmați pașii de mai jos:

1. Accesați raportul:

   - Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Raport securitate** din meniul derulant.
   - Faceți clic-dreapta pe pictograma Bitdefender din bara de sistem și selectați **Afișează Raport de securitate**.
   - Odată ce raportul este finalizat, veți primi o notificare de tip pop-up. Faceți clic pe **Afișare** pentru a accesa raportul de securitate.

     Se va deschide o pagină web în browserul dumneavoastră, unde puteți vizualiza raportul generat.

2. Priviți în partea de sus a ferestrei pentru a vedea starea generală de securitate.
3. Citiți recomandările noastre din partea de jos a paginii.

Culoarea secțiunii stării de securitate se schimb în funcție de problemele detectate și, astfel, sunt afișate diferite mesaje:

- **Zona este colorată în verde.** Nu există probleme de rezolvat. Calculatorul și datele dumneavoastră sunt protejate.
- **Zona este colorată în galben.** Există probleme non-critice care afectează securitatea sistemului dumneavoastră. Ar trebui să verificați și să le remediați atunci când aveți timp.
- **Zona este colorată în roșu.** Există probleme critice care afectează securitatea sistemului dumneavoastră. Ar trebui să vă ocupați de aceste probleme imediat.

5.5.2. Activarea/dezactivarea notificării privind raportul de securitate

Pentru a activa sau dezactiva notificarea referitoare la raportul de securitate, urmați acești pași:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Setări generale**.

3. Faceți clic pe butonul corespunzător pentru a activa sau dezactiva notificarea privind raportul de securitate.

   Notificarea privind raportul de securitate este activată implicit.

6. BITDEFENDER CENTRAL

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

- Descărcați și instalați Bitdefender pe sistemele de operare Windows, OS X și Android. Produsele disponibile pentru descărcare sunt:
  - Bitdefender Internet Security 2016
  - Antivirus Bitdefender pentru Mac
  - Securitate mobilă Bitdefender
- Administrați și reînnoiți abonamentele Bitdefender.
- Adăugați dispozitive noi la rețeaua dvs. și administrați-le oriunde v-ați afla.

6.1. Accesarea contului Bitdefender Central

Aveți mai multe posibilități de a accesa contul Bitdefender Central. În funcție de sarcina pe care doriți să o efectuați, puteți utiliza oricare dintre următoarele posibilități:

- Din interfața principală Bitdefender:
  1. Faceți clic pe link-ul **Mergi la Bitdefender Central** din stânga interfeței Bitdefender.
- Din Informații cont:
  1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender, apoi selectați **Informații cont** din meniul derulant.
  2. Facți clic pe link-ul **Mergi la Bitdefender Central** din partea de jos a ferestrei afișate.
- Din browser-ul web:
  1. Deschideți un browser web pe orice dispozitive cu acces la Internet.
  2. Mergeți la: https://central.bitdefender.com.

3. Conectați-vă la contul dumneavoastră cu ajutorul adresei de e-mail și parolei.

6.2. Abonamentele mele

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

6.2.1. Verificați abonamentele disponibile

Pentru a verifica abonamentele disponibile:

1. Accesați-vă contul Bitdefender Central.
2. Selectați fereastra **Abonamentele mele**.

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

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

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

6.2.2. Adaugă dispozitiv nou

Dacă abonamentul dvs. acoperă mai multe dispozitive, puteți adăuga un dispozitiv nou și puteți instala Bitdefender Internet Security 2016 pe acesta, după cum urmează:

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.
3. În fereastra **Dispozitivele mele**, faceți clic pe **INSTALARE Bitdefender**.
4. Alegeți una dintre cele doua opțiuni disponibile:
   - **DESCARCĂ**

     Dați clic pe buton și salvați fișierul de instalare.
   - **Pe alt dispozitiv**

Selectați **Windows** pentru a descărca produsul dumneavoastră Bitdefender și apoi dați clic pe **CONTINUARE**. Introduceți adresa de e-mail în câmpul corespunzător și faceți clic pe **TRIMITERE**.

5. Așteptați să se finalizeze descărcare și apoi executați aplicația de instalare.

6.2.3. Reînnoire abonament

Dacă nu ați optat pentru reînnoirea automată a abonamentului Bitdefender, puteți efectua manual reînnoirea urmând pașii de mai jos:

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

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

6.2.4. Activare abonament

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

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

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

1. Accesați-vă contul Bitdefender Central.
2. Selectați fereastra **Abonamentele mele**.
3. Apăsați pe butonul **COD DE ACTIVARE**, apoi introduceți codul în câmpul corespunzător.
4. Faceți clic pe **TRIMITE**.

Abonamentul este acum activat. Mergeți la fereastra **Dispozitivele mele** și selectați **INSTALARE Bitdefender** pentru a instala produsul pe unul dintre dispozitive.

6.3. Dispozitivele mele

Zona **Dispozitivele mele** din contul Bitdefender Central vă oferă posibilitatea de a instala, administra și efectua operațiuni de la distanță pe produsul Bitdefender de pe orice dispozitiv pornit și conectat la internet. Cardurile dispozitivului afișează denumirea produsului, starea de protecție și perioada de disponibilitate a abonamentului dvs.

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

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.
3. Faceți clic pe pictograma ⋮ de pe cardul dispozitivului dorit, apoi selectați **Setări**.
4. Modificați denumirea dispozitivului în câmpul corespunzător și selectați **Salvare**.

Dacă funcția Autopilot este oprită, o puteți activa făcând clic pe selector. Faceți clic pe **Salvare** pentru a aplica setările.

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

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.
3. Faceți clic pe pictograma ⋮ de pe cardul dispozitivului dorit, apoi selectați **Profil**.
4. Faceți clic pe **Adăugare deținător**, apoi completați câmpurile corespunzătoare, selectați Sexul, Data nașterii și adăugați chiar și o Poză de profil.
5. Faceți clic pe **ADAUGĂ** pentru a salva profilul.
6. Selectați deținătorul dorit din lista **Deținător dispozitiv**, apoi faceți clic pe **ALOCARE**.

Pentru a activa de la distanță Bitdefender pe un dispozitiv, urmați pașii de mai jos:

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.
3. Faceți clic pe pictograma ⋮ de pe cardul dispozitivului dorit, apoi selectați **Actualizare**.

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

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

- **Panou de bord**. În această fereastră, puteți verifica starea de protecție a produselor Bitdefender și zilele rămase din abonament. Starea de protecție poate fi verde, dacă nu există probleme care să vă afecteze produsul sau roșie dacă dispozitivul este expus unui risc. Dacă există probleme care vă afectează produsul, faceți clic pe **Vizualizare probleme** pentru mai multe detalii. De aici, puteți remedia manual problemele care afectează securitatea dispozitivelor.
- **Securitate**. Din această fereastră, puteți executa de la distanță o Scanare rapidă sau de sistem pe dispozitive. Faceți clic pe butonul **SCANARE** pentru a începe procesul. De asemenea, puteți afla data ultimei scanări a dispozitivului și puteți primi un raport cu privire la cea mai recentă scanară, cu cele mai importante informații disponibile.Pentru mai multe informații referitoare la aceste două proceduri de scanare, consultați *„Executarea unei scanări a sistemului”* (p. 89) și *„Rularea unei scanări rapide”* (p. 89).
- **Vulnerabilități**. Pentru a verifica existența unor vulnerabilități pe un dispozitiv, cum ar fi lipsa actualizărilor Windows, aplicații expirate sau parole slabe, faceți clic pe butonul **SCANARE** din secțiunea Vulnerabilități. Vulnerabilitățile nu pot fi remediate de la distanță. În cazul în care se identifică o vulnerabilitate, trebuie să executați o nouă scanare pe dispozitivul respectiv și apoi să întreprindeți acțiunile recomandate. Pentru detalii referitoare la această funcție, consultați *„Vulnerabilități”* (p. 122).

7. ACTUALIZAREA PERMANENTĂ A BITDEFENDER

Zi de zi sunt descoperite și identificate noi programe virale. De aceea, este foarte importantă actualizarea Bitdefender cu ultimele semnături de aplicații malițioase.

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

Procesul de actualizare este realizat progresiv, ceea ce înseamnă că fișierele care trebuie actualizate sunt înlocuite unul câte unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

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

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

- Dacă computerul dumneavoastră este conectat la internet printr-un server proxy, trebuie să configurați setările proxy, după cum se specifică în *„Cum pot configura Bitdefender să utilizeze o conexiune la internet de tip proxy?"* (p. 74).
- În timpul descărcării actualizărilor pe o conexiune lentă de internet pot apărea erori. Pentru a afla cum să procedați în cazul unor astfel de erori, vă rugăm să consultați *„Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet"* (p. 182).
- Dacă vă conectați la Internet prin dial-up, atunci este recomandat să actualizați manual Bitdefender în mod regulat. Pentru mai multe informații, consultați *„Efectuarea unei actualizări"* (p. 46).

7.1. Cum verificați dacă Bitdefender este actualizat

Pentru a verifica data ultimei actualizări a Bitdefender, accesați **Zona stării de securitate** din partea stângă a barei de instrumente.

Pentru mai multe informații despre cele mai recente actualizări, verificați evenimentele privind actualizările:

1. În fereastra principală, faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Events** din meniul derulant.
2. În fereastra **Evenimente**, selectați **Actualizare** din meniul derulant corespunzător.

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

7.2. Efectuarea unei actualizări

Pentru efectuarea actualizărilor este necesară existența unei conexiuni la internet.

Pentru a iniția o actualizare, aplicați una dintre metodele de mai jos:

- Deschideți interfața Bitdefender și faceți clic pe butonul de acțiune **Actualizare**.
- Faceți clic dreapta pe pictograma Bitdefender  din tăvița de sistem și selectați opțiunea **Actualizează acum**.

Modulul Actualizare se va conecta la serverul de actualizare al Bitdefender și va căuta noi actualizări. În cazul în care este detectată o actualizare, în funcție de setările de actualizare, vi se va cere fie să confirmați actualizarea, fie aceasta va fi realizată automat.

Important

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

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

Pentru a activa de la distanță Bitdefender pe un dispozitiv, urmați pașii de mai jos:

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.

3. Faceți clic pe pictograma ⋮ de pe cardul dispozitivului dorit, apoi selectați **Actualizare**.

7.3. Activarea sau dezactivarea actualizării automate

Pentru a dezactiva funcția de actualizare automată, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Actualizare**.
3. Faceți clic pe comutator pentru a activa sau dezactiva actualizarea automată.
4. Se deschide o fereastră de avertizare. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării actualizarii automate. Puteți dezactiva actualizarea automată pentru 5, 15 sau 30 de minute, pentru o oră, permanent sau doar până la repornirea sistemului.

Avertisment

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

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 vă mai avertiza.

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

Pentru ajustarea setărilor de actualizare, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați window, secțiunea **Actualizare** și configurați setările pentru a corespunde preferințelor dvs.

Frecvența actualizărilor

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

Locație actualizare

Produsul Bitdefender este configurat să efectueze online actualizări de pe serverele de actualizare ale Bitdefender. Locația de actualizare este o adresă de Internet generică, ce este redirecționată automat către cel mai apropiat server de actualizare al Bitdefender din regiunea dumneavoastră.

Nu schimbați locația pentru actualizări decât dacă sunteți sfătuit de un reprezentant al Bitdefender sau de administratorul rețelei (dacă sunteți conectat la o rețea de birou) să faceți acest lucru.

Puteți reveni la locația de actualizare online generică făcând clic pe **Implicit**.

Reguli de procesare a actualizării

Puteți alege una dintre cele trei metode de mai jos pentru a descărca și instala actualizări:

- **Actualizare discretă** - Bitdefender descarcă și realizează actualizarea automat.
- **Anunță înainte de descărcare** - de fiecare dată când o actualizare este disponibilă, veți fi anunțat înainte de a o descărca.
- **Anunța înainte de instalare** - de fiecare dată când o actualizare a fost descărcată, veți fi întrebat înainte de a o instala.

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 doriți să fiți notificat în momentul în care este necesară o repornire în urma unei actualizări, dezactivați opțiunea **Amânare repornire**, făcând clic pe comutatorul corespunzător.

CUM SĂ

8. INSTALARE

8.1. Cum instalez Bitdefender pe un al doilea calculator?

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

Pentru a instala Bitdefender pe un al doilea calculator, urmați pașii de mai jos:

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.
3. În fereastra **Dispozitivele mele**, faceți clic pe **INSTALARE Bitdefender**.
4. Alegeți una dintre cele doua opțiuni disponibile:
   - **DESCARCĂ**

     Dați clic pe buton și salvați fișierul de instalare.
   - **Pe alt dispozitiv**

     Selectați **Windows** pentru a descărca produsul dumneavoastră Bitdefender și apoi dați clic pe **CONTINUARE**. Introduceți adresa de e-mail în câmpul corespunzător și faceți clic pe **TRIMITERE**.
5. Rulați produsul Bitdefender descărcat. Așteptați până la finalizarea procesului de instalare și închideți fereastra.

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

8.2. Când este cazul să reinstalez Bitdefender?

Există anumite cazuri în care poate fi necesar să reinstalați produsul dumneavoastră Bitdefender.

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

- ați reinstalat sistemul de operare.
- ați achiziționat un nou computer.

- doriți să schimbați limba de afișare a interfeței Bitdefender.

Pentru a reinstala Bitdefender, puteți folosi discul de instalare achiziționat sau puteți descărca o nouă versiune din contul Bitdefender Central.

Pentru mai multe informații cu privire la procesul de instalare Bitdefender, consultați *„Instalarea produsului dumneavoastră Bitdefender"* (p. 5).

8.3. De unde se poate descărca produsul Bitdefender?

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

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

Pentru a instala Bitdefender din contul Bitdefender Central, urmați pașii de mai jos:

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.
3. În fereastra **Dispozitivele mele**, faceți clic pe **INSTALARE Bitdefender**.
4. Alegeți una dintre cele doua opțiuni disponibile:
   - **DESCARCĂ**

     Dați clic pe buton și salvați fișierul de instalare.
   - **Pe alt dispozitiv**

     Selectați **Windows** pentru a descărca produsul dumneavoastră Bitdefender și apoi dați clic pe **CONTINUARE**. Introduceți adresa de e-mail în câmpul corespunzător și faceți clic pe **TRIMITERE**.
5. Rulați produsul Bitdefender descărcat.

8.4. Cum folosesc abonamentul Bitdefender după un upgrade Windows?

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

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

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

Pot apărea două situații:

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

  În acest caz, trebuie să reinstalați produsul folosind cea mai recentă versiune disponibilă.

  Pentru a soluționa această problemă, urmați pașii de mai jos:

  1. Ștergeți Bitdefender urmând pașii de mai jos:
     - În **Windows 7**:
       a. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
       b. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
       c. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.
       d. Faceți clic pe **Înainte** pentru a continua.
       e. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
     - În **Windows 8 și Windows 8.1**:
       a. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.
       b. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
       c. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
       d. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.

e. Faceți clic pe **Înainte** pentru a continua.

f. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

- În **Windows 10**:

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

b. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.

c. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.

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

e. Faceți clic pe **Șterge** și apoi selectați **Vreau să reinstalez**.

f. Faceți clic pe **Înainte** pentru a continua.

g. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

2. Descărcați fișierul de instalare:

a. Accesați-vă contul Bitdefender Central.

b. Selectați secțiunea **Dispozitivele mele**.

c. În fereastra **Dispozitivele mele**, faceți clic pe **INSTALARE Bitdefender**.

d. Alegeți una dintre cele doua opțiuni disponibile:

- **DESCARCĂ**

  Dați clic pe buton și salvați fișierul de instalare.

- **Pe alt dispozitiv**

  Selectați **Windows** pentru a descărca produsul dumneavoastră Bitdefender și apoi dați clic pe **CONTINUARE**. Introduceți adresa de e-mail în câmpul corespunzător și faceți clic pe **TRIMITERE**.

3. Rulați produsul Bitdefender descărcat.

- Ați modificat sistemul dumneavoastră și doriți să utilizați în continuare protecția Bitdefender.

  Prin urmare, trebuie să reinstalați produsul folosind cea mai recentă versiune.

  Pentru a rezolva această problemă:

1. Descărcați fișierul de instalare:
   a. Accesați-vă contul Bitdefender Central.
   b. Selectați secțiunea **Dispozitivele mele**.
   c. În fereastra **Dispozitivele mele**, faceți clic pe **INSTALARE Bitdefender**.
   d. Alegeți una dintre cele doua opțiuni disponibile:
      - **DESCARCĂ**

        Dați clic pe buton și salvați fișierul de instalare.
      - **Pe alt dispozitiv**

        Selectați **Windows** pentru a descărca produsul dumneavoastră Bitdefender și apoi dați clic pe **CONTINUARE**. Introduceți adresa de e-mail în câmpul corespunzător și faceți clic pe **TRIMITERE**.
2. Rulați produsul Bitdefender descărcat.

Pentru mai multe informații cu privire la procesul de instalare Bitdefender, consultați *„Instalarea produsului dumneavoastră Bitdefender”* (p. 5).

8.5. Cum repar Bitdefender?

Dacă doriți să reparați Bitdefender Internet Security 2016 din meniul de start Windows, urmați acești pași:

- În **Windows 7**:
  1. Faceți clic pe **Start** și mergeți la **Toate programele**.
  2. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
  3. Faceți clic pe **Repară** din fereastra care se afișează.

     Aceasta va dura câteva minute.
  4. După finalizarea procesului, va fi necesar să reporniți computerul.
- În **Windows 8 și Windows 8.1**:
  1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.
  2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
  3. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.

4. Faceți clic pe **Repară** din fereastra care se afișează.

   Aceasta va dura câteva minute.

5. După finalizarea procesului, va fi necesar să reporniți computerul.

- În **Windows 10**:

1. Faceți clic pe **Start**, apoi pe Setări.
2. Faceți clic pe pictograma **Sistem** din zona Setări și selectați **Aplicații & funcții**.
3. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Faceți clic pe **Reparare**.

   Aceasta va dura câteva minute.

6. După finalizarea procesului, va fi necesar să reporniți computerul.

9. ABONAMENTE

9.1. Ce produs Bitdefender folosesc?

Pentru a afla ce program Bitdefender ați instalat:

1. Deschideți interfața Bitdefender.
2. În partea superioară a ferestrei, ar trebui să vedeți afișată una dintre următoarele denumiri de produse:
   - Bitdefender Antivirus Plus 2016
   - Bitdefender Internet Security 2016
   - Bitdefender Total Security 2016

9.2. Cum activez abonamentul Bitdefender folosind un cod de licență?

Dacă aveți un cod de licență valabil și doriți să îl utilizați pentru a activa abonamentul pentru Bitdefender Internet Security 2016, există două situații posibile:

- Ați trecut de la o versiune anterioară a Bitdefender la cea nouă:
  1. După ce trecerea la Bitdefender Internet Security 2016 s-a încheiat, vi se solicită să vă autentificați la contul Bitdefender Central.
  2. Introduceți datele de autentificare și faceți clic pe **CONECTARE**
  3. Pe ecranul contului dvs. se afișează o notificare privind crearea abonamentului. Abonamentul creat va fi valabil pentru zilele rămase din codul dvs. de licență și pentru același număr de utilizatori.

     Dispozitivele care folosesc versiunile Bitdefender anterioare și sunt înregistrate cu codul de licență pe care l-ați transformat în abonament trabuie să înregistreze produsul cu același cont Bitdefender Central.
- Bitdefender neinstalat anterior pe sistem:
  1. Imediat după încheierea procesului de instalare, vi se solicită să vă conectați la contul Bitdefender Central.
  2. Introduceți datele de autentificare și faceți clic pe **CONECTARE**
  3. Selectați fereastra **Abonamentele mele**.

4. Faceți clic pe butonul **COD DE ACTIVARE** și introduceți codul de licență.
5. Faceți clic pe **TRIMITE**. Un abonament cu același nivel de disponibilitate și număr de utilizatori ai codului de licență este asociat contului dvs.

10. BITDEFENDER CENTRAL

10.1. Cum mă autentific la Bitdefender Central folosind un alt cont online?

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

Pentru a utiliza un alt cont, urmați acești pași:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Informații cont** din meniul derulant.
2. Faceți clic pe butonul **Schimbare Cont** pentru a schimba contul asociat calculatorului.
3. Introduceți adresa e-mail și parola contului în câmpurile corespunzătoare și faceți clic pe **Conectare**.

Notă
Produsul Bitdefender de pe dispozitivul dvs. trece automat la abonamentul asociat noului cont Bitdefender Central.
Dacă nu există niciun abonament disponibil asociat noului cont Bitdefender Central sau dacă doriți să îl transferați pe contul anterior, puteți contacta Bitdefender pentru asistență, în modul descris în secțiunea *„Solicitarea ajutorului"* (p. 204).

10.2. Cum resetez parola pentru contul Bitdefender Central?

Pentru a seta o nouă parolă pentru contul dumneavoastră Bitdefender Central, urmați acești pași:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Informații cont** din meniul derulant.
2. Faceți clic pe butonul **Schimbare Cont** pentru a schimba contul asociat calculatorului.

   Se afișează o nouă fereastră.
3. Faceți clic pe link-ul **Resetare parolă**.

4. Introduceți adresa e-mail utilizată pentru a crea contul Bitdefender Central și faceți clic pe butonul **RESETARE PAROLĂ**.
5. Verificați adresa de e-mail și faceți click pe link-ul furnizat.
6. Introduceți adresa e-mail în câmpul corepsunzător.
7. Introduceți noua parolă. Parola trebuie să aibă cel puțin 8 caractere și să includă cifre.
8. Faceți clic pe **Accesează**.

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

11. SCANAREA CU BITDEFENDER

11.1. Cum scanez un fișier sau un director?

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

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

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

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

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

11.2. Cum îmi scanez sistemul?

Pentru a efectua o scanare completă a sistemului, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antivirus**, selectați **Scanare sistem**.
4. Urmați programul asistent Scanare Sistem pentru a încheia scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate.

   Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultați *„Asistentul de scanare antivirus”* (p. 93).

11.3. Cum programez o scanare?

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

Pentru a programa o scanare, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antivirus**, selectați **Administrare scanări**.
4. Selectați tipul de scanare pe care doriți să îl programați, Scanare de sistem sau Scanare rapidă și faceți clic pe **Opțiuni de scanare**.

   Alternativ, puteți crea un tip de scanare care să corespundă necesităților dvs. făcând clic pe **Sarcină personalizată nouă**.
5. Activați selectorul **Programare**.

   Selectați una dintre opțiunile corespunzătoare pentru a seta un program:

   - La pornirea sistemului
   - O singură dată
   - Periodic

În fereastra **Scanare ținte**, puteți selecta locațiile pe care doriți să le scanați.

11.4. Cum creez o activitate de scanare personalizată?

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

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

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antivirus**, selectați **Administrare scanări**.

4. Faceți click pe **Sarcină personalizată nouă**. În fila **Basic** introduceți o denumire pentru scanare și selectați locațiile ce urmează a fi scanate.
5. Dacă doriți să configurați opțiunile de scanare în detaliu, selectați secțiunea **Avansat**.

   Puteți configura ușor opțiunile de scanare reglând nivelul de scanare. Trageți cursorul deasupra scalei pentru a seta nivelul de scanare dorit.

   De asemenea, aveți posibilitatea de a închide computerul după finalizarea scanării în cazul în care nu a fost detectată nicio amenințare. Rețineți faptul că acesta va fi modul implicit de reacție, de fiecare dată când executați această activitate.
6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.
7. Folosiți selectorul corespunzător dacă doriți să programați o sarcină de scanare.
8. Faceți clic pe **Pornire scanare** și urmați instrucțiunile asistentului de scanare pentru a finaliza operația de scanare. După finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.
9. Dacă doriți, puteți relua rapid rularea scanării personalizate anterioare, făcând clic pe înregistrarea corespunzătoare din lista valabilă.

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

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

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

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

Pentru a adăuga directorul pe lista de excepții, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Excepții**.
4. Asigurați-vă că este activă opțiunea **Excepții fișiere** apăsând butonul corespunzător.
5. Faceți clic pe link-ul **Fișiere și directoare excluse**.
6. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
7. Faceți clic pe **Caută**, selectați directorul care doriți să fie exclus de la scanare și faceți clic pe **OK**.
8. Faceți clic pe **Adaugă** și apoi pe **OK** pentru a salva modificările și a închide fereastra.

11.6. 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, adăugați fișierul în secțiunea de excluderi a Bitdefender:

1. Dezactivați protecția antivirus în timp real a Bitdefender:
   a. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
   b. Selectați secțiunea **Protecție**.
   c. Faceți clic pe modulul **Antivirus**.
   d. În fereastra **Antivirus**, selectați secțiunea **Protecție**.
   e. Faceți clic pe comutator pentru a dezactiva **scanarea la accesare**.

      Se deschide o fereastră de avertizare. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real. Puteți dezactiva protecția în timp real pentru 5, 15 sau 30 de minute, pentru o oră, permanent sau doar până la repornirea sistemului.

2. Afișați elementele ascunse din Windows. Pentru a afla cum să procedați, consultați *„Cum pot afișa elementele ascunse din Windows?"* (p. 76).
3. Restaurați fișierul din zona de carantină:
   a. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
   b. Selectați secțiunea **Protecție**.
   c. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Carantină**.
   d. Selectați fișierul și faceți clic pe **Restabilire**.
4. Adăugați fișierul la lista de Excepții. Pentru a afla cum să procedați, consultați *„Cum exclud un director de la procesul de scanare?"* (p. 62).
5. Activați protecția antivirus în timp real a Bitdefender.
6. Contactați un reprezentant al echipei noastre de asistență tehnică și solicitați eliminarea semnăturii de detectare. Pentru a afla cum să procedați, consultați *„Solicitarea ajutorului"* (p. 204).

11.7. Cum aflu ce viruși au fost detectați 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.

Puteți deschide raportul de scanare direct din asistentul de scanare, după ce scanarea a luat sfârșit, apăsând **Afișează jurnal**.

Pentru a verifica un jurnal de scanare sau orice infestare detectată ulterior, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Evenimente** din meniul derulant.
2. În fereastra **Evenimente**, selectați **Antivirus** din meniul derulant corespunzător.

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

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

   Dacă doriți să reluați aceeași scanare,faceți clic pe butonul **Reluare scanare**.

12. ASISTENȚĂ PARENTALĂ

12.1. Cum îmi protejez copiii împotriva amenințărilor online?

Opțiunea Asistență Parentală Bitdefender vă oferă posibilitatea de a restricționa accesul la internet și la anumite aplicații, astfel încât copiii dumneavoastră să nu poată vizualiza site-uri și aplicații cu conținut neadecvat atunci când nu vă aflați prin preajmă să-i supravegheați.

Pentru a configura modulul Asistență Parentală, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. În modulul **Asistență Parentală**, selectați **Configurare**.

   Sunteți redirecționat(ă) la pagina web Bitdefender Central. Asigurați-vă că sunteți conectat(ă) cu datele dumneavoastră de autentificare.
4. Panoul de Asistență Parentală se deschide într-o nouă fereastră. De aici puteți verifica și configura setările funcției de Asistență Parentală.
5. Faceți clic pe **ADĂUGARE PROFIL** în partea dreapta a ferestrei **Copiii mei**.
6. Introduceți informațiile specifice în câmpurile corespunzătoare, cum ar fi: numele, adresa de e-mail, sexul și data nașterii și apoi faceți clic pe **CONTINUARE**.

   În baza standardelor de dezvoltare a copilului, setarea datei nașterii copilului încarcă automat specificații considerate corespunzătoare pentru categoria sa de vârstă.
7. Dacă dispozitivul copilului dumneavoastră are deja instalat Bitdefender Internet Security 2016, selectați dispozitivul acestuia din lista disponibilă și apoi faceți clic pe **CONTINUARE**.

   Dacă dispozitivul copilului dumneavoastră nu are Bitdefender instalat cu funcția Asistență Parentală inclusă, faceți clic pe **Adaugă dispozitiv nou**. Selectați sistemul de operare al dispozitivului acestuia și apoi faceți clic pe **CONTINUARE**.

Introduceți adresa de e-mail la care să vă trimitem link-ul de descărcare pentru instalarea aplicației Bitdefender Asistență Parentală.

Pe dispozitivele Windows, Bitdefender Internet Security 2016 inclus în abonamentul dumneavoastră trebuie descărcat și instalat. Pe dispozitivele Android, Agentul de Asistență Parentală Bitdefender trebuie descărcat și instalat.

Verificați activitatea copiilor dumneavoastră și modificați setările de Asistență Parentală folosind Bitdefender Central de la orice calculator sau dispozitiv mobil conectat la internet.

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

Funcția de Asistență Parentală Bitdefender vă permite să controlați conținutul accesat de copilul dumneavoastră în timpul utilizării dispozitivului său și să blocați accesul la un site web.

Pentru a bloca accesul la un site web, trebuie să adăugați site-ul web respectiv pe lista de Excluderi, după cum urmează:

1. Mergeți la: https://central.bitdefender.com.
2. Conectați-vă la contul dumneavoastră cu ajutorul adresei de e-mail și parolei.
3. Faceți clic pe **Asistență Parentală** pentru a accesa panoul de comandă.
4. Selectați profilul copilului dumneavoastră din fereastra **Copiii mei**.
5. Selectați secțiunea **Interese**.
6. Faceți clic pe butonul **ADMINISTRARE**.
7. Introduceți pagina web pe care doriți să o blocați în câmpul corespunzător.
8. Selectați **Permite** sau **Blocare**.
9. Faceți clic pe **Finalizare** pentru a salva modificările.

12.3. Cum împiedic copilul meu să se joace pe calculator?

Funcția de Asistență Parentală Bitdefender vă permite să controlați conținutul pe care îl accesează copilul dumneavoastră în timp ce utilizează calculatorul.

Pentru a bloca accesul la un joc, urmați pașii de mai jos:

1. Mergeți la: https://central.bitdefender.com.
2. Conectați-vă la contul dumneavoastră cu ajutorul adresei de e-mail și parolei.
3. Faceți clic pe **Asistență Parentală** pentru a accesa panoul de comandă.
4. Selectați profilul copilului dumneavoastră din fereastra **Copiii mei**.
5. Selectați secțiunea **Activități**.

   Se afișează o listă cu carduri. Cardurile reprezintă aplicațiile pe care le utilizează copilul dumneavoastră.
6. Selectați cardul cu aplicația a cărei utilizare de către copilul dumneavoastră doriți să o blocați.

   Marcarea cu simbolul de bifare indică faptul că aplicația nu va putea fi utilizată de copilul dumneavoastră.

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

Funcția Asistență Parentală Bitdefender vă oferă posibilitatea de a bloca apeluri telefonice de la numere de telefon necunoscute sau de la prieteni din agenda copilului dumneavoastră.

Pentru a bloca un anumit contact, urmați pașii de mai jos:

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

   Asigurați-vă că sunteți conectat(ă) cu datele dumneavoastră de autentificare.
2. Faceți clic pe **Asistență Parentală** pentru a accesa panoul de comandă.
3. Faceți clic pe pictograma ⋮ de pe cardul de profil dorit și apoi selectați **Editare**.
4. Introduceți în câmpul corespunzător numărul de telefon al copilului dumneavoastră, apoi faceți clic pe **SALVARE**.
5. Selectați profilul copilului în legătură cu care doriți să stabiliți restricțiile.
6. Selectați secțiunea **Prieteni**.

Se afișează o listă cu carduri. Card-urile reprezintă contactele din telefonul copilului dumneavoastră.

7. Selectați cardul cu numărul de telefon pe care doriți să îl blocați.

   Marcarea cu simbolul de bifare indică faptul că numărul de telefon selectat nu poate lua legătura cu copilul dumneavoastră.

Pentru a bloca numere de telefon necunoscute, activați butonul **Blochează interacțiunile cu apelurile cu număr necunoscut**.

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

Funcția Asistență Parentală Bitdefender vă permite să setați o locație ca fiind sigură sau restricționată pentru copilul dumneavoastră.

Pentru a seta o locație, urmați pașii de mai jos:

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

   Asigurați-vă că sunteți conectat(ă) cu datele dumneavoastră de autentificare.

2. Faceți clic pe **Asistență Parentală** pentru a accesa panoul de comandă.
3. Selectați profilul copilului dumneavoastră din fereastra **Copiii mei**.
4. Selectați secțiunea **Locuri**.
5. Faceți clic pe **Dispozitive** în cadrul din fereastra **Locuri**.
6. Faceți clic pe **SELECTARE DISPOZITIVE** și apoi selectați dispozitivul pe care doriți să îl configurați.
7. În fereastra **Zone**, faceți clic pe butonul **ADĂUGARE ZONĂ**.
8. Selectați tipul locației **Sigură** sau **Restricționată**.
9. Introduceți un nume valid pentru zona pe care copilul dumneavoastră o poate sau nu accesa.
10. În **Locație inițială**, introduceți orașul în care se află copilul dumneavoastră și apoi alegeți județul din lista care apare pe ecran.
11. Stabiliți raza care urmează a fi aplicată pentru monitorizare din bara glisantă **Rază**.
12. Faceți clic pe **ADĂUGARE ZONĂ** pentru a salva setările.

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

12.6. Ștergerea profilului de copil

Dacă doriți să ștergeți un profil de copil existent, urmați acești pași:

1. Mergeți la: https://central.bitdefender.com.
2. Conectați-vă la contul dumneavoastră cu ajutorul adresei de e-mail și parolei.
3. Faceți clic pe **Asistență Parentală** pentru a accesa panoul de comandă.
4. Faceți clic pe pictograma ⋮ de pe profilul de copil pe care doriți să îl ștergeți și apoi selectați **Ștergere**.

13. CONTROL DATE PERSONALE

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

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

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

Pentru a vă menține activitatea online în deplină siguranță și confidențialitate, urmați pașii de mai jos:

1. Faceți clic pe butonul de acțiuni **Safepay** de pe interfața Bitdefender.
2. Faceți clic pe butonul pentru a accesa **Tastatura virtuală**.
3. Folosiți **Tastatura virtuală** atunci când introduceți informații confidențiale, cum ar fi parolele.

13.2. Cum șterg definitiv un fișier cu ajutorul Bitdefender?

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

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

1. Faceți clic dreapta pe fișierul sau directorul pe care doriți să-l ștergeți definitiv, alegeți Bitdefender și selectați **Ștergere definitivă fișiere**.
2. Va apărea o fereastră de confirmare. Faceți clic pe **Da** pentru a porni asistentul Ștergere definitivă fișiere.
3. Așteptați ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.
4. Sunt afișate rezultatele. Faceți clic pe **Închide** pentru a părăsi asistentul.

14. INFORMAȚII UTILE

14.1. Cum îmi testez soluția antivirus?

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

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

Pentru a vă testa soluția antivirus, urmați acești pași:

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

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

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

Dacă nu primiți nicio alertă Bitdefender, vă recomandăm să contactați Bitdefender pentru asistență, așa cum este indicat la secțiunea *„Solicitarea ajutorului”* (p. 204).

14.2. Cum dezinstalez Bitdefender?

Dacă doriți să ștergeți Bitdefender Internet Security 2016, urmați acești pași:

- În **Windows 7**:
  1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
  2. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
  3. Selectați **Șterge** și apoi selectați **Vreau să șterg permanent**.

4. Faceți clic pe **Înainte** pentru a continua.
5. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

- În **Windows 8 și Windows 8.1**:

1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control" direct în ecranul de Start) și faceți clic pe pictograma acestuia.
2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
3. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
4. Selectați **Șterge** și apoi selectați **Vreau să șterg permanent**.
5. Faceți clic pe **Înainte** pentru a continua.
6. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

- În **Windows 10**:

1. Faceți clic pe **Start**, apoi pe Setări.
2. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.
3. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Selectați **Șterge** și apoi selectați **Vreau să șterg permanent**.
6. Faceți clic pe **Înainte** pentru a continua.
7. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

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

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

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

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

Iată cum trebuie să configurați Bitdefender pentru a închide automat sistemul la finalizarea scanării:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antivirus**, selectați **Administrare scanări**.
4. În fereastra **Administrare sarcini scanare**, faceți clic pe **Sarcină personalizată nouă** pentru a introduce un nume pentru scanare și a selecta locațiile pe care doriți să le scanați.
5. Dacă doriți să configurați opțiunile de scanare în detaliu, selectați secțiunea **Avansat**.
6. Selectați opțiunea de închidere a calculatorului după finalizarea scanării în cazul în care nu a fost detectată nicio amenințare.
7. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.
8. Faceți clic pe butonul **Pornire scanare** pentru a vă scana sistemul.

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

Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultați *„Asistentul de scanare antivirus"* (p. 93).

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

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

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

Pentru a gestiona setările proxy, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Avansat**.
3. Activați utilizarea proxy făcând clic pe buton.
4. Faceți clic pe link-ul **Administrare proxy**.
5. Există două opțiuni de configurare a setărilor proxy:
   - **Importă setări proxy din browserul implicit** - setări proxy ale utilizatorului curent, extrase din browserul implicit. Dacă serverul proxy necesită un nume de utilizator și o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.

     Notă
     Bitdefender poate importa setări proxy de la browserele cele mai des folosite, inclusiv cele mai noi versiuni pentru Internet Explorer, Mozilla Firefox și Opera.

   - **Setări proxy personalizate** - setări proxy pe care le puteți configura cum doriți. Următoarele setări trebuie specificate:
     - **Adresă** - introduceți adresa IP a serverului proxy.
     - **Port** - introduceți portul folosit Bitdefender pentru a se conecta la serverul proxy.
     - **Utilizator** - introduceți un nume de utilizator recunoscut de proxy.
     - **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.
6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

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

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

Pentru a identifica dacă utilizați un sistem de operare pe 32 sau 64 de biți, urmați acești pași:

- În **Windows 7**:
  1. Faceți clic pe **Start**.
  2. Localizați **Computer** din meniul **Start**.
  3. Faceți clic-dreapta pe **Computer** și selectați **Properties**.
  4. Sub **System** veți găsi informații referitoare la sistemul dumneavoastră.
- În **Windows 8 și Windows 8.1**:
  1. Din ecranul de Start al Windows, localizați **Computer** (de exemplu, puteți începe să tastați „Computer" direct în ecranul de Start) și faceți clic dreapta pe pictograma acestuia.
  2. Selectați **Proprietăți** din meniul din partea de jos.
  3. Mergeți la secțiunea Sistem pentru a vedea tipul sistemului.
- În **Windows 10**:
  1. Introduceți "System" în caseta de căutare din bara de sarcini și faceți clic pe pictogramă.
  2. Căutați în zona System pentru a afla informații referitoare la tipul de sistem.

14.6. Cum pot afișa elementele ascunse din Windows?

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

Urmați acești pași pentru a afișa obiectele ascunse din Windows:

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

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

2. Selectează **Opțiunile dosarului**:

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

În **Windows 10**:

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

14.7. Cum elimin celelalte soluții de securitate?

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

Atunci când utilizați mai multe soluții de securitate pe același calculator, sistemul devine instabil. Programul de instalare a Bitdefender Internet Security 2016 detectează în mod automat alte programe de securitate și vă oferă opțiunea de a le dezinstala.

Dacă nu ați dezinstalat celelalte soluții de securitate în timpul instalării inițiale, urmați acești pași:

- În **Windows 7**:
  1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
  2. Așteptați câteva momente până când este afișată lista programelor instalate.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Dezinstalare**.
  4. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

- În **Windows 8 și Windows 8.1**:
  1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.
  2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
  3. Așteptați câteva momente până când este afișată lista programelor instalate.
  4. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Dezinstalare**.
  5. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
- În **Windows 10**:
  1. Faceți clic pe **Start**, apoi pe Setări.
  2. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Dezinstalare**.
  4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
  5. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

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

14.8. 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 virușii 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 virușilor sunt inactivi atunci când Windows se află în Safe Mode și pot fi eliminați cu ușurință.

Pentru a porni Windows în Safe Mode:

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

ADMINISTRAREA SECURITĂȚII DUMNEAVOASTRĂ

15. PROTECȚIE ANTIVIRUS

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

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

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

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

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

Bitdefender scanează în mod automat orice fișier media amovibil care este conectat la computer pentru a vă asigura că este sigur să îl accesați. Pentru mai multe informații, consultați *„Scanarea automată a suporturilor media amovibile"* (p. 97).

Utilizatorii avansați pot configura excepțiile de la scanare în cazul în care nu doresc ca anumite fișiere sau tipuri de fișiere să fie scanate. Pentru mai multe informații, consultați *„Configurarea excepțiilor de la scanare"* (p. 99).

Atunci când detectează un virus sau un alt cod periculos, Bitdefender va încerca în mod automat să elimine codul periculos din fișierul infectat și să reconstruiască fișierul original. Această operațiune este denumită dezinfectare. Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere. Pentru mai multe informații, consultați *„Gestionarea fișierelor aflate în carantină"* (p. 102).

În cazul în care calculatorul dumneavoastră a fost infectat cu malware, consultați *„Eliminarea programelor malware din sistemul dumneavoastră"* (p. 194). Pentru a vă ajuta să vă curățați computerul de programele malware care

nu pot fi eliminate din sistemul de operare Windows, Bitdefender vă pune la dispoziție Mediul de recuperare. Acesta este un mediu sigur, creat în special pentru eliminare acțiunilor malware, care vă permite să porniți computerul în mod independent de Windows. Atunci când computerul rulează în Mediul de recuperare, Windows malware este inactiv și, în consecință, poate fi șters cu ușurință.

Pentru a vă proteja împotriva aplicațiilor periculoase, Bitdefender folosește Active Threat Control, o tehnologie euristică avansată care monitorizează în permanență aplicațiile ce rulează pe sistemul dumneavoastră. Active Threat Control blochează în mod automat aplicațiile care prezintă un comportament tipic malware pentru a preveni daunele pe care le pot provoca acestea asupra computerului dumneavoastră. Ocazional, pot fi blocate aplicații legitime. În astfel de situații, puteți configura Active Threat Control să nu blocheze aceste aplicații a doua oară, creând reguli de excludere. Pentru a afla mai multe, consultați *„Active Threat Control”* (p. 103).

15.1. Scanare la accesare (protecție în timp real)

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

Setările implicite de protecție în timp real asigură o bună protecție împotriva malware cu un impact minor asupra performanțelor sistemului. Puteți modifica ușor setările de protecție în timp real în funcție de dorințele dumneavoastră prin comutarea la unul dintre nivelurile de protecție predefinite. Sau, dacă sunteți un utilizator experimentat, puteți configura setările de scanare în detaliu prin crearea unui nivel de protecție personalizat.

15.1.1. Activarea sau dezactivarea protecției în timp real

Pentru a activa sau dezactiva protecția în timp real împotriva programelor periculoase, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Scut**.

4. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea de scanare la accesare.
5. Dacă doriți să dezactivați protecția în timp real, se afișează o fereastră de avertizare. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real. Puteți dezactiva protecția în timp real pentru 5, 15 sau 30 de minute, pentru o oră, permanent sau doar până la repornirea sistemului. Protecția în timp real se va activa automat la expirarea intervalului de timp selectat.

Avertisment

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

15.1.2. Reglarea nivelului de protecție în timp real

Nivelul de protecție în timp real definește setările de scanare pentru acest tip de protecție. Puteți modifica ușor setările de protecție în timp real în funcție de dorințele dumneavoastră prin comutarea la unul dintre nivelurile de protecție predefinite.

Pentru a ajusta nivelul de protecție în timp real, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Scut**.
4. Trageți de cursor de-a lungul scalei pentru a seta nivelul de protecție dorit. Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de protecție care se potrivește mai bine nevoilor dumneavoastră de securitate.

15.1.3. Configurarea setărilor de protecție în timp real

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

Pentru a configura setările de protecție în timp real, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Scut**.
4. Faceți clic pe **Personalizare**.
5. Configurați setările de scanare după cum este nevoie.
6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Informații cu privire la opțiunile de scanare

Aceste informații vă pot fi de folos:

- Dacă nu sunteți familiarizat cu anumiți termeni, verificați-i în glosar. De asemenea, puteți găsi informații utile pe Internet.
- **Opțiuni de scanare pentru fișierele accesate.** Puteți seta Bitdefender să scaneze toate fișierele sau doar aplicațiile scanate (fișiere de program). Scanarea tuturor fișierelor accesate asigură cea mai bună protecție, în timp ce scanarea exclusivă a aplicațiilor poate fi utilizată pentru asigurarea unei performanțe ridicate a sistemului.

  În mod implicit, atât directoarele locale, cât și partajările în rețea fac obiectul scanării la accesare. Pentru performanțe superioare ale sistemului, puteți exclude locațiile din rețea din scanarea la accesare.

  Aplicațiile (sau fișierele de program) sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Această categorie include următoarele extensii de fișiere:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript;

vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

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

  Dacă decideți să utilizați această opțiune, puteți stabili o limită maximă acceptată de mărime pentru arhivele ce vor fi scanate la accesare. Selectați căsuța corespunzătoare și introduceți dimensiunea maximă a arhivei (exprimată în MB).

- **Opțiunile de scanare pentru e-mail și trafic HTTP.** Pentru a împiedica descărcarea fișierelor infectate pe calculatorul dumneavoastră, Bitdefender scanează automat următoarele puncte de intrare:
  - e-mail-uri primite sau trimise
  - Trafic HTTP

  Scanarea traficului web poate încetini puțin navigarea pe internet, însă aceasta va bloca programele malware provenite de pe internet, inclusiv descărcările ascunse.

  Deși nu se recomandă, puteți dezactiva scanarea antivirus e-mail sau web pentru a extinde performanțele sistemului. Dacă dezactivați opțiunile de scanare corespunzătoare, e-mailurile și fișierele primite sau descărcate de pe internet nu vor fi scanate, permițând astfel fișierelor infectate să fie salvate pe calculatorul dumneavoastră. Aceasta nu reprezintă o amenințare majoră deoarece protecția în timp real va bloca programul malware atunci când fișierele infectate sunt accesate (deschise, mutate, copiate sau executate).

- **Scanare sectoare de boot.** Puteți seta Bitdefender să scaneze sectoarele de boot ale hard-discului. Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot. Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.

- **Scanează doar fișierele noi și cele modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.

- **Scanare după keyloggers.** Selectați această opțiune pentru a scana sistemul în vederea identificării aplicațiilor de tip keylogger. Aplicațiile keyloggers înregistrează ceea ce introduceți de pe tastatură și trimit raporte pe Internet către o persoană rău intenționată (hacker). Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.
- **Scanare la pornirea sistemului.** Selectați opțiunea de Scanare la pornirea sistemului pentru a scana sistemul la inițializare, imediat după încărcarea tuturor sistemelor critice. Misiunea acestei caracteristici este de a îmbunătăți detecția virușilor la pornirea sistemului și timpul de încărcare a sistemului dumneavoastră.

Acțiuni luate împotriva atacurilor malware detectate

Puteți configura acțiunile inițiate de protecția în timp real.

Pentru a configura acțiunile, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Scut**.
4. Faceți clic pe **Personalizare**.
5. Selectați secțiunea **Acțiuni** și configurați setările de scanare după caz.
6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Acțiunile de mai jos 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 unei semnături malware din baza de date cu semnături malware a Bitdefender. Bitdefender va încerca în mod automat să elimine codul malware din fișierul infectat și să refacă fișierul original. Această operațiune este denumită dezinfectare.

  Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

Pentru mai multe informații, consultați *„Gestionarea fișierelor aflate în carantină"* (p. 102).

Important
Pentru anumite tipuri de malware, 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 malware. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

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

Mută fișierele în carantină
Mută fișierele detectate în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Pentru mai multe informații, consultați *„Gestionarea fișierelor aflate în carantină"* (p. 102).

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

15.1.4. Restaurarea setărilor implicite

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

Pentru a restabili setările implicite pentru protecția în timp real, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Scut**.
4. Faceți clic pe **Implicit**.

15.2. Scanare la cerere

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

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

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

15.2.1. Scanarea unui fișier sau a unui director pentru detectarea malware

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

15.2.2. Rularea unei scanări rapide

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

Pentru a executa o scanare rapidă, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antivirus**, selectați **Scanare rapidă**.
4. Urmați programul asistent de scanare antivirus pentru a finaliza scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate. Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Sau, mai rapid, faceți clic pe butonul de acțiune **Scanare rapidă** din interfața Bitdefender.

15.2.3. Executarea unei scanări a sistemului

Sarcina de Scanare a sistemului scanează întregul calculator pentru identificarea tuturor tipurilor de programe periculoase care îi amenință securitatea, cum ar fi virușii, aplicațiile spion, adware, rootkiturile și altele.

Notă

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

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

- Asigurați-vă că Bitdefender este actualizat cu semnăturile malware. Scanarea calculatorului folosind semnături vechi poate împiedica Bitdefender să detecteze noi aplicații malițioase descoperite după ultima actualizare efectuată. Pentru mai multe informații, consultați *„Actualizarea permanentă a Bitdefender"* (p. 45).
- Închideți toate programele deschise.

Dacă doriți să scanați anumite locații de pe computer sau pentru a configura opțiunile de scanare, puteți configura și rula o sarcină de scanare personalizată. Pentru mai multe informații, consultați *„Configurarea unei scanări personalizate"* (p. 90).

Pentru a executa o Scanare a sistemului, urmați pașii de mai jos:

1. Faceți clic pe pictograma din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antivirus**, selectați **Scanare sistem**.
4. Urmați programul asistent de scanare antivirus pentru a finaliza scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate. Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

15.2.4. Configurarea unei scanări personalizate

Pentru a configura o scanare antimalware în detaliu și pentru a o lansa, urmați pașii de mai jos:

1. Faceți clic pe pictograma din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antivirus**, selectați **Administrare scanări**.
4. Faceți click pe **Sarcină personalizată nouă**. În fila **Basic** introduceți o denumire pentru scanare și selectați locațiile ce urmează a fi scanate.
5. Dacă doriți să configurați opțiunile de scanare în detaliu, selectați secțiunea **Avansat**. Se afișează o nouă fereastră. Urmați acești pași:
   a. Puteți configura ușor opțiunile de scanare reglând nivelul de scanare. Trageți cursorul deasupra scalei pentru a seta nivelul de scanare dorit. Utilizați descrierea din partea dreaptă a scalei pentru a identifica nivelul de scanare care se potrivește mai bine nevoilor dumneavoastră.

      Utilizatorii avansați pot beneficia în urma ofertelor Bitdefender în ceea ce privește setările de scanare. Pentru a configura în detaliu opțiunile de scanare, faceți clic pe **Personalizare**. La sfârșitul acestei secțiuni, veți găsi informații privitoare la acestea.

b. De asemenea, puteți configura aceste opțiuni generale:

- **Rulează sarcina cu prioritate scăzută .** Reduce prioritatea procesului de scanare. Veți permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va crește.
- **Minimizează Asistent de scanare în bara de sistem .** Minimizează fereastra de scanare în bara de sistem. Faceți dublu-clic pe simbolul Bitdefender pentru a o deschide.
- Specificați acțiunea care trebuie luată în cazul în care nu sunt identificate niciun fel de amenințări.

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

6. Dacă doriți să programați o sarcină de scanare, folosiți butonul **Programare** din fereastra de bază. Selectați una dintre opțiunile corespunzătoare pentru a seta un program:
   - La pornirea sistemului
   - O singură dată
   - Periodic
7. Faceți clic pe **Pornire scanare** și urmați instrucțiunile asistentului de scanare antivirus pentru a finaliza operația de scanare. Procesul de scanare poate dura ceva timp, în funcție de locațiile ce vor fi scanate. După finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.
8. Dacă doriți, puteți relua rapid rularea scanării personalizate anterioare, făcând clic pe înregistrarea corespunzătoare din lista valabilă.

Informații cu privire la opțiunile de scanare

Aceste informații vă pot fi de folos:

- Dacă nu sunteți familiarizat cu anumiți termeni, verificați-i în glosar. De asemenea, puteți găsi informații utile pe Internet.
- **Scanează fișiere.** Puteți seta Bitdefender să scaneze toate tipurile de fișiere sau doar aplicațiile (fișiere de program) only. Scanarea tuturor fișierelor asigură cea mai bună protecție în timp ce scanarea aplicațiilor poate fi utilizată pentru efectuarea unei scanări mai rapide.

  Aplicațiile (sau fișierele de program) sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Această categorie include următoarele

extensii de fișiere: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Opțiuni de scanare a arhivelor.** Arhivele ce conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului dumneavoastră. Codurile periculoase (malware) vă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția în timp real. Cu toate acestea, se recomandă să utilizați această opțiune pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

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

- **Scanare sectoare de boot.** Puteți 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 un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.
- **Scanează memoria.** Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului dumneavoastră.
- **Scanează regiștrii.** Selectați această opțiune pentru a scana cheile de regiștri. Regiștrii Windows sunt o bază de date care stochează setările de configurare și opțiunile pentru componentele sistemului de operare Windows, precum și pentru aplicațiile instalate.
- **Scanează fișiere cookie.** Selectați această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe computerul dumneavoastră.

- **Scanează doar fișierele noi și cele modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
- **Ignoră keyloggeri comerciali.** Selectați această opțiune dacă aveți instalat și folosiți un software comercial de înregistrare taste pe computerul dumneavoastră. Înregistratoarele comerciale de taste sunt software-uri legitime de monitorizare a computerului, a căror funcție de bază este de a înregistra tot ce este tastat pe tastatură.
- **Scanează după rootkituri.** Selectați această opțiune pentru a lansa procesul de scanare pentru identificarea rootkit-urilor și a obiectelor ascunse, cu ajutorul acestui software.

15.2.5. Asistentul de scanare antivirus

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

Notă

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

Pasul 1 - Realizarea scanării

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

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

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

Arhive protejate prin parolă. Atunci când este identificată o arhivă protejată prin parolă, în funcție de setările de scanare, este posibil să fiți rugat să

introduceți parola. Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizați parola. Sunt disponibile următoarele opțiuni:

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

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

Pasul 2 - Selectarea acțiunilor

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

Notă

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

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

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

Aplică acțiunile optime

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

- **Fișiere infectate.** Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date cu semnături malware a Bitdefender. Bitdefender va încerca în mod automat să elimine codul

malware din fișierul infectat și să refacă fișierul original. Această operațiune este denumită dezinfectare.

Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Pentru mai multe informații, consultați *„Gestionarea fișierelor aflate în carantină"* (p. 102).

Important

Pentru anumite tipuri de malware, 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 malware. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

- **Arhive ce conțin fișiere infectate.**

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

Ștergere

Îndepărtează fișierele identificate ca fiind infectate de pe disc.

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

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

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

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

Pasul 3 - Rezumat

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

Faceți clic pe **Închide** pentru a închide fereastra.

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, reporniți sistemul pentru a finaliza procesul de curățare. Pentru mai multe informații și instrucțiuni privind modul de eliminare a programelor malware în mod manual, consultați *„Eliminarea programelor malware din sistemul dumneavoastră"* (p. 194).

15.2.6. Examinarea jurnalelor de scanare

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

Puteți deschide raportul de scanare direct din asistentul de scanare, după ce scanarea a luat sfârșit, apăsând **Afișează jurnal**.

Pentru a verifica un jurnal de scanare sau orice infestare detectată ulterior, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Evenimente** din meniul derulant.

2. În fereastra **Evenimente**, selectați **Antivirus** din meniul derulant corespunzător.

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

3. În lista de evenimente puteți verifica ce operațiuni de scanare au fost realizate recent. Faceți clic pe un eveniment pentru a vizualiza detaliile acestuia.

4. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**. Dacă doriți să reluați aceeași scanare,faceți clic pe butonul **Reluare scanare**.

15.3. Scanarea automată a suporturilor media amovibile

Bitdefender detectează automat unitățile mobile de stocare pe care le conectați la computer și le scanează în fundal. Acest lucru este recomandat pentru a preveni pătrunderea virușilor și a altor aplicații periculoase pe calculatorul dumneavoastră.

Unitățile detectate fac parte din următoarele categorii:

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

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

15.3.1. Cum funcționează?

Când detectează un dispozitiv de stocare amovibil, Bitdefender inițiază scanarea în fundal pentru depistarea programelor periculoase (cu condiția ca scanarea automată să fie activată pentru acel tip de dispozitiv). O pictogramă de scanare Bitdefender se va afișa în tăvița de sistem. Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

Dacă opțiunea Pilot automat este activată, nu veți fi întrerupt de scanare. Scanarea va fi doar înregistrată, iar informații privind scanarea pot fi vizualizate în fereastra Evenimente

Dacă opțiunea Pilot automat este dezactivată:

1. Veți fi notificat prin intermediul unei ferestre pop-up că a fost detectat un nou dispozitiv și că aceasta este scanat.
2. În majoritatea cazurilor, Bitdefender elimină automat programele periculoase detectate sau izolează fișierele infectate în carantină. Dacă există amenințări nesoluționate după finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

   Notă
   Luați 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.

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

Următoarele informații vă pot fi de folos:

- Vă rugăm să acordați atenție maximă atunci când folosiți un CD/DVD infectat cu programe malware, deoarece un program malware nu poate fi șters de pe CD/DVD (suportul media este de tip read-only). Asigurați-vă că protecția în timp real este activată pentru a preveni răspândirea acțiunilor periculoase în cadrul sistemului Cea mai bună metodă este să copiați datele inmportante de pe CD pe sistemul dumneavoastră și apoi să aruncați CD-ul.
- Există posibilitatea ca, în unele cazuri, Bitdefender să nu poată elimina elementele periculoase 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 să procedați în cazul programelor periculoase, consultați *„Eliminarea programelor malware din sistemul dumneavoastră”* (p. 194).

15.3.2. Administrarea scanării a fișierelor media amovibile

Pentru a gestiona suporturile media amovibile, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Excepții**.

Pentru cea mai bună protecție, este recomandat să activați funcția de scanare automată pentru toate tipurile de dispozitive de stocare amovibile.

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 periculos) sau să le mute în carantină. Dacă ambele acțiuni eșuează, asistentul de scanare Antivirus vă va permite să specificați alte acțiuni pentru a fi aplicate în cazul fișierelor infectate. Opțiunile de scanare sunt standard și nu le puteți modifica.

15.4. Configurarea excepțiilor de la scanare

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

Puteți configura ca excepțiile să se aplice doar în cazul scanării la accesare sau scanării la cerere, sau în cazul ambelor scanări. Obiectele excluse de la scanarea la acces nu vor fi scanate, indiferent dacă acestea sunt accesate de către dumneavoastră sau de către o aplicație.

Notă

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

15.4.1. Excluderea fișierelor sau directoarelor de la scanare

Pentru a exclude anumite fișiere sau directoare de la scanare, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus**.
4. În fereastra **Antivirus**, selectați secțiunea **Excluderi**.
5. Pentru a activa excepțiile pentru fișiere, utilizați comutatorul corespunzător.
6. Faceți clic pe link-ul **Fișiere și directoare excluse**. În fereastra care va apărea, puteți administra fișierele și directoarele excluse de la scanare.
7. Pentru a adăuga excepții, urmați pașii de mai jos:
   a. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
   b. Faceți clic pe **Caută**, selectați fișierul sau directorul care doriți să fie exclus de la scanare și faceți clic pe **OK**. Ca o alternativă, puteți introduce (sau copia și lipi) calea către fișier sau director în câmpul editabil.
   c. În mod implicit, fișierul sau directorul selectat este exclus atât de la scanarea la accesare cât și de la scanarea la cerere. Pentru a modifica când anume se aplică aceste excepții, selectați una dintre celelalte opțiuni.
   d. Faceți clic pe **Adaugă**.
8. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

15.4.2. Excluderea extensiilor de fișiere de la scanare

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
Acționați cu grijă atunci când excludeți extensii de la scanare deoarece asemenea excepții pot face computerul vulnerabil în fața acțiunilor periculoase.

Pentru a exclude de la scanare extensii de fișiere, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus**.
4. În fereastra **Antivirus**, selectați secțiunea **Excluderi**.
5. Pentru a activa excepțiile pentru fișiere, utilizați comutatorul corespunzător.
6. Faceți clic pe link-ul **Extensii excluse** În fereastra care va apărea, puteți administra extensiile de fișiere excluse de la scanare.
7. Pentru a adăuga excepții, urmați pașii de mai jos:
   a. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
   b. Introduceți extensiile ce doriți 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, selectați una dintre celelalte opțiuni.
   d. Faceți clic pe **Adaugă**.
8. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

15.4.3. Administrarea excepțiilor de la scanare

Dacă excluderile de la scanare configurate nu mai sunt necesare, se recomandă să le ștergeți sau să dezactivați utilizarea lor.

Pentru a gestiona excepțiile de la scanare, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Excepții**. Folosiți opțiunile din secțiune **Fișiere și directoare** pentru a gestiona excepțiile de la scanare.
4. Pentru a șterge sau a edita excepțiile de la scanare, faceți clic pe unul dintre link-urile disponibile. Procedați astfel:
   - Pentru a șterge o intrare din tabel, selectați-o și faceți clic pe butonul **Șterge**.
   - Pentru a edita o intrare din table, faceți dublu clic pe aceasta (sau selectați-o și faceți clic pe butonul **Editare**). Apare o nouă fereastră unde puteți schimba extensia sau calea care va fi exclusă, precum și tipul de scanare de la care acestea să fie excluse. Efectuați modificările necesare, apoi faceți clic pe **Modifică**.
5. Pentru a dezactiva excepțiile de la scanare, utilizați comutatorul corespunzător.

15.5. Gestionarea fișierelor aflate în carantină

Bitdefender izolează fișierele infectate cu malware ce nu pot fi dezinfectate, precum și fișierele suspecte într-o zonă sigură numită carantină. Atunci când sunt în carantină virușii sunt inofensivi, pentru că nu pot fi executați sau citiți.

Implicit, fișierele aflate în carantină sunt trimise automat către Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender în materie de malware. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

În plus, Bitdefender scanează fișierele din carantină după fiecare actualizare a semnăturilor malware. Fișierele curățate sunt mutate automat în locația lor originală.

Pentru a verifica și administra fișierele aflate în carantină, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.

2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Carantină**.
4. Fișierele aflate în carantină sunt gestionat în mod automat de Bitdefender, în funcție de setările implicite pentru carantină. Deși nu este recomandat, puteți ajusta setările carantinei în funcție de preferințele dumneavoastră.

   Rescanează carantina după actualizarea definițiilor de viruși
   Mențineți activată această opțiune pentru a scana în mod automat fișiere aflate în carantină după fiecare actualizare a definițiilor de viruși Fișierele curățate sunt mutate automat în locația lor originală.

   Trimiteți fișierele suspecte din carantină pentru o analiză ulterioară
   Mențineți această opțiune activată pentru ca fișierele aflate în carantină să fie trimise automat către Laboratoarele Bitdefender. Fișierele mostră vor fi analizate de către cercetătorii Bitdefender în materie de malware. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

   Ștergere conținut mai vechi de {30} zile
   Implicit, fișierele aflate în carantină de mai mult de 30 de zile sunt șterse automat. Dacă doriți să schimbați acest interval, introduceți o nouă valoare în câmpul corespunzător. Pentru a dezactiva ștergerea fișierelor vechi aflate în paranteză, introduceți 0.
5. Pentru a șterge un fișier aflat în carantină, selectați-l și faceți clic pe butonul **Șterge**. Dacă doriți să restaurați un fișier aflat în carantină în locația sa originală, selectați-l și faceți clic pe **Restaurează**.

15.6. Active Threat Control

Bitdefender Active Threat Control este o tehnologie inovatoare de detecție proactivă, care folosește metode euristice avansate pentru a detecta potențiale amenințări în timp real.

Modulul Active Threat Control monitorizează continuu aplicațiile care rulează pe calculatorul dumneavoastră, căutând acțiuni periculoase. Fiecare dintre aceste acțiuni are un anumit punctaj iar punctajul global este calculat pentru fiecare proces. În cazul în care scorul total pentru un proces atinge un anumit prag, procesul este considerat dăunător și este blocat în mod automat.

Dacă funcția de Pilot automat este dezactivată, veți fi notificat prin intermediul unei ferestre pop-up despre aplicația blocată. În caz contrar,

aplicația va fi blocată fără nicio notificare în prealabil. Puteți verifica ce aplicații au fost detectate de Active Threat Control, în fereastra Evenimente.

15.6.1. Verificarea aplicațiilor detectate

Pentru a verifica aplicațiile detectate de Active Threat Control, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Evenimente** din meniul derulant.
2. În fereastra **Evenimente**, selectați **Antivirus** din meniul derulant corespunzător.
3. Faceți clic pe un eveniment pentru a vizualiza detaliile acestuia.
4. Dacă considerați că aplicația este sigură, puteți configura ca Active Threat Control să nu o mai blocheze pe viitor, făcând clic pe **Permite și monitorizează**. Active Threat Control va monitoriza în continuare aplicațiile excluse. Dacă sunt detectate acțiuni suspecte efectuate de o aplicație exclusă, acest eveniment va fi înregistrat și raportat către Bitdefender Cloud ca eroare de detecție.

15.6.2. Activarea sau dezactivarea funcției Active Threat Control

Pentru a activa sau dezactiva funcția Active Threat Control, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus**.
4. În fereastra **Antivirus**, selectați secțiunea **Protecție**.
5. Faceți clic pe buton pentru a activa sau dezactiva opțiunea Active Threat Control.

15.6.3. Ajustarea protecției Active Threat Control

În cazul în care Active Threat Control detectează adesea aplicații legitime, încercați să setați un nivel de protecție mai permisiv.

Pentru a ajusta protecția Active Threat Control, trageți de cursor de-a lungul scalei pentru a seta nivelul de protecție dorit.

Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de protecție care se potrivește mai bine nevoilor dumneavoastră de securitate.

Notă
După ce setați un nivel de protecție superior, Active Threat Control va necesita mai puține semne de comportament tipic malware pentru a raporta un anumit proces. Acest lucru va contribui la raportarea unui număr mai mare de aplicații și, în același timp, la o probabilitate sporită de false pozitive (aplicații legitime detectate ca fiind nocive).

15.6.4. Administrarea proceselor excluse

Puteți configura regulile de excludere pentru aplicațiile sigure astfel încât Active Threat Control să nu blocheze aceste aplicații în cazul în care acestea întreprind acțiuni ce pot părea periculoase. Active Threat Control va monitoriza în continuare aplicațiile excluse. Dacă sunt detectate acțiuni suspecte efectuate de o aplicație exclusă, acest eveniment va fi înregistrat și raportat către Bitdefender Cloud ca eroare de detecție.

Pentru a gestiona excepțiile de la procesul Active Threat Control, urmați pașii de mai jos:

1. Faceți clic pe pictograma din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Excepții**.
4. Faceți clic pe link-ul **Procese excluse**. În fereastra care va apărea, puteți gestiona excepțiile de la procesul Active Threat Control.

   Notă
   Excepțiile se aplică și în cazul Modulului de detecție a intruziunilor.

5. Pentru a adăuga excepții, urmați pașii de mai jos:
   a. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.

b. Faceți clic pe **Caută**, identificați și selectați aplicația care doriți să fie exclusă și faceți clic pe **OK**.

c. Mențineți selectată opțiunea **Permite** pentru a preveni blocarea aplicației de către Active Threat Control.

d. Faceți clic pe **Adaugă**.

6. Pentru a șterge sau pentru a edita excepțiile, urmați pașii de mai jos:

   - Pentru a șterge un obiect din listă, selectați-l și faceți clic pe butonul **Șterge**.
   - Pentru a edita o intrare din tabel, faceți dublu clic pe aceasta (sau selectați-o) și faceți clic pe butonul **Modificare**. Efectuați modificările necesare, apoi faceți clic pe **Modifică**.

7. Salvați schimbarea și închideți fereastra.

16. ANTISPAM

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

Bitdefender Antispam utlizează remarcabile inovații tehnologice și filtre antispam standard pentru a ține la distanță spamul de căsuțele de mesaje ale utilizatorilor. Pentru mai multe informații, consultați *„Detalii privind modulul Antispam"* (p. 108).

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

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

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

- În Microsoft Outlook, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Deleted Items**. Directorul **Spam** este creat în timpul instalării Bitdefender.
- În Outlook Express și Windows Mail, mesajele spam sunt mutate direct în **Deleted Items**.
- În Mozilla Thunderbird, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Trash**. Directorul **Spam** este creat în timpul instalării Bitdefender.

Dacă utilizați alt client de mail, trebuie să creați o regulă pentru a muta mesajele e-mail marcate ca [spam] de Bitdefenderîntr-un anumit director de carantină.

16.1. Detalii privind modulul Antispam

16.1.1. Filtrele Antispam

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

Lista de prieteni/Lista de spanmmeri

Majoritatea oamenilor comunică în mod regulat cu un grup de cunoștințe sau chiar primesc mesaje de la companii sau organizații cu același domeniu de activitate. Prin utilizarea **listei de prieteni sau de spammeri**, puteți clasifica ușor persoanele de la care doriți să primiți e-mail-uri (prieteni) indiferent de conținutul mesajului sau persoanele de la care nu mai doriți să primiți deloc mesaje (spammeri).

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

Filtrul de caractere

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

16.1.2. Funcționarea Antispam

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

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

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

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

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

16.1.3. Clienți și protocoale de e-mail compatibile

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

- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express și Windows Mail (pe sisteme de 32 bit)
- Mozilla Thunderbird 3.0.4

16.2. Activarea sau dezactivarea protecției antispam

Protecția antispam este activată implicit.

Pentru a dezactiva modulul antispam, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antispam** și apoi pe buton pentru activa sau dezactiva opțiunea **Antispam**.

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

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

Important

Bitdefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, consultați *„Clienți și protocoale de e-mail compatibile"* (p. 109).

Fiecare buton al barei de comenzi este explicat mai jos:

Setări - deschide o fereastră în care puteți configura filtrele antispam și setările barei de instrumente.

Este Spam - indică faptul că mesajul e-mail selectat este spam. Mesajul e-mail va fi mutat imediat în directorul **Spam**. Dacă serviciile antispam cloud sunt activate, mesajul va fi trimis către Bitdefender Cloud pentru a fi analizat în detaliu.

Nu este spam - indică faptul că mesajele e-mail selectate nu sunt de tip spam și Bitdefender nu ar fi trebuit să le eticheteze astfel. E-mailul va fi mutat din directorul **Spam** în directorul **Inbox** (Mesaje primite). Dacă serviciile antispam cloud sunt activate, mesajul va fi trimis către Bitdefender Cloud pentru a fi analizat în detaliu.

Important

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

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

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

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

Prieteni - deschide **lista de prieteni** care conține adrese de e-mail de la care doriți întotdeauna să primiți mesaje, indiferent de conținutul acestora. Pentru mai multe informații, consultați *„Configurarea listei de prieteni"* (p. 112).

16.3.1. Indicarea erorilor de detecție

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

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

16.3.2. Indicarea mesajelor spam nedetectate

Dacă folosiți un client de mail admis, puteți indica cu ușurință care mesaje e-mail ar fi trebuit detectate ca spam. Astfel, veți îmbunătăți eficiența filtrului antispam. Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți la directorul Inbox.
3. Selectați mesajele spam nedetectate.
4. Faceți clic pe butonul **Spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail). Acestea sunt marcate imediat ca [spam] și mutate în directorul de mesaje nesolicitate (junk).

16.3.3. Configurarea setărilor barei de instrumente

Pentru a configura setările barei de instrumente antispam pentru clientul de e-mail, faceți clic pe butonul **Setări** din bara de instrumente și apoi pe fila **Setări bară din instrumente**

Aici aveți la dispoziție următoarele opțiuni:

- **Mută mesajul la Obiecte șterse** (doar pentru Microsoft Outlook Express / Windows Mail)

  Notă
  În Microsoft Outlook / Mozilla Thunderbird, mesajele de tip spam detectate sunt mutate automat în directorul Spam, localizat în directorul Elemente șterse / Reciclare.

- **Marchează e-mail-urile spam ca 'citite'** - marchează, în mod automat, mesajele e-mail de tip spam ca fiind citite, astfel încât să nu fiți deranjat la primirea unui astfel de mesaj.
- Puteți alege dacă să fie afișate sau nu ferestrele de confirmare când faceți clic pe butoanele **Adaugă Spammer** și **Adaugă prieten** din bara de instrumente antispam.

  Ferestrele de confirmare pot preveni adăugarea accidentală a expeditorilor de mesaje e-mail la lista de prieteni/contacte care trimit mesaje spam.

16.4. Configurarea listei de prieteni

Lista de Prieteni este o listă care conține toate adresele de e-mail de la care doriți să primiți mesaje, indiferent de conținutul acestora. Mesajele de la prieteni nu vor fi etichetate ca Spam, chiar dacă au conținut asemănător mesajelor Spam.

Notă
Orice mesaj venit de la o adresă inclusă pe **lista de prieteni** va fi trimis automat în directorul Inbox, fără a mai fi procesat.

Pentru a configura și administra lista de prieteni:

- Dacă utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, faceți clic pe butonul **Prieteni** de pe bara de instrumente antispam Bitdefender
- Alternativ, urmați acești pași:

  1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
  2. Selectați secțiunea **Protecție**.
  3. În modulul **Antispam**, selectați **Administrare prieteni**.

Pentru a adăuga o adresă de e-mail, selectați opțiunea **Adresă e-mail**, introduceți adresa și apoi faceți clic pe **Adaugă**. Sintaxă: nume@domeniu.com.

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectați opțiunea **Nume domeniu**, introduceți numele domeniului și faceți clic pe **Adaugă**. Sintaxă:

- @domeniu.com, *domeniu.com și domeniu.com - toate mesajele primite de la domeniu.com vor ajunge în directorul **Inbox** indiferent de conținut;
- *domeniu* - toate mesajele primite de la domeniu (indiferent de sufixul domeniului) vor ajunge în directorul **Inbox** indiferent de conținut;
- *com - toate mesajele primite având sufixul domeniului com vor ajunge în directorul **Inbox** indiferent de conținut;

Se recomandă să evitați adăugarea de domenii, însă acest lucru poate fi util în anumite situații. De exemplu, puteți adăuga domeniul de e-mail al companiei pentru care lucrați sau pe cele ale partenerilor dumneavoastră de încredere.

Pentru a șterge un element de pe listă, faceți clic pe link-ul **Elimină** corespunzător. Pentru a șterge toate înregistrările din listă, faceți clic pe butonul **Ștergere listă**.

Puteți salva Lista de prieteni într-un fișier, astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului. Pentru a salva Lista de prieteni, faceți clic pe butonul **Salvează** și salvați-o în locația dorită. Fișierul va avea extensia .bwl.

Pentru a încărca o Listă de prieteni salvată anterior, faceți clic pe butonul **Încarcă** și deschideți fișierul .bwl corespunzător. Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior, selectați **Suprascrie lista curentă**.

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

16.5. Configurarea listei de spammeri

Lista de spammeri este o listă care conține toate adresele de e-mail de la care nu doriți să primiți mesaje, indiferent de conținutul acestora. Orice mesaj primit de la o adresă din **lista de spammeri** va fi automat etichetat ca Spam, fără altă procesare.

Pentru a configura și administra lista de spammeri:

- Dacă utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, faceți clic pe butonul **Spammeri** de pe bara de instrumente antispam Bitdefender integrată în clientul dumneavoastră de e-mail.
- Alternativ, urmați acești pași:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antispam**, selectați **Administrare spammeri**.

Pentru a adăuga o adresă de e-mail, selectați opțiunea **Adresă e-mail**, introduceți adresa și apoi faceți clic pe **Adaugă**. Sintaxă: nume@domeniu.com.

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectați opțiunea **Nume domeniu**, introduceți numele domeniului și faceți clic pe **Adaugă**. Sintaxă:

- @domeniu.com, *domeniu.com și domeniu.com - toate mesajele primite de la domeniu.com vor fi etichetate ca SPAM;
- *domeniu* - toate mesajele primite de la domeniu (indiferent de sufixul domeniului) vor fi etichetate ca SPAM;
- *com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate ca SPAM.

Se recomandă să evitați adăugarea de domenii, însă acest lucru poate fi util în anumite situații.

Avertisment

Nu adăugați nume de domenii legitime ale unor servicii de e-mail bazate pe web (Yahoo, Gmail, Hotmail sau altele asemenea) pe Lista de spammeri. În caz contrar, mesajele e-mail primite de la orice utilizator înregistrat al unui astfel de serviciu va fi detectat ca spam. Dacă, de exemplu, adăugați yahoo.com pe Lista de spammeri, toate mesajele e-mail care provin de la adrese yahoo.com vor fi marcate ca [spam].

Pentru a șterge un element de pe listă, faceți clic pe link-ul **Elimină** corespunzător. Pentru a șterge toate înregistrările din listă, faceți clic pe butonul **Ștergere listă**.

Puteți salva Lista de spammeri într-un fișier astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului. Pentru a salva Lista de

spammeri, faceți clic pe butonul **Salvează** și salvați-o în locația dorită. Fișierul va avea extensia .bwl.

Pentru a încărca o Listă de spammeri salvată anterior, faceți clic pe butonul **Încarcă** și deschideți fișierul .bwl corespunzător. Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior, selectați **Suprascrie lista curentă**.

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

16.6. Se configurează filtrele locale antispam

Conform descrierii de la *„Detalii privind modulul Antispam"* (p. 108), Bitdefender utilizează o combinație de diferite filtre antispam pentru a identifica mesajele spam. Filtrele antispam sunt preconfigurate pentru asigurarea unei protecții eficiente.

Important

Dacă primiți e-mailuri legitime scrise cu caractere asiatice sau chirilice, dezactivați setarea care blochează în mod automat aceste e-mailuri. Setarea corespunzătoare este dezactivată pentru versiunile localizate ale programului care utilizează astfel de seturi de caractere (de exemplu, în cazul versiunii în limba rusă sau chineză).

Pentru a configura filtrele locale antispam, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antispam** și apoi pe butoane pentru activa sau dezactiva filtrele antispam locale.

În cazul în care utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, puteți configura filtrele locale antispam direct din clientul de e-mail. Faceți clic pe butonul **Setări** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail) și apoi pe fila **Filtre antispam**.

16.7. Configurarea setărilor cloud

Detecția cloud folosește serviciile Bitdefender Cloud pentru a vă oferi protecție antispam eficientă și întotdeauna actualizată.

Protecția cloud funcționează cât timp funcția Antispam a Bitdefender este menținută activă.

Mostre de mesaje e-mail legitime și de tip spam pot fi trimise către Bitdefender Cloud în cazul în care identificați erori de detecție sau mesaje e-mail de tip spam nedetectate. Acest lucru vă ajută să îmbunătățiți rata de detecție antispam a Bitdefender.

Configurați trimiterea mostrelor de e-mail către Bitdefender Cloud, selectând opțiunile dorite și urmărind pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antispam** și apoi selectați opțiunile dorite din secțiunea **Setări**.

În cazul în care utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, puteți configura detecția cloud direct de la clientul dumneavoastră de e-mail. Faceți clic pe butonul **Setări** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail) și apoi pe fila **Setări Cloud**.

17. PROTECȚIE WEB

Protecția web Bitdefender asigură o experiență de navigare sigură informându-vă cu privire la poibilele pagini web care includ tentative de phishing.

Bitdefender oferă protecție în timp real pentru:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Pentru a configura setările de protecție pe Internet, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Protecție web**.

Faceți clic pe comutatoare pentru a activa sau dezactiva:

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

  Nu este recomandat să vizitați această pagină web.

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

  Această pagină este sigură.

  Funcția de Asistență pentru căutare clasifică rezultatele generate de următoarele motoare de căutare:
  - Google
  - Yahoo!
  - Bing
  - Baidu

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

- Scanarea traficului web SSL

  Atacurile mai sofisticate pot folosi trafic de web securizat pentru a induce în eroare victimele. Așadar, este recomandat să activați scanarea SSL.

- Protecție împotriva fraudelor.
- Protecție împotriva tentativelor de phishing.

Puteți crea o listă de site-uri care nu vor fi scanate de motoarele contra programelor periculoase, tentativelor de phishing și antifraudă Bitdefender. Este recomandat ca lista să conțină doar site-uri web în care aveți deplină încredere. De exemplu, adăugați site-urile web de unde cumpărați produse online.

Pentru a configura și administra site-urile web folosind protecția web oferită de Bitdefender, faceți clic pe link-ul **Listă albă**. Se afișează o nouă fereastră.

Pentru a adăuga un site pe lista albă, introduceți adresa acestuia în câmpul corespunzător și faceți clic pe **Adăugă**.

Pentru a șterge un site web din listă, selectați-l din listă și faceți clic pe link-ul corespunzător **Ștergere**.

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

17.1. Alertele Bitdefender sunt afișate în browser

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

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

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

- Navigați în afara paginii făcând clic pe **Revenire la pagina securizată**.
- Dezactivați blocarea paginilor ce pot conține tentative de phishing făcând clic pe **Dezactivare filtru antiphishing**.
- Dezactivați blocarea paginilor ce pot conține programe periculoase făcând clic pe **Dezactivare filtru antimalware**.
- Adăugați pagina la lista albă Antiphishing făcând clic pe **Adaugă pe lista albă**. Pagina nu va mai fi scanată de motoarele Bitdefender Antiphishing.

- Vizitați pagina web în ciuda avertismentului, făcând clic pe **Înțeleg riscurile, vreau să continui oricum**.

18. PROTECȚIE DATE

18.1. Ștergerea permanentă a fișierelor

Atunci când ștergeți un fișier, acesta nu mai poate fi accesat prin mijloace normale. Cu toate acestea, fișierul continuă să existe pe hard disc până ce este suprascris prin copierea altor fișiere.

Opțiunea de ștergere definitivă a fișierelor Bitdefender vă permite să ștergeți definitiv date prin eliminarea fizică a acestora de pe hard disk.

Puteți șterge definitiv și rapid fișiere și directoare din computerul dumneavoastră, cu ajutorul meniul contextual Windows, urmând pașii de mai jos:

1. Faceți clic dreapta pe un fișier sau director pe care doriți să-l ștergeți definitiv.
2. Selectați **Bitdefender** > **Ștergere definitivă fișiere** din meniul contextual afișat.
3. Va apărea o fereastră de confirmare. Faceți clic pe **Da** pentru a porni asistentul Ștergere definitivă fișiere.
4. Așteptați ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.
5. Sunt afișate rezultatele. Faceți clic pe **Închide** pentru a părăsi asistentul.

Ca alternativă, puteți șterge definitiv fișierele din interfața Bitdefender.

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. În modulul **Protecție date**, selectați **Distrugere fișiere**.
4. Urmați pașii asistentului de ștergere definitivă a fișierelor:
   a. **Adaugă director**

      Adăugați fișierele sau directoarele pe care doriți să le ștergeți definitiv.

   b. Faceți clic pe **Next** și confirmați că doriți să continuați procesul.

      Așteptați ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.

   c. **Rezultate**

Sunt afișate rezultatele. Faceți clic pe **Închide** pentru a părăsi asistentul.

19. VULNERABILITĂȚI

Un pas important în protejarea calculatorului dumneavoastră împotriva acțiunilor și aplicațiilor periculoase este de a menține actualizat sistemul de operare și aplicațiile pe care le utilizați în mod regulat. Ar trebui, de asemenea, să luați în considerare dezactivarea setărilor Windows, care fac sistemul mai vulnerabil în fața programelor periculoase. De asemenea, pentru a preveni accesul fizic neautorizat la calculatorul dumneavoastră, trebuie configurate parole puternice (parole care nu pot fi ghicite cu ușurință) pentru fiecare cont de utilizator Windows.

Bitdefender verifică automat dacă există vulnerabilități în sistemul dumneavoastră și vă informează în legătură cu acestea. În categoria vulnerabilităților sistemului intră:

- aplicațiile neactualizate de pe calculatorul dvs.
- actualizări Windows lipsă.
- parolele simple ale conturilor de utilizator Windows.

Bitdefender permite remedierea cu ușurință a vulnerabilităților sistemului dumneavoastră prin oricare dintre cele două metode de mai jos:

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

Ar trebui să verificați și să remediați vulnerabilitățile sistemului săptămânal sau o dată la două săptămâni.

19.1. Scanarea sistemului pentru identificarea vulnerabilităților

Pentru a remedia vulnerabilitățile sistemului folosind opțiunea Scanare vulnerabilități, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Vulnerabilitate**, selectați **Scanare vulnerabilitate**.

4. Așteptați până când Bitdefender finalizează verificarea sistemului dvs. pentru descoperirea vulnerabilităților. Pentru a opri procesul de scanare, faceți clic pe butonul**Sari peste** din partea de sus a ferestrei.

   Sau, mai rapid, faceți clic pe butonul de acțiune **Scanare vulnerabilități** din interfața Bitdefender.

   - **Actualizări Windows importante**

     Faceți clic pe **Vizualizare detalii** pentru a vedea o listă a actualizărilor Windows critice care nu sunt instalate în prezent pe calculatorul dvs.

     Pentru a începe instalarea actualizărilor selectate, faceți clic pe **Instalare actualizări**. Rețineți că este posibil ca instalarea actualizărilor să dureze ceva timp iar pentru unele dintre ele poate fi necesară repornirea sistemului pentru ca instalarea să se finalizeze. Dacă este necesar, reporniți sistemul cât mai curând posibil.

   - **Actualizări aplicații**

     Dacă o aplicație nu este la zi, faceți clic pe link-ul **Descărcare versiune nouă** pentru a descărca versiunea ce mai recentă.

     Faceți clic pe **Vizualizare detalii** pentru a vedea informații referitoare la aplicația care trebuie actualizată.

   - **Parole slabe pentru contul Windows**

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

     Faceți clic pe **Modificare parolă la autentificare** pentru a seta o nouă parolă pentru sistemul dvs.

     Faceți clic pe **Vizualizare detalii** pentru a modifica parolele slabe. Puteți să-i solicitați utilizatorului să schimbe parola la următoarea autentificare sau puteți schimba dumneavoastră parola imediat. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

În colțul din dreapta sus a ferestrei puteți filtra rezultatele după preferințe.

19.2. Cu ajutorul monitorizării automate a vulnerabilităților

Bitdefender scanează sistemul împotriva vulnerabilităților la intervale regulate, în fundal și păstrează înregistrări ale problemelor detectate în fereastra Evenimente.

Pentru a verifica și remedia problemele detectate, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Evenimente** din meniul derulant.
2. În fereastra **Evenimente**, selectați **Vulnerabilitate** din lista Selectare evenimente.
3. Puteți vizualiza informații detaliate cu privire la vulnerabilitățile sistemului detectate. În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedați după cum urmează:
   - Dacă sunt disponibile actualizări Windows, faceți clic pe **Actualizează acum**.
   - Dacă actualizarea automată Windows este dezactivată, faceți clic **Activare**.
   - Dacă o aplicație nu este actualizată, faceți clic pe **Actualizează acum** pentru a găsi un link către pagina furnizorului, de unde puteți instala cea mai recentă versiune a aplicației respective.
   - Dacă un cont de utilizator Windows are o parolă slabă, faceți clic pe **Modificare parolă** pentru a forța utilizatorul să modifice parola la următoarea conectare sau schimbați-o chiar dumneavoastră. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).
   - Dacă funcția de executare automată Windows este activată, faceți clic pe **Remediere** pentru a o dezactiva.

Pentru a configura setările de monitorizare a vulnerabilităților, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.

3. Faceți clic pe modulul **Vulnerabilitate**.
4. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea de scanare a Vulnerabilităților.

> **Important**
> Pentru a primi informări automate cu privire la vulnearibilitățile sistemului sau aplicației, mențineți opțiunea **Scanare vulnerabilitate** activată.

5. Selectați vulnerabilitățile sistemului care doriți să fie verificate în mod regulat, cu ajutorul comutatoarelor corespunzătoare.

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

   Actualizări aplicații
   Verificați dacă aplicațiile instalate pe sistemul dvs. sunt actualizate. Aplicațiile neactualizate pot fi exploatate de software-uri periculoase, expunându-vă computerul la atacuri din exterior.

   Parole slabe
   Verificați dacă parolele pentru conturile de Windows configurate pe sistem sunt ușor de descoperit sau nu. Setând parole care sunt greu de ghicit (parole puternice), va fi mai mult mai dificil pentru hackeri să pătrundă în sistemul dumneavoastră. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

   Executare automată a fișierelor media
   Verificați starea caracteristicii de executare automată Windows. Această caracteristică permite pornirea aplicațiilor în mod automat direct de pe CD, DVD, unități USB sau alte dispozitive externe.

   Anumite tipuri programe periculoase folosesc funcția de executare automată pentru a se răspândi de la suporturile media amovibile în computer. De aceea se recomandă să dezactivați această caracteristică Windows.

> **Notă**
> Dacă dezactivați monitorizarea pentru o anumită vulnerabilitate, posibilele probleme aferente nu vor mai fi înregistrate în fereastra Evenimente.

20. FIREWALL

Firewall-ul vă protejează calculatorul contra tentativelor de conectare interne și externe neautorizate, atât în rețele locale, cât și pe Internet. Este asemănător unui paznic - ține evidența tentativelor de conectare și decide pe care să le permite și pe care să le blocheze.

Firewall-ul Bitdefender folosește un set de reguli pentru a filtra datele transmise către și de la sistemul dumneavoastră. Regulile sunt grupate în 2 categorii:

Reguli generale
: Reguli care determină protocoalele pe care este permisă comunicarea.

  Este utilizat un set de reguli implicite care oferă o protecție optimă. Puteți edita regulile permițând sau respingând conexiunile față de anumite protocoale.

Reguli privind aplicația
: Reguli care determină modul în care fiecare aplicație poate accesa internetul și resursele rețelei.

  În condiții normale, Bitdefender creează în mod automat o regulă de fiecare dată când o aplicație încearcă să acceseze internetul. De asemenea, puteți edita sau adăuga manual reguli pentru aplicații.

Bitdefender alocă automat un nou tip fiecărei conexiuni la rețea detectate. În funcție de tipul de rețea, protecția firewall este setată la nivelul corespunzător pentru fiecare conexiune.

Pentru a afla mai multe despre setările firewall pentru fiecare tip de rețea și despre modul în care puteți edita setările rețelei, consultați *„Administrarea setărilor de conectare"* (p. 131).

20.1. Activarea sau dezactivarea protecției firewall.

Pentru a activa sau dezactiva protecția firewall, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Firewall** și apoi pe butonul Firewall.

Avertisment

Deoarece vă expune computerul unor conexiuni neautorizate, dezactivarea firewallului trebuie să fie doar o măsură temporară. Reactivați firewall-ul cât mai repede posibil.

20.2. Administrarea regulilor firewall

20.2.1. Reguli generale

De fiecare dată când sunt transmise date prin interne, sunt folosite anumite protocoale.

Regulile generale vă permit să configurați protocoalele pe care este permis traficul. În mod implicit, regulile generale nu sunt afișate atunci când deschideți Firewall-ul. Pentru a edita regulile, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Firewall**.
4. În fereastra **Firewall**, selectați secțiunea **Reguli**.
5. Bifați caseta **Afișare reguli generale** din colțul din stânga jos al ferestrei.

Sunt afișate regulile implicite. Pentru a modifica prioritatea unei reguli, faceți clic pe săgeata corespunzătoare din coloana **Permisiune** și selectați **Permite** sau **Respinge**.

DNS față de UDP / TCP
Permite sau respinge DNS față de UDP și TCP.

În mod implicit, acest tip de conexiune este permis.

Trimitere mesaje e-mail
Permite sau respinge trimiterea de mesaje e-mail prin SMTP.

În mod implicit, acest tip de conexiune este permis.

Navigare internet HTTP
Permite sau respinge navigare web HTTP.

În mod implicit, acest tip de conexiune este permis.

ICMP / ICMPv6 în curs de recepționare
Permite sau respinge mesajele ICMP / ICMPv6.

Mesajele ICMP sunt folosite adesea de hackeri pentru a lansa atacuri asupra rețelelor computerului. În mod implicit, acest tip de conexiune nu este permis.

Conexiuni desktop de la distanță în curs de recepționare
Permite sau respinge accesul altor computere la conexiunile desktop de la distanță.

În mod implicit, acest tip de conexiune este permis.

Trafic Windows Explorer pe HTTP / FTP
Permite sau respinge traficul HTTP sau FTP de la Windows Explorer.

În mod implicit, acest tip de conexiune nu este permis.

20.2.2. Reguli privind aplicațiile

Pentru a vizualiza și a administra regulile pentru firewall, ce controlează accesul aplicațiilor la resursele rețelei și la internet, urmați acești pași:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Firewall**.
4. În fereastra **Firewall**, selectați secțiunea **Reguli**.

Puteți vedea în tabel programele (procesele) pentru care au fost create reguli firewall. Pentru a vizualiza regulile create pentru o anumită aplicație, pur și simplu faceți dublu clic pe ea.

Pentru fiecare regulă sunt afișate următoarele informații:

- **Denumire** - denumirea procesului pentru care se aplică regulile.
- **Tip de rețea** - procesul și tipul de adaptor de rețea cărora li se aplică regula. Regulile sunt create automat pentru a filtra accesul la rețea sau Internet prin oricare adaptor. În mod implicit, regula se aplică oricărei rețele. Pentru a filtra accesul aplicațiilor la rețea și Internet printr-un anumit adaptor (de exemplu, printr-un adaptor de rețea wireless), puteți crea reguli manual sau puteți edita regulile existente.

- **Protocol** - protocolul IP căruia i se aplică regula. În mod implicit, regula se aplică oricărui protocol.
- **Permisiune** - dacă aplicației îi este permis sau nu accesul la rețea sau la internet în circumstanțele date.

Pentru administrarea regulilor, folosiți butoanele de deasupra tabelului:

- **Adăugare regulă** - deschide o fereastră acolo unde puteți crea o nouă regulă.
- **Șterge regulă** - șterge regula selectată.
- **Resetare reguli** - deschide o fereastră acolo unde puteți opta pentru ștergerea setului de reguli actual, revenind la cele implicite.

Adăugarea/Editarea regulilor pentru aplicații

Pentru a adăuga sau modifica o regulă pentru aplicație, faceți clic pe butonul **Adăugare regulă** de deasupra tabelului sau faceți clic pe o regulă actuală. Se afișează o nouă fereastră. Procedați astfel:

În secțiunea **Setări**, puteți aplica următoarele modificări:

- **Cale program.** Faceți clic pe **Caută** și selectați aplicația căreia i se aplică regula.
- **Tip rețea.** Selectați tipul de rețea pentru care se aplică regula. Puteți modifica tipul deschizând meniul vertical **Tip de rețea** și selectând unul dintre tipurile disponibile din listă.

Tip rețea	Description
Sigură	Dezactivează firewallul pentru adaptorul respectiv.
Acasă/Birou	Permite tot traficul dintre calculatorul dumneavoastră și calculatoarele din rețeaua locală.
Publică	Tot traficul este filtrat.
Nesigură	Blochează complet traficul de rețea și Internet prin adaptorul respectiv.

- **Permisiune.** Selectați una dintre permisiunile disponibile:

Permisiune	Description
Permite	Aplicației specificate îi va fi permis accesul la rețea / Internet în condițiile specificate.
Interzice	Aplicației specificate îi va fi refuzat accesul la rețea / Internet în condițiile specificate.

În secțiunea **Setări avansate** puteți personaliza următoarele setări:

- **Adresă locală personalizată.** Specificați adresa IP locală și portul local cărora li se aplică regula.
- **Adresă remote personalizată.** Specificați adresa IP și portul la distanță cărora li se aplică regula.
- **Direcție.** Selectați din meniu direcția traficului căreia i se aplică regula.

Direcție	Description
La ieșire	Regula nu se va aplica decât pentru traficul la ieșire.
La intrare	Regula nu se aplica decât pentru traficul la intrare.
Ambele	Regula se va aplica în ambele direcții.

- **Protocol.** Selectați din meniu protocolul IP căruia i se aplică regula.
  - Dacă doriți ca regula să fie aplicată tuturor protocoalelor, selectați **Oricare**.
  - Dacă doriți ca regula să fie aplicată pentru TCP, selectați **TCP**.
  - Dacă doriți ca regula să fie aplicată pentru UDP, selectați **UDP**.
  - Dacă doriți ca o regulă să se aplice unui anumit protocol, introduceți în câmpul gol numărul alocat protocolului pe care doriți să-l filtrați.

> **Notă**
>
> Numerele protocoalelor IP sunt atribuite de către Internet Assigned Numbers Authority (IANA). Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa http://www.iana.org/assignments/protocol-numbers.

20.3. Administrarea setărilor de conectare

Pentru fiecare conexiune la rețea puteți configura zone speciale sigure și nesigure.

O zonă sigură reprezintă un dispozitiv în care aveți încredere deplină, ca de exemplu un computer sau o imprimantă. Este permis în întregime traficul dintre computerul dumneavoastră și un dispozitiv de încredere. Pentru a putea partaja resurse cu calculatoare din rețele fără fir (wireless) nesecurizate, adăugați-le ca fiind calculatoare permise.

O zonă nesigură reprezintă un dispozitiv care nu doriți să comunice sub nicio formă cu computerul dumneavoastră.

Pentru a vizualiza și gestiona zonele de pe adaptoarele rețelei dumneavoastră, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Firewall**.
4. În fereastra **Firewall**, selectați secțiunea **Adaptoare**.

În această secțiune sunt afișate adaptoarele de rețea cu conexiuni active și zonele curente, dacă există.

Pentru fiecare zonă sunt afișate următoarele informații:

- **Tip rețea** - tipul de rețea la care este conectat computerul dumneavoastră.
- **Mod ascuns** - dacă puteți fi detectat de alte calculatoare.

  Pentru a configura modul Stealth, selectați opțiunea dorită din meniul derulant corespunzător.

Opțiune	Description
Activ	Modul ascuns este activat. Computerul dumneavoastră nu poate fi detectat nici din rețeaua locală, nici de pe internet.
Inactiv	Modul ascuns este dezactivat. Oricine din rețeaua locală sau de pe Internet poate da ping și detecta calculatorul dumneavoastră.

- **Generic** - dacă sunt aplicate reguli generice pentru această conexiune.

  Dacă se schimbă adresa IP a unui adaptor de rețea, Bitdefender va modifica automat și tipul de rețea. Dacă doriți să mențineți același tip, selectați **Da** din meniul derulant corespunzător.

Adăugare/modificare excepții

Pentru a adăuga sau modifica o excepție, faceți clic pe butonul **Excepții rețea** de deasupra tabelului. Va apărea o nouă fereastră în care vor fi afișate adaptoarele de rețea disponibile conectate la rețea. Procedați astfel:

1. Selectați adresa de IP a computerului pe care doriți să-l adăugați sau introduceți o adresă sau un interval de adrese în căsuța corespunzătoare.
2. Selectați permisiunea:
   - **Permite** - pentru a permite tot traficul dintre calculatorul dumneavoastră și calculatorul selectat.
   - **Blochează** - pentru a bloca tot traficul dintre calculatorul dumneavoastră și calculatorul selectat.
3. Faceți clic pe butonul + pentru a adăuga excepția și închideți fereastra.

   Dacă doriți să ștergeți un IP, faceți clic pe butonul corespunzător și închideți fereastra.

20.4. Configurarea setărilor avansate

Pentru a configra setările de firewall avansate, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Firewall**.
4. În fereastra **Firewall**, selectați secțiunea **Setări** tab.

Funcția de mai jos poate fi activată sau dezactivată.

- **Blocare scanări de porturi în rețea** - detectează și blochează tentativele de a descoperi care porturi sunt deschise.

Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculatorul dumneavoastră. Dacă este detectat un port vulnerabil, aceștia pot pătrunde în calculatorul dumneavoastră.

20.5. Configurarea intensității alertei

Bitdefender Internet Security 2016 a fost creat să deranjeze cât mai puțin posibil. În condiții normale, nu sunteți nevoit să luați decizii privind permiterea sau respingerea conexiunilor sau acțiunilor pe care le lansează anumite aplicații ce rulează pe sistemul dumneavoastră.

Dacă doriți să dețineți controlul deplin și să luați dumneavoastră toate deciziile, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale** selectați secțiunea **Setări generale**.
3. Activați **Paranoid Mode** făcând clic pe selectorul corespunzător.

> **Notă**
> Dacă ați activat modul Paranoid, funcțiile Autopilot și Profiluri sunt dezactivate automat.
> **Mod Paranoid** poate fi folosit în același timp cu **Mod Baterie**.

Atâta timp cât Paranoid Mode este activat, vi se va solicita intervenția de fiecare dată când apare una dintre următoarele situații:

- O aplicație încearcă să se conecteze la internet.
- O aplicație încearcă să efectueze o acțiune considerată a fi periculoasă de către funcțiile Detecția intruziunilor sau Active Threat Control.

Alerta conține informații detaliate cu privire la aplicație și la comportamentul detectat. Selectați fie **Permite** fie **Respinge** în cazul acțiunii cu ajutorul butonului corespunzător.

21. DETECȚIA INTRUZIUNILOR

Modulul Bitdefender de detecție a intruziunilor monitorizează activitățile din rețea și din sistem pentru detectarea operațiunilor periculoase și a încălcărilor politicii. Poate, de asemenea, detecta și bloca tentativele de modificare a fișierelor de sistem importante, a fișierelor Bitdefender sau a intrărilor de regiștri, instalarea de drivere periculoase și atacurile realizate prin injectarea de coduri (injectare DLL).

Pentru a configura modulul de detecție a intruziunilor, urmați acești pași:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Detecția intruziunilor**.
4. Pentru a porni modulul de detecție a intruziunilor, faceți clic pe butonul corespunzător.
5. Trageți de cursor de-a lungul scalei pentru a seta nivelul de agresivitate dorit. Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul care se potrivește mai bine nevoilor dumneavoastră de securitate.

Puteți verifica ce aplicații au fost detectate de Modulul de detecție a intruziunilor în fereastra Evenimente.

Dacă există aplicații în care aveți încredere și care nu doriți să fie scanate de Modulul de detecție a intruziunilor, puteți adăuga reguli de excludere pentru acestea. Pentru a exclude o aplicație de la scanare, urmați pașii descriși în secțiunea *„Administrarea proceselor excluse”* (p. 105).

Notă

Funcționarea modulului de Detecție a intruziunilor este strict legată de funcționarea Active Threat Control. Regulile de excludere a anumitor procese se aplică în cazul ambelor sisteme.

22. PROTECȚIE RANSOMWARE

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 aplicațiile.

Folosind cea mai recentă tehnologie, Protecția contra programelor periculoase ransomware Bitdefender asigură integritatea sistemului protejând zonele critice ale sistemului contra pericolelor fără a afecta sistemul. Cu toate acestea, poate fi recomandabil și să vă protejați fișierele personale, cum ar fi documentele, fotografiile, filmele sau fișierele stocate în cloud.

22.1. Activarea sau dezactivarea Protecției ransomware

Pentru a dezactiva modulul de protecție ransomware, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe **Protecția ransomware**.
4. Faceți clic pe selector pentru a activa sau dezactiva **Protecția ransomware**.

De fiecare dată când o aplicație încearcă să acceseze un fișier protejat, se afișează o fereastră derulantă Bitdefender. Puteți permite sau bloca accesul.

22.2. Protejați fișierele personale contra atacurilor ransomware

Dacă doriți să introduceți fișierele personale într-o zonă projată, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Protecție ransomware** și apoi pe butonul **Adaugă**.
4. Mergeți la folderul pe care doriți să-l protejați și apoi dați clic pe **OK** pentru a adăuga folderul selectat în mediul de protecție.

În mod implicit, directoarele Documents, Pictures, Public Documents și Public Pictures sunt protejate contra atacurilor de tip malware. 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.

Notă
Directoarele personalizate pot fi protejate doar pentru utilizatorii curenți. Fișierele de sistem și de aplicații nu pot fi adăugate la excepții.

22.3. Configurarea aplicațiilor de încredere

Dezactivați protecția ransomware pentru anumite aplicații, dar adăugați-le în listă doar pe cele în care aveți încredere.

Pentru a adăuga aplicații de încredere la excepții, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Protecție ransomware**, selectați **Aplicații de încredere**.
4. Faceți clic pe **Adaugă** și selectați aplicațiile pe care doriți să le protejați.

5. Faceți clic pe **OK** pentru a adăuga aplicația selectată la mediul protejat.

22.4. Configurarea aplicațiilor blocate

Dintre aplicațiile pe care le aveți instalate pe calculator, este posibil ca unele să dorească să vă acceseze fișierele personale.

Pentru a restricționa acele aplicații, urmați pașii de mai jos:

1. Faceți clic pe pictograma din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Protecție ransomware**, selectați **Aplicații blocate**.
4. Faceți clic pe **Adaugă** și selectați aplicațiile pe care doriți să le restricționați.
5. Faceți clic pe **OK** pentru a adăuga aplicația selectată în lista restricționată.

22.5. 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. De asemenea, se oferă protecția contra anumitor atacuri care se bazează pe executarea codurilor de tip stack sau heap, injectări de coduri sau asocieri la anumite biblioteci dinamice principale.

Pentru a dezactiva protecția la pornire, urmați pașii de mai jos:

1. Faceți clic pe pictograma din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe **Protecția ransomware**.
4. Faceți clic pe buton pentru a porni sau opri **Protecția la pornire**.

23. SECURITATE SAFEPAY PENTRU TRANZACȚIILE ONLINE

Calculatorul a început să devină principalul instrument pentru cumpărături și tranzacții bancare. Achitarea facturilor, transferul de bani, achiziționarea a cam tot ce vă puteți imagina nu au fost niciodată mai rapide sau mai ușoare.

Aceasta implică transmiterea de informații personale, date de cont și credit, parole și alte tipuri de informații personale prin Internet, cu alte cuvinte, exact tipul de informații pe care infractorii cibernetici sunt foarte interesați să le obțină. Hackerii se străduiesc în permanență să sustragă aceste informații, deci, nu puteți fi niciodată suficient de precauți cu privire la securizarea tranzacțiilor online.

Bitdefender Safepay™ este, în primul rând, un browser protejat, un mediu proiectat pentru a ca tranzacțiile dvs. online să rămână confidențiale și securizate.

Pentru cea mai bună protecție a confidențialității, Administratorul de parolă Bitdefender a fost integrat în Bitdefender Safepay™ pentru a vă proteja datele ori de câte ori doriți să accesați locații private online. Pentru mai multe informații, consultați *„Protecția datele dumneavoastră cu Administratorul de parolă”* (p. 143).

Bitdefender Safepay™ vă oferă următoarele funcții:

- Blochează accesul la calculatorul dumneavoastră și orice încercări de a realiza capturi ale ecranului dumneavoastră.
- Aceasta vă protejează parolele secrete când navigați pe internet, cu ajutorul Administratorului de parolă.
- Include o tastatură virtuală care, dacă este utilizată, nu permite hackerilor să citească ceea ce introduceți de pe aceasta.
- Este complet idependentă de celelalte browsere ale dumneavoastră.
- Include protecție pentru punctele wireless de acces la Internet încorporată pe care o puteți utiliza în cazul conectării la rețele Wi-fi nesecurizate.
- Acceptă marcajele și vă permite să navigați pe site-urile dumneavoastră preferate de tranzacții bancare/cumpărături.

- Nu se limitează la tranzacții bancare și cumpărături online. Orice site poate fi deschis în Bitdefender Safepay™.

23.1. Utilizarea Bitdefender Safepay™

În mod implicit, Bitdefender detectează dacă navigați către un site de tranzacții online sau de cumpărături online în orice browser de pe calculatorul dumneavoastră și vă solicită să îl lansați în Bitdefender Safepay™.

Pentru a accesa interfața Bitdefender Safepay™ principală, folosiți una dintre metodele următoare:

- Din interfața Bitdefender:
  1. Faceți clic pe butonul de acțiune **Safepay** din interfața Bitdefender.
- Din Windows:
  - În **Windows 7**:
    1. Faceți clic pe **Start** și mergeți la **Toate programele**.
    2. Faceți clic pe **Bitdefender**.
    3. Faceți clic pe **Bitdefender Safepay™**.
  - În **Windows 8 și Windows 8.1**:

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

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

> **Notă**
> Dacă plugin-ul Adobe Flash Player nu este instalat sau actualizat, se va afișa un mesaj Bitdefender. Faceți clic pe butonul corespunzător pentru a continua. După ce procesul de instalare este finalizat, va trebui să redeschideți manual browserul Bitdefender Safepay™ pentru a continua.

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

- introduceți URL-urile pe care doriți să le accesați în bara de adrese.

- adăugați secțiuni pentru a vizita mai multe site-uri în fereastra Bitdefender Safepay™ făcând clic pe .
- reveniți la navigarea anterioară, mergeți către o altă pagină și reîmprospătați pagini folosind .
- accesați setările Bitdefender Safepay™ făcând clic pe și selectând **Setări**.
- protejați-vă parolele cu Administrator parolă făcând clic pe .
- administrați marcajele făcând clic pe de lângă bara de adrese.
- activați tastatura virtuală făcând clic pe .
- măriți sau micșorați dimensiunea browser-ului apăsând simultan tastele **Ctrl** și **+/-** de pe tastatura numerica.
- vizualizați informațiile despre produsul dvs. Bitdefender făcând clic pe și selectând **Despre**.
- tipăriți informațiile importante făcând clic pe .

23.2. Configurarea setărilor

Faceți clic pe și alegeți **Setări** pentru a configura Bitdefender Safepay™:

Setări generale

Selectați ce se va deschide când accesați un site de cumpărături online sau de tranzacții bancare prin Internet, în browserul dumneavoastră Internet obișnuit:

- Deschide automat site-urile web în Safepay.
- Sugerează-mi utilizarea Safepay.
- Nu-mi sugera utilizarea Safepay.

Listă domenii

Selectați cum se va comporta Bitdefender Safepay™ la vizitarea site-urilor Internet de pe anumite domenii în browserul dumneavoastră Internet obișnuit, adăugându-le la lista domeniilor și selectând comportamentul fiecăruia dintre ele.

- Deschide automat în Bitdefender Safepay™.
- Setați Bitdefender să vă interogheze cu privire la acțiuni de fiecare dată.
- Nu utiliza niciodată Bitdefender Safepay™ la accesarea unei pagini din domeniu într-un browser obișnuit.

Blocare pop-up-uri

Puteți opta pentru blocarea pop-up-urilor făcând clic pe comutatorul corespunzător.

De asemenea, puteți crea o listă a site-urilor pe care permiteți afișarea pop-up-urilor. Este recomandat ca lista să conțină doar site-uri web în care aveți deplină încredere.

Pentru a adăuga un site în listă, introduceți adresa acestuia în câmpul corespunzător și faceți clic pe **Adaugă domeniu**.

Pentru a șterge un site web din listă, selectați-l din listă și faceți clic pe link-ul corespunzător **Ștergere**.

Activarea protecției Hotspot

Puteți activa un nivel suplimentar de protecție atunci când sunteți conectat la rețele Wi-fi nesecurizate activând această caracteristică.

Accesați *„Protecție pentru punctele wireless de acces la Internet în rețele nesecurizate”* (p. 142) pentru mai multe informații.

23.3. Administrarea marcajelor

Dacă ați dezactivat detectarea automată a unei părți dintre site-uri sau a tuturor site-urilor sau dacă Bitdefender pur și simplu nu detectează anumite site-uri internet, puteți adăuga marcați în Bitdefender Safepay™ pentru a putea lansa cu ușurință site-urile Internet în viitor.

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

1. Faceți clic pe pictograma de lângă bara de adrese pentru a deschide pagina Marcaje.

   Notă
   Pagina Marcaje se deschide în mod implicit la lansarea Bitdefender Safepay™.

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

23.4. Protecție pentru punctele wireless de acces la Internet în rețele nesecurizate

Dacă utilizați Bitdefender Safepay™ în timp ce sunteți conectat la rețele Wi-fi nesecurizate (de exemplu, un punct de acces Internet wireless public) vi se oferă un nivel suplimentar de securizate prin funcția de protecție Hotspot. Acest serviciu criptează comunicarea pe Internet între conexiunile nesecurizate, ajutându-vă să vă mențineți confidențialitatea, indiferent de rețeaua la care sunteți conectat.

Protecția Hotspot funcționează numai dacă sistemul dumneavoastră este conectat la o rețea nesecurizată.

Conexiunea securizată va fi inițiată și se va afișa un mesaj în fereastra Bitdefender Safepay™ după conectare. Simbolul se afișează în fața URL-ului în bara de adrese pentru a vă ajuta să identificați cu ușurință conexiunile securizate.

Pentru a vă îmbunătăți experiența vizuală de navigare, puteți opta pentru activarea plugin-urilor **Adobe Flash** și **Java** făcând clic pe **Afișează setările avansate**.

Este posibil să fie necesar să confirmați acțiunea.

24. PROTECȚIA DATELE DUMNEAVOASTRĂ CU ADMINISTRATORUL DE PAROLĂ

Folosim calculatorul pentru a face cumpărături online sau pentru a ne plăti facturile, pentru a ne conecta la platformele de socializare sau pentru a ne autentifica în aplicațiile de mesagerie instant.

Dar toată lumea știe că nu este ușor să-ți reamintești parolele.

Iar dacă nu suntem atenți atunci când navigăm pe internet, datele noastre confidențiale, precum adresa de e-mail, ID-ul de mesagerie instant sau datele cardului de credit pot fi compromise.

Păstrarea parolelor sau a datelor personale scrise pe hârtie sau în calculator poate fi periculoasă datorită faptului că acestea ar putea fi accesate și folosite de persoane care vor să fure sau să utilizeze aceste informații. Și nu este un lucru ușor să vă reamintiți fiecare parolă setată pentru conturile dumneavoastră sau pentru site-urile preferate.

Prin urmare, există oare vreo modalitate prin care să ne asigurăm că ne găsim parolele atunci când avem nevoie de ele? Și putem fi siguri că parolele noastre sunt în deplină siguranță întotdeauna?

Funcția Administrare parolă vă permite să gestionați parolele, vă protejează confidențialitatea și vă oferă o experiență de navigare sigură.

Folosind o singură parolă master pentru a accesa datele dumneavoastră, Administrator parolă vă ajută să vă păstrați parolele în deplină siguranță într-un Portofel.

Pentru a asigura cea mai bună protecție pentru activitățile dumneavoastră online, Administratorul de parolp este integrat cu Bitdefender Safepay™, oferindu-vă o soluție unificată pentru diversele modalități în care vă pot fi compromise datele.

Administratorul de parolă 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

24.1. Configurarea Administratorului de parolă

După ce instalarea s-a finalizat și deschideți browserul, se va afișa o fereastră pop-up de notificare informându-vă că puteți folosi Portofelul pentru o experiență de navigare mai ușoară.

Protofelul Bitdefender este locația în care vă puteți păstra datele personale.

Faceți clic pe **Deschidere** pentru a porni asistentul de configurare pentru Portofel. Urmați instrucțiunile asistentului pentru a finaliza procesul de instalare.

În cadrul acestui pas se pot efectua două operațiuni:

- Creați o nouă bază de date pentru Portofel pentru a vă proteja parolele.

  În timpul procesului de instalare, vi se va solicita să vă protejați Portofelul cu ajutorul unei parole master. Parola ar trebui să fie puternică și să conțină cel puțin 7 caractere.

  Pentru a crea o parolă puternică, folosiți minim o cifră sau un simbol și un caracter cu majusculă. După ce ați setat o parolă, aceasta va trebui introdusă de fiecare dată când cineva încearcă să acceseze Portofelul.

  După ce ați configurat parola principală, vi se dă posibilitatea de a sincroniza informațiile din Portofel în cloud pentru a le putea folosi pe toate dispozitivele.

  La sfârșitul procesului de instalare, se vor activa următoarele setări implicite pentru Portofel:

  - **Salvare automată a datelor de autentificare în Portofel**.
  - **Solicitare parolă generală la deschiderea browser-elor și aplicațiilor**.
  - **Blocare automată portofel atunci când calculatorul este lăsat nesupravegheat**.
  - **Datele de autentificare se completează automat de fiecare dată**.
  - **Afișează opțiunile mele de completare atunci când vizitez o pagină cu formulare**.

- Se importă o bază de date existentă dacă ați folosit anterior Portofelul pe sistemul dumneavoastră.

Exportați baza de date a Portofelului

Pentru a exporta baza de date a Portofelului, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. Faceți clic pe modulul **Administrator parolă** și selectați secțiunea **Portofele**.
4. Selectați baza de date Portofel dorită din secțiunea **Portofelele mele** și faceți clic pe butonul **Export**.
5. Urmați acești pași pentru a exporta baza de date a Portofelului către o anumită locație din sistemul dumneavoastră.

Notă
Pentru ca butonul **Export** să fie disponibil, Portofelul trebuie să fie deschis.

Creare bază de date nouă pentru Portofel

Pentru a crea o bază nouă de date a Portofelului, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. Faceți clic pe modulul **Administrator parolă** și selectați secțiunea **Portofele**.
4. Faceți clic pe pictograma + din fereastra care se deschide.
5. În zona **Start Fresh**, faceți clic pe **Creare nou**.
6. Introduceți informațiile solicitate în câmpurile corespunzătoare.
   - Eticheta Portofel - introduceți o denumire unică pentru baza de date Portofel.
   - Parola principală - introduceți o parolă pentru Portofel.
   - Reintroducere parolă - reintroduceți parola configurată
   - Indiciu - introduceți un indiciu pentru a vă aminti mai ușor parola.
7. Faceți clic pe **Continue**.

8. În acest punct, puteți opta pentru stocarea informațiilor în cloud. Dacă selectați da, datele bancare vor rămâne stocate local pe dispozitiv. Selectați opțiunea dorită și faceți clic pe **Continuare**.
9. Selectați browser-ul web din care doriți să importați datele.
10. Faceți clic pe **Finalizare**.

Sincronizați portofelele în cloud

Pentri a activa sau dezactiva sincronizarea portofelelor în cloud, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. Faceți clic pe modulul **Administrator parolă** și selectați secțiunea **Portofele**.
4. Selectați baza de date Portofel dorită din secțiunea **Portofelele mele** și faceți clic pe butonul **Setări**.
5. Selectați opțiunea dorită din fereastra afișată și faceți clic pe **Salvare**.

Notă
Pentru ca butonul **Setări** să fie disponibil, Portofelul trebuie să fie deschis.

Gestionați datele de autentificare pentru Portofel

Pentru a gestiona parolele dumneavoastră, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. Faceți clic pe modulul **Administrator parolă** și selectați secțiunea **Portofele**.
4. Selectați baza de date Portofel dorită din secțiunea **Portofelele mele** și faceți clic pe butonul **Deschidere**.

Se afișează o nouă fereastră. Selectați categoria dorită din partea de sus a ferestrei:

- Identitate

- Site-uri web
- Banking online
- Adrese e-mail
- Aplicații
- Rețele Wi-Fi

Adăugarea/ modificarea datelor de autentificare

- Pentru a adăuga o nouă parolă, selectați categoria dorită din partea de sus, faceți clic pe **+ Adăugare**, introduceți informațiile în câmpurile corespunzătoare și faceți clic pe butonul de Salvare.
- Pentru a edita un obiect din listă, selectați-l și faceți clic pe butonul **Editează**.
- Pentru ieșire, faceți clic pe **Anulare**.
- Pentru a șterge o înregistrare, selectați-o, faceți clic pe butonul **Modificare** și selectați **Ștergere**.

24.2. Activarea sau dezactivarea protecției Administrator parolă

Pentru a activa sau dezactiva protecția Administrator parolă, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. Faceți clic pe modulul **Administrator parolă**.
4. Faceți clic pe selecrorul **Stare modul** pentru a activa sau dezactiva Administratorul de parolă.

24.3. Administrarea setărilor Administratorului de parolă

Pentru a configura în detaliu parola master, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. Faceți clic pe modulul **Administrator parolă** și selectați secțiunea **Setări securitate**.

Sunt disponibile următoarele opțiuni:

- **Solicită parola principală la conectarea la calculatorul meu** - vi se va solicita să introduceți parola master atunci când accesați calculatorul dumneavoastră.
- **Solicită parola master la deschiderea browserului sau a aplicațiilor** - vi se va solicita să introduceți parola master atunci când accesați un browser sau o aplicație.
- **Blochează automat Portofelul atunci când calculatorul e lăsat nesupravegheat** - vi se va solicita să introduceți parola master atunci când reveniți la calculator după 15 minute.

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

Îmbunătățiți-vă experiența în utilizare

Pentru a selecta browserele sau aplicațiile în care doriți să integrați Administratorul de parolă, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. Faceți clic pe modulul **Administrator parolă** și selectați secțiunea **Plugin**.

   Bifați o aplicație pentru a utiliza Administratorul de parolă și îmbunătățiți-vă experiența de utilizare:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome

- Safepay
- Skype
- Yahoo! Messenger

Configurarea funcției de Completare automată

Funcția de Completare automată vă permite să vă conectați mai ușor la site-urile web preferate sau să vă autentificați în conturile dumneavoastră 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 funcției de **Completare automată**, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. Faceți clic pe modulul **Administrator parolă** și selectați secțiunea **Completare automată setări**.
4. Configurați următoarele opțiuni:
   - **Completare automată a datelor de autentificare**:
     - **Datele de autentificare se completează automat de fiecare dată** - informațiile dumneavoastră sunt introduse automat în browser.
     - **Doresc să specific când să se introducă automat datele mele de autentificare** - puteți selecta când se vor introduce automat datele în browser.
   - **Configurați modul în care Administratorul de parolă vă securizează datele de autentificare**:
     - **Salvează datele automat în Portofel** - datele de autentificare și alte informații care pot fi identificate, cum ar fi datele personale și cele ale cardului de credit, sunt salvate și actualizate automat în Portofel.
     - **Întreabă-mă de fiecare dată** - vi se va solicita de fiecare dată să confirmați dacă doriți să adăugați datele dumneavoastră în Portofel.
     - **Nu permite salvarea datelor, voi actualiza informațiile manual** - datele pot fi adăugate doar manual în Portofel.

- **Formulare de completare automată**:
  - **Solicită opțiunile mele de completare când accesez o pagină cu formulare** - se va afișa o fereastră cu opțiunile de completare de fiecare dată când Bitdefender detectează că doriți să efectuați o plată online sau să vă autentificați.

Administrarea informațiilor referitoare la Administratorul de parolă din browser

Puteți administra cu ușurință Administratorul de parolă direct din browser, pentru a avea toate datele importante la îndemână. Aplicați suplimentară Portofel Bitdefender este acceptată de următoarele browsere: Google Chrome, Internet Explorer și Mozilla Firefox și este, de asemenea, integrată cu Safepay.

Pentru a accesa extensia Portofel Bitdefender, deschideți browser-ul, permiteți instalarea aplicației suplimentare și faceți clic pe pictograma  de pe bara de instrumente.

Extensia Portofel Bitdefender include următoarele opțiuni:

- Deschide Portofelul - deschide aplicația Portofel.
- Blochează Portofelul - blochează portofelul.
- Website-uri - deschide un submeniu cu toate autentificările la site-uri Internet stocate în Portofel. Faceți clic pe **Adaugă site** pentru a adăuga site-uri noi în listă.
- Completează formularele - deschide un submeniu cu informațiile adăugate de dvs. pentru o anumită categorie. De aici, puteți adăuga date noi în Portofel.
- Generator parolă - enables vă permite să generați parole aleatorii pe care le puteți utiliza pentru conturile noi sau existente. Faceți clic pe **Afișare setări avansate** pentru a seta complexitatea parolei.
- Setări - deschide fereastra de setări a Administratorului de parolă.
- Raportează problema - raportează orice problemă întâmpinată cu Administratorul de parolă Bitdefender.

25. ASISTENȚĂ PARENTALĂ

Funcția Asistență Parentală vă permite să controlați accesul la internet și la aplicații specifice pentru fiecare dispozitiv pe care este instalată această funcție. De îndată ce ați configurat funcția Asistență Parentală, puteți afla cu ușurință în ce scop utilizează copilul dvs. aceste dispozitive și ce anume a accesat acesta în ultimele 24 de ore. În plus, pentru a vă ajuta să aflați mai multe despre ceea ce face copilul dvs., aplicația vă oferă și statistici cu privire la activitățile și interesele sale.

Tot ce vă trebuie este un calculator cu conexiune la internet și un browser web.

Puteți configura funcția Asistență Parentală să blocheze:

- pagini web inadecvate.
- jocuri, aplicații de chat, partajare de fișiere și altele.
- contacte cărora nu le este permis să comunice prin telefon cu copilul dumneavoastră.

Verificați activitatea copiilor dumneavoastră și modificați setările de Asistență Parentală folosind Bitdefender Central de la orice calculator sau dispozitiv mobil conectat la internet.

25.1. Accesarea funcției Asistență Parentală - Copiii mei

De îndată ce accesați secțiunea Asistență Parentală, este disponibilă fereastra **Copiii mei**. Aici puteți vizualiza și edita toate profilurile pe care le-ați creat pentru copiii dumneavoastră. Profilurile sunt afișate sub forma unor carduri de profil, permițându-vă să le gestionați și să verificați status-ul acestora rapid.

De îndată ce ați creat un profil, puteți începe să configurați setări personalizate mai detaliate pentru a monitoriza și controla accesul copiilor dumneavoastră la internet și la anumite aplicații.

Puteți accesa setările funcției Asistență Parentală din contul Bitdefender Central de pe orice calculator sau dispozitiv mobil conectat la internet.

Accesați-vă contul online:

- Pe orice dispozitiv cu acces la Internet:

1. Accesați-vă contul Bitdefender Central.

   Asigurați-vă că sunteți conectat(ă) cu datele dumneavoastră de autentificare.

2. Selectați secțiunea **Asistență Parentală**.
3. În fereastra **Copiii mei**, puteți gestiona și configura profilurile de Asistență Parentală pentru fiecare dispozitiv.

- Din interfața Bitdefender:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Confidențialitate**.
3. În modulul **Asistență Parentală**, selectați **Configurare**.

   Sunteți redirecționat(ă) la pagina web Bitdefender Central. Asigurați-vă că sunteți conectat(ă) cu datele dumneavoastră de autentificare.

4. Selectați secțiunea **Asistență Parentală**.
5. În fereastra **Copiii mei**, puteți gestiona și configura profilurile de Asistență Parentală pentru fiecare dispozitiv.

Notă
Asigurați-vă că sunteți conectat la calculator pe contul de administrator. Doar utilizatorii cu drepturi administrative pe sistem (administratorii de sistem) pot accesa și configura Asistența Parentală.

25.2. Adăugarea profilului pentru copilul dumneavoastră

Pentru a începe monitorizarea activităților copilului dvs., este necesar să configurați un profil și să instalați Agentul de Asistență Parentală Bitdefender pe dispozitivele utilizate de acesta.

Pentru a adăuga profilul copilului dumneavoastră în modulul de Asistență Parentală:

1. Accesați secțiunea Asistență Parentală din contul dumneavoastră Bitdefender Central.
2. Faceți clic pe **ADĂUGARE PROFIL** în partea dreapta a ferestrei **Dispozitivele mele**.

3. Introduceți informațiile specifice în câmpurile corespunzătoare, cum ar fi: numele, adresa de e-mail, sexul și data nașterii și apoi faceți clic pe **CONTINUARE**.

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

4. Dacă dispozitivul copilului dumneavoastră are deja instalat Bitdefender Internet Security 2016, selectați dispozitivul acestuia din lista disponibilă și apoi faceți clic pe **CONTINUARE**.

   Dacă dispozitivul copilului dumneavoastră nu are Bitdefender instalat cu funcția Asistență Parentală inclusă, faceți clic pe **Adaugă dispozitiv nou**. Selectați sistemul de operare al dispozitivului acestuia și apoi faceți clic pe **CONTINUARE**.

   Introduceți adresa de e-mail la care să vă trimitem link-ul de descărcare pentru instalarea aplicației Bitdefender Asistență Parentală.

   Pe dispozitivele Windows, Bitdefender Internet Security 2016 inclus în abonamentul dumneavoastră trebuie descărcat și instalat. Pe dispozitivele Android, Agentul de Asistență Parentală Bitdefender trebuie descărcat și instalat.

25.2.1. Atribuirea aceluiași profil către mai multe dispozitive

Puteți atribui același profil către mai multe dispozitive aparținând aceluiași copil, astfel încât să se aplice aceleași restricții.

Pentru atribuirea unui profil pe mai multe dispozitive:

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea Asistență Parentală.
3. Faceți clic pe pictograma ⋮ de pe cardul de profil dorit și apoi selectați **Editare**.
4. Dați clic pe semnul + pe fiecare dintre dispozitivele disponibile cărora doriți să le atribuiți profilul.

   Dacă dispozitivul copilului dumneavoastră nu are Bitdefender instalat cu funcția Asistență Parentală inclusă, faceți clic pe **Adaugă dispozitiv nou**. Selectați sistemul de operare al dispozitivului acestuia și apoi faceți clic pe **CONTINUARE**.

Introduceți adresa de e-mail la care să vă trimitem link-ul de descărcare pentru instalarea aplicației Bitdefender Asistență Parentală. Verificați căsuța de pe e-mail și dați clic pe linkul furnizat pentru a instala agentul.

După finalizarea procesului de instalare pe noul dispozitiv, selectați-l din listă pentru a aplica profilul.

5. Selectați **Salvare**.

25.2.2. Asocierea funcției de Asistență Parentală cu Bitdefender Central

Pentru a monitoriza activitatea online a copilului dumneavoastră pe dispozitivele Android, este necesar să asociați dispozitivul acestuia cu contul dumneavoastră Bitdefender Central conectându-vă la acest cont din aplicație.

Pentru legarea dispozitivului de cont dvs. Bitdefender Central, urmați acești pași:

1. Deschideți aplicația Asistență Parentală.
2. Bifați caseta **Declar că sunt deținătorul legal al dispozitivului** și atingeți **Următorul**.
3. Conectați-vă la contul dumneavoastră Bitdefender Central.

   Dacă nu aveți cont, creați-vă unul folosind butonul corespunzător.

   Notă
   Puteți introduce un nume pentru dispozitivul dumneavoastră. Dacă legați mai multe dispozitive la contul dumneavoastră, acesta vă va ajuta să identificați mai ușor dispozitivele.

4. Selectați **Conectare**.
5. Selectați din listă profilul copilului pe care doriți să îl monitorizați și atingeți **Continuare**.

   Alternativ, atingeți **Adăugare alt copil** pentru a crea un nou profil și completați câmpurile corespunzătoare.

6. Activați drepturile de administrare a dispozitivului pentru aplicație atingând **Activare**.

   Aceasta va împiedica dezinstalarea de către copilul dumneavoastră a Agentului de Asistență Parentală.

25.2.3. Monitorizarea activității copilului

Bitdefender vă ajută să urmăriți exact ce face copilul dumneavoastră in mediul online.

În acest mod, puteți întotdeauna afla exact ce site-uri web au vizitat, ce aplicații au utilizat sau ce activități au fost blocate de către funcția de Asistență Parentală.

În funcție de setările introduse, rapoartele pot conține informații detaliate despre fiecare eveniment, cum ar fi:

- Starea evenimentului.
- Severitatea de notificare.
- Numele dispozitivului.
- Data și ora producerii evenimentului.

Pentru a monitoriza traficul pe Internet, aplicațiile accesate sau activitatea pe Facebook a copilului dumneavoastră, urmați pașii de mai jos:

1. Accesați secțiunea Asistență Parentală din contul dumneavoastră Bitdefender Central.
2. Selectați cardul dispozitivului dorit.

   În fereastra Panou de control puteți vizualiza informațiile de care sunteți interesat(ă).

25.2.4. Configurarea setărilor generale

În mod implicit, atunci când funcția de Asistență Parentală este activată, activitățile copiilor dumneavoastră sunt înregistrate în fișiere jurnal.

Pentru a primi notificări prin e-mail, urmați pașii de mai jos:

1. Accesați secțiunea Asistență Parentală din contul dumneavoastră Bitdefender Central.
2. Faceți clic pe pictograma  din colțul din dreapta sus.
3. Activați opțiunea corespunzătoare pentru a primi rapoarte de activitate.
4. Introduceți adresa de e-mail la care vor fi trimise notificările de e-mail.
5. Stabiliți frecvența selectând: săptămânal sau lunar.

6. Primiți notificări prin e-mail pentru următoarele:
   - Site-uri web blocate
   - App blocate
   - Zone restricționate
   - SMS de la un contact blocat
   - Apel primit de la un număr de telefon blocat
   - Înlăturare aplicație Asistență Parentală Facebook
7. Faceți clic pe **Salvează**.

25.2.5. Editarea profilului

Pentru a edita un profil existent:

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Asistență Parentală**.
3. Faceți clic pe pictograma ⋮ de pe cardul de profil dorit și apoi selectați **Editare**.
4. După personalizarea setărilor dorite, selectați **Salvare**.

25.2.6. Ștergerea unui profil

Pentru a șterge un profil existent:

1. Accesați-vă contul Bitdefender Central.
2. Selectați secțiunea **Asistență Parentală**.
3. Faceți clic pe pictograma ⋮ de pe cardul de profil dorit și apoi selectați **Ștergere**.

25.3. Configurarea profilurilor de Asistență Parentală

Pentru a începe monitorizarea copilului dumneavoastră, trebuie alocat un profil dispozitivului pe care este instalat Agentul de Asistență Parentală Bitdefender.

După adăugarea unui profil pentru copilul dumneavoastră, puteți personaliza în detaliu setările de monitorizare și control privind accesul la internet și la anumite aplicații.

Pentru a începe configurarea unui profil, selectați cardul de profil dorit din fereastra **Copiii mei**.

Faceți clic pe o filă pentru a configura funcția corespunzătoare de Asistență Parentală pentru dispozitiv:

- Panou de control - afișează toate activitățile, interesele, locațiile și interacțiunile cu prietenii din ziua curentă.
- Activități - vă permite să blocați accesul la anumite aplicații, precum jocuri, programe de mesagerie, filme etc.
- Interese - vă permite să filtrați navigarea pe internet.
- Prieteni - aici puteți menționa care dintre contactele din lista copilului dumneavoastră pot intra în contact cu acesta prin intermediul telefonului.
- Locuri - aici puteți stabili locațiile care sunt sigure sau nesigure pentru copilul dumneavoastră.
- Socializare - vă permite să blocați accesul la rețelele de socializare.

25.3.1. Cont online

Fereastra Panou de control vă oferă informații detaliate despre activitățile copiilor dumneavoastră în ultimele 24 de ore, în interiorul și exteriorul casei dumneavoastră.

În funcție de activitate, fereastra panoului de comandă poate include informații despre:

- **Locații** - aici puteți vizualiza locațiile vizitate de copilul dumneavoastră în cursul zilei. Faceți clic pe link-ul **Stabilire mod sleep** pentru a stabili o oră la care monitorizarea activităților va trece automat în modul standby.
- **Interese** - aici puteți vizualiza informații despre categoriile de site-uri web vizitate de copilul dumneavoastră. Dați clic pe linkul **Revizuire conținut necorespunzător** pentru a permite sau interzice accesul la anumite interese.
- **Interacțiuni sociale** - aici puteți vizualiza contactele cu care a comunicat copilul dumneavoastră. Dați clic pe **Administrare contacte** pentru a selecta contactele cu care copilul dumneavoastră ar trebui să mențină sau nu legătura.

- **Aplicații** - aici puteți vizualiza aplicațiile utilizate de copilul dumneavoastră.
- **Activitate zilnică** - aici puteți vedea timpul petrecut online pe toate dispozitivele atribuite copilului dumneavoastră și locul unde acesta a fost activ. Informațiile colectate sunt din ziua curentă.

> **Notă**
> Pentru informații detaliate, faceți clic pe opțiunea dorită situată în colțul din dreapta al fiecărei secțiuni.

25.3.2. Activități

Fereastra Activități vă ajută să blocați rularea unor aplicații. Astfel puteți bloca jocurile, fișierele media și aplicațiile de mesagerie, precum și alte categorii de aplicații.

Modulul poate fi activat sau dezactivat utilizând butonul corespunzător.

Pentru a configura Controlul aplicației pentru un anumit cont de utilizator, urmați pașii de mai jos:

1. Se afișează o listă cu carduri. Cardurile reprezintă aplicațiile pe care le utilizează copilul dumneavoastră.
2. Selectați cardul cu aplicația a cărei utilizare de către copilul dumneavoastră doriți să o blocați.

   Marcarea cu simbolul de bifare indică faptul că aplicația nu va putea fi utilizată de copilul dumneavoastră.

25.3.3. Interese

Fereastra Interese vă ajută să blocați site-urile web cu conținut neadecvat. Astfel puteți bloca site-urile web care găzduiesc clipuri video, jocuri, fișiere media și aplicații de mesagerie, precum și alte categorii de conținuturi negative.

Modulul poate fi activat sau dezactivat utilizând butonul corespunzător.

În funcție de vârsta copilului, lista de Interese include implicit o selecție de categorii activate. Pentru a permite sau bloca accesul la o anumită categorie, faceți clic pe aceasta.

Marcarea cu simbolul de bifare indică faptul că un anumit conținut dintr-o anumită categorie nu poate fi accesat de copilul dumneavoastră.

Acceptarea sau blocarea unui site web

Pentru a permite sau restricționa accesul la anumite pagini web, trebuie să le adăugați la lista de Excluderi, după cum urmează:

1. Faceți clic pe butonul **ADMINISTRARE**.
2. Introduceți pagina web a cărei accesare doriți să o permiteți sau să o blocați în câmpul corespunzător.
3. Selectați **Permite** sau **Blocare**.
4. Faceți clic pe **Finalizare** pentru a salva modificările.

25.3.4. Prieteni

Fereastra Prieteni vă dă posibilitatea de a specifica prietenii din lista copilului dumneavoastră care pot sau nu pot intra în contact cu acesta prin intermediul telefonului.

Pentru a restricționa un anumit număr de telefon al unui prieten, mai întâi adăugați numărul de telefon al copilului dumneavoastră la profilul acestuia:

1. Selectați secțiunea **Asistență Parentală** din contul dumneavoastră Bitdefender Central.
2. Faceți clic pe pictograma ⋮ de pe cardul de profil dorit și apoi selectați **Editare**.
3. Introduceți în câmpul corespunzător numărul de telefon al copilului dumneavoastră, apoi faceți clic pe **SALVARE**.
4. Selectați profilul copilului în legătură cu care doriți să stabiliți restricțiile.
5. Selectați secțiunea **Prieteni**.

   Se afișează o listă cu carduri. Card-urile reprezintă contactele din telefonul copilului dumneavoastră.
6. Selectați cardul cu numărul de telefon pe care doriți să îl blocați.

   Marcarea cu simbolul de bifare indică faptul că numărul de telefon selectat nu poate lua legătura cu copilul dumneavoastră.

Pentru a bloca numere de telefon necunoscute, activați butonul **Blochează interacțiunile cu apelurile cu număr necunoscut**.

25.3.5. Locuri

Vizualizați locația curentă a dispozitivului pe Google Maps. Locația este actualizată la fiecare 5 secunde, așadar îl puteți localiza dacă este în mișcare.

Precizia locației depinde de cum poate Bitdefender să o stabilească:

- Dacă funcția GPS este activată pe dispozitiv, locația sa poate fi indicată cu precizie pe o rază de câțiva metri atâta timp cât se află în raza sateliților GPS (mai exact, nu într-o clădire).
- Dacă dispozitivul este înăuntru, locația sa poate fi stabilită la intervale de zeci de metri dacă funcția Wi-Fi este activată și există pe raza sa rețele wireless.
- Altfel, locația va fi stabilită utilizând numai informațiile rețelei mobile, care nu poate oferi o precizie mai mare de câteva sute de metri.

Pentru a fi sigur(ă) că numai anumite locații sunt accesate de copilul dumneavoastră, puteți face o listă cu locurile sigure și nesigure.

Pentru a configura o locație:

1. Faceți clic pe **Dispozitive** în cadrul din fereastra **Locuri**.
2. Faceți clic pe **SELECTARE DISPOZITIVE** și apoi selectați dispozitivul pe care doriți să îl configurați.
3. În fereastra **Zone**, faceți clic pe butonul **ADĂUGARE ZONĂ**.
4. Selectați tipul locației **Sigură** sau **Restricționată**.
5. Introduceți un nume valid pentru zona pe care copilul dumneavoastră o poate sau nu accesa.
6. În **Locație inițială**, introduceți orașul în care se află copilul dumneavoastră și apoi alegeți județul din lista care apare pe ecran.
7. Stabiliți raza care urmează a fi aplicată pentru monitorizare din bara glisantă **Rază**.
8. Faceți clic pe **ADĂUGARE ZONĂ** pentru a salva setările.

25.3.6. Social

Funcția de Asistență Parentală monitorizează contul de Facebook al copilului dumneavoastră și raportează principalele activități efectuate.

Aceste activități online sunt verificate și veți primi o notificare dacă ele se dovedesc a fi o amenințare la adresa datelor confidențiale ale copilului dumneavoastră.

Printre elementele monitorizate ale contului online se numără:

- numărul de prieteni
- comentariile copilului dumneavoastră sau cele ale prietenilor săi la pozele sau link-urile publicate de acesta
- mesaje
- postări pe perete
- fotografii și filme încărcate
- setări de confidențialitate ale contului

Pentru a configura protecția pentru Facebook pentru un anumit cont de utilizator:

1. Introduceți adresa de e-mail a contului copilului monitorizat, apoi faceți clic pe **TRIMITERE**.

   Informați-vă copilul cu privire la intențiile dumneavoastră și solicitați-i să facă clic pe link-ul de activare pe care l-a primit de la noi prin e-mail.

2. Pentru a proteja contul de Facebook al copilului, acesta trebuie să facă clic pe butonul **INSTALARE APLICAȚIE** care apare de îndată ce acesta își accesează contul de Facebook.

Pentru a opri monitorizarea contului de Facebook, utilizați butonul **Anulare asociere** din partea de sus.

26. BITDEFENDER USB IMMUNIZER

Funcția Autorun încorporată în sistemele de operare Windows este un instrument foarte util care permite calculatoarelor să execute automat un fișier de pe un suport conectat la acestea. De exemplu, instalările aplicațiilor pot începe automat când introduceți un CD în unitatea optică.

Din nefericire, această funcție poate fi utilizată și de programele periculoase pentru lansarea automată și infiltrarea în calculatorul dumneavoastră de pe medii reinscriptibile, cum ar fi unitățile USB și cardurile de memorie conectate prin cititoare de carduri. În ultimii ani au fost create numeroase atacuri bazate pe Autorun.

Cu USB Immunizer, puteți împiedica orice unități flash formatate NTFS, FAT32 sau FAT să mai execute programe periculoase. După ce un dispozitiv USB a fost imunizat, programele periculoase nu îl mai pot configura să ruleze o anumită aplicație când dispozitivul este conectat la un calculator pe care rulează Windows.

Pentru imunizarea unui dispozitiv USB, urmați pașii de mai jos:

1. Conectați unitatea flash la calculatorul dumneavoastră.
2. Navigați în calculator pentru a localiza dispozitivul amovibl de stocare și faceți clic dreapta pe această pictogramă.
3. În meniul contextual, evidențiați **Bitdefender** și selectați **Imunizează această unitate**.

> **Notă**
> Dacă dispozitivul a fost deja imunizat, în locul opțiunii Imunizare va apărea mesajul **Dispozitivul USB este protejat împotriva programelor periculoase cu executare automată**

Pentru a preveni lansarea programelor periculoase de către calculatorul dumneavoastră de pe dispozitive USB neimunizate, dezactivați funcția de rulare automată a mediilor. Pentru mai multe informații, consultați *„Cu ajutorul monitorizării automate a vulnerabilităților”* (p. 124).

OPTIMIZARE DE SISTEM

27. PROFILURI

Activitățile de serviciu zilnice, vizionarea filmelor sau jocurile pot încetini performanțele sistemului, cu precădere dacă rulează simultan cu procesele de actualizare Windows și sarcinile de actualizare. Cu Bitdefender, puteți acum alege și aplica profilul dorit, care efectuează ajustările sistemului adecvate pentru îmbunătățirea performanțelor aplicațiilor specifice instalate.

Bitdefender oferă următoarele profiluri:

- Profil Lucru
- Profil Film
- Profil Joc

Dacă decideți să nu utilizați **Profiluri**, se activează un profil implicit numit **Standard**, care nu vă optimizează sistemul.

În funcție de activitatea dvs., se aplică următoarele setări ale produsului la activarea unui profil:

- Toate alertele și pop-upurile Bitdefender sunt dezactivate.
- Actualizarea automată este amânată.
- Scanările programate sunt amânate.
- Modulul Asistență pentur căutare este dezactivat.
- Modulul de detecție a intruziunilor este setat pe nivelul de protecție **Permisiv**.
- Ofertele speciale și notificările de produse sunt dezactivate.

În funcție de activitatea dvs., se aplică următoarele setări ale sistemului la activarea unui profil:

- 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.

27.1. Profil Lucru

Rularea mai multor sarcini la serviciu, cum ar fi trimiterea de e-mail-uri, comunicarea video cu colegi aflați la distanță sau lucrul cu aplicații de proiectare, vă pot afecta performanțele sistemului. Profilul de serviciu a fost proiectat pentru a vă ajuta să vă îmbunătățiți eficiența la lucru, prin dezactivarea unora dintre serviciile și sarcinile care rulează în fundal.

Configurarea profilului Serviciu.

Pentru a configura operațiunile ce vor fi efectuate în Profilul Serviciu, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.
3. Faceți clic pe modulul **Profiluri**.
4. În fereastra **Setări Profiluri**, faceți clic pe butonul **Configurare** din zona Profil Serviciu.
5. Selectați ajustările sistemului care doriți să fie aplicate, prin bifarea opțiunilor de mai jos:
   - Crește performanța aplicațiilor de lucru
   - Optimizați setările de produs pentru Profilul Lucru
   - Amânați programele de fundal și activitățile de întreținere
   - Amânare actualizare Windows automată
6. Faceți clic pe **Salvează** pentru a salva modificările și închide fereastra.

Adăugarea manuală a aplicațiilor la lista Profil Serviciu

Dacă Bitdefender nu intră automat în Profilul Serviciu când lansați o anumită aplicație de serviciu, puteți adăuga manual aplicația la **Lista aplicațiilor**.

Pentru a adăuga manual aplicații în Lista aplicațiilor din Profilul Serviciu:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.

3. Faceți clic pe modulul**Profiluri** și apoi pe butonul **Configurare** din zona Profil Lucru.
4. În fereastra **profil Serviciu**, faceți clic pe link-ul **Listă aplicații**.
5. Faceți clic pe **Adaugă** pentru a adăuga o nouă aplicație în **Listă aplicații**.

   Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil al aplicației, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.

27.2. Profil Film

Afișarea videoclipurilor de calitate superioară, cum ar fi filmele de înaltă definiție, necesită resurse semnificative de sistem. Profilul Film adaptează setările sistemului și ale produsului, astfel încât să vă puteți bucura de o experiență plăcută și fără întreruperi.

Configurarea Profilului Film

Pentru a configura măsurile implementate în Profilul Film:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.
3. Faceți clic pe modulul **Profiluri**.
4. În fereastra **Setări profiluri**, faceți clic pe butonul **Configurare** din zona Profil film.
5. Selectați ajustările sistemului care doriți să fie aplicate, prin bifarea opțiunilor de mai jos:
   - Crește performanța aplicațiilor media
   - Optimizați setările de produs pentru Profilul Film
   - Amânați programele de fundal și activitățile de întreținere
   - Amânare actualizare Windows automată
   - Ajustați configurările planului de energie pentru filme
6. Faceți clic pe **Salvează** pentru a salva modificările și închide fereastra.

Adăugarea manuală a dispozitivelor de redare video în lista Profil Film

Dacă Bitdefender nu intră automat în Profilul Film când lansați o anumită aplicație pentru redarea video clipurilor, puteți adăuga manual aplicația în **Lista dispozitivelor de redare**.

Pentru a adăuga manual dispozitive de redare video în Lista dedicată din Profilul Film:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.
3. Faceți clic pe modulul **Profiluri** și apoi pe butonul **Configurare** din zona Profil Film.
4. În fereastra **Profil film**, faceți clic pe link-ul **Lista dispozitivelor de redare**.
5. Faceți clic pe **Adaugă** pentru a adăuga o nouă aplicație la **Lista dispozitivelor de redare**.

   Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil al aplicației, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.

27.3. Profil Joc

Pentru o experiență plăcută a jocului trebuie reduse încărcările de sistem și încetinirile. Folosind metoda euristică comportamentală, alături de o listă de jocuri cunoscute, Bitdefender poate detecta automat jocurile active și poate optimiza resursele sistemului pentru ca dvs. să vă puteți bucura de pauza de joc.

Configurarea Profilului Joc

Pentru a configura operațiunile ce vor fi efectuate în Profilul Joc, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.

3. Faceți clic pe modulul **Profiluri**.
4. În fereastra **Setări Profiluri**, faceți clic pe butonul **Configurare** din zona Profil Joc.
5. Selectați ajustările sistemului care doriți să fie aplicate, prin bifarea opțiunilor de mai jos:
   - Crește performanța jocurilor
   - Optimizați setările de produs pentru Profilul Joc
   - Amânați programele de fundal și activitățile de întreținere
   - Amânare actualizare Windows automată
   - Ajustați configurările planului de energie pentru jocuri
6. Faceți clic pe **Salvează** pentru a salva modificările și închide fereastra.

Adăugare manuală de jocuri la lista de jocuri

În cazul în care Bitdefender nu intră automat în Profilul Joc atunci când ați lansat un anumit joc sau o aplicație, aveți posibilitatea să adăugați aplicația manual la **Lista de jocuri**.

Pentru a adăuga manual jocuri în Lista Jocurilor din Profilul Joc:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.
3. Faceți clic pe modulul **Profiluri** și apoi pe butonul **Configurare** din zona Profil Joc.
4. În fereastra **Profil Joc**, faceți clic pe link-ul **Listei Jocurilor**.
5. Faceți clic pe **Adaugă** pentru a adăuga un nou joc în **Lista Jocurilor**.

   Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil al jocului, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.

27.4. Optimizare în timp real

Optimizarea în timp real Bitdefender este un plugin care îmbunătățește silențios performanțele sistemului dvs., în fundal, asigurându-se că nu sunteți

întrerupt când vă aflați în modul profil. În funcție de solicitarea CPU, plugin-ul monitorizează toate procesele, concentrându-se pe cele care necesită mai multe resurse, pentru a le adapta necesităților dvs.

Pentru a dezactiva Optimizarea în timp real, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Instrumente**.
3. Faceți clic pe modulul **Profiluri** și apoi selectați secțiunea **Setări Profiluri**.
4. Activați sau dezactivați Optimizarea în timp real făcând clic pe comutatorul corespunzător.

REMEDIEREA PROBLEMELOR

28. SOLUȚIONAREA PROBLEMELOR FRECVENTE

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

- *„Sistemul meu funcționează lent"* (p. 171)
- *„Nu începe scanarea"* (p. 173)
- *„Nu mai pot utiliza o anumită aplicație"* (p. 175)
- *„Ce trebuie să faceți atunci când Bitdefender blochează un site sigur sau o aplicație online"* (p. 176)
- *„Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet"* (p. 182)
- *„Serviciile Bitdefender nu răspund"* (p. 182)
- *„Filtrul Antispam nu funcționează corespunzător"* (p. 183)
- *„Funcția Completare automată din Portofel nu funcționează"* (p. 188)
- *„Nu s-a reușit dezinstalarea Bitdefender"* (p. 189)
- *„Sistemul meu nu pornește după ce am instalat Bitdefender"* (p. 190)

Dacă problema dumneavoastră nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic a Bitdefender folosind informațiile din capitolul *„Solicitarea ajutorului"* (p. 204).

28.1. Sistemul meu funcționează lent

De obicei, după instalarea unui program de securitate, este posibil să se producă o ușoară încetinire a funcționării sistemului, fapt ce este normal într-o anumită măsură.

În cazul în care observați o încetinire semnificativă, această problemă poate apărea din următoarele motive:

- **Bitdefender nu este singurul program de securitate instalat în sistem.**

  Deși Bitdefender caută și dezinstalează programele de securitate detectate în timpul instalării, se recomandă să îndepărtați orice alte programe antivirus pe care le-ați utilizat înainte de a iniția instalarea Bitdefender.

Pentru mai multe informații, consultați *„Cum elimin celelalte soluții de securitate?"* (p. 77).

- **Nu sunt îndeplinite cerințele minime de sistem pentru rularea Bitdefender.**

  În cazul în care computerul dumneavoastră nu îndeplinește cerințele minime de sistem, acesta va începe să răspundă lent, mai ales atunci când mai multe aplicații rulează în același timp. Pentru mai multe informații, consultați *„Cerințe minime de sistem"* (p. 3).

- **Ați instalat aplicații pe care nu le utilizați**.

  Orice calculator are programe sau aplicații care nu sunt utilizate. Și multe programe nedorite rulează în fundal, ocupând spațiu pe disc și încărcând memoria calculatorului. Dacă nu folosiți un program, dezinstalați-l. Acest lucru este valabil și pentru orice alte programe software sau aplicații de evaluare pe care omiteți să le ștergeți.

  Important

  Dacă suspectați că un program sau o aplicație este o parte esențială a sistemului dumneavoastră de operare, nu le ștergeți, ci contactați Serviciul de asistență clienți al Bitdefender.

- **Sistemul dumneavoastră poate fi infectat**.

  Programele malware pot afecta, de asemenea, viteza sistemului dumneavoastră, precum și comportamentul general al acestuia. Programele periculoase de tip spyware, viruși, troieni și adware afectează performanța calculatorului dumneavoastră. Scanați sistemul periodic, cel puțin o dată pe săptămână. Este recomandat să utilizați funcția de Scanare sistem a Bitdefender deoarece aceasta scanează toate tipurile de programe periculoase care amenință securitatea sistemului dumneavoastră.

  Pentru a iniția un proces de scanare a sistemului, urmați pașii de mai jos:

  1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
  2. Selectați secțiunea **Protecție**.
  3. În modulul **Antivirus**, selectați **Scanare sistem**.
  4. Urmați pașii asistentului.

28.2. 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, urmați acești pași:

  1. Dezinstalați complet Bitdefender din sistem:
     - În **Windows 7**:
       a. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
       b. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
       c. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.
       d. Faceți clic pe **Înainte** pentru a continua.
       e. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
     - În **Windows 8 și Windows 8.1**:
       a. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.
       b. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
       c. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
       d. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.
       e. Faceți clic pe **Înainte** pentru a continua.
       f. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
     - În **Windows 10**:
       a. Faceți clic pe **Start**, apoi pe Setări.
       b. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.

c. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.

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

e. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.

f. Faceți clic pe **Înainte** pentru a continua.

g. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

2. Reinstalați produsul dumneavoastră Bitdefender.

- **Bitdefender nu este singura soluție de securitate instalată în sistemul dumneavoastră**.

  În acest caz, urmați acești pași:

  1. Dezinstalați cealaltă soluție de securitate. Pentru mai multe informații, consultați *„Cum elimin celelalte soluții de securitate?”* (p. 77).
  2. Dezinstalați complet Bitdefender din sistem:
     - În **Windows 7**:
       a. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
       b. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
       c. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.
       d. Faceți clic pe **Înainte** pentru a continua.
       e. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
     - În **Windows 8 și Windows 8.1**:
       a. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.
       b. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
       c. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
       d. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.

e. Faceți clic pe **Înainte** pentru a continua.

f. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

- În **Windows 10**:

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

b. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.

c. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.

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

e. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.

f. Faceți clic pe **Înainte** pentru a continua.

g. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

3. Reinstalați produsul dumneavoastră Bitdefender.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 204).

28.3. Nu mai pot utiliza o anumită aplicație

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

După instalarea Bitdefender ar putea apărea următoarele situații:

- Este posibil să primiți un mesaj din partea Bitdefender referitor la faptul că programul încearcă să efectueze o modificare asupra sistemului.
- Este posibil să primiți un mesaj de eroare din partea programului pe care încercați să-l utilizați.

Acest tip de situație apare când Active Threat Control detectează din greșeală anumite aplicații ca fiind rău intenționate.

Active Threat Control este un modul Bitdefender care monitorizează în mod constant aplicațiile care rulează pe sistemul dumneavoastră și raportează acele aplicații care sunt posibil rău intenționate. Deoarece această opțiune

se bazează pe un sistem euristic, pot exista situații în care aplicații legitime să fie raportate de Active Threat Control.

Atunci când se întâmplă aceasta, puteți exclude aplicația respectivă de la monitorizarea efectuată de Active Threat Control.

Pentru a adăuga programul în lista de excluderi, urmați acești pași:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Excepții**.
4. Faceți clic pe link-ul **Procese excluse**. În fereastra care va apărea, puteți gestiona excepțiile de la procesul Active Threat Control.
5. Pentru a adăuga excepții, urmați pașii de mai jos:
   a. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
   b. Faceți clic pe **Caută**, identificați și selectați aplicația care doriți să fie exclusă și faceți clic pe **OK**.
   c. Mențineți selectată opțiunea **Permite** pentru a preveni blocarea aplicației de către Active Threat Control.
   d. Faceți clic pe **Adaugă**.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului"* (p. 204).

28.4. Ce trebuie să faceți atunci când Bitdefender blochează un site sigur sau o aplicație online

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 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 aceeași pagină sau aplicație este blocată în mod repetat, acestea pot fi adăugate la lista albă astfel încât acestea să nu fi scanate de

motoarele Bitdefender, asigurând o experiență de navigare pe internet fără probleme.

Pentru a adăuga un site la **Lista albă**, urmați acești pași:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Protecție web**.
4. În secțiunea **Setări**, faceți clic pe link-ul **Lista albă**.
5. Introduceți în câmpul corespunzător adresa site-ului sau a aplicației online blocate și faceți clic pe **Adăugare**.
6. Faceți clic pe **Salvează** pentru a salva modificările și închide fereastra.

Adăugați în această listă doar site-urile și aplicațiile în care aveți totală încredere. Acestea vor fi excluse din procesul de scanare de către motoarele contra programelor periculoase, a tentativelor de phishing și fraudelor.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului"* (p. 204).

28.5. Nu mă pot conecta la internet

Este posibil să observați că un program sau un browser de internet nu se mai poate conecta la internet sau accesa serviciile de rețea după instalarea Bitdefender.

În acest caz, cea mai bună soluție este să configurați Bitdefender să permită în mod automat conexiunile către și de la aplicația software respectivă.

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Firewall** și selectați secțiunea **Reguli**.
4. Pentru a adăuga o regulă pentru aplicație, faceți clic pe butonul **Adăugare regulă**.

5. Va apărea o nouă fereastră în care puteți adăuga detaliile. Asigurați-vă că ați selectat toate tipurile de rețea disponibile și în secțiunea **Permisiune** selectați **Permite**.

Închideți Bitdefender, deschideți aplicația software și încercați din nou să vă conectați la internet.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului"* (p. 204).

28.6. Nu pot accesa un dispozitiv din rețeaua mea

În funcție de rețeaua la care sunteți conectat, firewallul Bitdefender poate bloca conexiunea dintre sistemul dumneavoastră și un alt dispozitiv (cum ar fi un alt computer sau o imprimantă). În consecință, nu mai puteți partaja sau imprima fișiere.

În acest caz, cea mai bună soluție este să configurați Bitdefender să permită în mod automat conexiunile către și de la dispozitivul respectiv. Pentru fiecare conexiune din rețea, puteți configura o zonă specială securizată.

O zonă de încredere este un dispozitiv în care aveți deplină încredere. Este permis necondiționat traficul dintre computerul dumneavoastră și un dispozitiv de încredere. Pentru a partaja resursele cu anumite dispozitive, precum computere sau imprimante, adăugați aceste dispozitive ca fiind de încredere.

Pentru a adăuga o zonă de încredere pe adaptorii rețelei dumneavoastră, urmați pașii de mai jos:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Faceți clic pe modulul **Firewall** și selectați secțiunea **Reguli**.
4. Pentru a adăuga o zonă, faceți clic pe butonul **Adăugare regulă**. Va apărea o nouă fereastră în care vor fi afișate adresele IP ale dispozitivelor conectate la rețea.
5. Selectați adresa de IP a computerului sau a imprimantei pe care doriți să o adăugați sau introduceți un interval de adrese în căsuța corespunzătoare.
6. În câmpul **Permisiune**, selectați **Permite** și apoi faceți clic pe **OK**.

Dacă tot nu vă puteți conecta la dispozitiv, este posibil ca problema să nu fie cauzată de Bitdefender.

Verificați alte cauze posibile, cum ar fi:

- Firewallul de pe celălalt calculator poate bloca partajarea de fișiere și imprimante cu calculatorul dumneavoastră.
  - Dacă se folosește Windows Firewall, acesta poate fi configurat să permită partajarea de fișiere, după cum urmează:
    - În **Windows 7**:
      1. Faceți clic pe **Start**, mergeți la **Control Panel** și selectați **System and Security**.
      2. Mergeți la **Windows Firewall** și faceți clic pe **Permite aplicației să comunice prin Paravanul de protecție Windows**.
      3. Selectați căsuța **File and Printer Sharing**.
    - În **Windows 8 și Windows 8.1**:
      1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control" direct în ecranul de Start) și faceți clic pe pictograma acestuia.
      2. Faceți clic pe **Sistem și securitate**, mergeți la **Windows Firewalld** și selectați **Permite aplicației să comunice prin Paravanul de protecție Windows**.
      3. Selectați căsuța **File and Printer Sharing** si faceți click pe **OK**.
    - În **Windows 10**:
      1. Introduceți "Allow an app through Windows Firewall" în caseta de căutare din bara de sarcini și faceți clic pe pictogramă.
      2. Faceți clic pe **Modificare setări**.
      3. Din lista **Aplicații și funcții permise**, bifați caseta **Partajare fișiere și imprimată** și faceți clic pe **OK**.
  - Dacă se folosește un alt program firewall, consultați documentația sau fișierul de ajutor ale acestuia.
- Cauze generale care pot împiedica folosirea sau conectarea la imprimanta partajată:

- Poate fi necesar să vă conectați la un cont Windows de administrator pentru a avea acces la imprimanta partajată.
- Numai anumite calculatoare și anumiți utilizatori pot accesa imprimanta partajată. Dacă partajați imprimanta dumneavoastră, verificați restricțiile de acces stabilite pentru aceasta pentru a vedea dacă utilizatorul de pe celălalt calculator o poate accesa. Dacă încercați să vă conectați la o imprimantă partajată, întrebați utilizatorul de pe celălalt calculator dacă vi se permite accesul la imprimantă.
- Imprimanta conectată la calculatorul dumneavoastră sau la celălalt calculator nu este partajată.
- Imprimanta partajată nu este adăugată pe calculator.

Notă
Pentru a afla cum să administrați imprimantele partajate (partajarea unei imprimante, stabilirea sau eliminarea permisiunilor de acces la o imprimantă, conectarea la o imprimantă de rețea sau partajată), mergeți la Centrul de Asistență și Suport al Windows (în meniul Start, faceți clic pe **Help and Support**).

- Accesul la o imprimantă din rețea poate fi restricționat pentru anumite computere sau pentru anumiți utilizatori. Este recomandat să consultați administratorul rețelei pentru a afla dacă vă puteți conecta la imprimanta în cauză.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 204).

28.7. Conexiunea mea la internet este lentă

Această situație poate apărea după instalarea Bitdefender. Problema poate fi cauzată de erori de configurare a firewallului Bitdefender.

Pentru a remedia această situație, urmați acești pași:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.

3. Faceți clic pe modulul **Firewall**, apoi faceți clic pe selector pentru a dezactiva **Firewall-ul**.
4. Verificați dacă, după ce ați dezactivat firewallul Bitdefender, conexiunea dumneavoastră la internet s-a îmbunătățit.
   - Dacă nu se remediază problema cu viteza redusă a conexiunii la Internet, este posibil ca problema să nu fie cauzată de Bitdefender. Trebuie să contactați furnizorul dumneavoastră de servicii de internet pentru a verifica dacă conexiunea este funcțională la nivelul acestuia.

     În cazul în care primiți o confirmare din partea furnizorului dumneavoastră de servicii de internet că respectiva conexiune este funcțională la nivelul său, iar problema încă persistă, contactați Bitdefender conform descrierii din secțiunea *„Solicitarea ajutorului”* (p. 204).
   - În cazul în care conexiunea la internet s-a îmbunătățit după dezactivarea firewallului Bitdefender, urmați acești pași:
     a. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
     b. Selectați secțiunea **Protecție**.
     c. Faceți clic pe modulul **Firewall** și selectați secțiunea **Setări**.
     d. Mergeți la **Blocare scanare porturi în rețea** și faceți clic pe buton pentru dezactivare.
     e. Mergeți la secțiunea **Adaptoare** și selectați conexiunea dumneavoastră la Internet.
     f. În coloana **Tip de rețea**, selectați **Acasă/Birou**.
     g. În coloana **Mod ascuns**, selectați **ACTIVAT**. Setați coloana **Generic** la valoarea **Activ**.
     h. Închideți Bitdefender, reporniți sistemul ș verificați viteza conexiunii la internet.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 204).

28.8. Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet

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

Pentru a vă menține actualizat sistemul cu cele mai recente semnături malware Bitdefender, urmați acești pași:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Setări generale** din meniul derulant.
2. În fereastra **Setări generale**, selectați secțiunea **Actualizare**.
3. De lângă **Actualizare reguli procesare**, selectați **Întreabă-mă înainte de a descărca** fin meniul derulant.
4. Reveniți la fereastra principală și faceți clic pe butonul de acțiune **Actualizare** din interfața Bitdefender.
5. Selectați numai **Actualizări semnături** și apoi faceți clic pe **OK**.
6. Bitdefender va descărca și va instala numai actualizările semnăturilor malware.

28.9. Serviciile Bitdefender nu răspund

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

- Pictograma Bitdefender din bara de sistem este afișată în culoarea gri și veți fi notificat de faptul să serviciile Bitdefender nu răspund.
- Fereastra Bitdefender indică faptul că serviciile Bitdefender nu răspund.

Problema poate fi cauzată de:

- erori temporare de comunicare între serviciile Bitdefender.
- unele dintre serviciile Bitdefender sunt oprite.
- alte soluții de securitate rulează pe calculatorul dumneavoastră, în același timp cu Bitdefender.

Pentru a remedia această problemă, încercați următoarele soluții:

1. Așteptați câteva momente pentru a vedea dacă apar schimbări. Eroarea poate fi temporară.

2. Reporniți calculatorul și așteptați câteva momente până când se încarcă Bitdefender. Deschideți Bitdefender pentru a vedea dacă eroarea persistă. De obicei, repornirea calculatorului rezolvă problema.
3. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați Bitdefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați Bitdefender.

   Pentru mai multe informații, consultați *„Cum elimin celelalte soluții de securitate?"* (p. 77).

Dacă eroarea persistă, vă rugăm să contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea *„Solicitarea ajutorului"* (p. 204).

28.10. Filtrul Antispam nu funcționează corespunzător

Acest articol vă ajută să remediați următoarele probleme legate de funcționarea filtrului antispam al Bitdefender:

- Mai multe mesaje e-mail legitime sunt marcate ca [spam].
- Multe mesaje spam nu sunt marcate corespunzător de filtrul antispam.
- Filtrul antispam nu detectează niciun mesaj spam.

28.10.1. Mesaje legitime sunt marcate ca [spam]

Mesaje legitime sunt marcate ca [spam] pentru că filtrul antispam Bitdefender le percepe ca atare. În mod normal, puteți rezolva această problemă printr-o configurare adecvată a filtrului Antispam.

Bitdefender adaugă automat într-o Listă de prieteni destinatarii mesajelor e-mail trimise de dumneavoastră. Mesajele e-mail primite de la persoanele de pe Lista de prieteni sunt considerate a fi legitime. Ele nu sunt verificate de filtrul antispam și, astfel, nu sunt marcate niciodată ca [spam].

Configurarea automată a Listei de prieteni nu previne erorile de detecție care pot apărea în următoarele situații:

- Primiți multe mesaje comerciale nesolicitate, ca urmare a înscrierii pe diferite site-uri web. În acest caz, soluția este să adăugați adresele de e-mail de la care primiți astfel de mesaje în Lista de prieteni.

- O parte semnificativă a mesajelor e-mail pe care le primiți sunt trimise de oameni cărora nu le-ați scris niciodată pe e-mail, cum ar fi: clienți, potențiali parteneri de afaceri și alții. În acest caz, sunt necesare alte soluții.

  Dacă folosiți unul dintre clienții de e-mail în care se integrează Bitdefender, indicați erorile de detecție.

  Notă
  Bitdefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, consultați *„Clienți și protocoale de e-mail compatibile”* (p. 109).

Adăugați-vă contactele pe Lista de prieteni

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje legitime pe Lista de prieteni. Urmați acești pași:

1. În clientul dumneavoastră de mail, selectați un mesaj e-mail al expeditorului pe care doriți să-l adăugați pe Lista de prieteni.
2. Faceți clic pe butonul **Adaugă prieten** din bara de instrumente antispam Bitdefender.
3. Vi se poate cere să confirmați adresa adăugată pe Lista de prieteni. Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.

Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.

Dacă folosiți un alt client de mail, puteți adăuga contacte pe Lista de prieteni din interfața Bitdefender. Urmați acești pași:

1. Faceți clic pe pictograma din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antispam**, selectați **Administrare prieteni**.

   Va apărea o fereastră de configurare.
4. Introduceți adresa de e-mail de la care doriți să primiți mereu mesaje și apoi faceți clic pe **Adăugare**. Puteți adăuga oricâte adrese de e-mail doriți.
5. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Indicați erorile de detecție

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

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

28.10.2. Numeroase mesaje spam nu sunt detectate

Dacă primiți multe mesaje spam care nu sunt marcate [spam], trebuie să configurați filtrul antispam Bitdefender, pentru a-i îmbunătăți eficiența.

Încercați următoarele soluții:

1. Dacă folosiți unul dintre clienții de e-mail în care se integrează Bitdefender, indicați mesajele spam nedetectate.

   Notă

   Bitdefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, consultați *„Clienți și protocoale de e-mail compatibile” (p. 109)*.

2. Adăugați spammerii pe Lista de spammeri. Mesajele e-mail primite de la adrese de pe Lista de spammeri sunt marcate automat ca [spam].

Indicați mesajele spam nedetectate

Dacă folosiți un client de mail admis, puteți indica cu ușurință care mesaje e-mail ar fi trebuit detectate ca spam. Astfel, veți îmbunătăți eficiența filtrului antispam. Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți la directorul Inbox.
3. Selectați mesajele spam nedetectate.
4. Faceți clic pe butonul **Spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail). Acestea sunt marcate imediat ca [spam] și mutate în directorul de mesaje nesolicitate (junk).

Adăugați spammeri pe Lista de spammeri

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje spam pe Lista de spammeri. Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele pe care Bitdefender le-a marcat ca [spam].
4. Faceți clic pe butonul **Adaugă spammer** din bara de instrumente antispam Bitdefender.
5. Vi se poate cere să confirmați adresa adăugată pe Lista de spammeri. Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.

Dacă folosiți un alt client de mail, puteți adăuga manual spammeri în Lista de spammeri din interfața Bitdefender. Este recomandat să procedați astfel numai atunci când ați primit mai multe mesaje spam de la aceeași adresă de e-mail. Urmați acești pași:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. În modulul **Antispam**, selectați **Administrare spammeri**.

   Va apărea o fereastră de configurare.

4. Introduceți adresa de e-mail a spammer-ului și apoi faceți clic pe **Adaugă**. Puteți adăuga oricâte adrese de e-mail doriți.
5. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

28.10.3. Filtrul antispam nu detectează niciun mesaj spam

Dacă niciun mesaj spam nu este marcat ca [spam], este posibil să existe probleme legate de filtrul Antispam Bitdefender. Înainte de a remedia această problemă, asigurați-vă că ea nu se datorează următoarelor cauze:

- Este posibil ca protecția antispam să fie dezactivată. Pentru a verifica starea de protecție antispam, faceți clic pe săgeata din colțul din stânga jos al interfeței Bitdefender, selectați secțiunea **Protecție**, faceți clic pe modulul **Antispam** și bifați selectorul din fereastra **Setări**.

  Dacă protecția Antispam este dezactivată, aceasta este cauza problemei dvs. Faceți clic pe selector pentru a activa protecția anstispam.

- Protecția antispam Bitdefender este disponibilă numai pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3. Aceasta înseamnă că:

  - Mesajele e-mail primite prin servicii de e-mail oferite online (cum ar fi Yahoo, Gmail, Hotmail sau altele) nu sunt supuse verificării antispam de către Bitdefender.
  - Dacă aveți un client de e-mail configurat să primească mesaje prin alt protocol decât POP3 (de exemplu IMAP4), Bitdefender nu supune aceste mesaje unei verificări antispam.

  > **Notă**
  >
  > POP3 este unul dintre cele mai des folosite protocoale de descărcare a mesajelor e-mail de pe un server de mail. Dacă nu știți ce protocol folosește clientul dumneavoastră de e-mail pentru a descărca mesajele, întrebați persoana care l-a configurat.

- Bitdefender Internet Security 2016 nu scanează traficul POP3 generat de Lotus Notes.

O soluție posibilă este repararea sau reinstalarea produsului. Dacă doriți, puteți contacta Bitdefender pentru suport, folosind informațiile din secțiunea *„Solicitarea ajutorului”* (p. 204).

28.11. Funcția Completare automată din Portofel nu funcționează

Ați salvat datele dumneavoastră de autentificare în Portofelul Bitdefender și ați observat că funcția de completare automată nu funcționează. De obicei, această problemă apare atunci când extensia Administratorului de parolă Bitdefender nu este instalată în browserul dumneavoastră.

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

- În **Internet Explorer:**
  1. Deschideți Internet Explorer.
  2. Faceți clic pe Instrumente.
  3. Faceți clic pe Gestionare programe de completare.
  4. Faceți clic pe Bare de instrumente și extensii.
  5. Poziționați cursorul pe **Administrator parolă Bitdefender** și faceți clic pe Activare.
- În **Mozilla Firefox:**
  1. Deschideți Mozilla Firefox.
  2. Faceți clic pe Instrumente.
  3. Faceți clic pe Programe de completare.
  4. Faceți clic pe Extensii.
  5. Poziționați cursorul pe **Administrator parolă Bitdefender** și faceți clic pe Activare.
- În **Google Chrome:**
  1. Deschideți Google Chrome.
  2. Mergeți la pictograma Meniului.
  3. Faceți clic pe Setări.
  4. Faceți clic pe Extensii.
  5. Poziționați cursorul pe **Administrator parolă Bitdefender** și faceți clic pe Activare.

Notă
Programul de completare se va activa după repornirea browserului.

Apoi verificați dacă funcția de completare automată din Portofel funcționează pentru conturile dumneavoastră online.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 204).

28.12. Nu s-a reușit dezinstalarea Bitdefender

Dacă doriți să ștergeți produsul Bitdefender și observați că procesul este suspendat sau sistemul se blochează, faceți clic pe **Anulare** pentru a abandona acțiunea. Dacă anularea nu este posibilă, reporniți sistemul.

Dacă dezinstalarea eșuează, în sistemul dumneavoastră pot rămâne unele chei de regiștri și fișiere Bitdefender. Aceste rămășite pot împiedica instalarea ulterioară a Bitdefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului.

Pentru a șterge definitiv Bitdefender de pe sistemul dumneavoastră, urmați pașii de mai jos:

- În **Windows 7**:
  1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
  2. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
  3. Selectați **Șterge** și apoi selectați **Vreau să șterg permanent**.
  4. Faceți clic pe **Înainte** pentru a continua.
  5. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
- În **Windows 8 și Windows 8.1**:
  1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți clic pe pictograma acestuia.
  2. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
  3. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.

4. Selectați **Șterge** și apoi selectați **Vreau să șterg permanent**.
5. Faceți clic pe **Înainte** pentru a continua.
6. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

- În **Windows 10**:

1. Faceți clic pe **Start**, apoi pe Setări.
2. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.
3. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.
4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
5. Selectați **Șterge** și apoi selectați **Vreau să șterg permanent**.
6. Faceți clic pe **Înainte** pentru a continua.
7. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

28.13. Sistemul meu nu pornește după ce am instalat Bitdefender

Dacă se întâmplă ca, după ce tocmai ați instalat Bitdefender,să nu puteți reporni sistemul în modul normal, pot exista mai multe motive pentru această problemă.

Cel mai probabil această problemă este cauzată fie de o instalare anterioară a Bitdefender care nu a fost dezinstalată corespunzător fie de o altă soluție de securitate care este instalată pe sistem.

Mai jos sunt prezentate modurile în care să acționați pentru fiecare situație:

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

  Pentru a soluționa această problemă, urmați pașii de mai jos:

  1. Reporniți sistemul în Safe Mode. Pentru a afla cum să procedați, consultați *„Cum pot să repornesc sistemul în Safe Mode?"* (p. 78).
  2. Ștergeți Bitdefender din sistemul dumneavoastră:

     - În **Windows 7**:

a. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.

b. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.

c. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.

d. Faceți clic pe **Înainte** pentru a continua.

e. Așteptați până când procesul de dezinstalare este finalizat.

f. Reporniți sistemul în modul normal.

- În **Windows 8 și Windows 8.1**:

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

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

c. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.

d. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.

e. Faceți clic pe **Înainte** pentru a continua.

f. Așteptați până când procesul de dezinstalare este finalizat.

g. Reporniți sistemul în modul normal.

- În **Windows 10**:

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

b. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.

c. Găsiți **Bitdefender Internet Security 2016** și selectați **Dezinstalare**.

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

e. Faceți clic pe **Șterge** din fereastra care se afișează și apoi selectați **Vreau să reinstalez**.

f. Faceți clic pe **Înainte** pentru a continua.

g. Așteptați până când procesul de dezinstalare este finalizat.

h. Reporniți sistemul în modul normal.

3. Reinstalați produsul dumneavoastră Bitdefender.

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

  Pentru a soluționa această problemă, urmați pașii de mai jos:

  1. Reporniți sistemul în Safe Mode. Pentru a afla cum să procedați, consultați *„Cum pot să repornesc sistemul în Safe Mode?"* (p. 78).
  2. Ștergeți cealaltă soluție de securitate din sistem:
     - În **Windows 7**:
       a. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programe și Caracteristici**.
       b. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Ștergere**.
       c. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
     - În **Windows 8 și Windows 8.1**:
       a. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control" direct în ecranul de Start) și faceți clic pe pictograma acestuia.
       b. Faceți clic pe **Dezinstalare programe** sau **Programe și Caracteristici**.
       c. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Ștergere**.
       d. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
     - În **Windows 10**:
       a. Faceți clic pe **Start**, apoi pe Setări.
       b. Faceți clic pe pictograma **Sistem** din secțiunea Setări, apoi selectați **Aplicații instalate**.
       c. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Dezinstalare**.
       d. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

Pentru a dezinstala celălalt software în mod corect, mergeți pe site-ul web al producătorului și lansați instrumentul de dezinstalare sau contactați direct producătorul, solicitând instrucțiunile de dezinstalare.

3. Reporniți sistemul în modul normal și reinstalați Bitdefender.

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

Pentru a soluționa această problemă, urmați pașii de mai jos:

1. Reporniți sistemul în Safe Mode. Pentru a afla cum să procedați, consultați *„Cum pot să repornesc sistemul în Safe Mode?”* (p. 78).
2. Cu ajutorul funcției System Restore din Windows puteți restabili computerul la o dată anterioară instalării produsului Bitdefender.
3. Reporniți sistemul în modul normal și contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea *„Solicitarea ajutorului”* (p. 204).

29. ELIMINAREA PROGRAMELOR MALWARE DIN SISTEMUL DUMNEAVOASTRĂ

Virușii și celelalte amenințări malware vă pot afecta sistemul în moduri diferite, iar modul de acțiune al Bitdefender depinde de tipul de atac malware. Deoarece virușii 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 infecția malware din sistemul dumneavoastră. În astfel de cazuri, este necesară intervenția dumneavoastră.

- *„Mediul de recuperare Bitdefender"* (p. 194)
- *„Ce trebuie să faceți atunci când Bitdefender detectează viruși pe computerul dumneavoastră?"* (p. 196)
- *„Cum elimin un virus dintr-o arhivă?"* (p. 198)
- *„Cum elimin un virus dintr-o arhivă de e-mail?"* (p. 199)
- *„Ce trebuie să fac dacă suspectez că un fișier este periculos?"* (p. 200)
- *„Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?"* (p. 201)
- *„Ce reprezintă elementele omise din jurnalul de scanare?"* (p. 201)
- *„Ce reprezintă fișierele supracomprimate din jurnalul de scanare?"* (p. 201)
- *„De ce Bitdefender a șters în mod automat un fișier infectat?"* (p. 202)

Dacă problema dumneavoastră nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic a Bitdefender folosind informațiile din capitolul *„Solicitarea ajutorului"* (p. 204).

29.1. Mediul de recuperare Bitdefender

Mediu de recuperare este o caracteristică a Bitdefender care vă permite să scanați și să dezinfectați toate partițiile hard discului de pe sistemul de operare.

După ce ați instalat Bitdefender Internet Security 2016, Mediu de recuperare poate fi utilizat chiar dacă nu mai puteți reporni sistemul din Windows.

Pornirea sistemului în Mediu de recuperare

Puteți accesa Mediul de recuperare în unul dintre următoarele două moduri:

Din interfața Bitdefender

Pentru a accesa Mediul de recuperare direct din Bitdefender, urmați acești pași:

1. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
2. Selectați secțiunea **Protecție**.
3. Din modulul **Antivirus**, selectați **Mediul de recuperare**.

   Va apărea o fereastră de confirmare. Faceți clic pe **Da** pentru a reporni calculatorul.
4. După ce este repornit computerul, va apărea un meniu care vă va solicita să selectați un sistem de operare. Selectați **Mediul de recuperare Bitdefender** și apăsați tasta **Enter** pentru a porni într-un mediu Bitdefender din care puteți elibera partiția Windows.
5. În cazul în care vi se solicită, apăsați **Enter** și ajustați rezoluția ecranului la valoarea cea mai apropiată de cea pe care o folosiți de obicei. Apoi apăsați din nou pe **Enter**.

   Mediul de recuperare pentru Bitdefender se va încărca în câteva momente.

Porniți computerul direct în Mediul de recuperare

În cazul în care nu mai pornește Windows, puteți porni computerul direct în Mediul de recuperare al Bitdefender, urmând pașii de mai jos:

1. Porniți / reporniți computerul și începeți să apăsați pe tasta **space** de pe tastatură înainte de apariția logoului Windows.
2. Va fi afișat un meniu care vă va ruga să selectați un sistem de operare pentru a începe. Apăsați pe **TAB** pentru a accesa zona instrumentelor. Alegeți **imaginea de salvare Bitdefender** și apăsați pe tasta **Enter** pentru a reporni dintr-un mediu Bitdefender de unde vă puteți curăța partiția Windows.
3. În cazul în care vi se solicită, apăsați **Enter** și ajustați rezoluția ecranului la valoarea cea mai apropiată de cea pe care o folosiți de obicei. Apoi apăsați din nou pe **Enter**.

Mediul de recuperare pentru Bitdefender se va încărca în câteva momente.

Scanarea sistemului în Mediul de recuperare

Pentru a scana sistemul atunci când se află în Mediul de recuperare, urmați pașii de mai jos:

1. Accesați Mediul de recuperare, conform descrierii din „Pornirea sistemului în Mediu de recuperare" (p. 195).
2. Va apărea logo-ul Bitdefender și motoarele antivirus vor începe să fie copiate.
3. Va fi afișată o fereastră de întâmpinare. Faceți clic pe **Continue**.
4. Este inițiată o actualizare a semnăturilor antivirus.
5. După ce s-a finalizat actualizarea, va apărea fereastra pentru scanarea antivirus la cerere a Bitdefender.
6. Faceți clic pe **Scanează acum**, selectați locația de scanat din fereastra care apare și faceți clic pe **Deschidere** pentru a începe scanarea.

   Este recomandat scanarea întregii partiții Windows.

   > **Notă**
   > Atunci când lucrați în Mediul de recuperare, veți întâlni denumiri de partiții de tip Linux. Partițiile discului vor fi afișate ca sda1 corespunzând probabil (C:) partiție de tip Windows, sda2 corespunzând (D:) și așa mai departe..

7. Așteptați finalizarea procesului de scanare. Dacă este detectat vreun program malware, urmați instrucțiunile pentru a elimina amenințarea.
8. Pentru a ieși din Mediul de recuperare, faceți clic dreapta în secțiunea liberă de pe desktop, selectați **Ieșire** din meniul care apare și apoi selectați dacă doriți să reporniți sau să închideți computerul.

29.2. Ce trebuie să faceți atunci când Bitdefender detectează viruși pe computerul dumneavoastră?

Puteți afla că în calculatorul dumneavoastră se află un virus într-unul dintre aceste moduri:

- V-ați scanat calculatorul și Bitdefender a găsit elemente infectate pe acesta.
- O alertă de viruși vă informează că Bitdefender a blocat unul sau mai mulți viruși pe calculatorul dumneavoastră.

În astfel de situații, actualizați Bitdefender pentru a vă asigura că aveți cele mai recente semnături malware și efectuați o scanare a sistemului pentru analizarea acestuia.

După finalizarea scanării sistemului, selectați acțiunea dorită pentru elementele infectate (dezinfectare, ștergere, mutare în carantină).

Avertisment
În cazul în care considerați că fișierul face parte din sistemul de operare Windows sau că nu este un fișier infectat, nu urmați acești pași și contactați serviciul de asistență clienți Bitdefender cât mai curând posibil.

Dacă acțiunea selectată nu a putut fi efectuată, iar jurnalul de scanare indică o infectare care nu a putut fi eliminată, trebuie să ștergeți fișierul/fișierele manual:

Prima metodă poate fi utilizată în modul normal:

1. Dezactivați protecția antivirus în timp real a Bitdefender:
   a. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
   b. Selectați secțiunea **Protecție**.
   c. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Scut**.
   d. Faceți clic pe comutator pentru a dezactiva **scanarea la accesare**.
2. Afișați elementele ascunse din Windows. Pentru a afla cum să procedați, consultați *„Cum pot afișa elementele ascunse din Windows?"* (p. 76).
3. Mergeți la locația unde se găsește fișierul infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Activați protecția antivirus în timp real a Bitdefender.

În cazul în care prima metodă nu a reușit să elimine infecția, urmați acești pași:

1. Reporniți sistemul în Safe Mode. Pentru a afla cum să procedați, consultați *„Cum pot să repornesc sistemul în Safe Mode?"* (p. 78).

2. Afișați elementele ascunse din Windows. Pentru a afla cum să procedați, consultați *„Cum pot afișa elementele ascunse din Windows?”* (p. 76).
3. Mergeți la locația unde se găsește fișierul infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Reporniți sistemul în mod normal.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 204).

29.3. Cum elimin un virus 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 virușilor din acestea însă nu poate lua niciun fel de măsură în acest sens.

Dacă Bitdefender vă anunță că a fost detectat un virus într-o arhivă și nu este disponibilă nicio acțiune, aceasta înseamnă că eliminarea virusului nu este posibilă din cauza restricțiilor legate de setările referitoare la permisiunile arhivelor.

Iată cum puteți elimina un virus stocat într-o arhivă:

1. Identificați arhiva care conține virusul în urma unei scanări a sistemului.
2. Dezactivați protecția antivirus în timp real a Bitdefender:
   a. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
   b. Selectați secțiunea **Protecție**.
   c. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Scut**.
   d. Faceți clic pe comutator pentru a dezactiva **scanarea la accesare**.
3. Accesați locația arhivei și dezarhivați-o utilizând o aplicație de arhivare, cum ar fi WinZip.

4. Identificați fișierul infectat și ștergeți-l.
5. Ștergeți arhiva inițială pentru a vă asigura că fișierul infectat este eliminat în totalitate.
6. Recomprimați fișierele într-o nouă arhivă utilizând o aplicație de arhivare, cum ar fi WinZip.
7. Activați protecția antivirus în timp real a Bitdefender și executați o scanare completă a sistemului pentru a vă asigura că sistemul nu este infectat.

Notă
Este important de reținut faptul că un virus aflat într-o arhivă nu reprezintă o amenințare imediată la adresa sistemului dumneavoastră deoarece virusul trebuie să fie dezarhivat și executat pentru a putea infecta calculatorul.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 204).

29.4. Cum elimin un virus dintr-o arhivă de e-mail?

Bitdefender poate de asemenea să identifice viruși 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 puteți elimina un virus stocat într-o arhivă de e-mail:

1. Scanați baza de date de e-mail folosind Bitdefender.
2. Dezactivați protecția antivirus în timp real a Bitdefender:
   a. Faceți clic pe pictograma  din colțul din stânga jos al interfeței Bitdefender.
   b. Selectați secțiunea **Protecție**.
   c. Faceți clic pe modulul **Antivirus** și apoi selectați secțiunea **Scut**.
   d. Faceți clic pe comutator pentru a dezactiva **scanarea la accesare**.
3. Deschideți raportul de scanare și utilizați informațiile de identificare (Subiect, De la, Către) aferente mesajelor infectate pentru a le localiza în clientul de e-mail.

4. Ștergeți mesajele infectate. Majoritatea clienților de e-mail mută mesajul șters într-un director de recuperare, de unde acesta poate fi recuperat. Trebuie să vă asigurați că mesajul este șters și din acest director de recuperare.
5. Arhivați directorul în care se află mesajul infectat.
   - În Outlook Express: În meniul File, faceți clic pe Folder și apoi pe Compact All Folders.
   - În Microsoft Outlook 2007: În meniul File, faceți clic pe Data File Management. Selectați fișierele din directoarele personale (.pst) pe care intenționați să le compactați și faceți clic pe Settings. Faceți clic pe Compactare acum.
   - În Microsoft Outlook 2010 / 2013: Din meniul Fișier, selectați Detalii și apoi Setări cont (Adăugare sau eliminare conturi sau modificare setări de conectare existente) Apoi faceți clic pe Fișier de date, selectați fișierele din directoarele personale (.pst) pe care intenționați să le compactați și faceți clic pe Setări. Faceți clic pe Compactare acum.
6. Activați protecția antivirus în timp real a Bitdefender.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 204).

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

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

Pentru a vă asigura că sistemul dumneavoastră este protejat, urmați pașii de mai jos:

1. Executați o **scanare a sistemului** cu Bitdefender. Pentru a afla cum să procedați, consultați *„Cum îmi scanez sistemul?”* (p. 60).
2. Dacă procesul de scanare nu a detectat nimic, dar încă aveți dubii cu privire la fișier, contactați reprezentanții serviciul de asistență pentru ajutor.

   Pentru a afla cum să procedați, consultați *„Solicitarea ajutorului”* (p. 204).

29.6. Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?

Aceasta reprezintă doar o notificare referitoare la faptul că Bitdefender a detectat aceste fișiere ca fiind protejate fie prin parolă, fie cu o anumită formă de criptare.

Cel mai frecvent, elementele protejate prin parolă sunt următoarele:

- Fișiere care aparțin unei alte soluții de securitate.
- Fișiere care aparțin sistemului de operare.

Pentru a putea scana conținutul, aceste fișiere trebuie să fie extrase sau decriptate.

În cazul în care conținutul respectiv este extras, Bitdefender va scana automat conținutul pentru a vă proteja calculatorul. Dacă doriți să scanați acele fișiere folosind Bitdefender, trebuie să contactați producătorul produsului pentru a obține mai multe detalii despre respectivele fișiere.

Noi vă recomandăm să ignorați acele fișiere deoarece acestea nu reprezintă o amenințare pentru sistemul dumneavoastră.

29.7. 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.

29.8. 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.

29.9. 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 malware, 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 vă aflați într-o astfel de situație, descărcați fișierul de instalare de pe site-ul web al producătorului sau de pe un alt site web sigur.

CONTACTAȚI-NE

30. SOLICITAREA AJUTORULUI

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

Secțiunea *„Soluționarea problemelor frecvente"* (p. 171) vă oferă informațiile necesare referitoare la cele mai frecvent întâlnite probleme atunci când utilizați acest produs.

Dacă nu găsiți un răspuns la întrebarea dumneavoastră printre resursele puse la dispoziție, ne puteți contacta direct:

- „Contactați-ne direct din cadrul produsului dumneavoastră Bitdefender" (p. 204)
- „Contactați-ne prin intermediul Centrului nostru de asistență online" (p. 205)

Contactați-ne direct din cadrul produsului dumneavoastră Bitdefender

Dacă dispuneți de o conexiune la internet funcțională, puteți contacta Bitdefender pentru asistență direct din interfața produsului dumneavoastră.

Urmați acești pași:

1. Faceți clic pe pictograma  din partea de sus a interfeței Bitdefender și selectați **Ajutor & asistență** din meniul derulant.
2. Aveți la dispoziție următoarele opțiuni:
   - **Documentație de produs**

     Accesați baza noastră de date și căutați informațiile necesare.
   - **Contactați serviciul de asistență**

     Folosiți butonul **Contactare asistență** pentru a lansa Instrumentul de asistență Bitdefender și pentru a contacta Serviciul de asistență clienți.

Puteți naviga prin programul asistent cu ajutorul butonului **Înainte**. Pentru a părăsi asistentul, faceți clic pe **Anulează**.

a. Selectați căsuța de acceptare și faceți clic pe **Înainte**.

b. Completați formularul cu datele necesare:

   i. Introduceți adresa dumneavoastră de e-mail.

   ii. Introduceți numele complet.

   iii. Introduceți o descriere a problemei întâmpinate.

   iv. Bifați opțiunea **Încercare de reproducere a problemei înainte de transmitere** în cazul în care întâmpinați o problemă cu produsul. Continuați cu următorii pași.

c. Vă rugăm să așteptați câteva minute pentru ca Bitdefender să adune informații referitoare la produs. Aceste informații îi vor ajuta pe inginerii noștri să găsească o soluție la problema dumneavoastră.

d. Faceți clic pe **Finalizare** pentru a transmite informațiile la Departamentul de asistență clienți Bitdefender. Veți fi contactat cât mai curând posibil.

Contactați-ne prin intermediul Centrului nostru de asistență online

Dacă nu puteți accesa informațiile necesare utilizând produsul Bitdefender, consultați Centrul nostru online de asistență:

1. Mergeți la http://www.bitdefender.ro/support/consumer.html.

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

2. Folosiți bara de căutare din partea de sus a ferestrei pentru a găsi articole care v-ar putea oferi o soluție la problema dumneavoastră. Pentru a efectua o căutare, introduceți un cuvând în bara de căutare și faceți clic pe **Căutare**.

3. Citiți articolele sau documentele relevante și încercați soluțiile propuse.

4. Dacă soluția propusă nu vă ajută să rezolvați problema, mergeți la

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

31. RESURSE ONLINE

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

- Centrul de asistență Bitdefender:

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

- Forumul de suport al Bitdefender:

  http://forum.bitdefender.com

- Portalul de securitate informatică HOTforSecurity:

  http://www.hotforsecurity.com

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

31.1. 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 virușilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Centrul de asistență Bitdefender este deschis publicului și pot fi realizate căutări în mod liber. Prin intermediul informațiilor extinse pe care le conține, putem oferi clienților Bitdefender cunoștințele tehnice și înțelegerea de care au nevoie. Toate solicitările valide 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

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

31.2. Forumul de suport al Bitdefender

Forumul de suport al Bitdefender le oferă utilizatorilor Bitdefender o modalitate facilă de a obține ajutor și de a-i ajuta pe alții.

În cazul în care produsul dumneavoastră Bitdefender nu funcționează bine, nu poate înlătura anumiți viruși de pe calculator sau dacă aveți întrebări referitoare la modul de funcționare, postați problema sau întrebarea pe forum.

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

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

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

31.3. Portalul HOTforSecurity

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

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

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

32. INFORMAȚII DE CONTACT

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 10 ani BitDefender a câștigat o reputație indisputabilă în depășirea așteptărilor clienților și partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

32.1. Adrese web

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

32.2. Distribuitori locali

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

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergeți la http://www.bitdefender.com/partners/partner-locator.html.
2. Selectați țara și orașul folosind opțiunile corespunzătoare.
3. În cazul în care nu găsiți un distribuitor Bitdefender în țara dumneavoastră, nu ezitați să ne contactați prin e-mail la adresa sales@bitdefender.com. Vă rugăm să scrieți mesajul în engleză pentru a ne da posibilitatea să vă ajutăm cu promptitudine.

32.3. 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: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.com

Germania

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

Spania

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Vânzări: comercial@bitdefender.es
Suport tehnic: http://www.bitdefender.es/support/consumer.html
Site-ul web: http://www.bitdefender.es

România

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest

Fax: +40 21 2641799
Telefon vânzări: +40 21 2063470
E-mail vânzări: sales@bitdefender.ro
Suport tehnic: http://www.bitdefender.ro/support/consumer.html
Site-ul web: http://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: http://www.bitdefender.com/support/consumer.html
Site-ul web: http://www.bitdefender.com

Vocabular

ActiveX

ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe și sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini Web interactive care se comportă ca niște aplicații și nu ca niște simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane și să interacționeze și în alte moduri cu pagina Web. Controalele ActiveX sunt adesea scrise utilizând limbajul Visual Basic.

Active X este cunoscut pentru lipsa totală de control al securității; experții în securitatea calculatoarelor descurajează utilizarea lui pe Internet.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

Bitdefender dispune de modulul său propriu care realizează actualizarea automatică sau manuală.

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.

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 acest program malware.

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 virusului în rețea este prin intermediul unui fișier PDF sau un 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.

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 furnizorului.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în bara de sarcini Windows (de obicei în partea de jos, lângă ceas) și conține pictograme miniaturale pentru accesul rapid la aplicații de sistem cum ar fi cele legate de fax, imprimantă, modem, volum și altele. Faceți dublu-clic sau clic dreapta cu mouse-ul pe o pictogramă pentru a vizualiza și accesa detaliile și comenzile.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza și încărca pagini de Web. Browserele cele mai des folosite includ Microsoft Internet Explorer, Mozilla Firefox și Google Chrome. Acestea sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafice cât și text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet și animație.

Cale fișier

Reprezintă direcția exactă către un fișier de pe un calculator. Această direcție este specificată utilizând sistemul ierarhic de organizare a fișierelor de sus în jos.

Ruta între două puncte, cum ar fi de exemplu canalul de comunicație între două computere.

Client de mail

Un client de mail este o aplicație care vă permite să trimiteți și să recepționați mesaje.

Cod de activare

Este o cheie unică ce poate fi cumpărată de la distribuitorii retail și folosită pentru a activa un anumit produs sau serviciu. Codul de activare permite activarea unui abonament valabil pentru o anumită perioadă de timp și un anumit număr de dispozitive și poate fi, de asemenea, folosit pentru prelungirea unui abonament, cu condiția ca acesta să fie generat pentru același produs sau serviciu.

Cookie

În domeniul Internetului, cookie-urile reprezintă mici fișiere ce conțin informații despre fiecare calculator care pot fi analizate și folosite de către cei care publică reclame pentru a vă urmări interesele și preferințele online. În acest domeniu, tehnologia cookie-urilor este în curs de dezvoltare, iar intenția este de a afișa direct acele anunțuri care corespund intereselor dumneavoastră. Această facilitate are avantaje și dezavantaje pentru mulți deoarece, pe de o parte, este eficientă și pertinentă din moment ce vizualizați doar acele anunțuri despre subiecte care vă interesează. Pe de altă parte, cookie-urile implică de fapt o "monitorizare" și "urmărire" a site-urilor vizitate și a link-urilor accesate. Astfel, în mod logic, părerile sunt împărțite în ceea ce privește confidențialitatea și mulți se simt jigniți de faptul că sunt văzuți ca un

simplu "număr SKU" (este vorba de codul de bare de pe spatele ambalajelor care este scanat pe bandă la supermarket). Deși acest punct de vedere poate fi considerat extrem, în anumite cazuri el reprezintă chiar ceea ce se întâmplă în realitate.

Descărcare

Reprezintă copierea (de obicei a unui întreg fișier) de pe o sursă principală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fișier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi și la copierea unui fișier de pe un server de rețea pe un calculator din rețea.

Drive de disc

Este un dispozitiv care citește date de pe un disc și scrie date pe un disc.

Un drive de hard disc citește / scrie date de pe / pe hard disc.

Un drive de floppy accesează dischetele floppy.

Drive-ele de disc pot fi sau interne (incorporate în interiorul unui calculator) sau externe (plasate într-o locație separată care este conectată la calculator).

E-mail

Se referă la poșta electronică. Acesta este un serviciu care transmite mesaje către alte calculatoare prin intermediul rețelei locale sau globale.

Elemente din startup

Orice fișier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, și nu direct fișierul.

Evenimente

O acțiune sau întâmplare detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

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.

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 keylogger este o aplicație care înregistrează orice tastați.

Keyloggerele nu au o natură periculoasă. Pot fi folosite în scopuri legitime, cum ar fi monitorizarea activității angajaților sau a companiilor subordonate. Cu toate acestea, utilizarea lor de către infractorii cibernetici în scopuri negative este din ce în ce mai răspândită (de exemplu, pentru colectarea informațiilor cu caracter privat, cum ar fi acreditările de înregistrare și codurile numerice personale).

Licențiere

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.

Linie de comandă

Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruși noi. Această metodă de scanare nu se bazează pe semnături de viruși cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. 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 semnături de viruși cunoscuți. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus 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 protecției antivirus asupra performanțelor. Prin monitorizarea activității calculatorului dvs. 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 vă dau posibilitatea de a arhiva un fișier astfel încât să ocupe mai putină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați.

Totuși, un program care arhivează fișiere va înlocui caracterele de spațiu printr-un caracter special reprezentând spațiu, urmat de un număr care reprezintă numărul de spații înlocuite. În acest caz, cele zece caractere reprezentând spațiu ar necesita doar doi biți. Aceasta este doar un exemplu de comprimare - există multe alte metode în afară de aceasta.

Ransomware

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

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

Rootkit

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

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

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

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.

Semnătură virus

Reprezintă tiparul binar al unui virus, utilizat de un program antivirus pentru detecția și eliminarea virusului.

Spam

Termen ce acoperă întreaga gamă a mesajelor electronice nesolicitate (junk). În general, acestea sunt cunoscute sub numele de mesaje electronice nesolicitate.

Spyware

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

Asemănarea dintre spyware și un 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.

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 viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină virușii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruși pe calculatorul dumneavoastră.

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.

Utilizare 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.

Vierme

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

Virus

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

Virus de boot

Reprezintă un virus 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 virusul să devină activ în memorie. Din acest moment de fiecare dată când veți realiza boot-area sistemului, virusul va deveni activ în memorie.

Virus de macro

Un tip de virus informatic este acela inclus 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

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