ANTIVIRUS PLUS 2012

Manual de utilizare

Bitdefender Antivirus Plus 2012
Manual de utilizare

Publication date 2011.07.27

Termeni legali


Bitdefender

Cuprins

1. Instalare 1
1.1. Pregătirea pentru instalare 1
1.2. Cerințe de sistem 1
1.2.1. Cerințe minime de sistem 1
1.2.2. Cerințe recomandate de sistem 2
1.2.3. Cerințe software 2
1.3. Instalarea produsului dumneavoastră Bitdefender 2
1.3.1. Promovarea de la o versiune mai veche 5
2. Primii pași 6
2.1. Deschiderea Bitdefender 6
2.2. Ce trebuie să faceți după instalare 6
2.3. Înregistrare produs 7
2.3.1. Specificarea seriei de licență 7
2.3.2. Autentificare în MyBitdefender 8
2.3.3. Achiziționarea sau reînnoirea seriilor de licență 10
2.4. Reparare probleme 10
2.4.1. Asistentul de remediere a tuturor problemelor 11
2.4.2. Configurarea alertelor de stare 12
2.5. Evenimente 12
2.6. Pilot automat 13
2.7. Modul pentru jocuri și Modul pentru laptop 14
2.7.1. Mod jocuri 14
2.7.2. Mod laptop 16
2.8. Protecție cu parolă pentru setările Bitdefender 16
2.9. Rapoarte anonime privind consumul 17
2.10. Repararea sau dezinstalarea Bitdefender 17
3. Interfața Bitdefender 19
3.1. Pictograma barei de sistem 19
3.2. Fereastra principală 20
3.2.1. Bara de instrumente din partea superioară 21
3.2.2. Secțiunea panourilor 21
3.3. Fereastra setărilor 24
4. Cum să 26
4.1. Cum pot înregistra o versiune de încercare? 26
4.2. Cum înregistrez Bitdefender fără a fi conectat la internet? 27
4.3. Cum trec la un produs superior din gama Bitdefender 2012? 28
4.4. Când este cazul să reinstalez Bitdefender? 28
4.5. Când expiră protecția oferită de produsul meu Bitdefender? 29
4.6. Cum îmi reînnoiesc protecția Bitdefender? 29
4.7. Ce produs Bitdefender folosesc? 29
4.8. Cum scanez un fișier sau un director? 30
4.9. Cum îmi scanez sistemul? 30
4.10. Cum creez o activitate de scanare personalizată? 30
4.11. Cum exclud un director de la procesul de scanare? 31
4.12. Ce să fac atunci când Bitdefender a detectat un fișier curat ca fiind infectat? ... 31

4.13. Cum îmi protejez informațiile personale? 32
4.14. Cum pot configura Bitdefender să utilizeze o conexiune la internet de tip proxy? 33

5. Protecție antivirus 35
5.1. Scanare la accesare (protecție în timp real) 36
5.1.1. Verificarea programelor periculoase detectate în urma scanării la accesare 36
5.1.2. Reglarea nivelului de protecție în timp real 37
5.1.3. Crearea unui nivel de protecție personalizat 37
5.1.4. Restaurarea setărilor implicite 39
5.1.5. Activarea sau dezactivarea protecției în timp real 39
5.1.6. Acțiuni luate împotriva atacurilor malware detectate 40
5.2. Scanare la cerere 41
5.2.1. Scanare automată 41
5.2.2. Scanarea unui fișier sau a unui director pentru detectarea malware 41
5.2.3. Rularea unei scanări rapide 42
5.2.4. Executarea unei scanări complete a sistemului 42
5.2.5. Configurarea și executarea unui proces de scanare personalizat 43
5.2.6. Programul asistent de scanare 45
5.2.7. Examinarea jurnalelor de scanare 48
5.3. Scanarea automată a suporturilor media amovibile 49
5.3.1. Cum funcționează? 49
5.3.2. Administrarea scanării a fișierelor media amovibile 50
5.4. Configurarea excepțiilor de la scanare 50
5.4.1. Excluderea fișierelor sau directoarelor de la scanare 51
5.4.2. Excluderea extensiilor de fișiere de la scanare 51
5.4.3. Administrarea excepțiilor de la scanare 52
5.5. Gestionarea fișierelor aflate în carantină 53
5.6. Active Virus Control 54
5.6.1. Verificarea aplicațiilor detectate 54
5.6.2. Activarea sau dezactivarea funcției Active Virus Control 54
5.6.3. Ajustarea protecției Active Virus Control 55
5.6.4. Administrarea proceselor excluse 55
5.7. Remedierea vulnerabilităților sistemului 56
5.7.1. Scanarea sistemului pentru identificarea vulnerabilităților 56
5.7.2. Cu ajutorul monitorizării automate a vulnerabilităților 57

6. Control date 60
6.1. Protecție antiphishing 60
6.1.1. Protecție Bitdefender în browser-ul web 61
6.1.2. Alertele Bitdefender sunt afișate în browser 62
6.2. Protecție date 63
6.2.1. Despre protecția datelor 63
6.2.2. Configurarea protecției datelor 64
6.2.3. Administrarea regulilor 65
6.3. Criptare chat 65

7. Hartă rețea 67
7.1. Activarea rețelei Bitdefender 67
7.2. Adăugarea computerelor la rețeaua Bitdefender 68

7.3. Administrarea rețelei Bitdefender 68
8. Actualizare 71
8.1. Cum verificați dacă Bitdefender este actualizat 71
8.2. Efectuarea unei actualizări 72
8.3. Activarea sau dezactivarea actualizării automate 72
8.4. Ajustarea setărilor de actualizare 73
9. Protecție Safego pentru rețelele sociale 75
10. Remedierea problemelor 76
10.1. Sistemul meu funcționează lent 76
10.2. Nu începe scanarea 77
10.3. Nu mai pot utiliza o anumită aplicație 77
10.4. Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet 78
10.5. Computerul meu nu este conectat la internet. Cum actualizez Bitdefender? 79
10.6. Serviciile Bitdefender nu răspund 79
10.7. Nu s-a reușit dezinstalarea Bitdefender 80
10.8. Sistemul meu nu pornește după ce am instalat Bitdefender 81
11. Eliminarea programelor malware din sistemul dumneavoastră 83
11.1. Modul de salvare Bitdefender 83
11.2. Ce trebuie să faceți atunci când Bitdefender detectează viruși pe computerul dumneavoastră? 85
11.3. Cum elimin un virus dintr-o arhivă? 86
11.4. Cum elimin un virus dintr-o arhivă de e-mail? 87
11.5. Ce trebuie să fac dacă suspectez că un fișier este periculos? 88
11.6. Cum să curățați fișierele infectate din System Volume Information 88
11.7. Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare? 90
11.8. Ce reprezintă elementele omise din jurnalul de scanare? 90
11.9. Ce reprezintă fișierele supracomprimate din jurnalul de scanare? 90
11.10. De ce Bitdefender a șters în mod automat un fișier infectat? 91
12. Obținere ajutor 92
12.1. Suport 92
12.1.1. Resurse online 92
12.1.2. Solicitarea ajutorului 93
12.2. Informații de contact 95
12.2.1. Adrese web 95
12.2.2. Distribuitori locali 95
12.2.3. Filialele Bitdefender 96
13. Informații utile 98
13.1. Cum dezinstalez alte soluții de securitate? 98
13.2. Cum pot să repornesc sistemul în Safe Mode? 99
13.3. Utilizez o versiune Windows pe 32 biți sau pe 64 biți? 99
13.4. Cum folosesc funcția System Restore în Windows? 100
13.5. Cum pot afișa elementele ascunse din Windows? 100
Vocabular 102

1. Instalare

1.1. Pregătirea pentru instalare

Pentru a instala Bitdefender Antivirus Plus 2012 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. 1).
- 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.
- 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.

1.2. Cerințe de sistem

Puteți instala Bitdefender Antivirus Plus 2012 doar pe calculatoare pe care rulează următoarele sisteme de operare:

- Windows XP cu Service Pack 3 (32 bit)
- Windows Vista cu Service Pack 2
- Windows 7 cu Service Pack 1

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

Notă

Pentru a afla sistemul de operare Windows care rulează pe calculatorul dumneavoastră, precum și informații hardware, faceți clic-dreapta pe iconița **My Computer** de pe desktop și apoi selectați **Properties** din meniu.

1.2.1. Cerințe minime de sistem

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

1.2.2. Cerințe recomandate de sistem

- 2.8 GB spațiu liber disponibil pe hard disk (cel puțin 800 MB pe unitatea de sistem)
- Intel Core Duo (1.66 GHz) sau procesor echivalent
- RAM:
  - 1 GB pentru Windows XP
  - 1.5 GB pentru Windows Vista și Windows 7

1.2.3. Cerințe software

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

- Internet Explorer 7 sau o versiune mai recentă
- Mozilla Firefox 3.6 sau avansat
- Yahoo! Messenger 8.1 sau o versiune mai recentă
- .NET Framework 3

1.3. Instalarea produsului dumneavoastră Bitdefender

Puteți instala Bitdefender de pe CD-ul de instalare Bitdefender sau folosind fișierul de instalare web descărcat pe computerul dumneavoastră de pe site-ul Bitdefender sau de pe alte site-uri web autorizate (de exemplu, site-ul web al unui partener Bitdefender sau un magazin online).Puteți descărca fișierul de instalare de pe site-ul Bitdefender: http://www.bitdefender.com/site/Downloads/.

- Pentru a instala Bitdefender de pe CD-ul de instalare, introduceți CD-ul în unitatea optică.Un ecran de întâmpinare ar trebui să apară în câteva secunde. Urmați instrucțiunile pentru a începe instalarea.

  Notă

  Ecranul de întâmpinare 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.

  În cazul în care nu apare ecranul de întâmpinare, mergeți la directorul rădăcină al CD-ului și faceți dublu clic pe fișierul `autorun.exe`.

- Pentru a instala Bitdefender folosind fișierul de instalare web descărcat pe calculator, localizați fișierul și faceți dublu-clic pe el.Aceasta va iniția descărcarea fișierelor de instalare, lucru ce poate dura o anumită perioadă de timp, în funcție de conexiunea dumneavoastră la internet.

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.

Notă

Este posibil să fie nevoie să reporniți computerul pentru a finaliza dezinstalarea programelor antivirus detectate.

Urmați instrucțiunile asistentului de instalare pentru a instala Bitdefender Antivirus Plus 2012.

Pasul 1 - Bun venit

Vă rugăm să citiți Contractul de licență și să selectați **Sunt de acord & Continuă**.Contractul de licență conține termenii și condițiile conform cărora puteți folosi Bitdefender Antivirus Plus 2012.

Notă

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

Pasul 2 - Înregistrați-vă produsul

Pentru a finaliza înregistrarea produsului dumneavoastră e nevoie să introduceți o cheie de licență și de a crea contul MyBitdefender.Este necesară o conexiune activă la internet.

Procedați în funcție de situația dumneavoastră:

- **Am achiziționat produsul**

  În acest caz, înregistrați produsul urmând acești pași:

  1. Selectați **Am achiziționat produsul și doresc să-l înregistrez acum**.
  2. Introduceți seria de licență în câmpul corespunzător.

Notă

Puteți găsi seria dumneavoastră de înregistrare:

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

3. Introduceți adresa dumneavoastră de e-mail în câmpul corespunzător.

Important

Este necesară o adresă de e-mail validă.Un mesaj de confirmare va fi trimis la adresa pe care ne-ați pus-o la dispoziție.

4. Faceți clic pe **Înregistrare**.

- **Doresc să evaluez Bitdefender**

  În acest caz, puteți utiliza produsul pe o perioadă de 30 de zile.Pentru a începe perioada de evaluare, selectați **Doresc să evaluez acest produs**.

  Pentru a utiliza caracteristicile online ale produsului, e necesară crearea contului MyBitdefender.Pentru a crea un cont, introduceți adresa dumneavoastră de e-mail în câmpul corespunzător.Un mesaj de confirmare va fi trimis la adresa pe care ne-ați pus-o la dispoziție.Dacă aveți deja un cont, introduceți adresa de e-mail aferentă acestuia pentru a vă înregistra produsul în contul respectiv.

Setări personalizate

Opțional, pe parcursul acestei etape, puteți personaliza setările de instalare făcând clic pe **Setări personalizate**.

Calea de instalare

În mod implicit, Bitdefender Antivirus Plus 2012 va fi instalat în `C:\Program Files\Bitdefender\Bitdefender 2012`.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

Pentru înregistrarea produsului, Bitdefender Antivirus Plus 2012 necesită acces la internet, descărcarea actualizărilor produsului și a celor de securitate, ale componentelor opțiunii 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.

Activare actualizare P2P

Puteți partaja fișierele produsului și semnăturile cu alți utilizatori Bitdefender.În acest mod, actualizările Bitdefender pot fi realizate mai rapid.Dacă nu doriți să activați această funcție, bifați căsuța corespunzătoare.

Notă

Nicio informație personală identificabilă nu va fi partajată dacă această funcție este activată.

Dacă doriți să reduceți impactul traficului din rețea asupra performanței sistemului în timpul actualizărilor, utilizați opțiunea de partajare a actualizărilor. Bitdefender utilizează porturile 8880 - 8889 pentru actualizarea peer-to-peer (P2P).

Trimite rapoarte anonime privind consumul

Rapoartele anonime privind consumul sunt activate implicit.Prin activarea 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.

Faceți clic pe **OK** pentru a vă confirma preferințele.

Faceți clic pe **Instalare** pentru a iniția instalarea.

Pasul 3 - Progres instalare

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 - Finalizare

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 **Finalizare**.

1.3.1. Promovarea de la o versiune mai veche

Dacă utilizați deja o versiune anterioară a Bitdefender, există două modalități de a trece la Bitdefender Antivirus Plus 2012:

- Instalați Bitdefender Antivirus Plus 2012 direct peste versiunea mai veche.Bitdefender va identifica versiunea anterioară și vă va ajuta să o îndepărtați înainte de a instala versiunea cea nouă.Trebuie să reporniți computerul în timpul actualizării.
- Dezinstalați vechea versiune, apoi reporniți computerul și instalați noua versiune, conform instrucțiunilor din paginile anterioare.Folosiți această metodă de trecere la o versiune superioară de produs dacă cealaltă nu funcționează.

Notă

Setările produsului și conținutul de carantină nu vor fi importate din versiunea anterioară.

2. Primii pași

Odată ce ați instalat Bitdefender Antivirus Plus 2012, calculatorul dumneavoastră este protejat împotriva tuturor tipurilor de programe periculoase (cum ar fi virușii,programele spion și troienii).

Pilotul automat este activat în mod implicit și nu trebuie să configurați nicio setare.Cu toate acestea, puteți profita de setările oferite de Bitdefender pentru a vă ajusta și îmbunătăți protecția.

Bitdefender va lua majoritatea deciziilor legate de securitate în locul dumneavoastră și va afișa rareori alerte pop-up.În fereastra Evenimente sunt disponibile acțiunile aplicate și informații cu privire la funcționarea programului. Pentru mai multe informații, consultați *„Evenimente”* (p. 12).

Din când în când, trebuie să deschideți Bitdefender și să remediați 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.

Dacă nu ați înregistrat produsul (inclusiv prin crearea unui cont MyBitdefender), amintiți-vă să faceți acest lucru până la încheierea perioadei de evaluare.Trebuie să vă creați un cont pentru a putea utiliza caracteristicile online ale produsului.Pentru mai multe informații cu privire la procesul de înregistrare, consultați *„Înregistrare produs”* (p. 7).

2.1. Deschiderea Bitdefender

Pentru a accesa fereastra principală a Bitdefender Antivirus Plus 2012, folosiți meniul Start al Windows, urmând calea **Start → All Programs → Bitdefender 2012 → Bitdefender Antivirus Plus 2012** sau, mai rapid, faceți dublu-clic pe pictograma Bitdefender din bara de sistem.

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

2.2. Ce trebuie să faceți după instalare

Dacă doriți ca Bitdefender să ia toate deciziile legate de securitate în locul dumneavoastră, mențineți activat modul Pilot automat.Pentru mai multe informații, consultați *„Pilot automat”* (p. 13).

Aici aveți o lista de activități pe care este posibil să doriți să le efectuați după instalare:

- 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. 33).

- Dacă ați instalat Bitdefender pe mai multe computere din rețeaua de acasă, puteți gestiona toate produsele Bitdefender la distanță de pe un singur computer.Pentru mai multe informații, consultați *„Hartă rețea”* (p. 67).
- Creați reguli de protecție a datelor pentru a preveni dezvăluirea datelor dumneavoastră importante fără acordul dumneavoastră.Pentru mai multe informații, consultați *„Protecție date”* (p. 63).

2.3. Înregistrare produs

Pentru a beneficia de protecție din partea Bitdefender, trebuie să vă înregistrați produsul, introducând a serie de licență și creând un cont MyBitdefender.

Seria de înregistrare precizează pentru cât timp aveți dreptul de a utiliza produsul.Imediat după expirarea seriei de înregistrare, Bitdefender se va opri din funcționare și nu vă va mai proteja calculatorul.

Este recomandat să achiziționați o serie de înregistrare sau să vă reînnoiți licența cu câteva zile înainte de expirarea seriei actuale de înregistrare.Pentru mai multe informații, consultați *„Achiziționarea sau reînnoirea seriilor de licență”* (p. 10).În cazul în care utilizați o versiune de încercare a Bitdefender, trebuie să o înregistrați cu o serie de licență dacă doriți să utilizați produsul în continuare, după expirarea perioadei de evaluare.

Un cont MyBitdefender vă asigură accesul la actualizări ale produsului și vă permite să utilizați serviciile online oferite de Bitdefender Antivirus Plus 2012.Dacă aveți deja un cont, trebuie să vă înregistrați produsul Bitdefender pe acel cont.

Un cont MyBitdefender vă permite următoarele:

- Mențineți-vă produsul actualizat.
- Notați-vă seria de licență, pentru în cazul în care se întâmplă să o pierdeți.
- Contactați Serviciul de asistență clienți Bitdefender.
- Beneficiați de protecție pentru contul dumneavoastră de Facebook prin intermediul Safego.

2.3.1. Specificarea seriei de licență

Dacă, în timpul instalării, selectați să evaluați produsul, puteți folosi produsul pe o perioadă de încercare de 30 de zile.Pentru a folosi în continuare Bitdefender după expirarea perioadei de încercare, trebuie să înregistrați produsul cu o serie de licență.

Pentru a înregistra produsul cu o serie de licență sau pentru a modifica seria de licență actuală, faceți clic pe link-ul **Informații licență**, situat în partea de jos a ferestrei Bitdefender.Va apărea fereastra de înregistrare.

Puteți vedea starea înregistrării produsului dumneavoastră Bitdefender, seria actuală de înregistrare și câte zile au mai rămas până la expirarea licenței.

Pentru a înregistra Bitdefender Antivirus Plus 2012:

1. Introduceți seria de înregistrare în câmpul editabil.

Notă

Puteți găsi seria dumneavoastră de înregistrare:

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

Dacă nu aveți o serie de licență pentru Bitdefender faceți clic pe link-ul specificat în fereastră pentru a deschide o pagină web, de pe care puteți achiziționa o serie.

2. Faceți clic pe **Înregistrare**.

2.3.2. Autentificare în MyBitdefender

Dacă ați specificat o adresă de e-mail în timpul instalării, v-a fost trimis un e-mail de confirmare la adresa pe care ați menționat-o.Faceți clic pe link-ul primit prin e-mail pentru a finaliza înregistrarea.

În cazul în care nu ați finalizat procesul de înregistrare, Bitdefender vă va notifica de faptul că este necesar să îl finalizați.

Important

Trebuie să creați un cont în 30 de zile după instalarea Bitdefender.În caz contrar, Bitdefender nu se va mai actualiza.

Pentru a crea sau pentru a vă autentifica într-un cont MyBitdefender, faceți clic pe link-ul **Finalizare înregistrare** / **MyBitdefender** din partea inferioară a ferestrei Bitdefender.

Se va deschide fereastra MyBitdefender.Continuați în funcție de situația dumneavoastră.

Doresc să creez un cont MyBitdefender

Pentru a crea cu succes un cont MyBitdefender, urmați acești pași:

1. Selectați **Creare cont nou**.

   Va apărea o nouă fereastră.

2. Introduceți informațiile solicitate în câmpurile corespunzătoare.Informațiile furnizate aici vor rămâne confidențiale.

   - **Nume** - introduceți un nume de utilizator pentru contul dumneavoastră. Acest câmp este opțional.

- **E-mail** - introduceți adresa de e-mail.
- **Parola** - introduceți o parolă pentru contul dumneavoastră.Parola trebuie să aibă cel puțin 6 caractere.
- **Confirmare parolă** - introduceți din nou parola.
- Opțional, Bitdefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră.Pentru a activa această opțiune, selectați **Sunt de acord să primesc e-mail-uri de la Bitdefender**.

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

3. Faceți clic pe **Trimite**.
4. Înainte de a vă putea utiliza contul, trebuie să finalizați înregistrarea. Verificați-vă e-mail-ul și urmați instrucțiunile din e-mail-ul de confirmare trimis de Bitdefender.

Notă
De asemenea. vă puteți autentifica prin intermediul contului de Facebook sau de Google.Pentru mai multe informații, consultați„Doresc să mă autentific prin intermediul contului de Facebook sau Google” (p. 9)

Doresc să mă autentific prin intermediul contului de Facebook sau Google

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

1. Faceți clic pe pictograma serviciului pe care doriți să-l folosiți pentru a vă autentifica.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.

Am deja un cont MyBitdefender

Dacă v-ați conectat și înainte cu un cont de la produsul dumneavoastră, Bitdefender va detecta acest cont și vă va conecta la acel cont.Puteți vizita contul dumneavoastră la http://my.bitdefender.com făcând clic pe **Mergeți la MyBitdefender**.

Dacă doriți să vă autentificați cu un alt cont, faceți clic pe link-ul corespunzător și urmați instrucțiunile din secțiunile anterioare.

Dacă aveți deja un cont activ, dar Bitdefender nu îl detectează, urmați pașii de mai jos pentru a vă autentifica cu contul respectiv.

1. Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.

Notă
Dacă v-ați uitat parola, faceți clic pe **V-ați uitat parola** și urmați instrucțiunile pentru a o recupera.

2. Faceți clic pe **Autentificare**.

2.3.3. Achiziționarea sau reînnoirea seriilor de licență

Dacă perioada de evaluare se va încheia în curând, trebuie să achiziționați o serie de înregistrare și să vă înregistrați produsul.În mod similar, dacă seria de înregistrare actuală va expira în curând, trebuie să vă reînnoiți licența.

Bitdefender vă va avertiza atunci când se apropie data de expirare a licenței dumneavoastră actuale. Urmați instrucțiunile din mesajul de avertizare pentru a achiziționa o nouă licență.

Puteți vizita o pagină web de unde puteți achiziționa oricând o serie de licență, urmând pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe link-ul **Informații licență**, în partea inferioară a ferestrei Bitdefender, pentru a deschide fereastra de înregistrare a produsului.
3. Faceți clic pe link-ul specificat în partea inferioară a ferestrei.

2.4. Reparare probleme

Bitdefender folosește un sistem de monitorizare pentru a detecta și a vă informa despre problemele care pot afecta securitatea calculatorului și a 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 includ 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** - împiedicăBitdefender 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:

Culoarea roșie: Probleme grave de securitate afectează calculatorul dumneavoastră. Acestea necesită atenția dumneavoastră imediat și trebuie remediate în cel mai scurt timp.

Culoarea galben: Probleme de o importanță redusă afectează securitatea sistemului dvs. Este recomandat să le examinați și să le remediați când aveți timp.

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

Când deschideți fereastra Bitdefender, zona de stare a securității de pe bara de instrumente superioară va indica numărul și tipul de probleme care afectează sistemul dvs.

2.4.1. 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 **Remediază toate problemele**.În funcție de problemele detectate, pictograma este fie de culoare roșie (indicând probleme critice) fie de culoare galbenă (indicând probleme neimportante).
   - Deschideți fereastra Bitdefender și faceți clic oriunde în interiorul zonei stării de securitate din partea superioară a barei de instrumente (de exemplu puteți face clic pe butonul **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 **Amânare** și nu se va lua nicio măsură pentru remedierea problemei.
3. Pentru a rezolva problemele selectate, faceți clic pe **Start**. 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.

2.4.2. Configurarea alertelor de stare

Sistemul de alertare este preconfigurat pentru a monitoriza și pentru a vă alerta în legătură cu principalele probleme care pot afecta securitatea calculatorului și datelor dumneavoastră.În afară de problemele monitorizate în mod implicit, există o serie de alte probleme despre care puteți fi informat.

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

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **General** în meniul din stânga și apoi pe fila **Avansat**.
4. Identificați și faceți clic pe link-ul **Configurare alerte de stare**.
5. Faceți clic pe selectoare pentru a activa sau a dezactiva alertele de stare, în funcție de preferințele dumneavoastră.

2.5. Evenimente

Bitdefender menține un jurnal detaliat al evenimentelor legate de activitatea sa pe computerul 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 deschide fereastra Evenimente, deschideți mai întâi fereastra Bitdefender și faceți clic pe butonul **Evenimente** de pe bara de instrumente din partea superioară.

Pentru a filtra mai ușor evenimentele Bitdefender, vă stau la dispoziție următoarele categorii în meniul din partea stângă:

- **Antivirus**
- **Control date**
- **Hartă rețea**
- **Actualizare**
- **SafeGo**
- **Înregistrare**

Pentru fiecare categorie este disponibilă o listă de evenimente.Pentru a afla informații cu privire la un anumit eveniment din listă, faceți clic pe acesta. Detaliile despre eveniment vor fi afișate în partea inferioară 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 acestora.Există trei tipuri de evenimente, fiecare marcat printr-o anumită pictogramă:

Evenimentele de tip **Informații** indică operațiile finalizate cu succes.
Evenimentele de tip **Avertizare** indică probleme care nu sunt de foarte mare importanță. Puteți să le verificați și să le remediați oricând aveți timp.
Evenimentele **importante** indică problemele principale. Acestea ar trebui verificate imediat.

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.

2.6. Pilot automat

Pentru toți acei utilizatori care nu-și doresc nimic altceva de la soluția lor de securitate decât să fie protejați fără a fi deranjați, a fost creat Bitdefender Antivirus Plus 2012 cu un mod integrat de pilot automat.

Atunci când se află în modul Pilot automat, 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 Pilot automat, Bitdefender remediază în mod automat problemele critice și gestionează în mod silențios:

- Protecție antivirus, asigurată de funcția de scanare la accesare și scanare continuă.
- Protecție firewall.
- Protecția confidențialității asigurată de filtrele antiphishing și antimalware pentru activitatea dumneavoastră de navigare pe internet.
- Actualizări automate.

În mod implicit, Pilotul automat este activat la momentul în care se finalizează instalarea Bitdefender.Atunci când Pilotul automat este activat, pictograma Bitdefender de pe bara de sistem va deveni .

Pentru a activa sau dezactiva funcția de Pilot automat, deschideți fereastra Bitdefender și faceți clic pe selectorul **Pilot automat** pe bara de instrumente din partea superioară.

Important
În cazul în care modificați vreo setare administrată de funcția Pilot automat 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 Pilot automat, deschideți fereastra Evenimente.

2.7. Modul pentru jocuri și Modul pentru laptop

Unele activități efectuate pe calculator, cum ar fi jocurile sau prezentările, necesită o viteză sporită de reacție și funcționare 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 Antivirus Plus 2012 are două moduri de funcționare speciale:

- Mod jocuri
- Mod laptop

2.7.1. Mod jocuri

Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului.Cât timp modul pentru jocuri este activat, se aplică următoarele setări:

- Toate alertele și pop-upurile Bitdefender sunt dezactivate.
- Funcția de Scanare automată este dezactivată.Scanarea automată detectează și folosește intervale de timp pentru a efectua scanări repetate ale întregului sistem, atunci când consumul de resurse de sistem scade sub un anumit prag.
- Funcția de Actualizare automată este dezactivată.
- Bara de instrumente Bitdefender din browser-ul dumneavoastră este dezactivată atunci când vă jucați online, direct din browser-ul de internet.

Cât timp modul pentru jocuri este activat, puteți vedea litera G pe  iconița Bitdefender.

Utilizarea modului pentru jocuri

În mod implicit, Bitdefender intră automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a Bitdefender sau când o aplicație ocupă întreg

ecranul (fullscreen).Bitdefender va reveni automat la modul de funcționare normal atunci când închideți jocul sau când aplicația detectată iese din modul Ecran întreg.

Dacă doriți să activați modul pentru jocuri manual, folosiți una dintre următoarele metode:

- Faceți clic-dreapta pe icoana Bitdefender din bara de sistem și selectați **Activează modul pentru jocuri**.
- Apăsați simultan tastele `Ctrl+Shift+Alt+G` (combinația de taste implicită).

Important
Nu uitați să dezactivați modul pentru jocuri atunci când ați încheiat jocul. În acest scop, utilizați aceleași metode ca și la activarea sa.

Schimbarea combinației de taste pentru Modul de joc

Puteți intra manual în modul pentru jocuri utilizând combinația de taste implicită `Ctrl+Alt+Shift+G`.Pentru a schimba combinația de taste, urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **General** în meniul din stânga și apoi pe fila **Setări**.
4. Sub opțiunea **Activează tasta Mod de joc** puteți seta combinația de taste dorită:
   a. Bifați tastele speciale pe care doriți să le folosiți: tasta Control (`Ctrl`), tasta Shift (`Shift`) sau tasta Alternate (`Alt`).
   b. În câmpul editabil, tastați litera corespunzătoare tastei normale pe care doriți să o folosiți.

   De exemplu, dacă doriți să folosiți combinația de taste `Ctrl+Alt+D`, trebuie să bifați doar `Ctrl` și `Alt` și să tastați `D`.

Notă
Pentru a dezactiva combinația de taste, debifați opțiunea **Activare combinație de taste în modul joc**.

Activarea sau dezactivarea modului automat de joc

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

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **General** în meniul din stânga și apoi pe fila **Setări**.

4. Activați sau dezactivați modul de joc automat, făcând clic pe selectorul corespunzător.

2.7.2. Mod laptop

Modul pentru laptop este creat special pentru utilizatorii de laptopuri. Scopul acestuia este să minimizeze impactul pe care îl are Bitdefender asupra consumului bateriei atunci când aceste dispozitive funcționează pe baterie.Atunci când Bitdefender funcționează în modul Laptop, funcțiile de scanare automată și actualizare automată sunt dezactivate, deoarece necesită mai multe resurse de sistem și implicit sporesc consumul de energie.

Bitdefender detectează când laptopul dumneavoastră a trecut pe baterie și intră automat în modul pentru laptop.De asemenea, Bitdefender iese automat din modul pentru laptop, atunci când detectează că laptopul nu mai funcționează pe baterie.

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

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **General** în meniul din stânga și apoi pe fila **Setări**.
4. Activați sau dezactivați modul automat pentru laptop, făcând clic pe selectorul corespunzător.

Dacă Bitdefender nu este instalat pe un laptop, dezactivați modul automat pentru laptop.

2.8. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **General** în meniul din stânga și apoi pe fila **Setări**.
4. La secțiunea **Setări protejate prin parolă**, activați protecția prin intermediul unei parole făcând clic pe comutator.
5. Faceți clic pe link-ul **Modificare parolă**.
6. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **General** în meniul din stânga și apoi pe fila **Setări**.
4. La secțiunea **Setări protejate prin parolă**, dezactivați protecție cu parolă, făcând clic pe comutator.
5. Introduceți parola și faceți clic pe **OK**.

2.9. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **General** în meniul din stânga și apoi pe fila **Avansat**.
4. Dezactivați rapoartele anonime de utilizare făcând clic pe selectorul corespunzător.

2.10. Repararea sau dezinstalarea Bitdefender

Dacă doriți să reparați sau să dezinstalați Bitdefender Antivirus Plus 2012, urmați calea din meniul Start al Windows: **Start → All Programs → Bitdefender 2012 → Repair or Remove**.

Selectați acțiunea pe care doriți s-o efectuați:

- **Reparare** - pentru a reinstala toate componentele programului.
- **Dezinstalare** - pentru dezinstalarea tuturor componentelor instalate.

Notă

Vă recomandăm să alegeți **Dezinstalare** pentru a asigura o reinstalare corectă.

Așteptați ca Bitdefender să finalizeze acțiunea pe care ați selectat-o.Aceasta va dura câteva minute.

După finalizarea procesului, va fi necesar să reporniți computerul.

3. Interfața Bitdefender

Bitdefender Antivirus Plus 2012 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.

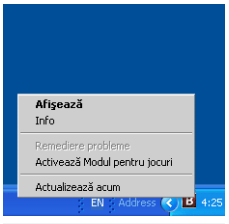
Pentru a vizualiza starea produsului și pentru a efectua activități esențiale, pictograma brei de sistem a Bitdefender este disponibilă în permanență.

Fereastra principală vă asigură accesul rapid la modulele de produse și informațiile importante despre produse, permițându-vă să realizați sarcini obișnuite.

Pentru a configura produsul Bitdefender în detaliu și pentru a realiza sarcini administrative avansate, puteți găsi toate instrumentele de care aveți nevoie în fereastra setărilor.

3.1. Pictograma barei de sistem

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

- **Afișează** - 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.
- **Remediază** - 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. 10).
- **Activează/Dezactivează Modul pentru jocuri** - activează/dezactivează modul pentru jocuri.
- **Actualizează acum** - inițiază o actualizare imediată.Puteți urmări starea actualizării pe panoul de actualizare din fereastra principală Bitdefender.

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 grave de securitate afectează calculatorul dumneavoastră. Acestea necesită atenția dumneavoastră imediat și trebuie remediate în cel mai scurt timp.

Probleme nu foarte importante afectează securitatea sistemului dumneavoastră.Ar trebui să verificați și să le remediați atunci când aveți timp.

Produsul funcționează în Modul pentru jocuri.

Bitdefender Auto Pilot is engaged.

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

3.2. Fereastra principală

Principala fereastră Bitdefender vă permite să realizați sarcini obișnuite, să remediați rapid probleme legate de securitate, să vizualizați informații referitoare la evenimente din cadrul funcționării produsului și să vă personalizați setările produsului.Puteți accesa tot ce vă doriți făcând clic de câteva ori.

Fereastra este organizată în trei secțiuni principale:

Bara de instrumente din partea superioară
: De aici puteți verifica starea securității computerului dumneavoastră și activitățile importante de acces.

Secțiunea panourilor
: De aici puteți administra modulele principale Bitdefender.

În plus, puteți în partea inferioară a ferestrei, puteți găsi câteva link-uri utile:

Link	Descriere
Trimiteți feedback	Deschide o pagină web în browser-ul dumneavoastră, unde puteți completa un scurt chestionar privind experiența dumneavoastră în legătură cu utilizarea produsului.Ne bazăm pe feedback-ul primit de la dumneavoastră pentru a ne îmbunătăți în mod constant produsele Bitdefender.
Înregistrare completă / MyBitdefender	Deschide fereastra contului MyBitdefender, de unde puteți crea un cont sau vă puteți autentifica într-un cont.Pentru a primi actualizări și a beneficia de caracteristicile online ale produsului, aveți nevoie de un cont MyBitdefender.Pentru a afla mai multe despre modul în care puteți crea un cont și beneficiile asigurate, consultați *„Autentificare în MyBitdefender”* (p. 8).
Informații licență	Deschide o fereastră în care puteți vedea informații despre licența actuală și unde vă puteți înregistra produsul cu o nouă serie de înregistrare.
Asistență	Faceți clic pe acest link dacă aveți nevoie de ajutor cu Bitdefender.

Link	Descriere
	Adaugă semne de întrebare în diferite zone ale ferestrei Bitdefender pentru a vă ajuta să găsiți cu ușurință informații despre diferite elemente ale interfeței. Deplasați cursorul mouse-ului peste un marcaj pentru a vizualiza informații sumare despre elementul de lângă acesta.

3.2.1. 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 neimportante 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.

  Făcând clic pe butonul **Vizualizare probleme** din centrul barei de instrumente sau oriunde în partea stângă a zonei de stare a securității, puteți accesa un program asistent care vă va ajuta să eliminați cu ușurință toate amenințările de pe computerul dumneavoastră.Pentru mai multe detalii, consultați *„Reparare probleme”* (p. 10).

- **Evenimente** vă permite să accesați un istoric detaliat al evenimentelor relevante care s-au produs în timpul funcționării produsului.Pentru mai multe detalii, consultați *„Evenimente”* (p. 12).
- Funcția **Setări** vă permite să accesați fereastra de setări, din care puteți configura setările produsului.Pentru mai multe detalii, consultați *„Fereastra setărilor”* (p. 24).
- **Pilotul automat** vă pemite să activați funcția Pilot automat și să vă bucurați de securitate complet silențioasă.Pentru mai multe detalii, consultați *„Pilot automat”* (p. 13).

3.2.2. Secțiunea panourilor

Din secțiunea panourilor puteți administra direct modulele Bitdefender.

Puteți organiza panourile după cum doriți.să rearanjați zona în funcție de nevoile dumneavoastră, să trageți panouri individuale și să le plasați în alte locuri.

Pentru a naviga printre panouri, folosiți cursorul de sub secțiunea panourilor sau săgețile localizate la dreapta și la stânga.

Începând din partea superioară spre partea inferioară, fiecare modul conține următoarele elemente:

- Numele modulului.
- Un mesaj de stare.
- Pictograma modulului.Faceți clic pe pictograma unui modul pentru a configura setările acestuia din fereastra setărilor.
- Un buton care vă permite să efectuați activități importante care au legătură cu modulul.
- Un selector este disponibil pe anumite panouri, permițându-vă să activați sau să dezactivați o caracteristică importantă a modulului.

Panourile disponibile în această zonă 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 meniul Antivirus, puteți accesa cu ușurință sarcini de scanare importante.Faceți clic pe **Scanează acum** și selectați o sarcină din meniul vertical:

- QuickScan
- Scanare completă
- Scanare adaptabilă
- Vulnerabilități
- Mod de salvare

Selectorul de **Scanare automată** vă permite să activați sau să dezactivați funcția de scanare automată.

Pentru mai multe informații referitoare la activitățile de scanare și modul de configurare a protecției antivirus, consultați *„Protecție antivirus”* (p. 35).

Actualizare

Într-o lume în care infractorii cibernetici încearcă să descopere noi metode de a face rău, este esențial să vă mențineți actualizată soluția de securitate pentru a fi mereu cu un pas înainte acestora.

În mod implicit, Bitdefender verifică automat în fiecare oră dacă au fost lansate actualizări. Dacă doriți să dezactivați actualizările automate, folosiți selectorul **Actualizare automată** din panoul Actualizare.

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.

Faceți clic pe butonul **Actualizează acum** din panou, pentru a iniția imediat o actualizare.

Pentru mai multe informații despre actualizările de configurare, consultați *„Actualizare”* (p. 71).

Control date

Modulul de control al datelor vă ajută să mențineți confidențialitatea datelor dumneavoastră personale importante.Atunci când navigați pe internet, vă protejează împotriva atacurilor de tip phishing, încercărilor de fraudă, scurgerilor de date personale și împotriva altor amenințări.

Faceți clic pe butonul **Administrare reguli** de pe panoul de control al confidențialității pentru a ajunge la secțiunea de protecție a datelor unde puteți configura regulile de confidențialitate.

Selectorul pentru Antiphishing vă permite să activați sau să dezactivați protecția antiphishing.

Pentru mai multe informații referitoare la modul de configurare Bitdefender pentru a vă proteja confidențialitatea, consultați *„Control date”* (p. 60).

Hartă rețea

Cu ajutorul Hărții de rețea puteți administra cu ușurință securitatea tuturor computerelor din locuința dumneavoastră de la un singur computer.

Pentru a începe, faceți clic pe **Gestionare** de pe panoul cu Harta rețelei și selectați **Activare rețea**.

După ce a fost activată rețeaua, puteți face clic pe **Administrează** din secțiunea Hartă rețea pentru a avea acces la următoarele opțiuni.

- **Dezactivare conexiune** - dezactivați rețeaua.
- **Scanează tot** - lansează o scanare rapidă a întregului sistem pe toate computerele administrare.
- **Actualizare toate computerele** - actualizați produseleBitdefender de pe computerele gestionate.

Pentru mai multe informații, consultați *„Hartă rețea”* (p. 67).

Safego

Pentru a vă asigura protecția în timp ce navigați pe Facebook, puteți accesa Safego, soluția de securitate a Bitdefender pentru rețele sociale direct de la produsul dumneavoastră.

Faceți clic pe **Activează** pentru a activa și administra opțiunea aplicația Safego din contul dumneavoastră de Facebook.

Dacă ați activat deja Safego, veți putea să accesați statisticile referitoare la activitatea sa făcând clic pe butonul **Vizualizare rapoarte**.

Pentru mai multe informații, consultați *„Protecție Safego pentru rețelele sociale”* (p. 75).

3.3. Fereastra setărilor

Cu ajutorul ferestrei de setări aveți acces la toate componentele produsului și îl puteți personaliza.Aici puteți configura Bitdefender în detaliu.

În partea stângă a ferestrei există un meniu care conține toate modulele de securitate.Fiecare modul are unul sau mai multe taburi în care puteți configura setările de securitate corespunzătoare sau puteți efectua sarcini de securitate sau administrative.Următoarea listă descrie pe scurt fiecare modul.

General
: Vă permite să configurați setările generale ale produsului, precum parola pentru setări, Modul pentru joc, Modul laptop, setările pentru proxy și alertele de stare.

Antivirus
: Vă permite să vă configurați protecția împotriva malware, să detectați și să remediați punctele vulnerabile ale sistemului dumneavoastră, să setați excepții de scanare și să gestionați fișierele aflate în carantină.

Control date
: Vă permite să preveniți furtul de date de pe calculatorul dumneavoastră și să vă protejați confidențialitatea în timp ce sunteți online.Configurați protecția pentru browser-ul dumneavoastră web, software-ul pentru mesageria instant, gestionați protecția datelor și multe altele.

Hartă rețea
: Vă permite să configurați și să administrați produsele Bitdefender instalate pe computerele personale de pe un singur computer.

Actualizare
: Vă permite să obțineți informații despre cele mai recente actualizări, să actualizați produsul și să configurați procesul de actualizare în detaliu.

În plus, puteți în partea inferioară a ferestrei, puteți găsi câteva link-uri utile:

Link	Descriere
Trimiteți feedback	Deschide o pagină web în browser-ul dumneavoastră, unde puteți completa un scurt chestionar privind experiența dumneavoastră în legătură cu utilizarea produsului.Ne bazăm

Link	Descriere
	pe feedback-ul primit de la dumneavoastră pentru a ne îmbunătăți în mod constant produsele Bitdefender.
Înregistrare completă / MyBitdefender	Deschide fereastra contului MyBitdefender, de unde puteți crea un cont sau vă puteți autentifica într-un cont.Pentru a primi actualizări și a beneficia de caracteristicile online ale produsului, aveți nevoie de un cont MyBitdefender.Pentru a afla mai multe despre modul în care puteți crea un cont și beneficiile asigurate, consultați *„Autentificare în MyBitdefender”* (p. 8).
Informații licență	Deschide o fereastră în care puteți vedea informații despre licența actuală și unde vă puteți înregistra produsul cu o nouă serie de înregistrare.
Asistență	Faceți clic pe acest link dacă aveți nevoie de ajutor cu Bitdefender.
	Adaugă semne de întrebare în diferite zone ale ferestrei Bitdefender pentru a vă ajuta să găsiți cu ușurință informații despre diferite elemente ale interfeței. Deplasați cursorul mouse-ului peste un marcaj pentru a vizualiza informații sumare despre elementul de lângă acesta.

Pentru a reveni la fereastra principală, faceți clic pe butonul **Acasă** din colțul din dreapta sus al ferestrei.

4. Cum să

Acest capitol prezintă instrucțiuni de configurare pas cu pas a celor mai des folosite setări sau pentru finalizarea activităților comune cu Bitdefender.Anumite subiecte includ referințe la alte teme în cadrul cărora puteți găsi informații detaliate.

- *„Cum pot înregistra o versiune de încercare?”* (p. 26)
- *„Cum înregistrez Bitdefender fără a fi conectat la internet?”* (p. 27)
- *„Cum trec la un produs superior din gama Bitdefender 2012?”* (p. 28)
- *„Când este cazul să reinstalez Bitdefender?”* (p. 28)
- *„Când expiră protecția oferită de produsul meu Bitdefender?”* (p. 29)
- *„Cum îmi reînnoiesc protecția Bitdefender?”* (p. 29)
- *„Ce produs Bitdefender folosesc?”* (p. 29)
- *„Cum scanez un fișier sau un director?”* (p. 30)
- *„Cum îmi scanez sistemul?”* (p. 30)
- *„Cum creez o activitate de scanare personalizată?”* (p. 30)
- *„Cum exclud un director de la procesul de scanare?”* (p. 31)
- *„Ce să fac atunci când Bitdefender a detectat un fișier curat ca fiind infectat?”* (p. 31)
- *„Cum îmi protejez informațiile personale?”* (p. 32)
- *„Cum pot configura Bitdefender să utilizeze o conexiune la internet de tip proxy?”* (p. 33)

4.1. Cum pot înregistra o versiune de încercare?

Dacă ați instalat o versiune de încercare, o puteți folosi doar pentru o anumită perioadă.Pentru a folosi în continuare Bitdefender după expirarea perioadei de evaluare, trebuie să înregistrați produsul cu o serie de licență și să vă creați un cont MyBitdefender.

- Pentru a înregistra Bitdefender, urmați pașii de mai jos:

  1. Deschideți fereastra Bitdefender.
  2. Faceți clic pe link-ul **Informații licență** din partea inferioară a ferestrei.Va apărea fereastra de înregistrare.
  3. Introduceți seria de înregistrare și faceți clic pe **Înregistrare**.

     Dacă nu aveți o serie de licență, faceți clic pe link-ul specificat în fereastră pentru a vizita pagina web de unde puteți achiziționa o serie.
  4. Așteptați până la finalizarea procesului de înregistrare și închideți fereastra.

- Pentru a crea un cont MyBitdefender, urmați acești pași:

  1. Deschideți fereastra Bitdefender.
  2. Faceți clic pe link-ul **Înregistrare completă** din partea inferioară a ferestrei.Va fi afișată fereastra contului.
  3. Selectați link-ul corespunzător pentru a crea un nou cont.
  4. Introduceți informațiile solicitate în câmpurile corespunzătoare.Informațiile furnizate aici vor rămâne confidențiale.

     Faceți clic pe **Trimite**.
  5. Verificați-vă e-mail-ul și urmați instrucțiunile primite pentru a finaliza înregistrarea.

     Notă
     Puteți utiliza adresa de e-mail și parola indicate pentru a vă accesa contul la http://my.bitdefender.com.

4.2. Cum înregistrez Bitdefender fără a fi conectat la internet?

Dacă tocmai ați achiziționat Bitdefender dar nu aveți acces la o conexiune la internet, puteți înregistra Bitdefender offline.

Pentru a vă înregistra Bitdefender cu seria de licență, urmați pașii de mai jos:

1. Accesați un computer conectat la internet.De exemplu, puteți utiliza computerul unui prieten sau un computer dintr-o locație publică.
2. Mergeți la https://my.bitdefender.com pentru a crea un cont MyBitdefender.
3. Autentificați-vă cu contul dumneavoastră și selectați **Obține înregistrare offline**.
4. Introduceți seria de licență pe care ați achiziționat-o.
5. Faceți clic pe **Trimitere** pentru a obține un cod de confirmare.

   Important
   Notați-vă codul de confirmare.

6. Reveniți la computer cu codul de confirmare.
7. Deschideți fereastra Bitdefender.
8. Faceți clic pe link-ul **Informații licență** din partea inferioară a ferestrei.Va apărea fereastra de înregistrare.
9. Selectați această opțiune pentru a înregistra produsul cu un cod de confirmare.
10. Introduceți codul de confirmare în câmpul corespunzător și faceți clic pe **Trimitere**.

11. Așteptați până la finalizarea procesului de înregistrare și faceți clic pe **Finalizare**.

4.3. Cum trec la un produs superior din gama Bitdefender 2012?

Puteți trece cu ușurință de la un produs Bitdefender 2012 la un altul.

Să ne imaginăm următorul scenariu: utilizați de ceva timp Bitdefender Antivirus Plus 2012 și, de curând, ați decis să alegeți Bitdefender Total Security 2012 și caracteristicile suplimentare pe care acesta le oferă.

Tot ce trebuie să faceți este să achiziționați o serie de licență pentru Bitdefender 2012 la care doriți să treceți și să o introduceți în fereastra de înregistrare a produsului Bitdefender 2012, pe care îl utilizați în prezent.

Urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe link-ul **Informații licență** din partea inferioară a ferestrei.Va apărea fereastra de înregistrare.
3. Introduceți seria de înregistrare și faceți clic pe **Înregistrare**.
4. Bitdefender vă va informa că respectiva serie de înregistrare este destinată unui alt produs și vă va oferi opțiunea de a-l instala.Faceți clic pe linkul corespunzător și urmați procedura pentru a efectua actualizarea.

4.4. 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 CD-ul de instalare pe care l-ați achiziționat sau puteți descărca o nouă versiune de pe site-ul web Bitdefender.

În timpul instalării, vi se va solicita să înregistrați seria de licență pentru produsul dumneavoastră.

Dacă nu puteți găsi seria de licență, vă puteți autentifica în cadrul https://my.bitdefender.com pentru a o recupera.Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.

4.5. Când expiră protecția oferită de produsul meu Bitdefender?

Pentru a afla numărul de zile rămase până la expirarea seriei de licență, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe link-ul **Informații licență** din partea inferioară a ferestrei.
3. În fereastra **Înregistrați-vă produsul** puteți vizualiza numărul de zile rămase.

4.6. Cum îmi reînnoiesc protecția Bitdefender?

Atunci când protecția Bitdefender se apropie de data expirării, trebuie să vă reînnoiți seria de licența.

- Urmați acești pași pentru a vizita un site web în care vă puteți reînnoi seria de licență Bitdefender:
  1. Deschideți fereastra Bitdefender.
  2. Faceți clic pe link-ul **Informații licență** din partea inferioară a ferestrei.
  3. Faceți clic pe **Nu aveți o serie de licență? Cumpărați una acum!**
  4. Se va deschide o pagină de web pe browser-ul dumneavoastră în care puteți achiziționa o serie de licență Bitdefender.

  Notă
  Drept alternativă, puteți contacta retailer-ul de la care ați achiziționat Bitdefender.

- Urmați acești pași pentru a vă înregistra Bitdefender cu noua serie de licență:
  1. Deschideți fereastra Bitdefender.
  2. Faceți clic pe link-ul **Informații licență** din partea inferioară a ferestrei.Va apărea fereastra de înregistrare.
  3. Introduceți seria de înregistrare și faceți clic pe **Înregistrare**.
  4. Așteptați până la finalizarea procesului de înregistrare și închideți fereastra.

Pentru mai multe informații și asistență puteți contacta Bitdefender, după cum este descris în secțiunea *„Suport”* (p. 92).

4.7. Ce produs Bitdefender folosesc?

Pentru a afla ce program Bitdefender ați instalat, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.

2. În partea superioară a ferestrei, ar trebui să vedeți afișată una dintre următoarele denumiri de produse:
   - BitDefender Antivirus Plus 2012
   - BitDefender Internet Security 2012
   - BitDefender Total Security 2012

4.8. Cum scanez un fișier sau un director?

Cea mai ușoară și recomandată metodă de a scana un fișier sau un director este de a face clic dreapta pe un obiect pe care doriți să-l scanați și să selectați **Scanează cu Bitdefender** din meniu.Pentru finalizarea procesului de scanare, urmați pașii asistentului de scanare antivirus.

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.

4.9. Cum îmi scanez sistemul?

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

1. Deschideți fereastra Bitdefender.
2. Mergeți la secțiunea **Antivirus**.
3. Faceți clic pe **Scanează acum** și selectați **Scanare completă sistem** din meniul vertical.
4. Urmați programul asistent de scanare pentru a finaliza scanarea.

4.10. Cum creez o activitate de scanare personalizată?

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

1. Deschideți fereastra Bitdefender.
2. Mergeți la secțiunea **Antivirus**.
3. Faceți clic pe **Scanează acum** și selectați **Scanare personalizată** din meniul vertical.
4. Faceți clic pe **Adaugă obiect** pentru a selecta fișierele sau directoarele ce vor fi scanate.
5. Dacă doriți să configurați în detaliu opțiunile de scanare, faceți clic pe **Opțiuni scanare**.

Puteți selecta opțiunea **Închidere Computer**.

În cazul în cazul nu este detectată nicio amenințare, computerul dumneavoastră se va opri după finalizarea procesului de scanare.Rețineți faptul că acesta va fi modul implicit de reacție, de fiecare dată când executați această activitate.

6. Faceți clic pe **Pornire scanare** pentru a executa această activitate.

4.11. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Excepții**.
4. Faceți clic pe link-ul **Fișiere și directoare excluse**.
5. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
6. Faceți clic pe **Caută**, selectați directorul care doriți să fie exclus de la scanare și faceți clic pe **OK**.
7. Faceți clic pe **Adaugă** și apoi pe **OK** pentru a salva modificările și a închide fereastra.

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

Există situații când Bitdefender marchează în mod greșit un fișier legitim ca fiind o amenințare.Pentru a corecta această eroare, adăugați fișierul în secțiunea de excluderi a Bitdefender:

1. Dezactivați protecția antivirus în timp real a Bitdefender:
   a. Deschideți fereastra Bitdefender.
   b. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
   c. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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. 100).
3. Restaurați fișierul din zona de carantină:
   a. Deschideți fereastra Bitdefender.
   b. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
   c. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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. 31).
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. 93).

4.13. Cum îmi protejez informațiile personale?

Cu ajutorul opțiunii Control date sunt monitorizate toate datele trimise de pe computerul dumneavoastră prin intermediul formularelor online, mesajelor e-mail sau mesajelor instante.

Pentru a vă asigura că nu vor fi trimise date private de pe computer fără acordul dumneavoastră, trebuie să creați reguli adecvate de protecție a datelor, precum și excepții de la aceste reguli.

Regulile de protecție a datelor specifică informațiile ce vor fi blocate.

Pentru a crea o regulă de protecție a datelor, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Control date** în meniul din stânga și apoi pe fila **Protecție date**.
4. Dacă opțiunea **Protecție date** este dezactivată, activați-o folosind selectorul corespunzător.
5. Selectați opțiunea **Adăugare regulă** pentru a lansa asistentul Protecție date.
6. Urmați pașii asistentului.

4.14. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **General** în meniul din stânga și apoi pe fila **Avansat**.
4. La secțiunea **Setări proxy**, activați consumul proxy, făcând clic pe comutator.
5. Faceți clic pe link-ul **Administrare proxy**.
6. 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, 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.
     - **Nume utilizator** - introduceți un nume de utilizator recunoscut de proxy.
     - **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.
7. 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.

Important

Nu uitați să dezactivați opțiunea proxy în momentul în care treceți la o conexiune la internet directă.

5. 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 computere.

  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.

  Atunci când este activată Scanarea automată, nu este necesar să activați manual scanările antimalware.Cu ajutorul opțiunii de Scanare automată, computerul dumneavoastră va fi scanat în mod repetat și vor fi aplicate acțiuni corespunzătoare în cazul în care sunt detectate acțiuni periculoase.Auto Scan rulează numai atunci când există suficiente resurse de sistem pentru a nu încetini funcționarea computerului.

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. 49).

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. 50).

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. 53).

În cazul în care calculatorul dumneavoastră a fost infectat cu malware, consultați *„Eliminarea programelor malware din sistemul dumneavoastră”* (p. 83).Pentru a vă

ajuta să v ă curățați computerul de programele malware care nu pot fi eliminate din sistemul de operare Windows, Bitdefender vă pune la dispoziție Modul de salvare.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 Modul de salvare, Windows malware este inactiv și, în consecință, poate fi șters cu ușurință.

Pentru a vă proteja împotriva aplicațiilor periculoase, Bitdefender folosește Active Virus Control, o tehnologie euristică avansată care monitorizează în permanență aplicațiile ce rulează pe sistemul dumneavoastră.Active Virus 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 Virus Control să nu blocheze aceste aplicații a doua oară, creând reguli de excludere.Pentru a afla mai multe, consultați *„Active Virus Control”* (p. 54).

Multe forme de programe malware sunt create să infecteze sistemele, exploatându-le vulnerabilitățile, ca de exemplu actualizări de sistem care lipsesc sau aplicații neactualizate.Bitdefendervă ajută să identificați și să soluționați cu ușurință vulnerabilitățile sistemului pentru a asigura securitatea computerului dumneavoastră împotriva programelor malware și împotriva hacker-ilor.Pentru mai multe informații, consultați *„Remedierea vulnerabilităților sistemului”* (p. 56).

5.1. Scanare la accesare (protecție în timp real)

Bitdefender oferă protecție continuă în timp real împotriva unui număr mare de amenințări malware scanând toate fișierele accesate, mesajele e-mail și comunicațiile prin programe de mesagerie instant (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

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.

5.1.1. Verificarea programelor periculoase detectate în urma scanării la accesare

Pentru a verifica programele periculoase detectate în urma scanării la accesare, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.

2. Faceți clic pe butonul **Evenimente** de pe bara de instrumente din partea superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Scanare viruși**.Aici puteți găsi toate evenimentele malware scanate, inclusiv amenințările detectate în urma scanării la accesare și a scanărilor inițiate la comanda utilizatorului și starea modificărilor pentru scanările automate.
4. Faceți clic pe un eveniment pentru a vizualiza detaliile acestuia.

5.1.2. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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.

5.1.3. Crearea unui nivel de protecție personalizat

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 crea un nivel de protecție personalizat, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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.

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.

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

- **Scanează arhivele.** 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).

- **Opțiuni de scanare pentru traficul e-mail, web și de mesagerie instant.** Pentru a împiedica descărcarea fișierelor infectate pe calculatorul dumneavoastră, Bitdefender scanează automat următoarele puncte de intrare:
  - e-mail-uri primite sau trimise
  - trafic web
  - fișiere primite prin Yahoo! Messenger și Windows Live Messenger

  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 funcția de scanare antivirus a e-mailurilor, paginilor web sau a mesageriei instantant pentru a spori 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).

- **Scanează sectoarele 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 numai 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.

5.1.4. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Scut**.
4. Faceți clic pe **Implicit**.

5.1.5. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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, va apărea o fereastră de avertizare.Va trebui să confirmați acțiunea selectând din meniu intervalul de timp pentru care să fie dezactivată protecția în timp real. Puteți dezactiva protecția

în timp real pentru 5, 15 sau 30 minute, pentru o oră, permanent sau doar până la repornirea sistemului.

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.

5.1.6. Acțiuni luate împotriva atacurilor malware detectate

Fișierele detectate cu ajutorul protecției în timp real sunt grupate în două categorii:

- **Fișiere infectate.** Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date cu semnături malware a Bitdefender.În mod normal, Bitdefender poate să elimine codul malware dintr-un fișier infectat și să reconstruiască fișierul original. Această operațiune este cunoscută sub denumirea de dezinfectare.

Notă

Semnăturile malware sunt fragmente de coduri extrase din mostre reale de malware. Acestea sunt utilizate de către programele antivirus pentru a realiza identificarea după model și detectarea programelor malware.
Baza de date cu semnături malware a Bitdefender reprezintă o colecție de semnături malware actualizate în fiecare oră de către cercetătorii malware ai Bitdefender.

- **Fișiere suspecte.** Fișierele sunt identificate ca fiind suspecte în urma analizei euristice.Deoarece B-HAVE este o tehnologie euristică de analiză, Bitdefender nu vă poate asigura dacă fișierul este într-adevăr virusat sau nu.Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

În funcție de tipul de fișier detectat, următoarele acțiuni sunt aplicate în mod automat:

- 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.

Important

Pentru anumite tipuri de malware, dezinfectarea nu este posibilă deoarece fișierul detectat este în întregime periculos. În astfel de situații, fișierul infectat este șters de pe disc.

- În cazul în care este detectat un fișier suspect, acesta va fi mutat în carantină pentru a previne o potențială 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 program periculos, va fi lansată o semnătură care să permită ștergerea acestuia.

5.2. Scanare la cerere

Principalul obiectiv Bitdefender este protejarea calculatorului dumneavoastră de viruși. Aceasta se face în primul rând nepermițând virușilor noi să pătrundă în sistem, prin scanarea mesajele 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 sarcini de scanare. Sarcinile de scanare sunt cele care specifică opțiunile de scanare și obiectele care să fie scanate.Puteți scana computerul oricând doriți prin executarea activităților implicite sau a propriilor activități (activități 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.

5.2.1. Scanare automată

Scanarea automată reprezintă o scanare rapidă la cerere care scanează în mod discret toate datele dumneavoastră verificând să nu existe malware și aplică acțiunile corespunzătoare în cazul infectărilor detectate. Scanarea automată detectează și folosește intervale de timp pentru a efectua scanări repetate ale întregului sistem, atunci când consumul de resurse de sistem scade sub un anumit prag.

Beneficiile utilizării opțiunii de scanare automată:

- Impactul asupra sistemului este aproape zero.
- Prin prescanarea întregului hard disk, următoarele activități de scanare la cerere vor fi finalizate extrem de ușor.
- De asemenea, scanare la accesare va dura foarte puțin timp.

Pentru a activa sau dezactiva funcția de scanare automată, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Mergeți la secțiunea **Antivirus**.
3. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea de scanare automată.

5.2.2. 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 care doriți să fie scanat și

selectați opțiunea **Scanează cu Bitdefender**.Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

5.2.3. 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 fracțiune din resursele de sistem necesare pentru o scanare antivirus obișnuită.

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

1. Deschideți fereastra Bitdefender.
2. Mergeți la secțiunea **Antivirus**.
3. Faceți clic pe **Scanează acum** și selectați **Scanare rapidă** din meniul vertical.
4. Urmați programul asistent de scanare antivirus pentru a finaliza scanarea.

5.2.4. Executarea unei scanări complete a sistemului

Sarcina de scanare completă a sistemului scanează computerul în totalitate pentru a depista toate tipurile de programe periculoase care-i amenință securitatea, cum ar fi virușii, aplicațiile spion, adware, rootkituri și altele.În cazul în care ați dezactivat Scanarea automată, vă recomandăm să rulați o Scanare completă a sistemului cel puțin o dată pe săptămână.

Notă

Deoarece funcția **Scanare completă a sistemului** realizează o scanare amănunțită a întregului sistem, procesul de scanare poate dura mai mult. În consecință, este recomandat să executați această activitate într-un moment când nu utilizați computerul.

Înainte de a realiza o scanare completă a sistemului, vă sunt recomandate următoarele:

- Asigurați-vă că Bitdefender este actualizat cu semnăturile malware. Dacă scanați computerul cu o bază de date neactualizată, este posibil ca Bitdefender să nu poată detecta cele mai noi malware găsite după ultima actualizare.Pentru mai multe informații, consultați *„Actualizare”* (p. 71).
- 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 și executarea unui proces de scanare personalizat”* (p. 43).

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

1. Deschideți fereastra Bitdefender.
2. Mergeți la secțiunea **Antivirus**.
3. Faceți clic pe **Scanează acum** și selectați **Scanare completă sistem** din meniul vertical.
4. Urmați programul asistent de scanare antivirus pentru a finaliza scanarea.

5.2.5. Configurarea și executarea unui proces de scanare personalizat

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

1. Deschideți fereastra Bitdefender.
2. Mergeți la secțiunea **Antivirus**.
3. Faceți clic pe **Scanează acum** și selectați **Scanare personalizată** din meniul vertical.
4. Faceți clic pe **Adăugare țintă**, selectați căsuțele corespunzătoare locațiilor care doriți să fie scanate împotriva programelor periculoase și apoi faceți clic pe **OK**.
5. Faceți clic pe **Opțiuni de scanare** dacă doriți să configurați opțiunile de scanare.Va apărea o nouă fereastră.Urmați acești pași:
   a. Puteți configura ușor opțiunile de scanare reglând nivelul de scanare. Mutați cursorul de-a lungul 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. Bitdefender încearcă, în mod implicit, să elimine codurile periculoase din fișierele infectate sau, în cazul în care dezinfectarea eșuează, să le mute în carantină.Dacă ambele acțiuni eșuează, vi se va cere să specificați o acțiune ce va fi aplicată în cazul amenințărilor nesoluționate.

      Dacă doriți doar să depistați programele periculoase, fără să fie aplicată nicio acțiune, selectați căsuța corespunzătoare din secțiunea **Acțiuni**

   c. 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 bară de sistem.** Minimizează fereastra de scanare în bara de sistem. Faceți dublu-clic pe iconița Bitdefender pentru a o deschide.
- Specificați acțiunea care trebuie luată în cazul în care nu sunt identificate niciun fel de amenințări.

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

6. 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.

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.

- **Scanează sectoarele 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.
- **Scanare memorie.** Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului dumneavoastră.
- **Scanează regiștrii.** Selectați această opțiunea pentru a scana seriile de regiștri.Windows Registry este 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 numai 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.
- **Ignorare înregistratoare de taste comerciale.** 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.

5.2.6. Programul asistent de scanare

Atunci când inițiați o scanare la cerere (de exemplu, faceți clic-dreapta pe un director și selectați **Scanează cu Bitdefender**), va apărea programul asistent de scanare.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 - Alegeți locațiile pentru scanare

Acest pas apare doar atunci când folosiți opțiunea de Scanare personalizată.Pentru mai multe informații, consultați *„Configurarea și executarea unui proces de scanare personalizat”* (p. 43).

Pasul 2 - Realizarea scanării

Bitdefender va începe scanarea obiectelor selectate.

Puteți vedea stadiul și statisticile scanării (viteza de scanare, timpul scurs de la începutul scanării, numărul obiectelor scanate / infectate / suspecte / ascunse și altele).

Așteptați ca Bitdefender să finalizeze scanarea.

Notă

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

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:

- **Introduceți parola.** Dacă doriți ca Bitdefender să scaneze arhiva, selectați această opțiune și introduceți parola.Dacă nu cunoașteți parola, selectați una dintre celelalte opțiuni.
- **Nu cere parola și omite acest obiect de 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.

Faceți clic pe **OK** pentru a continua scanarea.

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

Pasul 3 - Selectarea acțiunilor

După ce scanarea a fost finalizată, va apărea o nouă fereastră, unde puteți vedea rezultatele scanării.

Dacă nu există amenințări nesoluționate, faceți clic pe **Continuă**.În caz contrar, trebuie să configurați noi acțiuni pentru a vă proteja sistemul de amenințările nesoluționate.

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 luată asupra tuturor problemelor sau puteți alege acțiuni separate pentru fiecare grup de probleme.Una sau mai multe dintre opțiunile următoare pot apărea în meniu:

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.

Dezinfectează
Elimină codul malițios din fișierele infectate.

Șterge
Îndepărtează fișierele identificate de pe disc.

Mută în carantină
Mută fișierele detectate în carantină.Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.Pentru mai multe informații, consultați *„Gestionarea fișierelor aflate în carantină”* (p. 53).

Redenumește
Redenumește fișierele ascunse adăugând extensia `.bd.ren` la numele acestora.Ca urmare, veți putea căuta și găsi astfel de fișiere pe calculatorul dumneavoastră, dacă există.

Aceste fișiere ascunse nu sunt fișierele pe care le ascundeți deliberat din Windows. Ele sunt fișiere ascunse cu ajutorul unor programe speciale, cunoscute sub numele de rootkituri.Rootkiturile nu sunt în sine programe periculoase. Totuși, ele sunt utilizate frecvent pentru a împiedica detectarea virușilor sau aplicațiilor spion de către programele antivirus obișnuite.

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

Pasul 4 - Rezumat

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

Important
Dacă este necesar, reporniți sistemul pentru a finaliza procesul de curățare.

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

Bitdefender nu a putut remedia anumite probleme

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.Pentru mai multe informații și instrucțiuni privind modul de eliminare a programelor malware în mod manual, consultați *„Eliminarea programelor malware din sistemul dumneavoastră”* (p. 83).

Bitdefender a detectat fișiere suspecte

Fișierele suspecte sunt fișiere detectate în cadrul analizei euristice ca fiind posibil infectate cu malware a cărui semnătură nu a fost încă lansată.

Dacă au fost detectate fișiere suspecte în timpul scanării, vi se va cere să le trimiteți Laboratorului Bitdefender.Faceți clic pe **OK** pentru a trimite aceste fișiere Laboratorului Bitdefender spre a fi analizate.

5.2.7. Examinarea jurnalelor de scanare

De fiecare dată când realizați o scanare, se creează un raport de scanare.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 programul asistent de scanare, după ce scanarea a luat sfârșit, apăsând **Afișează jurnal**.

Pentru a verifica jurnalele de scanare ulterior, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Evenimente** de pe bara de instrumente din partea superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Scanare virușii**.Aici puteți găsi toate evenimentele malware scanate, inclusiv amenințările detectate în urma scanării la accesare și a scanărilor inițiate la comanda utilizatorului și starea modificărilor pentru scanările automate.
4. În lista de evenimente puteți verifica ce operațiuni de scanare au fost realizate recent.Faceți clic pe un eveniment pentru a vizualiza detaliile acestuia.
5. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**.Raportul de scanare va fi deschis în browserul dumneavoastră implicit.

5.3. 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/DVD
- 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.

5.3.1. 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 va fi afișată în bara 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. Atunci când, în timpul procesului de scanare, este detectată o arhivă protejată prin parolă, este posibil să fiți rugat să introduceți parola.Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizați parola.Puteți alege să introduceți parola, să nu scanați fișierul sau să dezactivați detectarea arhivelor protejate prin parolă.
3. 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 poate fi aplicată nicio acțiune în cazul fișierelor suspecte detectate pe CD-uri/DVD-uri. De asemenea, în cazul în care nu beneficiați de privilegiile corespunzătoare, nu poate fi aplicată nicio acțiune în cazul fișierelor infectate sau suspecte detectate pe unități mapate de rețea.

4. 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 sistemuluiCea 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. 83).

5.3.2. Administrarea scanării a fișierelor media amovibile

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

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Excepții**.
4. În secțiunea **Scanează dispozitivele detectate**, selectați tipurile ce dispozitive de stocare, ce doriți să fie scanate în mod automat.Faceți clic pe comutatoare pentru a activa sau dezactiva opțiunea de scanare automată.

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.

5.4. 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** .

5.4.1. Excluderea fișierelor sau directoarelor de la scanare

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

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Excepții**.
4. Pentru a activa excepțiile pentru fișiere, utilizați comutatorul corespunzător.
5. Faceți clic pe link-ul **Fișiere și directoare excluse**.În fereastra care va apărea, puteți administra fișierele și directoarele excluse de la scanare.
6. 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 această excepție, selectați una dintre celelalte opțiuni.
   d. Faceți clic pe **Adaugă**.
7. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

5.4.2. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Excepții**.
4. Pentru a activa excepțiile pentru fișiere, utilizați comutatorul corespunzător.
5. Faceți clic pe link-ul **Extensii excluse**În fereastra care va apărea, puteți administra extensiile de fișiere excluse de la scanare.
6. 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**.
7. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

5.4.3. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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**).Va apărea o nouă fereastră unde puteți

schimba extensia sau calea care va fi exclusă, precum și tipul de scanare de la care acestea vor fi excluse. Efectuați modificările necesare, apoi faceți clic pe **Modifică**.

5. Pentru a dezactiva excepțiile de la scanare, utilizați comutatorul corespunzător.

5.5. 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 program periculos, 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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.

   Trimite fișierele aflate în carantină la Bitdefender pentru a fi analizate în detaliu

   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 program periculos, 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**.

5.6. Active Virus Control

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

Active Virus Control monitorizează încontinuu aplicațiile care rulează pe calculator, verificând dacă nu există acțiuni similare programelor malware. 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 Virus Control, în fereastra Evenimente.

5.6.1. Verificarea aplicațiilor detectate

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

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Evenimente** de pe bara de instrumente din partea superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Active Virus Control**.
4. Faceți clic pe un eveniment pentru a vizualiza detaliile acestuia.
5. Dacă considerați că aplicația este sigură, puteți configura ca Active Virus Control să nu o mai blocheze pe viitor, făcând clic pe **Permite și monitorizează**.Active Virus 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.

5.6.2. Activarea sau dezactivarea funcției Active Virus Control

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

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Scut**.

4. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea Active Virus Control.

5.6.3. Ajustarea protecției Active Virus Control

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

Pentru a ajusta protecția Active Virus Control, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Scut**.
4. Asigurați-vă că opțiunea Active Virus Control este activată.
5. 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

Cu cât setați un nivel de protecție superior, cu atât Active Virus 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 rezultate fals pozitive (aplicații legitime detectate ca fiind periculoase).

5.6.4. Administrarea proceselor excluse

Puteți configura regulile de excludere pentru aplicațiile sigure astfel încât Active Virus Control să nu blocheze aceste aplicații în cazul în care acestea întreprind acțiuni ce pot părea periculoase.Active Virus 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 Virus Control, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Excepții**.
4. Faceți clic pe link-ul **Procese excluse**.În fereastra care va apărea, puteți gestiona excepțiile de la procesul Active Virus 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 Virus Control.

d. Faceți clic pe **Adaugă**.

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

- 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**).Efectuați modificările necesare, apoi faceți clic pe **Modifică**.

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

5.7. Remedierea vulnerabilităților sistemului

Un pas important în protejarea calculatorului dumneavoastră împotriva persoanelor răuvoitoare și a 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 permite remedierea cu ușurință a vulnerabilităților sistemului dumneavoastră prin oricare dintre cele două metode de mai jos:

- Puteți scana și remedia vulnerabilitățile sistemului, pas cu pas, cu ajutorul asistentului **Scanare vulnerabilități**.
- 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.

5.7.1. Scanarea sistemului pentru identificarea vulnerabilităților

Pentru a remedia vulnerabilitățile sistemului cu ajutorul asistentului de Scanare vulnerabilități, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Mergeți la secțiunea **Antivirus**.
3. Faceți clic pe **Scanează acum** și apoi selectați **Scanează vulnerabilități**.

4. Urmați procedura ghidată în șase pași pentru a îndepărta vulnerabilitățile din sistem.Puteți naviga prin programul asistent utilizând butonul **Înainte**. Pentru a părăsi asistentul, faceți clic pe **Anulează**.

   a. **Protejați-vă calculatorul**

      Selectați vulnerabilitățile de verificat

   b. **Verificare probleme**

      Așteptați ca Bitdefender să finalizeze verificarea sistemului dumneavoastră în sensul descoperirii vulnerabilităților.

   c. **Actualizări Windows**

      Puteți vedea lista actualizărilor critice și normale pentru Windows care nu sunt instalate pe calculatorul dumneavoastră.Selectați actualizările pe care doriți să le instalați.

      Pentru a iniția instalarea actualizărilor selectate, faceți clic pe **Înainte**.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.

   d. **Actualizări aplicații**

      Dacă o aplicație nu este la zi, faceți clic pe linkul furnizat pentru a descărca ultima versiune a acesteia.

   e. **Parole vulnerabile**

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

      Faceți clic pe **Remediază** pentru a modifica parolele simple.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 @).

   f. **Rezumat**

      Aici puteți vedea rezultatul operației.

5.7.2. 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. Deschideți fereastra Bitdefender.

2. Faceți clic pe butonul **Evenimente** de pe bara de instrumente din partea superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Vulnerabilitate**.
4. Puteți vizualiza informații detaliate cu privire la vulnerabilitățile sistemului detectate.În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedați după cum urmează:
   - În cazul în care sunt disponibile actualizări Windows, faceți clic pe **Actualizează acum** pentru a deschide asistentul de scanare a vulnerabilităților apoi instalați actualizările.
   - 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 **Repară 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 **Dezactivare** pentru a o dezactiva.

Pentru a configura setările de monitorizare a vulnerabilităților, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Vulnerabilitate**.
4. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea de scanare automată a vulnerabilităților.

   Important
   Pentru a fi informat automat despre vulnerabilitățile sistemului sau aplicațiilor, mențineți funcția **Scanare automată a vulnerabilităților** 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 Windows regulate
   Verificați dacă sistemul de operare Windows are instalate cele mai recente actualizări de securitate obișnuite de la Microsoft.

Actualizări aplicații

Verificați dacă aplicațiile importante ce folosesc internetul, instalate pe sistemul dumneavoastră sunt actualizate.Aplicațiile neactualizate pot fi exploatate de software-uri periculoase, expunându-vă computerul la atacuri din exterior.

Parole vulnerabile

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.

6. Control date

Informațiile dumneavoastră private reprezintă o țintă constantă pentru criminalii cibernetici.Din moment ce amenințările s-au răspândit aproape asupra întregului spectru de activități online, o protecție neadecvată a e-mail-ului, a mesajelor instante și a activităților de navigare pe internet poate duce la scurgeri de informații care vă pot compromite confidențialitatea.

Opțiunea Control date a Bitdefender cuprinde toate amenințările ce prezintă o multitudine de componente.

- Protecția antiphising - oferă un set complet de caracteristici care vă protejează permanent în timp ce navigați pe internet și, în plus, vă împiedică să oferiți informații personale site-urilor web frauduloase, ce par legitime la prima vedere.
- Protecție date - vă ajută să vă asigurați că informațiile personale nu sunt trimise de pe computer fără consimțământul dumneavoastră.Acesta scanează e-mail-ul și mesajele instant trimise de pe computerul dumneavoastră precum și orice date trimise prin intermediul paginilor web și blochează orice informație protejată de regulile de protecție a datelor pe care le-ați creat.
- Criptare chat - criptează mesajele instante pentru a vă asigura că conținutul lor rămân între dumneavoastră și partenerul de chat.

6.1. Protecție antiphishing

Bitdefender Antiphishing împiedică dezvăluirea informațiilor personale în timp ce navigați pe Internet alertându-vă despre paginile web cu conținut potențial phishing.

Bitdefender furnizează protecție antiphishing în timp real pentru:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Pentru a configura setările Antiphishing, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Control date** în meniul din stânga și apoi pe fila **Antiphishing**.

Setările sunt grupate în două categorii.

Funcții bară de instrumente

Faceți clic pe comutatoare pentru a activa sau dezactiva:

- Afișarea barei de instrumente Bitdefender în browser-ul de web.
- Consilier pentru căutare, o componentă care clasifică rezultatele afișate în urma căutărilor efectuate de dumneavoastră prin intermediul Google, Bing și Yahoo! precum și link-urile de pe Facebook și Twitter, plasând o pictogramă în fața fiecărui rezultat:

  Nu este recomandat să vizitați această pagină web.

  Această pagină web poate avea conținut periculos. Aveți mare grijă în cazul în care decideți s-o vizitați.

  Această pagină este una sigură.

- 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 pentru browserele de internet

Faceți clic pe comutatoare pentru a activa sau dezactiva:

- Protecție împotriva fraudelor.
- Protecție împotriva tentativelor de phishing.
- Protecția mesajelor instante.

Puteți configura o listă de site-uri web care nu vor fi scanate de către motoarele antiphishing 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 lista albă antiphishing, faceți clic pe link-ul **Listă albă**Va apărea 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.

6.1.1. Protecție Bitdefender în browser-ul web

Bitdefender se integrează direct, printr-o bară de comenzi intuitivă și ușor de folosit, cu următoarele browsere web:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

Bara de instrumente Bitdefender nu este aceeași cu bara de instrumente a browser-ului dumneavoastră obișnuit.Singurul lucru pe care îl adaugă browser-ului dumneavoastră este un mic instrument de glisare în partea superioară a fiecărei pagini web.Faceți clic pe acesta pentru a vizualiza bara de instrumente.

Bara de instrumente Bitdefender conține următoarele elemente:

Clasificarea paginii

În funcție de cum este clasificată pagina web pe care o vizualizați în acel moment de către Bitdefender, va fi afișată, în partea stângă a barei de instrumente, una dintre următoarele clasificări:

- Mesajul "Aceasta nu este o pagină sigură" este afișat pe fundal roșu - trebuie să părăsiți imediat pagina de internet.
- Mesajul "Atenție!" este afișat pe un fundal portocaliu - această pagină web poate avea un conținut periculos.Vizitați cu atenție această pagină.
- Mesajul "Această pagină este sigură" este afișat pe fundal verde - aceasta este o pagină securizată pe care o puteți vizita.

Sandbox

Faceți clic pe pentru a lansa browser-ul într-un mediu oferit de Bitdefender, izolându-l de sistemul de operare.În acest fel veți împiedica amenințările ce acționează prin intermediul browser-ului să exploateze vulnerabilitățile browser-ului și să câștige controlul asupra sistemului dumneavoastră.Atunci când vizitați pagini web care credeți că ar putea conține acțiuni periculoase, utilizați Sandbox.

Notă
Sandbox nu este disponibil pe computerele ce rulează pe Windows XP.

Setări

Faceți clic pe pentru a selecta caracteristici individuale, prin intermediul cărora să activați sau să dezactivați:

- Filtru Antiphishing
- Filtru antimalware
- Consilier pentru căutare

Întrerupător de rețea

Pentru a activa/dezactiva complet caracteristicile barei de instrumente, faceți clic pe , în partea dreaptă a barei de instrumente.

6.1.2. 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:

- Părăsiți această pagină web.
- Vizitați pagina web în ciuda avertismentului, făcând clic pe **Înțeleg riscurile, vreau să continui oricum**.
- Adăugați pagina la lista albă Antiphishing făcând clic pe **Adaugă pe lista albă**.Pagina nu va mai fi scanată de motoarele Bitdefender Antiphishing.

6.2. Protecție date

Funcția de protecție a datelor împiedică scurgerea de date personale atunci când sunteți online.

Luați în considerare un exemplu simplu: ați creat o regulă de protecție a datelor care vă protejează numărul cardului de credit.În cazul în care un software spyware reușește cumva să se instaleze pe computerul dumneavoastră, nu va putea să trimite numărul cărții de credit prin e-mail, prin intermediul mesajelor instante sau a paginilor web.În plus, copiii dumneavoastră nu le pot utiliza pentru achiziții online sau nu le pot dezvălui persoanelor pe care le-au cunoscut pe internet.

Pentru a afla mai multe, consultați aceste subiecte:

- *„Despre protecția datelor”* (p. 63).
- *„Configurarea protecției datelor”* (p. 64).
- *„Administrarea regulilor”* (p. 65).

6.2.1. Despre protecția datelor

Fie că este vorba de adresa e-mail sau de numărul cărții de credit, dacă acestea ajung în mâinile unor persoane nepotrivite vă pot aduce daune: puteți să vă treziți că aveți contul de mail plin de spam sau să constatați cu surprindere că aveți contul bancar golit.

Pe baza regulilor create de dumneavoastră, Protecția datelor scanează traficul web, e-mail sau de mesagerie instant care părăsește computerul dumneavoastră în căutare de șiruri de caractere specifice (de exemplu, numărul cardului dumneavoastră de credit). Dacă există o concordanță, site-ul web, e-mailul sau mesajul instant respectiv este blocat.

Puteți crea reguli pentru a proteja orice informație pe care o considerați personală sau confidențială, de la numărul dumneavoastră de telefon sau adresa dumneavoastră de e-mail până la informațiile referitoare la contul dumneavoastră bancar.Este oferit suport pentru mai mulți utilizatori, astfel încât utilizatorii care folosesc diferite conturi de utilizator Windows să poată configura și folosi propriile lor reguli.Dacă aveți un cont Windows de administrator, regulile pe care le creați

pot fi configurate să se aplice și atunci când alți utilizatori ai calculatorului sunt conectați la conturile lor Windows.

6.2.2. Configurarea protecției datelor

Dacă doriți să utilizați protecția datelor, urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Control date** în meniul din stânga și apoi pe fila **Protecție date**.
4. Asigurați-vă că funcția de protecție a datelor este activată.
5. Creați reguli pentru a vă proteja datele confidențiale.Pentru mai multe informații, consultați *„Crearea regulilor de protecție a datelor”* (p. 64).

Crearea regulilor de protecție a datelor

Pentru a crea o regulă, faceți clic pe butonul **Adăugare regulă** și urmați pașii programului asistent de configurare.Puteți naviga prin programul asistent cu ajutorul butoanelor **Înainte** și **Înapoi**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Furnizați tipul și argumentul regulii**

   Trebuie setați parametrii următori:

   - **Nume regulă** - introduceți numele regulii în acest câmp editabil.
   - **Tip regulă** - alegeți tipul regulii (adresă, nume, card de credit, PIN, etc.).
   - **Argument regulă** - introduceți datele pe care doriți să le protejați în acest câmp editabil.De exemplu, pentru a vă proteja numărul cardului dumneavoastră de credit, introduceți tot numărul sau doar o parte din el aici.

     Important
     Dacă introduceți mai puțin de trei caractere, vi se va solicita confirmarea acțiunii. Se recomandă introducerea a cel puțin trei caractere pentru a preveni blocarea greșită a mesajelor și a paginilor web.

   Tot ceea ce introduceți este criptat. Pentru mai multă siguranță, nu introduceți informația pe care vreți să o protejați în întregime, ci doar o parte a acesteia.

2. **Selectați tipurile de trafic și utilizatorii**

   a. Selectați tipul de trafic care doriți să fie scanat de Bitdefender.

   - **Scanează traficul web (HTTP)** - scanează traficul web (HTTP) și blochează la ieșire toate datele care corespund unei reguli.
   - **Scanează traficul e-mail (SMTP)** - scanează traficul mail (SMTP) și blochează trimiterea mesajelor e-mail care corespund unei reguli.

- **Scanează mesageria instant** - scanează traficul de mesagerie instant și blochează trimiterea mesajelor instant care corespund unei reguli.

  Puteți alege să aplicați regula doar dacă datele protejate apar ca șir independent sau ținând cont de majuscule și minuscule.

b. Precizați utilizatorii cărora li se aplică regula.

- **Numai pentru mine** - regula se va aplica numai contului dumneavoastră de utilizator.
- **Conturile de utilizatori cu drepturi limitate** - regula se va aplica dumneavoastră și tuturor conturilor Windows cu drepturi limitate.
- **Toți utilizatorii** - regula se va aplica tuturor conturilor Windows.

3. **Descrieți regula**

   Introduceți o scurtă descriere a regulei în câmpul editabil.Deoarece informația blocată (șirul respectiv de caractere) nu este afișată atunci când este accesată regula, descrierea trebuie să ajute la identificarea acesteia.

   Faceți clic pe **Finalizare**.Regula va apărea în tabel.

De acum înainte, va eșua orice tentativă de a trimite datele specificate (prin e-mail, mesaje instante sau prin intermediul unei pagini web).În fereastra Evenimente va fi afișată o intrare care indică faptul că Bitdefender a blocat trimiterea conținutului de identitate specific.

6.2.3. Administrarea regulilor

Pentru a gestiona regulile de protecție a datelor:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Control date** în meniul din stânga și apoi pe fila **Protecție date**.

Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge regula**.

Pentru a edita o regulă, selectați-o și faceți clic pe butonul **Editare regulă**. Va apărea o nouă fereastră.Aici puteți modifica numele, descrierea și parametrii regulii (tip, argument și trafic). Faceți clic pe **OK** pentru a salva modificările.

6.3. Criptare chat

Conținutul conversațiilor dumneavoastră prin mesagerie instant trebuie să rămână doar între dumneavoastră și interlocutorul dumneavoastră.Prin criptarea conversațiilor, vă puteți asigura că oricine încearcă să vă intercepteze mesajele instant trimise sau primite nu poate citi conținutul acestora.

În mod implicit, Bitdefender criptează toate conversațiile dumneavoastră prin mesagerie instant dacă sunt îndeplinite următoarele condiții:

- Partenerul dumneavoastră de chat are instalată o versiune de Bitdefender care suportă criptarea chat-ului, iar criptarea este activată pentru aplicația de mesagerie instantă folosită pentru chat.
- Atât dumneavoastră, cât si partenerul dumneavoastră de chat, să utilizați fie Yahoo Messenger, fie Windows Live (MSN) Messenger.

Important

Bitdefender nu va cripta o conversație dacă un partener de chat folosește o aplicație web pentru chat, cum ar fi Meebo, sau dacă un partener folosește Yahoo!, iar celălalt Windows Live (MSN).

Pentru a configura criptarea mesageriei instant:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Control date** în meniul din stânga și apoi pe fila **Criptare**.

Implicit, criptarea chat-ului este activată atât pentru Yahoo Messenger, cât și pentru Windows Live (MSN) Messenger.Puteți dezactiva opțiunea de criptare chat pentru una sau pentru ambele aplicații făcând clic pe comutatorul corespunzător.

7. Hartă rețea

Modulul Rețea personală vă permite să administrați produsele Bitdefender instalate pe calculatoarele personale de pe un singur calculator.

Pentru a putea administra produsele Bitdefender instalate pe calculatoarele personale, trebuie să urmați acești pași:

1. Activați rețeaua Bitdefender pe computerul dumneavoastră.Setați-vă computerul ca **Computer server**.
2. Mergeți la fiecare calculator pe care doriți să-l administrați și activați rețeaua (setați parola).Setați fiecare computer ca fiind **Computer obișnuit**.
3. Întoarceți-vă la calculatorul dumneavoastră și adăugați calculatoarele pe care doriți să le administrați.

7.1. Activarea rețelei Bitdefender

Pentru a activa rețeaua Bitdefender, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Hartă rețea** în meniul din stânga.
4. Faceți clic pe **Activează rețea**.Vi se va solicita să configurați parola de gestionare a hărții de rețea.
5. Introduceți aceeași parolă în ambele câmpuri editabile.
6. Setați rolul computerului în harta de rețele Bitdefender:
   - **Computer server** - selectați această opțiune pe computerul care va fi utilizat pentru a administra toate celelalte computere.
   - **Computer obișnuit** - selectați această opțiune pe computerele care vor fi administrate de către computerul server.
7. Faceți clic pe **OK**.

   Puteți vedea numele calculatorului apărând pe harta rețelei.

   Apare butonul **Dezactivare conexiune**.

Notă

Puteți, de asemenea, să activați harta de rețea din fereastra principală a Bitdefender:

1. Deschideți fereastra Bitdefender.
2. Mergeți la secțiunea **Hartă rețea**.
3. Faceți clic pe **Administrare** și selectați **Activare rețea** din meniul vertical.

7.2. Adăugarea computerelor la rețeaua Bitdefender

Orice calculator va fi adăugat în mod automat la rețea dacă întrunește următoarele criterii:

- harta de rețea Bitdefender a fost activată pe acesta.
- rolul a fost setat la calculator obișnuit.
- parola stabilită la activarea rețelei este identică cu parola setată pe calculatorul server.

Notă

Puteți scana oricând harta rețelei pentru a identifica computerele care îndeplinesc criteriile, făcând clic pe butonul **Identificare automată**

Pentru a adăuga manual un computer la rețeaua personală Bitdefender de pe computerul server, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Hartă rețea** în meniul din stânga.
4. Faceți clic pe **Adaugă calculator**.
5. Introduceți parola de administrare și faceți clic pe **OK**.Va apărea o nouă fereastră.

   Puteți vedea lista calculatoarelor din rețea.Semnificația iconițelor este după cum urmează:

    Indică un calculator online fără niciun produs Bitdefender instalat.

    Indică un calculator online cu Bitdefender instalat.

    Indică un calculator închis cu Bitdefender instalat.
6. Puteți proceda astfel:
   - Selectați din listă numele calculatorului pe care doriți să îl adăugați.
   - Introduceți în câmpul corespunzător adresa IP sau numele calculatorului pe care doriți să îl adăugați.
7. Faceți clic pe **Adaugă**.
8. Introduceți parola de management configurată pe computerul respectiv.
9. Faceți clic pe **OK**.Dacă ați furnizat parola corectă, numele calculatorului selectat va apărea pe harta rețelei.

7.3. Administrarea rețelei Bitdefender

După ce ați creat cu succes o hartă de rețea Bitdefender, puteți administra toate produsele Bitdefender de la computerul server.

Pentru a executa mai multe activități pe toate computerele administrate, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Mergeți la secțiunea **Hartă rețea**.
3. Faceți clic pe **Administrează** și selectați butoanele corespunzătoare din meniul vertical:
   - **Dezactivează conexiunea** - vă permite să dezactivați rețeaua.
   - **Scanează tot** - vă permite să scanați toate calculatoarele administrate în același timp.
   - **Actualizează tot** - vă permite să actualizați toate calculatoarele administrate în același timp.

Înainte de a executa o activitate pe un anumit computer, vi se va cere să furnizați parola locală de administrare.Introduceți parola de administrare și faceți clic pe **OK**.

Pentru a vedea întreaga Hartă de rețea și pentru a accesa activitățile de administrare, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Hartă rețea** în meniul din stânga.

Dacă plasați cursorul mouse-ului deasupra unui computer de pe harta rețelei, puteți vedea informații despre acesta (adresa IP, numărul de probleme ce afectează securitatea sistemului, starea înregistrării Bitdefender).

Dacă faceți clic pe numele unui calculator de pe harta rețelei, puteți vedea toate sarcinile administrative pe care le puteți rula de la distanță pe calculatorul respectiv.

Înregistrare produs
Vă permite să înregistrați Bitdefender pe acest calculator, prin introducerea unei serii de înregistrare.

Configurare parolă pentru setările produsului
Vă permite să configurați o parolă pentru a restricționa accesul la setările Bitdefender pe acest calculator.

Execută sarcina de scanare la cerere
Vă permite să executați o scanare la cerere pe computerul de la distanță. Aveți posibilitatea să efectuați oricare din următoarele activități de scanare: Scanare rapidă sau Scanare completă a sistemului.

Repară toate problemele
Vă permite să rezolvați problemele care afectează securitatea acestui calculator, urmând pașii programului asistent Remediază probleme.

Vizualizare evenimente

Vă permite să accesați modulul **Evenimente** al produsului Bitdefender instalat pe acest computer.

Actualizează

Inițiază procesul de actualizare a produsului Bitdefender instalat pe acest calculator.

Setează ca server de actualizare pentru această rețea

Vă permite să setați acest calculator ca server de actualizare pentru toate produsele Bitdefender instalate pe calculatoarele din aceasta rețea.Prin folosirea acestei opțiuni, se va reduce traficul pe internet, pentru că numai un calculator din rețea se va conecta la internet pentru a descărca actualizări.

Ștergere computer din harta rețelei

Vă permite să scoateți un calculator din rețea.

Notă

Dacă plănuiți să executați mai multe sarcini, puteți bifa **Nu mai afișa acest mesaj în sesiunea curentă**.Selectând această opțiune, nu vi se va mai cere să introduceți această parolă în sesiunea curentă.

8. Actualizare

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

Dacă sunteți conectat la Internet, prin bandă largă sau ADSL, Bitdefender se ocupă singur de actualizări. Implicit, Bitdefender caută actualizări când deschideți calculatorul și apoi la 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. 33).
- Dacă nu beneficiați de conexiune la internet, puteți efectua actualizarea Bitdefender manual, după cum este specificat în *„Computerul meu nu este conectat la internet. Cum actualizez Bitdefender?”* (p. 79).Fișierul de actualizare manuală este lansat o dată pe săptămână.
- 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. 78).
- 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. 72).

8.1. Cum verificați dacă Bitdefender este actualizat

Pentru a verifica dacă protecția oferită de produsul dumneavoastră Bitdefender este actualizată, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Mergeți la panoul **Actualizare**.

3. Data și ora ultimei actualizări sunt afișate chiar sub denumirea secțiunii.

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

1. În fereastra principală, faceți clic pe **Evenimente** din partea superioară a barei de instrumente.
2. Faceți clic pe **Actualizare** în meniul din stânga.

Puteți afla atunci 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.

8.2. 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 fereastra Bitdefender, mergeți la panoul **Actualizare** și faceți clic pe **Actualizează acum**.
- Faceți clic dreapta pe pictograma Bitdefender din bara de sistem și selectați **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. Este recomandat să faceți acest lucru cât mai repede posibil.

8.3. Activarea sau dezactivarea actualizării automate

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

1. Deschideți fereastra Bitdefender.
2. Mergeți la panoul **Actualizare**.
3. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea de actualizare automată.
4. Dacă doriți să dezactivați o actualizare automată, va apărea o fereastră de avertizare.Va trebui să confirmați acțiunea selectând din meniu intervalul de timp pentru care să fie dezactivată actualizarea automată. Puteți dezactiva actualizarea automată pentru 5, 15 sau 30 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.

8.4. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Actualizare** în meniul din stânga.
4. Ajustați setările în funcție de preferințele dumneavoastră.

Locație actualizare

Produsul Bitdefender este configurat să efectueze online actualizări de pe serverele de actualizare ale Bitdefender.Locația de actualizare este `http://upgrade.bitdefender.com`, 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.

Dacă aveți Bitdefender instalat pe mai multe computere acasă la dumneavoastră, puteți seta o rețea Bitdefender la domiciliu, după care puteți configura unul dintre computere ca server de actualizare. Mai multe informații puteți găsi în *„Hartă rețea”* (p. 67).Programul Bitdefender instalat pe serverul de actualizare respectiv va descărca actualizări de pe internet. Programele Bitdefender instalate pe alte computere își vor descărca actualizările de pe serverul local de actualizare (locația de actualizare a acestora se va modifica automat).Scopul acestei configurații este de a reduce traficul de internet și de a optimiza actualizările.

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.

Actualizări P2P

Pe lângă mecanismul obișnuit de actualizare, Bitdefender folosește, de asemenea, un sistem inteligent de partajare a actualizărilor bazat pe un protocol peer-to-peer prin intermediul căruia distribuie utilizatorilor Bitdefender actualizările semnăturilor programelor periculoase.

Puteți activa sau dezactiva opțiunile de actualizare P2P cu ajutorul comutatoarelor corespunzătoare.

Utilizare actualizare de sistem P2P

Activați această opțiune pentru a descărca actualizări de semnături malware de la alți utilizatori Bitdefender folosind sistemul de actualizare P2P.Bitdefender utilizează porturile 8880 - 8889 pentru actualizarea peer-to-peer (P2P).

Distribuire fișiere Bitdefender

Pentru a partaja cele mai recente semnături malware disponibile pe computerul dumneavoastră cu alți utilizatori Bitdefender, activați această opțiune.

9. Protecție Safego pentru rețelele sociale

Aveți încredere în prietenii dumneavoastră online.Aveți însă încredere în computerele acestora?Utilizați protecția Safego pentru rețelele sociale pentru a vă proteja contul și prietenii împotriva amenințărilor online.

Safego este o aplicație pentru Facebook dezvoltată de Bitdefender pentru a menține siguranța contului activat pe rețeaua de socializare.Rolul său este de a scana link-urile pe care le primiți de la prietenii de pe Facebook și de a monitoriza setările de confidențialitate a contului dumneavoastră.

Notă

Pentru a putea utiliza această funcție, este necesar un cont MyBitdefender. Pentru mai multe informații, consultați *„Înregistrare produs”* (p. 7).

Acestea sunt funcțiile sale principale:

- scanează automat postările din News Feed pentru link-uri periculoase.
- vă protejează contul împotriva amenințărilor online.

  În momentul în care detectează o postare sau un comentariu care este de tip spam, tentativă de phishing sau malware, veți primi un mesaj de avertizare.
- vă avertizează prietenii cu privire la link-urile suspecte postate în News Feed.
- vă ajută să vă creați o rețea sigură de prieteni cu ajutorul funcției **Friend’O’Meter**.
- efectuați o verificare a stării de securitate a sistemului cu ajutorul funcției de Scanare rapidă a Bitdefender.

Pentru a accesa Safego din produsul Bitdefender, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Mergeți la panoul **Safego**.
3. Faceți clic pe **Activare**.Veți fi direcționat către contul dumneavoastră.

   Dacă ați activat deja Safego, veți putea să accesați statisticile referitoare la activitatea sa făcând clic pe butonul **Vizualizare rapoarte**.
4. Utilizați informațiile de autentificare Facebook pentru a vă conecta la aplicația Safego.
5. Permiteți opțiunii Safego să acceseze contul dumneavoastră de Facebook.

10. Remedierea problemelor

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. 76)
- *„Nu începe scanarea”* (p. 77)
- *„Nu mai pot utiliza o anumită aplicație”* (p. 77)
- *„Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet”* (p. 78)
- *„Computerul meu nu este conectat la internet. Cum actualizez Bitdefender?”* (p. 79)
- *„Serviciile Bitdefender nu răspund”* (p. 79)
- *„Nu s-a reușit dezinstalarea Bitdefender”* (p. 80)
- *„Sistemul meu nu pornește după ce am instalat Bitdefender”* (p. 81)

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 *„Suport”* (p. 92).

10.1. 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 dezinstalez alte soluții de securitate?”* (p. 98).

- **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. 1).

- **Unitățile de hard disc sunt prea fragmentate.**

Fragmentarea fișierelor încetinește accesul la acestea și scade performanțele sistemului.

Pentru a vă defragmenta partițiile de disc folosind instrumentul din Windows, urmați calea din meniul Start al Windows: **Start → All Programs → Accessories → System Tools → Disk Defragmenter**.

10.2. 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:
     a. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
     b. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
     c. Reporniți calculatorul.
  2. Reinstalați Bitdefender în sistem.

- **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 dezinstalez alte soluții de securitate?”* (p. 98).
  2. Dezinstalați complet Bitdefender din sistem:
     a. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
     b. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
     c. Reporniți calculatorul.
  3. Reinstalați Bitdefender în sistem.

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. 93).

10.3. Nu mai pot utiliza o anumită aplicație

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

Vă puteți confrunta cu una dintre 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 Virus Control detectează din greșeală anumite aplicații ca fiind rău intenționate.

Active Virus 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 Virus Control.

Atunci când se întâmplă aceasta, puteți exclude aplicația respectivă de la monitorizarea efectuată de Active Virus Control.

Pentru a adăuga programul în lista de excluderi, urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară..
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Excepții**.
4. Faceți clic pe link-ul **Procese excluse**.În fereastra care va apărea, puteți gestiona excepțiile de la procesul Active Virus 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 Virus 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. 93).

10.4. 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. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Actualizare** în meniul din stânga și apoi pe fila **Actualizare**.
4. Sub opțiunea **Actualizare reguli de procesare**, selectați **Anunță înainte de descărcare**.
5. Faceți clic pe butonul **Acasă** de pe bara de instrumente din partea superioară.
6. Mergeți la panoul **Actualizare** și faceți clic pe **Actualizează acum**.
7. Selectați numai **Actualizări semnături** și apoi faceți clic pe **OK**.
8. Bitdefender va descărca și va instala numai actualizările semnăturilor malware.

10.5. Computerul meu nu este conectat la internet. Cum actualizez Bitdefender?

În cazul în care calculatorul dumneavoastră nu este conectat la internet, trebuie să descărcați manual actualizările pe un calculator cu acces la internet și apoi să le transferați pe calculatorul dumneavoastră utilizând un dispozitiv de stocare portabil, cum ar fi un stick USB.

Urmați acești pași:

1. Pe un calculator cu acces la internet, deschideți un browser și accesați:

   http://www.bitdefender.com/site/view/Desktop-Products-Updates.html

2. În coloana **Actualizare manuală**, faceți clic pe linkul corespunzător produsului și arhitecturii sistemului dumneavoastră.În cazul în care nu știți dacă sistemul dumneavoastră Windows rulează pe 32 sau 64 de biți, consultați *„Utilizez o versiune Windows pe 32 biți sau pe 64 biți?”* (p. 99).
3. Salvați fișierul denumit `weekly.exe` în sistem.
4. Transferați fișierul descărcat pe un dispozitiv de stocare portabil, cum ar fi un stick USB, și apoi în calculatorul dumneavoastră.
5. Faceți dublu-clic pe fișier și urmați indicațiile programului asistent.

10.6. 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:

- o actualizare importantă este în curs de instalare.
- 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. Verificați dacă aveți instalată orice altă soluție de securitate pentru că ea ar putea perturba funcționarea normală a Bitdefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați Bitdefender.

   Pentru mai multe informații, consultați *„Cum dezinstalez alte soluții de securitate?"* (p. 98).

Dacă eroarea persistă, vă rugăm să contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea *„Solicitarea ajutorului"* (p. 93).

10.7. Nu s-a reușit dezinstalarea Bitdefender

Acest articol vă ajută să remediați erorile care pot apărea la dezinstalarea Bitdefender.Sunt posibile două situații:

- În timpul dezinstalării apare un ecran de eroare.Ecranul oferă un buton pentru rularea unui instrument de dezinstalare, care va curăța sistemul.
- Dezinstalarea nu înaintează și, eventual, sistemul se blochează.Faceți clic pe **Anulează** pentru a abandona dezinstalarea. Dacă anularea nu este posibilă, reporniți sistemul.

Dacă dezinstalarea eșuează, unele chei de regiștri și fișiere Bitdefender pot rămâne în sistemul dumneavoastră. 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:

1. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
2. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
3. Reporniți 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. 93).

10.8. 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. 99).
  2. Ștergeți Bitdefender din sistemul dumneavoastră:
     a. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
     b. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
     c. Reporniți calculatorul.
  3. Reporniți sistemul în modul normal și reinstalați 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. 99).
  2. Ștergeți Bitdefender din sistemul dumneavoastră:
     a. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
     b. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
     c. Reporniți calculatorul.

3. 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.
4. 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. 99).
2. Cu ajutorul funcției System Restore din Windows puteți restabili computerul la o dată anterioară instalării produsului Bitdefender.Pentru a afla cum să procedați, consultați *„Cum folosesc funcția System Restore în Windows?”* (p. 100).
3. Reporniți sistemul în modul normal și contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea *„Solicitarea ajutorului”* (p. 93).

11. 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.

- *„Modul de salvare Bitdefender”* (p. 83)
- *„Ce trebuie să faceți atunci când Bitdefender detectează viruși pe computerul dumneavoastră?”* (p. 85)
- *„Cum elimin un virus dintr-o arhivă?”* (p. 86)
- *„Cum elimin un virus dintr-o arhivă de e-mail?”* (p. 87)
- *„Ce trebuie să fac dacă suspectez că un fișier este periculos?”* (p. 88)
- *„Cum să curățați fișierele infectate din System Volume Information”* (p. 88)
- *„Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?”* (p. 90)
- *„Ce reprezintă elementele omise din jurnalul de scanare?”* (p. 90)
- *„Ce reprezintă fișierele supracomprimate din jurnalul de scanare?”* (p. 90)
- *„De ce Bitdefender a șters în mod automat un fișier infectat?”* (p. 91)

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 *„Suport”* (p. 92).

11.1. Modul de salvare Bitdefender

Modul de salvare 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 Antivirus Plus 2012, Modul de salvare poate fi utilizat chiar dacă nu mai puteți reporni sistemul din Windows.

Pornirea sistemului în Modul de salvare

Puteți accesa Modul de salvare în unul dintre următoarele două moduri:

Din fereastra Bitdefender

Pentru a accesa Modul de salvare direct din Bitdefender, urmați acești pași:

1. Mergeți la secțiunea **Antivirus**.

2. Faceți clic pe **Scanează acum** și selectați **Mod de salvare** din meniul vertical.

   Va fi afișată o fereastră de confirmare. Faceți clic pe **Da** pentru a vă reporni computerul.

3. După ce este repornit computerul, va apărea un meniu care vă va solicita să selectați un sistem de operare.Alegeți **imaginea de salvare Bitdefender** și apăsați pe tasta **Enter** pentru a reporni dintr-un mediu Bitdefender de unde vă puteți curăța partiția Windows.

4. 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**.

   Modul de salvare pentru Bitdefender se va încărca în câteva momente.

Porniți computerul direct în Modul de salvare

În cazul în care nu mai pornește Windows, puteți porni computerul direct în Modul de salvare al Bitdefender, urmând pașii de mai jos.

Notă

Această metodă nu este disponibilă pe computerele pe care rulează Windows XP.

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**.

   Modul de salvare pentru Bitdefender se va încărca în câteva momente.

Scanarea sistemului în Modul de salvare

Pentru a scana sistemul atunci când se află în Modul de salvare, urmați pașii de mai jos:

1. Accesați modul de salvare, conform descrierii din „Pornirea sistemului în Modul de salvare” (p. 83).
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 ținta 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 Modul de salvare, 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 până se finalizează scanarea. Dacă este detectat vreun program malware, urmați instrucțiunile pentru a elimina amenințarea.
8. Pentru a ieși din Modul de salvare, faceți clic dreapta în secțiunea liberă de pe Desktop, selectați **Deconectare** din meniul care apare și apoi selectați dacă doriți să reporniți sau să închideți computerul.

11.2. 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 completă a sistemului pentru analizarea acestuia.

După finalizarea scanării, selectați acțiunii care doriți să fie aplicată în cazul elementelor 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. Deschideți fereastra Bitdefender.

b. Faceți clic pe butonul **Setări** de pe bara de instrumente din partea superioară.

c. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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. 100).
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. 99).
2. Afișați elementele ascunse din Windows.
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. 93).

11.3. 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 complete a sistemului.
2. Dezactivați protecția antivirus în timp real a Bitdefender:

a. Deschideți fereastra Bitdefender.

b. Faceți clic pe butonul **Setări** de pe bara de instrumente din partea superioară.

c. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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. 93).

11.4. 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. Deschideți fereastra Bitdefender.

b. Faceți clic pe butonul **Setări** de pe bara de instrumente din partea superioară.

c. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **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: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 Compact.
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. 93).

11.5. 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 completă a sistemului** cu Bitdefender.Pentru a afla cum să procedați, consultați *„Cum îmi scanez sistemul?”* (p. 30).
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. 93).

11.6. Cum să curățați fișierele infectate din System Volume Information

Directorul System Volume Information se află într-o zonă a hard-discului creată de către sistemul de operare și utilizată de Windows pentru stocarea de informații critice referitoare la configurația sistemului.

Motoarele Bitdefender pot detecta orice fișiere infectate stocate de către System Volume Information, însă aceasta fiind o zonă protejată, fișierele nu pot fi șterse.

Fișierele infectate detectate în directoarele System Restore vor apărea în jurnalul de scanare după cum urmează:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Pentru a șterge complet și imediat fișierele infectate din locul unde sunt stocate, dezactivați și reactivați funcția System Restore.

Atunci când funcția System Restore este dezactivată, toate punctele de restaurare sunt șterse.

Atunci când funcția System Restore este activată din nou, sunt create noi puncte de restaurare conform programării și evenimentelor apărute.

Pentru a dezactiva funcția System Restore, urmați acești pași:

- **Pentru Windows XP:**
  1. Urmați această cale: **Start** → **All Programs** → **Accessories** → **System Tool** → **System Restore**
  2. Faceți clic pe **System Restore Settings** în partea stângă a ferestrei.
  3. Bifați căsuța **Turn off System Restore** pentru toate unitățile și faceți clic pe **Apply**.
  4. Atunci când sunteți avertizat că toate punctele de restaurare vor fi șterse, faceți clic pe **Yes** pentru a continua.
  5. Pentru a activa funcția System Restore, debifați căsuța **Turn off System Restore** pentru toate unitățile și faceți clic pe **Apply**.
- **Pentru Windows Vista:**
  1. Urmăriți această cale: **Start** → **Control Panel** → **System and Maintenance** → **System**
  2. În panoul stâng, faceți clic pe **System protection**.

     Dacă vi se solicită să introduceți o parolă de administrator sau să confirmați, introduceți parola sau confirmați.
  3. Pentru a dezactiva funcția System Restore, debifați căsuțele corespunzătoare fiecărei unități și faceți clic pe **Ok**.
  4. Pentru a activa funcția System Restore, bifați căsuțele corespunzătoare fiecărei unități și faceți clic pe **Ok**.
- **Pentru Windows 7:**
  1. Faceți clic pe **Start**, clic-dreapta pe **Computer** și alegeți **Properties**.
  2. Faceți clic pe linkul **System protection** din panoul stâng.
  3. Din opțiunile **System protection**, selectați fiecare literă de unitate și faceți clic pe **Configure**.
  4. Selectați **Turn off system protection** și faceți clic pe **Apply**.
  5. Faceți clic pe **Delete**, pe **Continue** atunci când vi se solicită acest lucru și apoi pe **Ok**.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 93).

11.7. 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.

11.8. 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.

11.9. 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.

Supracomprimarea 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 în timp real, la accesare, dacă este cazul.

11.10. 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, dezinfectarea nu este posibilă deoarece fișierul detectat este în întregime periculos. 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.

12. Obținere ajutor

12.1. Suport

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

12.1.1. Resurse online

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

- Centrul de asistență Bitdefender: http://www.bitdefender.ro/site/contact/1/
- forumul de suport al Bitdefender:http://forum.bitdefender.com
- portalul de securitate informatică Malware City:http://www.malwarecity.com

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

Centrul de asistență Bitdefender

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

Centrul de asistență Bitdefender este deschis publicului și pot fi realizate căutări în mod liber.Prin intermediul informațiilor extinse pe care le conține, putem oferi clienților Bitdefender cunoștințele tehnice și înțelegerea de care au nevoie.Toate solicitările valide 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/site/contact/1/.

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.

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

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

Forumul de suport al Bitdefender este disponibil la 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.

Portalul Malware City

Portalul Malware City constituie o sursă bogată de informații privind securitatea informatică. Aici puteți afla informații despre diversele pericole la care este expus calculatorul dumneavoastră atunci când este conectat la internet (malware, phishing, spam, infracțiuni cibernetice).Un dicționar util vă ajută la înțelegerea termenilor de securitate a calculatoarelor cu care nu sunteți familiarizați.

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

Pagina web a Malware City este http://www.malwarecity.com.

12.1.2. Solicitarea ajutorului

Secțiunea **Depanare probleme** vă oferă informațiile necesare referitoare la cele mai frecvent întâlnite probleme atunci când utilizați acest produs.

Dacă nu găsiți o soluție la problema dumneavoastră printre resursele puse la dispoziție, ne puteți contacta direct:

- „Contactați-ne direct din cadrul produsului dumneavoastră Bitdefender” (p. 94)
- „Contactați-ne prin intermediul Centrului nostru de asistență online” (p. 94)

Important

Pentru a contacta serviciul de asistență clienți Bitdefender, produsul dumneavoastră Bitdefender trebuie să fie înregistrat.Pentru mai multe informații, consultați *„Înregistrare produs”* (p. 7).

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. Deschideți fereastra Bitdefender.
2. Faceți clic pe link-ul **Ajutor și asistență** din colțul dreapta jos al ferestrei.
3. Aveți la dispoziție următoarele opțiuni:
   - Citiți articolele sau documentele relevante și încercați soluțiile propuse.
   - Efectuați o căutare în baza noastră de date după informațiile de care aveți nevoie.
   - Cu ajutorul butonului **Contactare asistență** pentru a lansa Instrumentul de asistență și a contacta Departamentul Serviciu Clienți.Puteți naviga prin programul asistent utilizând butonul **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. Alegeți-vă țara din meniul corespunzător.
        iv. Introduceți o descriere a problemei întâmpinate.
     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 serviciului de asistență clienți al 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.com/help.Centrul de asistență Bitdefender include numeroase articole care cuprind soluții la problemele asociate Bitdefender.
2. Selectați produsul din coloana stângă și căutați articole care vă pot ajuta să soluționați problema în cadrul Centrului de asistență Bitdefender.
3. Citiți articolele sau documentele relevante și încercați soluțiile propuse.

4. Dacă soluția nu vă rezolvă problema, utilizați linkul din articol pentru a contacta serviciul de asistență clienți al Bitdefender.
5. Contactați reprezentanții BiDefender prin e-mail, pe chat sau la telefon.

12.2. 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.

12.2.1. Adrese web

Departament de vânzări: sales@bitdefender.ro
Centrul de asistență: http://www.bitdefender.ro/site/contact/1/
Documentație: documentation@bitdefender.com
Distribuitori locali:http://www.bitdefender.com/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

12.2.2. Distribuitori locali

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

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergeți la http://www.bitdefender.com/site/Partnership/list/.
2. Datele de contact ale distribuitorilor locali Bitdefender ar trebui să fie afișate automat. În caz contrar, selectați țara de reședință pentru a accesa aceste informații.
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.

12.2.3. Filialele Bitdefender

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

U.S.A

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefon (birou&vânzări): 1-954-776-6262
Vânzări: sales@bitdefender.com
Suport tehnic: http://www.bitdefender.ro/site/contact/1/
Web: http://www.bitdefender.ro

Marea Britanie și Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-mail: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096
Vânzări: sales@bitdefender.co.uk
Suport tehnic: http://www.bitdefender.ro/site/contact/1/
Web: http://www.bitdefender.co.uk

Germania

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Birou: +49 2301 91 84 0
Vânzări: vertrieb@bitdefender.de
Suport tehnic: http://kb.bitdefender.de
Web: http://www.bitdefender.de

Spania

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Vânzări: comercial@bitdefender.es

Suport tehnic: http://www.bitdefender.es/ayuda
Site web: http://www.bitdefender.es

România

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefon vânzări: +40 21 2063470
E-mail vânzări: sales@bitdefender.ro
Suport tehnic: http://www.bitdefender.ro/suport
Site web: http://www.bitdefender.ro

13. Informații utile

Acest capitol prezintă câteva proceduri importante pe care trebuie să le aveți în vedere înainte de a începe depanarea unei probleme tehnice.

Remedierea unei probleme de natură tehnică a Bitdefender necesită anumite cunoștințe despre Windows; ca atare, următoarele instrucțiuni se referă în mare măsură la sistemul de operare Windows.

- *„Cum dezinstalez alte soluții de securitate?”* (p. 98)
- *„Cum pot să repornesc sistemul în Safe Mode?”* (p. 99)
- *„Utilizez o versiune Windows pe 32 biți sau pe 64 biți?”* (p. 99)
- *„Cum folosesc funcția System Restore în Windows?”* (p. 100)
- *„Cum pot afișa elementele ascunse din Windows?”* (p. 100)

13.1. Cum dezinstalez alte 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 Antivirus Plus 2012 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:

- Pentru **Windows XP**:
  1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Add / Remove programs**.
  2. Așteptați câteva momente până când este afișată lista programelor instalate.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Remove**.
  4. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
- Pentru **Windows Vista** și **Windows 7**:
  1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programs and Features**.
  2. Așteptați câteva momente până când este afișată lista programelor instalate.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Uninstall**.
  4. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

Dacă nu reușiți să dezinstalați cealaltă soluție de securitate, faceți rost de instrumentul de dezinstalare de pe site-ul web al furnizorului sau contactați-l direct pentru a vă oferi instrucțiuni de dezinstalare.

13.2. 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.

13.3. 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:

- Pentru **Windows XP**:
  1. Faceți clic pe **Start**.
  2. Mergeți la **My Computer** din meniul **Start**.
  3. Faceți clic-dreapta pe **My Computer** și selectați **Properties**.
  4. Dacă vedeți **x64 Edition** sub **System**, sistemul care rulează pe calculatorul dumneavoastră este o versiune Windows XP pe 64 biți.

     Dacă nu vedeți **x64 Edition** în listă, sistemul care rulează pe computerul dumneavoastră este o versiune Windows XP pe 32 biți.
- Pentru **Windows Vista** și **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.

13.4. Cum folosesc funcția System Restore în Windows?

Dacă nu puteți porni computerul în modul normal, porniți-l în Safe Mode și, cu ajutorul System Restore, reveniți la un moment când puteați porni computerul fără probleme.

Pentru a putea efectua o restabilire a sistemului, trebuie să fiți autentificat pe Windows în calitate de administrator.

Pentru a folosi funcția System Restore, urmați pașii de mai jos:

- Pentru Windows XP:
  1. Conectați-vă la Windows în Safe Mode.
  2. Urmați această cale din meniul de start Windows: **Start → All Programs → System Tools → System Restore**.
  3. Pe pagina **Welcome to System Restore**, selectați prin clic opțiunea **Restore my computer to an earlier time** și apoi faceți clic pe Next.
  4. Pentru a porni sistemul în modul normal, urmați pașii programului asistent.
- Pentru Windows Vista și Windows 7:
  1. Conectați-vă la Windows în Safe Mode.
  2. Urmați această cale din meniul de start Windows: **All Programs → Accessories → System Tools → System Restore**.
  3. Pentru a porni sistemul în modul normal, urmați pașii programului asistent.

13.5. 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**, mergeți la **Control Panel** și selectați **Folder Options**.
2. Mergeți la fila **View**.
3. Selectați **Display contents of system folders** (exclusiv pentru Windows XP).
4. Selectați **Show hidden files and folders**.
5. Debifați **Hide file extensions for known file types**.

6. Debifați **Hide protected operating system files**.
7. Faceți clic pe **Aplicare** și apoi pe **Ok**.

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.

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, browserul 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 gaură 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 mentenanță produsului din partea vânzătorului.

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 web. Două din cele mai populare browsere sunt Mozilla Firefox și Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afișa atât imagini cât și text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet și animație.

Cale

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.

Cookie

Un cookie reprezintă un set de date pe care un server Web îl transmite către un browser atunci când utilizatorul vizitează prima oară site-ul și care este actualizat de fiecare dată când utilizatorul accesează din nou site-ul. Serverul, la fel ca și browserul, salvează informațiile despre utilizator conținute în cookie. Aceste informații sunt stocate sub forma unui fișier text în directoarele de sistem ale browserelor Netscape și Explorer;nu toate browserele suportă cookie. Fișierele cookie stochează informații cum ar fi numele utilizatorului și parola,

cât și ce părți din site au fost vizitate. Browserul împarte fiecare cookie doar cu server-ul care l-a generat, celelalte servere le pot citi doar pe cele generate de ele. Unele fișiere cookie sunt programate cu dată de expirare, astfel încât ele vor fi șterse automat după o anumită perioadă de timp.

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 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 caractere (unele sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: "txt" pentru fișierele text oarecare, "c" pentru fișierele sursă scrise în limbajul C, etc.

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.

Înregistratoarele de taste au o natură periculoasă. Acestea pot fi utilizate în scopuri legitime, ca de exemplu pentru monitorizarea activității copiilor sau angajaților. Totuși, sunt folosite din ce în ce mai mult de infractorii cibernetici în scopuri negative (ca de exemplu, pentru a colecta date personale, cum ar fi acreditările de înregistrare și codurile numerice personale).

Linie de comandă
Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Memorie
Reprezintă arii de stocare a datelor din interiorul calculatorului. Termenul de memorie desemnează locul de stocare a datelor pe chipuri și pe cel al cuvintelor pe casete sau cd-uri audio. Fiecare calculator dispune de o anumită capacitate de memorie fizică, referită de obicei prin memorie principală sau RAM.

Metoda euristică
Reprezintă o metodă bazată pe anumite reguli pentru identificarea de 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 specifice de viruși. 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.

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 din sistemele de operare și aplicații conțin comenzi care vă dau posibilitatea de a împacheta 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 împachetează fișiere va înlocui caracterele de spațiu printr-un caracter reprezentând spațiu, urmat de un număr care reprezintă numărul de spații care este înlocuit. 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.

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 întreagă gamă a mesajelor 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 insidioase tipuri de troieni este acela care pretinde că elimină virușii de pe calculatorul 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.

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.