bitdefender
ANTIVIRUS v10

10th anniversary

Manual de utilizare

Antivirus

Antispyware

bitdefender
secure your every bit

BitDefender Antivirus v10

Manual de utilizare

BitDefender

Publicat 2007.01.17
Version 10.2

Termeni legali


bitdefender
secure your every bit

Cuprins

Licență şi garanție

DACĂ NU SUNTEȚI DE ACORD CU ACEŞTI TERMENI ŞI CU ACESTE CONDIȚII NU INSTALAȚI ACEST SOFT. SELECTÂND "ACCEPT", "OK", "CONTINUĂ", "DA" SAU INSTALÂND SAU UTILIZÂND SOFTUL ÎN ORICE FEL INDICAȚI COMPLETA ÎNȚELEGERE ŞI ACCEPTARE A TERMENILOR CONTRACTULUI DE LICENȚĂ.

Aceşti Termeni acoperă soluțiile şi serviciile BitDefender, incluzând documentația asociată şi orice fel de actualizare a aplicației furnizată dumneavoastră în baza licenței achiziționate sau orice înțelegere de servicii asociată, definită în documentație, şi orice copie a acestor obiecte.

Acest Contract de Licență reprezintă o convenție legală între dumneavoastră (ca persoană fizică sau persoană juridică utilizator final) şi SOFTWIN pentru utilizarea produsului soft identificat mai sus, aparținând SOFTWIN, care include softul propriu-zis şi serviciile, şi poate include, medii de informație asociate, materiale tipărite şi documentație "on line" sau electronică (referite mai departe ca "BitDefender"). Toate acestea sunt protejate de legislația internațională privind drepturile de autor şi proprietatea intelectuală, precum şi de tratatele internaționale. Prin instalarea, copierea sau utilizarea, în orice alt mod, a produsului BitDefender, acceptați termenii acestui contract.

Dacă nu sunteți de acord cu termenii acestui contract, nu instalați şi nu utilizați produsul BitDefender.

Licența BitDefender. BitDefender este protejat de tratatele şi legile internaționale privind drepturile de autor, precum şi de celelalte legi şi tratate privind proprietatea intelectuală. BitDefender este oferit sub licență şi nu vândut.

ACORDAREA LICENȚEI. SOFTWIN vă oferă, dumneavoastră şi numai dumneavoastră, următoarea licență ne-exclusivă, limitată, netransferabilă pentru utilizarea produsului BitDefender.

APLICAȚIA SOFTWARE. Puteți instala şi utiliza BitDefender pe oricâte calculatoare este necesar în limita numărului total de licențe de utilizator deținute. Puteți face o singură copie adițională, ca rezervă.

LICENȚA UTILIZATORULUI DE DESKTOP. Această licență se aplică acelui soft BitDefender ce poate fi instalat doar pe un singur calculator şi care nu furnizează servicii pentru rețele. Fiecare utilizator principal poate instala acest soft pe un singur calculator şi poate face doar o singură copie adițională, ca rezervă, pe un dispozitiv diferit. Numărul de utilizatori principali permis este numărul de utilizatori ai licenței.

DURATA LICENȚEI. Licența acordată aici va începe la data la care veți instala BitDefender şi va continua doar până la sfârşitul perioadei pentru care licența a fost achiziționată.

ACTUALIZĂRI DE PRODUS (UPGRADE-URI). Dacă BitDefender este etichetat ca upgrade, va trebui să dețineți o licență de utilizare a unui produs identificat de SOFTWIN ca fiind eligibil pentru respectivul upgrade. Un produs BitDefender etichetat ca fiind upgrade, înlocuieşte şi/sau completează produsul care reprezintă baza dreptului dumneavoastră de a beneficia de actualizarea de produs. Puteți utiliza produsul rezultat în urma actualizării numai în concordantă cu termenii specificați în prezentul Contract de Licență. Dacă BitDefender este un upgrade al unei componente a unui pachet de programe soft care v-au fost licențiate ca un singur produs, atunci BitDefender poate fi utilizat sau transferat numai ca parte a acelui pachet individual de produse şi nu poate fi separat pentru utilizarea sa de către mai mulți utilizatori decât numărul de licențe. Termenii şi condițiile acestei licențe înlocuiesc şi prevalează orice alte înțelegeri care ar fi putut exista între dumneavoastră şi SOFTWIN privind produsul original sau produsul rezultat ca urmare a actualizării.

COPYRIGHT. Toate drepturile, titlurile şi beneficiile ce țin de BitDefender (inclusiv, dar fără a se limita la orice imagine, fotografie, animație, video, audio, muzică, text şi cod, încorporate în produsul BitDefender), toate materialele tipărite care însoțesc produsul şi orice copie a produsului BitDefender sunt proprietatea SOFTWIN. BitDefender este protejat de legile şi tratatele internaționale privind drepturile de autor şi proprietatea intelectuală. Prin urmare, BitDefender trebuie tratat ca orice alt material supus drepturilor de autor. Nu aveți dreptul să copiați materialele tipărite ce însoțesc BitDefender. Aveți obligația de a prezenta şi include toate notele privind drepturile de autor în forma lor originală în toate copiile create, indiferent de mediul de transmisie sau de forma în care BitDefender există. Sunt interzise sub-licențierea, închirierea, vinderea, cedarea sau împărțirea licenței BitDefender. De asemenea, sunt interzise piratarea, recompilarea, dezasamblarea, crearea de produse derivate, modificarea, traducerea sau orice altă încercare de a descoperi codul sursă al produsului BitDefender.

LIMITAREA GARANȚIEI. SOFTWIN garantează lipsa oricărui defect al suportului de distribuire al produsului BitDefender timp de 30 de zile de la data achiziționării acestuia. În cazul apariției unui defect al suportului de distribuire, ca unică modalitate de despăgubire pentru încălcarea acestei garanții, SOFTWIN poate înlocui, la latitudinea sa, suportul defect returnat, cu un altul în schimbul chitanței sau vă poate returna costul produsului BitDefender. SOFTWIN nu garantează funcționarea neîntreruptă a produsului, lipsa erorilor sau posibilitatea corectării acestora. SOFTWIN nu garantează că BitDefender vă va satisface cerințele.

CU EXCEPȚIA CELOR PRECIZATE ÎN MOD EXPLICIT ÎN ACEASTĂ ÎNȚELEGERE, SOFTWIN ÎŞI DECLINĂ RESPONSABILITATEA PENTRU ORICE ALTE GARANȚII,

EXPLICITE SAU IMPLICITE, CE PRIVESC PRODUSELE, ÎMBUNĂTĂȚIRILE, ÎNTREȚINEREA SAU SUPORTUL LEGAT DE ACESTEA, SAU ORICE ALTE MATERIALE (TANGIBILE SAU INTANGIBILE) SAU SERVICII FURNIZATE. SOFTWIN DECLINĂ ÎN MOD EXPLICIT ORICE GARANȚII ŞI CONDIȚII IMPLICITE, INCLUZÂND, FĂRĂ LIMITARE, GARANȚIILE IMPLICITE ALE VANDABILITĂȚII, UTILIZĂRII ÎNTR-UN ANUMIT SCOP, TITLULUI, NON-INTERFERENȚEI, ACURATEȚEI DATELOR, A CONȚINUTULUI INFORMAȚIONAL, INTEGRĂRII SISTEMULUI ŞI NEÎNCĂLCĂRII DREPTURILOR UNOR TERȚE PĂRȚI PRIN FILTRAREA, DEZACTIVAREA SAU ÎNDEPĂRTAREA SOFTULUI ACESTORA, A APLICAȚIILOR SPYWARE, ADWARE, A FIŞIERELOR COOKIE, MESAJELOR E-MAIL, DOCUMENTELOR, RECLAMELOR SAU A ALTORA DE GENUL, INDIFERENT DACĂ ACEASTA REIESE DIN STATUT, LEGE, FUNCȚIONARE SAU COMERȚ.

DECLINAREA RESPONSABILITĂȚII ÎN CAZ DE DAUNE. Orice persoană care utilizează, testează sau evaluează BitDefender îşi asumă riscul legat de calitatea şi performanța acestuia. SOFTWIN nu va fi responsabilă, în niciun caz, pentru daune de orice natură, incluzând, fără limitare, daune directe sau indirecte, rezultate din utilizarea, performanța sau livrarea BitDefender, chiar dacă SOFTWIN a fost informată de existența sau posibilitatea apariției acestora. UNELE STATE INTERZIC LIMITAREA SAU DECLINAREA RESPONSABILITĂȚII ÎN CAZUL DAUNELOR INDIRECTE, DECI CELE MENȚIONATE MAI SUS S-AR PUTEA SĂ NU SE APLICE ÎN CAZUL DUMNEAVOASTRĂ. ÎN NICIUN CAZ, RESPONSABILITATEA SOFTWIN NU VA DEPĂŞI PREȚUL DE ACHIZIȚIE AL PRODUSULUI BITDEFENDER. Declarațiile de limitare şi declinare a responsabilității de mai sus se vor aplica indiferent dacă acceptați să folosiți, evaluați sau testați BitDefender.

ANUNȚ IMPORTANT PENTRU UTILIZATORI. ACEST SOFT POATE CONȚINE ERORI ŞI NU ESTE PROIECTAT SAU DESTINAT UTILIZĂRII ÎNTR-UN MEDIU CU GRAD MARE DE RISC ŞI CARE NECESITĂ O PERFORMANȚĂ SAU FUNCȚIONARE ÎN CONDIȚII DE SECURITATE ABSOLUTĂ. ACEST PRODUS NU ESTE DESTINAT UTILIZĂRII ÎN OPERAȚIUNI DIN DOMENIUL AVIAȚIEI, SECTORUL NUCLEAR SAU SISTEME DE COMUNICAȚII, SECTORUL ARMAMENTULUI, SISTEME DIRECTE SAU INDIRECTE DE MENȚINERE A VIEȚII, CONTROLUL TRAFICULUI AERIAN SAU ORICE ALTĂ APLICAȚIE SAU INSTALAȚIE ÎN CARE APARIȚIA UNEI EROARI AR PUTEA CAUZA MOARTEA SAU RĂNIREA GRAVĂ A UNOR PERSOANE SAU DAUNE ALE PROPRIETĂȚII.

GENERAL. Această înțelegere se află sub incidența legilor din România şi a regulamentelor şi tratatelor internaționale privind drepturile de autor şi proprietatea intelectuală. Jurisdicția exclusivă şi locația judecării oricărei dispute ce ar putea reieşi din aceşti termeni de licență va fi cea a tribunalelor din Romania.

Prețurile, costurile şi sumele de bani pentru utilizarea BitDefender pot fi modificate fără să fiți anunțat în prealabil.

În eventualitatea invalidității oricărei porțiuni a acestei Înțelegeri, respectiva invaliditate nu va afecta validitatea celorlalte porțiuni ale acestei Înțelegeri.

BitDefender şi simbolurile BitDefender sunt mărci înregistrate ale SOFTWIN. Toate celelalte mărci înregistrate utilizate în produs sau în materialele asociate sunt proprietatea deținătorilor lor de drept.

Licența se va încheia imediat, fără a fi anunțat, în cazul în care încălcați oricare dintre termenii sau condițiile ei. În urma terminării licenței nu veți fi îndreptățit la returnarea banilor de către BitDefender sau oricare dintre distribuitorii BitDefender. Termenii şi condițiile privind confidențialitatea şi restricțiile de utilizare vor rămâne în vigoare şi după orice terminare a licenței.

SOFTWIN poate revizui aceşti termeni în orice moment, iar termenii revizuiți se vor aplica în mod automat versiunilor soft corespunzătoare, distribuite cu termenii revizuiți. Dacă oricare parte a acestor termeni este găsită nulă şi neavenită, acest lucru nu va afecta validitatea restului termenilor, ce vor rămâne în vigoare.

În cazul controverselor sau inconsistențelor dintre traducerile acestor termeni în alte limbi, va prevala versiunea în limba engleză publicată de SOFTWIN.

Contactați SOFTWIN la Str. Fabrica de Glucoză nr. 5, 72322-Sector 2, Bucureşti, România, sau la numărul de telefon: 40-21-2330780 sau Fax: 40-21-2330763, adresă e-mail: <office@bitdefender.com>.

Prefață

Acest manual se adresează tuturor utilizatorilor care au ales **BitDefender Antivirus v10** ca soluție de securitate pentru calculatoarele personale. Informațiile incluse în acest manual sunt destinate nu numai utilizatorilor avansați, ci şi oricărei persoane care poate lucra în sistemul Windows.

Acest manual vă prezintă **BitDefender Antivirus v10**, Compania şi echipa care l-au dezvoltat, vă ghidează în timpul procesului de instalare a produsului şi vă învață cum să-l configurați. Veți afla cum să utilizați **BitDefender Antivirus v10**, cum să-l actualizați, testați şi personalizați. Veți învăța cum să obțineți beneficii maxime din BitDefender.

Vă dorim o lectură plăcută şi utilă.

1. Convenții utilizate în manual

1.1. Convenții tipografice

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

Aspect	Descriere
`sample syntax`	Exemplele de sintaxă sunt tipărite cu caractere `monospațiate`.
http://www.bitdefender.com	Link-urile URL indică locații externe, pe serverele http sau ftp.
`<support@bitdefender.com>`	Adresele de e-mail sunt inserate în text ca adrese de contact.
“Prefață” (p. xiii)	Acesta este un link intern, către o locație din document.
`filename`	Numele fişierelor şi ale directoarelor sunt tipărite cu caractere `monospațiate`.
option	Toate opțiunile produsului sunt tipărite cu caractere **aldine**.

Aspect	Descriere
`sample code listing`	Liniile de cod sunt tipărite cu caractere monospațiate.

1.2. Atenționări

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

Notă

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

Important

Acest lucru necesită atenția dumneavoastră şi nu este recomandat să-l ocoliți. De obicei, aici sunt furnizate informații importante, dar nu cruciale.

Avertisment

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

2. Structura manualului

Manualul cuprinde şapte părți, care se referă la subiectele importante: Despre BitDefender, Instalare produs, Descriere şi caracteristici, Consola de administrare, Recomandări de utilizare, BitDefender Rescue CD şi Obținere ajutor. În plus, vă este oferit un vocabular pentru clarificarea înțelesului anumitor termeni tehnici.

Despre BitDefender. O scurtă introducere în BitDefender. Este explicat ce reprezintă BitDefender şi SOFTWIN.

Instalare produs. Instrucțiuni de instalare pas cu pas a BitDefender pe o stație de lucru. Acesta este un ghid complet pentru instalarea **BitDefender Antivirus v10**. Începând cu cerințele pentru o instalare corectă, sunteți ghidat de-a lungul întregului proces de instalare. La sfârşit este descrisă şi procedura de dezinstalare a BitDefender, pentru cazul în care doriți să faceți acest lucru.

Descriere şi caracteristici. Vă este prezentat **BitDefender Antivirus v10**, caracteristicile şi modulele produsului.

Consola de administrare. Descrierea unor noțiuni de bază privind administrarea şi întreținerea BitDefender. Capitolele explică în detaliu toate opțiunile **BitDefender**

Antivirus v10, cum să înregistrați produsul, cum să vă scanați calculatorul, cum să realizați actualizări. Sunteți învățat cum să configurați şi să utilizați modulele BitDefender.

Recomandări de utilizare. Urmați aceste instrucțiuni pentru a profita la maxim de BitDefender.

BitDefender Rescue CD. Conține descrierea BitDefender Rescue CD. Vă ajută să înțelegeți şi să utilizați caracteristicile oferite de acest CD de boot.

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

Vocabular. Vocabularul încearcă să explice unii termeni tehnici sau neobişnuiți pe care îi veți găsi în paginile acestui document.

3. Comentarii

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

Aveți la dispoziție următoarea adresă de e-mail <documentation@bitdefender.com>.

Important

Vă rugăm să scrieți în engleză sau română mailurile către adresa de mai sus pentru a le putea procesa cât mai eficient.

Despre BitDefender

1. Ce este BitDefender?

BitDefender este un furnizor global important de soluții de securitate care satisfac nevoia de protecție a mediului informațional contemporan. Compania oferă una dintre cele mai rapide şi eficiente linii de soft de securitate, stabilind noi standarde în ceea ce priveşte prevenirea amenințărilor, detecția rapidă a acestora şi diminuarea efectelor negative produse. BitDefender furnizează produse şi servicii unui număr de peste 41 de milioane de utilizatori din peste 180 dețări. BitDefender are filiale în **Statele Unite**, **Marea Britanie**, **Germania**, **Spania** şi **Romania**.

- Cuprinde antivirus, firewall, antispyware, antispam şi control parental pentru companii şi utilizatori individuali.
- Produsele BitDefender sunt menite a fi implementate pe structuri informaționale complexe (stații de lucru, servere de fişiere, servere de mail sau gateway-uri), pe platforme Windows, Linux sau FreeBSD.
- Distribuție la nivel global, produse disponibile în 18 limbi.
- Simplu de folosit, având un asistent ce ghidează utilizatorii prin procesul de instalare şi pune doar câteva întrebări.
- Produse certificate internațional: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, etc.
- Suport tehnic permanent - echipa de suport tehnic este disponibilă 24 de ore din 24, 7 zile pe săptămână.
- Răspuns prompt la noi atacuri informaționale.
- Cea mai bună rată de detecție.
- Actualizări ale semnăturilor de viruşi la fiecare oră de pe Internet - acțiuni automate sau programate ce oferă protecție împotriva celor mai noi viruşi.

1.1. De ce să alegeți BitDefender?

Demonstrat. Producătorul antivirus cu cea mai mare viteză de reacție. Viteza de reacție a BitDefender în cazul epidemiilor de viruşi informatici a fost confirmată începând cu cele mai recente atacuri ale CodeRed, Nimda şi Sircam, precum şi ale Badtrans.B sau ale altor coduri periculoase, care se răspândesc rapid. BitDefender a oferit primul protecție împotriva acestor coduri şi a pus soluțiile de securitate la dispoziția tuturor persoanelor afectate, gratuit, pe Internet. În prezent,având în vedere

răspândirea continuă a virusului Klez - în diverse versiuni- protecția antivirus promptă se dovedeşte a fi, încă o dată, o nevoie esențială a oricărui sistem informatic.

Inovator. Premiat pentru inovație de către Comisia Europeană şi EuroCase. BitDefender a fost declarat câştigător al Premiului European IST, acordat de către Comisia Europeană şi de reprezentanți ai 18 academii din Europa. Aflat în al optulea an de existență, Premiul European IST este o recompensă pentru produse excepționale care reprezintă campionii din domeniul inovației IT.

Complet. Acoperă fiecare punct al rețelei, oferind o securizare completă. Soluțiile de securitate BitDefender pentru mediul corporativ satisfac cerințele mediului de afaceri contemporan, permițând administrarea tuturor amenințărilor care periclitează securitatea tuturor rețelelor, indiferent că este vorba despre rețele mici, locale, sau despre rețele ce conțin mai multe servere sau platforme WAN.

Cea mai bună protecție de care puteți beneficia. Sistemul dumneavoastră dumneavoastră devine o fortăreață inexpugnabilă, în ciuda oricăror amenințări. Deoarece detecția viruşilor pe baza analizei codurilor nu s-a ridicat întotdeauna la înălțimea aşteptărilor, BitDefender a implementat protecția bazată pe comportament, oferind protecție împotriva codurilor virale nou apărute.

Acestea sunt **costurile** pe care organizațiile doresc să le evite şi pe care produsele de securitate sunt proiectate să le prevină:

- Atacurile viermilor
- Afectarea circuitului informațiilor de către mesajele infectate
- Căderea serverelor de mail
- Dezinfectarea sistemelor şi recuperarea datelor
- Scăderea productivității utilizatorilor finali din cauza indisponibilității sistemelor
- Atacurile hackerilor şi accesul neautorizat care produce daune

Prin utilizarea suitei de soluții de securitate BitDefender se pot obține anumite **beneficii**:

- Creşterea accesibilității rețelei prin oprirea răspândirii codurilor malițioase (ex. Nimda, cai troieni, DDoS).
- Protejarea utilizatorilor remote împotriva atacurilor.
- Reducerea costurilor administrative şi integrarea rapidă cu BitDefender Enterprise.
- Stoparea programelor virale care se răspândesc prin intermediul mesajelor, folosind protecția e-mail BitDefender la poarta de acces (gateway) a companiei. Blocarea, temporară sau permanentă, a conectării la rețea a aplicațiilor neautorizate, vulnerabile sau costisitoare.

Mai multe informații despre BitDefender pot fi obținute vizitând http://www.bitdefender.ro.

1.2. Despre SOFTWIN

Fondată în 1990, câştigătoare a premiului IST în 2002, SOFTWIN este considerată a fi liderul tehnologic al industriei de soft est-europene, având o rată de creştere anuală de mai mult de 50% în ultimii 5 ani şi mai mult de 70% din profit provenind din exporturi.

Având o echipă de peste 800 de profesionişti şi mai mult de 10000 de proiecte administrate până în prezent, SOFTWIN oferă, în principal, soluţii şi servicii soft complexe care permit companiilor care se dezvoltă rapid să facă faţă provocărilor esenţiale ale lumii afacerilor şi să profite din plin de noile oportunităţi de afaceri.

Activă pe cele mai avansate pieţe IT din SUA şi UE, SOFTWIN se dezvoltă urmărind patru **linii de afaceri** interconectate:

- eContent Solutions
- BitDefender
- Business Information Solutions
- Customer Relationship Management

Instalare produs

2. Instalarea BitDefender Antivirus v10

Secțiunea **Instalarea BitDefender Antivirus v10** a acestui manual de utilizare conține următoarele subiecte:

- Cerințe de sistem
- Etape de instalare
- Asistent inițial de configurare
- Actualizare produs
- Dezinstalare, reparare sau modificare

2.1. Cerințe de sistem

Pentru funcționarea corespunzătoare a produsului, înainte de instalare, asigurați-vă că unul dintre următoarele sisteme de operare rulează pe calculatorul dumneavoastră şi că sunt îndeplinite cerințele de sistem aferente:

Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit

- Procesor Pentium II 350 MHz sau superior
- Minimum 128 MB memorie RAM (256 MB recomandat)
- Minimum 60 MB spațiu disponibil pe hard disc
- Internet Explorer 5.5 sau superior

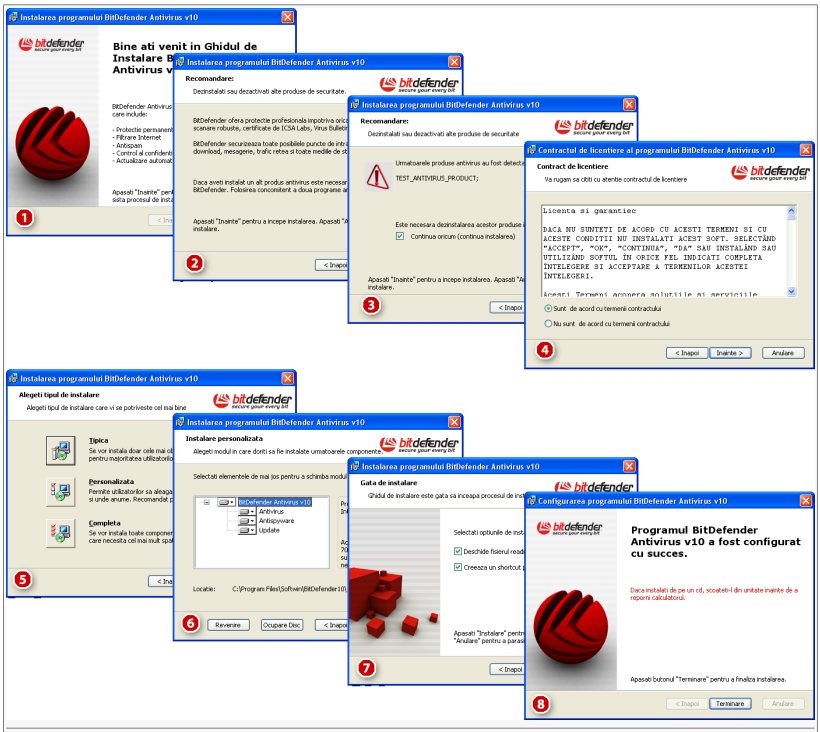
Microsoft Windows Vista 32-bit

- Procesor de 800 MHz sau superior
- Minimum 512 MB memorie RAM (1 GB recomandat)
- Minimum 60 MB spațiu disponibil pe hard disc

BitDefender Antivirus v10 poate fi descărcat pentru evaluare de la adresa http://www.bitdefender.ro, pagina web a corporației SOFTWIN dedicată securității datelor.

2.2. Etape de instalare

Localizați fişierul de instalare şi faceți dublu-clic. Astfel se va lansa programul asistent, care vă va ghida pe parcursul procesului de instalare.



Etape de instalare

1. Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** dacă doriți să părăsiți procesul de instalare.
2. Faceți clic pe **Înainte** pentru a continua sau pe **Înapoi** pentru a reveni la primul pas.
3. BitDefender Antivirus v10 vă alertează dacă aveți un alt produs antivirus instalat pe calculatorul dumneavoastră.

Avertisment

Este recomandat să dezinstalați produsele antivirus detectate înainte de a instala BitDefender. Rularea a două sau mai multor produse antivirus în acelaşi timp, pe acelaşi calculator, provoacă în general instabilitatea sistemului de operare.

Faceți clic pe **Înapoi** pentru a reveni la pasul anterior sau pe **Anulare** pentru a părăsi instalarea. Dacă doriți să continuați, faceți clic pe **Înainte**.

Notă

Dacă BitDefender Antivirus v10 nu detectează alte produse antivirus instalate pe sistemul dumneavoastră, veți sări acest pas.

4. Vă rugam să citiți cu atenție Contractul de Licență, selectați **Sunt de acord cu termenii contractului** şi faceți clic pe **Înainte**. Dacă nu sunteți de acord cu prevederile acestui contract faceți clic pe **Anulare**. Procesul de instalare va fi abandonat şi veți părăsi programul asistent.
5. Puteți alege ce tip de instalare doriți: tipică, personalizată sau completă.

   Tipică
   Programul va fi instalat cu cele mai folosite module BitDefender. Recomandată majorității utilizatorilor.

   Personalizată
   Puteți alege componentele pe care doriți să le instalați. Recomandată numai utilizatorilor avansați.

   Completă
   Pentru instalarea completă a produsului. Vor fi instalate toate modulele BitDefender.

   Dacă selectați **Tipică** sau **Completă** veți sări peste pasul 6.
6. Dacă ați selectat **Personalizată**, va apărea o nouă fereastră în care vor fi listate toate componentele BitDefender, din care le puteți selecta pe cele dorite.

   Dacă faceți clic pe oricare dintre componente, în partea dreaptă va apărea o scurtă descriere (inclusiv spațiul liber minim necesar pe hard disc). Dacă faceți clic pe oricare dintre icoanele componentelor, va apărea o fereastră în care puteți alege să instalați sau nu modulul selectat.

   Puteți alege directorul unde doriți să instalați produsul. Directorul setat implicit este `C:\Program Files\Softwin\BitDefender 10`.

   Dacă doriți să instalați în alt director, faceți clic pe butonul **Caută** şi, în fereastra care se va deschide, selectați directorul în care doriți să fie instalat BitDefender Antivirus v10. Faceți clic pe **Înainte**.
7. Există două opțiuni selectate implicit:

   - **Deschide fişierul readme** - pentru deschiderea fişierului readme la sfârşitul instalării.

- **Creează un shortcut pe desktop** - pentru a crea o scurtătură (shortcut) către BitDefender Antivirus v10 pe desktop la sfârşitul instalării.

Faceți clic pe **Instalare** pentru a lansa instalarea programului.

Important

În timpul procesului de instalare va apărea un asistent de configurare. Acesta vă va ajuta să înregistrați **BitDefender Antivirus v10**, să creați un cont BitDefender şi să setați BitDefender să execute sarcini importante de securitate.
Finalizați procesul de configurare ghidat de programul asistent pentru a trece la pasul următor.

8. Faceți clic pe **Terminare** pentru a încheia instalarea produsului. După instalare, dacă ați acceptat setările de cale implicite, veți observa că în directorul `Program Files` apare subdirectorul `Softwin`, conținând un alt subdirector, `BitDefender 10`.

Notă

Este posibil ca la finalul instalării să vi se ceară să reporniți sistemului.

2.3. Asistentul inițial de configurare

În timpul procesului de instalare va apărea un asistent de configurare. Acesta vă va ajuta să înregistrați **BitDefender Antivirus v10**, să creați un cont BitDefender şi să setați BitDefender să execute sarcini importante de securitate.

Nu este obligatoriu să urmați paşii programului asistent. Totuşi, vă recomandăm să faceți acest lucru pentru a economisi timp şi pentru a vă asigura că sistemul dumneavoastră nu era infectat înainte de a instala BitDefender Antivirus v10.

2.3.1. Pasul 1/8 - Asistentul inițial de configurare BitDefender

Fereastra de întâmpinare

Faceți clic pe **Înainte**.

2.3.2. Pasul 2/8 - Înregistrați BitDefender Antivirus v10

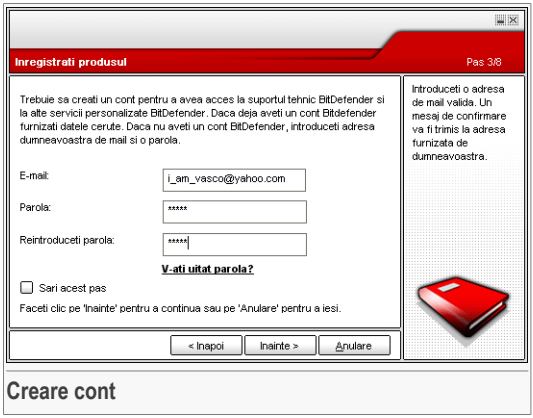
Înregistrare

Selectați **Înregistrează produsul** pentru a înregistra **BitDefender Antivirus v10**. Introduceți seria de înregistrare în câmpul **Introduceți seria nouă**.

Pentru a evalua produsul în continuare, selectați **Continuă evaluarea produsului**.

Faceți clic pe **Înainte**.

2.3.3. Pasul 3/8 - Creați un cont BitDefender



Creare cont

Nu am un cont BitDefender

Pentru a beneficia de suport tehnic gratuit şi alte servicii BitDefender gratuite trebuie să creați un cont.

Introduceți o adresă de mail validă în câmpul **E-mail**. Alegeți o parolă şi introduceți-o în câmpul **Parolă**. Confirmați parola în câmpul **Reintroduceți parola**. Utilizați adresa de mail şi parola pentru a accesa contul dumneavoastră la http://myaccount.bitdefender.com.

Notă

Parola trebuie să conțină minim patru caractere.

Pentru a crea un cont trebuie mai întâi să vă activați adresa de mail. Verificați-vă adresa de mail şi urmați instrucțiunile din e-mailul trimis de serviciul de înregistrare BitDefender.

Important

Vă rugăm să vă activați contul înainte de a trece la pasul următor.

Dacă nu doriți să creați un cont BitDefender, selectați **Sari acest pas**. Veți sări, de asemenea, şi peste pasul următor.

Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

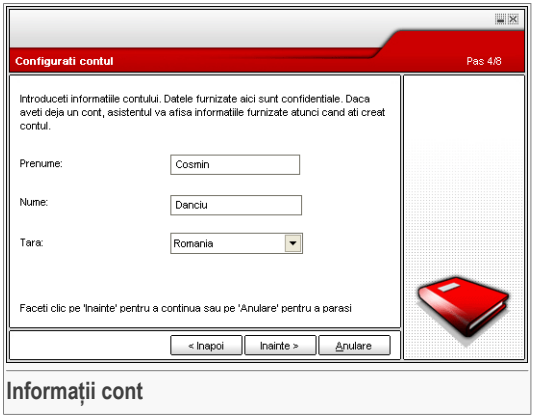
Deja am un cont BitDefender

Dacă aveți deja un cont activ, introduceți adresa de mail şi parola contului dumneavoastră. Dacă parola introdusă este incorectă, vi se va cere să o reintroduceți când faceți clic pe **Înainte**. Faceți clic pe **Ok** pentru a reintroduce parola sau pe **Anulare** pentru a părăsi programul asistent.

Dacă v-ați uitat parola, faceți clic pe **V-ați uitat parola?** şi urmați instrucțiunile.

Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

2.3.4. Pasul 4/8 - Introduceți informațiile contului



Informații cont

Notă

Nu veți urma acest pas dacă ați selectat opțiunea **Sari acest pas** în pasul anterior.

Introduceți numele şi prenumele dumneavoastră şi selectați țara în care locuiți.

Dacă aveți deja un cont, programul asistent va afişa informațiile furnizate anterior, dacă acestea există. Aici puteți modifica aceste informații, dacă doriți acest lucru.

Important

Informațiile furnizate aici vor rămâne confidențiale.

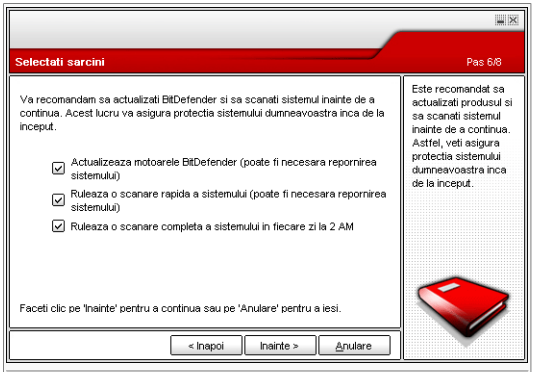
Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

2.3.5. Pasul 5/8 - Învățați despre RTVR

Informații despre RTVR

Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

2.3.6. Pasul 6/8 - Selectați sarcinile ce vor fi rulate



Selectare sarcini

Configurați BitDefender Antivirus v10 să execute sarcini importante privind securitatea sistemului dumneavoastră.

Următoarele opțiuni sunt disponibile:

- **Actualizează motoarele BitDefender Antivirus v10 (poate fi necesară repornirea sistemului)** - în timpul pasului următor va fi efectuată o actualizare a motoarelor BitDefender Antivirus v10 pentru a vă proteja sistemul împotriva celor mai noi amenințări.
- **Rulează o scanare rapidă a sistemului (poate fi necesară repornirea sistemului)** - în timpul pasului următor va fi efectuată o scanare rapidă a sistemului ce va permite BitDefender Antivirus v10 să se asigure că fişierele dumneavoastră din directoarele `Windows` şi `Program Files` nu sunt infectate.
- **Rulează o scanare completă a sistemului în fiecare zi la ora 2** - rulează o scanare completă a sistemului în fiecare zi la ora 2.

Important

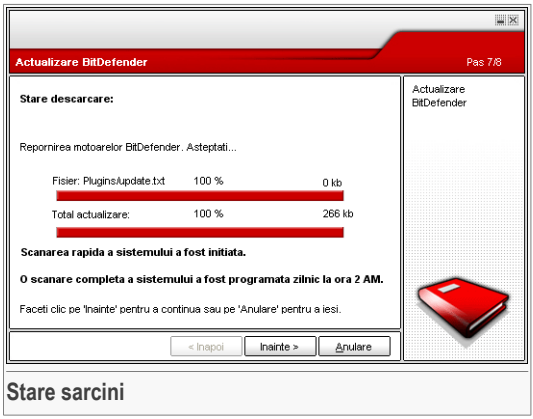
Vă recomandăm să păstrați aceste opțiuni selectate înainte de a trece la pasul următor pentru a păstra siguranța sistemului dumneavoastră.

Dacă selectați doar ultima opțiune sau nicio opțiune, veți sări peste pasul următor.

Puteți face orice modificări doriți revenind la paşii anteriori (faceți clic pe **Înapoi**). Mai departe, procesul este ireversibil: dacă alegeți să continuați, nu vă veți putea întoarce la paşii anteriori.

Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

2.3.7. Pasul 7/8 - Aşteptați finalizarea sarcinilor

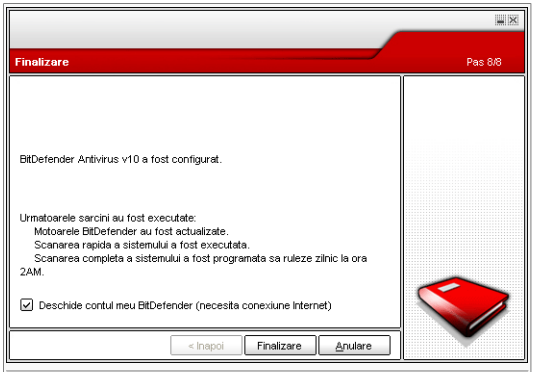


Stare sarcini

Aşteptați ca sarcinile să fie finalizate. Puteți vedea starea sarcinilor selectate în pasul anterior.

Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

2.3.8. Pasul 8/8 - Examinați rezumatul



Finalizare

Acesta este ultimul pas al asistentului de configurare.

Selectați **Deschide contul meu BitDefender** pentru a vă accesa contul BitDefender. Este necesară o conexiune la Internet.

Faceți clic pe **Finalizare** pentru a finaliza asistentul şi a continua procesul de instalare.

2.4. Actualizare produs

Procedura de actualizare a produsului poate fi realizată prin una dintre următoarele metode:

- **Instalați fără înlăturarea versiunii precedente - doar pentru v8 sau versiuni superioare, exceptând Internet Security.**

  Faceți dublu-clic pe fişierul de instalare şi urmați paşii programului asistent descris în secțiunea "*Etape de instalare*" (p. 9).

  Important

  În timpul instalării va apărea un mesaj de eroare cauzat de `serviciul Filespy`. Faceți clic pe **OK** pentru a continua procesul de instalare.

- **Dezinstalați vechea versiune şi instalați-o pe cea nouă - valabilă pentru toate versiunile BitDefender.**

În primul rând va trebui să dezinstalați vechea versiune, apoi să reporniți calculatorul și să instalați noua versiune conform instrucțiunilor din secțiunea "*Etape de instalare*" (p. 9).

Important

Dacă faceți o actualizare de produs pentru o versiune v8 sau superioară, vă recomandăm să salvați setările BitDefender. După finalizarea procesului de actualizare, veți putea să le încărcați.

2.5. Dezinstalare, reparare sau modificare

Dacă doriți să modificați, să reparați sau să dezinstalați componentele **BitDefender Antivirus v10** instalate inițial, urmați calea: **Start** → **Programe** → **BitDefender 10** → **Modificare, Reparare sau Dezinstalare** din meniul Windows.

Vi se va solicita să confirmați alegerea prin apăsarea butonului **Înainte**. Va apărea o nouă fereastră, de unde puteți selecta:

- **Modificare** - pentru instalarea unor noi componente sau dezinstalarea unora instalate anterior;
- **Reparare** - pentru reinstalarea tuturor componentelor programului;

  Important

  Înainte de a repara produsul vă recomandăm să salvați setările BitDefender. Astfel, după finalizarea procesului de reparare, le veți putea încărca.

- **Dezinstalare** - pentru dezinstalarea tuturor componentelor instalate.

Pentru a continua procesul de instalare, va trebui să selectați una dintre aceste trei opțiuni. Vă recomandăm să selectați **Dezinstalare** pentru o reinstalare corectă. După finalizarea procesului de dezinstalare vă recomandăm să ștergeți subdirectorul `Softwin` din directorul `Program Files`.

Descriere şi caracteristici

3. BitDefender Antivirus v10

Soluția antivirus şi antispyware ideală pentru calculatorul dumneavoastră!

BitDefender Antivirus v10 este o puternică unealtă antivirus şi antispyware cu funcții ce îndeplinesc cel mai bine nevoile dumneavoastră de securitate. Uşurința în utilizare şi actualizările automate fac din **BitDefender Antivirus** un produs antivirus de tip ”instalează şi uită”.

3.1. Antivirus

Misiunea modulului Antivirus este aceea de a detecta şi îndepărta toți viruşii care amenință securitatea datelor dumneavoastră. Antivirusul BitDefender utilizează motoare de scanare puternice, certificate de ICSA Labs, Virus Bulletin, Checkmark, Checkvir şi TÜV.

Detecție proactivă. B-HAVE este acronimul conceptului intitulat Behavioral Heuristic Analyzer in Virtual Environments;practic, un computer virtual este simulat în interiorul unui alt computer, unde sunt rulate diferite aplicații soft cu scopul de a le găsi pe cele având comportament malițios. Această tehnologie dezvoltată de BitDefender rezprezintă o nouă tendință în domeniul securității. Ea menține sistemul de operare în siguranță, protejându-l de viruşii necunoscuți, prin detectarea potențialelor elemente infectate sau a codurilor pentru care semnăturile de viruşi nu au fost încă lansate.

Protecție antivirus permanentă. Motoarele de scanare BitDefender, noi şi îmbunătățite, vor scana şi dezinfecta fişierele infectate la accesarea acestora, minimizând pierderile de date. Documentele infectate pot fi acum recuperate, în loc să fie şterse.

Detecție şi îndepărtare rootkit. Un nou modul BitDefender caută rootkituri (programe malițioase menite a controla calculatoarele victimă, fără a fi detectate) şi le îndepărtează la detecție.

Scanare web. Traficul web este acum filtrat în timp real, chiar înainte de a ajunge la browser, oferind o navigare plăcută şi sigură în rețea.

Protecție aplicații Peer-2-Peer şi de mesagerie. Filtrează împotriva viruşilor care se răspândesc prin mesageria instant şi prin aplicații soft de schimb de fişiere.

Protecție e-mail completă. BitDefender rulează la nivelul protocolului POP3/SMTP, filtrând mesajele primite sau trimise, indiferent de clientul de e-mail folosit (Outlook™, Outlook Express™ / Windows Mail™, The Bat™, Netscape®, etc.), fără a necesita o configurare adițională.

3.2. Antispyware

BitDefender monitorizează şi previne potențialele amenințări spyware în timp real, înainte ca acestea să producă daune în sistemul dumneavoastră. Folosind o bază de date cuprinzătoare cu semnături de spyware, BitDefender vă va proteja calculatorul de aplicațiile spyware.

Protecție Antispyware în timp real. BitDefender monitorizează zeci de puncte potențial sensibile ale sistemului de operare, acolo unde pot acționa aplicațiile spyware, şi verifică orice schimbare apărută. De asemenea, sunt blocate în timp real amenințările spyware cunoscute.

Scanare şi dezinfectare împotriva aplicațiilor spyware. BitDefender poate scana întregul sistem sau părți ale acestuia, împotriva amenințărilor spyware cunoscute. Motoarele de scanare folosesc o bază de date cu semnături de spyware actualizată continuu.

Protecție confidențialitate. Componenta de protecție a confidențialității monitorizează traficul HTTP (web) şi SMTP (mail) ce părăseşte calculatorul dumneavoastră în căutare de informații personale, cum ar fi numere de carduri de credit sau alte şiruri definite de utilizator, ca, de exemplu, părți ale unor parole.

Anti-Dialer. Un dispozitiv configurabil anti- dialer previne rularea aplicațiilor malițioase care au drept rezultat încărcarea facturii de telefon.

Controlul fişierelor cookie. Modulul Antispyware filtrează fişierele de tip cookie primite sau trimise, păstrând confidențialitatea identității şi a preferințelor dumneavoastră, pe toată durata navigării pe Internet.

Control activ al conținutului. Permite blocarea proactivă a rulării unor potențiale aplicații malițioase, cum ar fi: ActiveX, Java Applets sau codurile Java Scripts.

3.3. Alte caracteristici

Instalare şi utilizare. Un program asistent de configurare apare imediat după instalare, ajutând utilizatorii să actualizeze BitDefender, să efectueze o scanare rapidă a sistemului, să selecteze un program de scanare şi furnizând o modalitate simplă de a înregistra şi activa produsul.

Perspectivă utilizator. BitDefender a regândit interfața produsului, punând accent pe accesibilitatea produsului şi evitarea detaliilor nesemnificative. Ca rezultat, multe dintre modulele BitDefender v10 necesită mult mai puțină atenție din partea utilizatorului, datorită automatizării şi a capacității de autoeducare a produsului.

Actualizări la fiecare oră. Copia dumneavoastră BitDefender se va actualiza de 24 de ori pe zi direct de pe Internet sau prin intermediul unui server Proxy. Dacă este necesar, produsul este capabil să se repare singur, prin descărcarea de pe serverele BitDefender a fişierelor avariate sau lipsă.

Suport tehnic non-stop. Este oferit online de către reprezentanții de suport tehnic şi printr-o bază de date online cu răspunsuri la “Întrebări Frecvente”.

CD de boot. BitDefender Antivirus v10 este furnizat cu un CD de boot. Acest CD poate fi folosit pentru a analiza/repara/dezinfecta un sistem compromis care nu poate fi pornit.

4. Modulele BitDefender

BitDefender Antivirus v10 conține următoarele module: **General**, **Antivirus**, **Antispyware** şi **Actualizare**.

4.1. Modulul General

BitDefender este configurat pentru securitate maximă.

În modulul General puteți seta nivelul de securitate şi executa sarcini importante de securitate. De asemenea, aici puteți înregistra produsul şi puteți seta comportamentul general al BitDefender.

4.2. Modulul Antivirus

BitDefender vă protejează sistemul de viruşi, spyware şi alte programe virale scanând fişierele, mesajele e-mail şi orice alte date care intră în sistem.

Protecția oferită de BitDefender se împarte în două categorii:

- Scanare la acces - previne intrarea de noi viruşi, spyware şi alte programe virale în sistem. Această caracteristică se mai numeşte Scut Antivirus – fişierele sunt scanate atunci când sunt accesate de către utilizator. BitDefender va scana, de exemplu, un document Word atunci când îl deschideți şi mesajele e-mail la primire. BitDefender scanează fişierele atunci când le utilizați – la acces.
- Scanare la cerere - detectează viruşi, spyware sau alte programe virale deja existențe în sistem. Acesta este modul clasic de scanare, inițiată de utilizator – alegeți partițiile, directoarele sau fişierele pe care trebuie să le scaneze BitDefender, iar BitDefender le scanează – la cerere.

4.3. Modulul Antispyware

BitDefender monitorizează zeci de potențiale puncte sensibile ale sistemului dumneavoastră de operare, acolo unde pot acționa aplicațiile spyware, şi verifică orice schimbare apărută. Acest modul blochează în mod eficient caii troieni şi alte instrumente instalate de hackeri, care încearcă să vă dezvăluie identitatea şi să trimită informațiile personale, cum ar fi seria cărții de credit,din computerul dumneavoastră, către hacker.

4.4. Modulul Actualizare

Zi de zi sunt descoperite şi identificate noi programe virale. De aceea, este foarte importantă actualizarea BitDefender cu ultimele semnături.În mod implicit, BitDefender caută automat actualizări, la fiecare oră.

Actualizările sunt de mai multe tipuri:

- **Actualizări pentru motoarele Antivirus** - pentru că tot timpul apar noi ameninţări, fişierele ce conţin semnăturile de viruşi trebuie actualizate pentru a asigura protecţie permanentă, la zi, împotriva acestora. Acest tip de actualizare se mai numeşte **Actualizare definiţii viruşi**.
- **Actualizări ale motoarelor antispyware** - se vor adăuga noi semnături de spyware la baza de date. Acest tip de actualizare se mai numeşte **Actualizare Antispyware**.
- **Actualizare de produs** - la lansarea unei noi versiuni de produs, noi caracteristici şi tehnici de scanare sunt introduse pentru a îmbunătăţi performanţele produsului. Acest tip de actualizare se mai numeşte **Upgrade Produs**.

În ceea ce priveşte intervenţia utilizatorului, putem considera următoarele tipuri de actualizări:

- Actualizare automată - antivirusul contactează automat serverul BitDefender pentru a verifica dacă o nouă actualizare este disponibilă, caz în care BitDefender se actualizează automat. Actualizarea automată poate fi realizată oricând făcând clic pe butonul **Actualizează acum** din modulul Update.
- Actualizare manuală - trebuie să descărcaţi şi să instalaţi manual ultimele semnături.

Consola de administrare

5. Descriere generală

BitDefender Antivirus v10 a fost creat cu o consolă de administrare centralizată, care permite configurarea opțiunilor de protecție pentru toate modulele BitDefender. Cu alte cuvinte, este suficient să deschideți consola de administrare pentru a avea acces la toate modulele: **Antivirus**, **Antispyware** şi **Actualizare**.

Pentru a accesa consola de administrare, utilizați meniul Windows Start, urmând calea **Start → Programe → BitDefender 10 → BitDefender Antivirus v10** sau, mai rapid, făcând dublu-clic pe **icoana BitDefender** din bara de sistem.

Consola de administrare

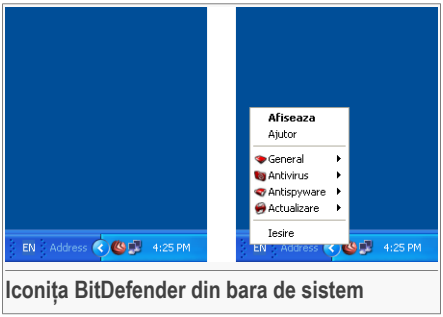
În partea stângă a consolei de administrare puteți vedea selectorul de module:

- General - în această secțiune puteți seta nivelul global de securitate şi executa sarcini importante de securitate. Tot aici puteți înregistra produsul şi vizualiza principalele setări BitDefender, detalii despre produs şi informații de contact.
- Antivirus - în această secțiune puteți configura modulul **Antivirus**.
- Antispyware - în această secțiune puteți configura modulul **Antispyware**.
- Actualizare - în această secțiune puteți configura modulul **Actualizare**.

În partea dreaptă a consolei de administrare puteți vizualiza informații legate de secțiunea în care vă aflați. Opțiunea **Ajutor**, plasată în dreapta jos, deschide fişierul **Help**.

5.1. Bara de sistem

Când consola este minimizată, în bara de sistem va apărea o icoană.



Iconița BitDefender din bara de sistem

Dacă faceți dublu-clic pe această icoană, se va deschide consola de administrare. De asemenea, făcând clic dreapta pe ea, va apărea un meniu. Acesta oferă posibilitatea unei administrări rapide a BitDefender:

- **Afişează / Închide** - deschide consola de administrare sau o minimizează în bara de sistem.
- **Ajutor** - deschide documentația electronică.
- **General** - administrarea modulului General.
  - **Introduceți seria nouă** - porneşte asistentul de înregistrare care vă va ghida prin procesul de înregistrare.
  - **Editați contul** - porneşte un program asistent care vă va ajuta să creați un cont BitDefender.
- **Antivirus** - administrarea modulului Antivirus.
  - **Protecția în timp real este activată / dezactivată** - indică starea protecției în timp real (activată / dezactivată). Faceți clic pe această opțiune pentru a dezactiva sau activa protecția în timp real.
  - **Scanează** - deschide un submeniu de unde puteți alege să rulați una dintre sarcinile de scanare disponibile din secțiunea Scanare.
- **Antispyware** - administrarea modulului Antispyware.
  - **Modulul Antispyware este activat / dezactivat** - indică starea modulului Antispyware comportamental (activat / dezactivat). Faceți clic pe această opțiune pentru a dezactiva sau activa modulul Antispyware comportamental.

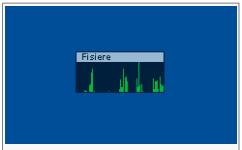
- **Setări avansate** - permite configurarea setărilor de control antispyware.
- **Actualizare** - administrarea modulului Actualizare.
  - **Actualizează acum** - realizează o actualizare imediată.
  - **Actualizarea automată este activată / dezactivată** - indică starea actualizării automate (activată / dezactivată). Faceți clic pe această opțiune pentru a dezactiva sau activa actualizarea automată.
- **Ieşire** - închide aplicația. Selectând această opțiune, icoana din bara de sistem va dispărea, iar pentru a deschide consola de administrare va trebui să o lansați din nou din meniul Start.

Notă

Dacă dezactivați unul sau mai multe module BitDefender, icoana din bara de sistem işi va schimba culoarea. Astfel puteți şti dacă anumite module sunt dezactivate fără deschiderea consolei de administrare.
Când există actualizări disponibile, icoana va clipi.

5.2. Bara de scanare

Bara de scanare este o reprezentare grafică a activității de scanare din sistemul dumneavoastră.



Bara de scanare

Barele verzi (zona **Fişiere**) reprezintă numărul de fişiere scanate pe secundă, pe o scară de la 0 la 50.

Notă

Bara de scanare vă va avertiza când Scutul Antivirus este dezactivat printr-un X roşu în zona corespunzătoare (zona **Fişiere**). Astfel, puteți şti dacă sunteți protejat fără a deschide consola de administrare.

Când nu mai doriți să vedeți reprezentarea grafică, faceți doar clic-dreapta pe ea şi selectați **Închide**.

Notă

Pentru a ascunde bara permanent, deselectați opțiunea **Afişează bara de scanare (graficul de pe ecran al activității produsului)** (din modulul **General**, secțiunea Setări).

6. Modulul General

Secțiunea **General** a acestui ghid de utilizare conține următoarele subiecte:

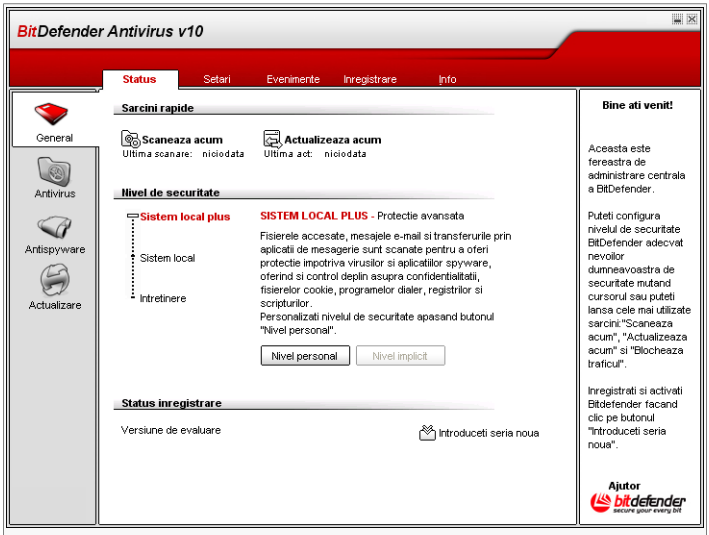
- Administrare centrală
- Setări consola de administrare
- Evenimente
- Înregistrare produs
- Info

Notă

Pentru mai multe detalii privind modulul **General** consultați "*Modulul General*" (p. 27).

6.1. Administrare centrală

Pentru a accesa această secțiune faceți clic pe tabul **Status** din modulul **General**.



Administrare centrală

În această secțiune puteți configura nivelul global de securitate şi executa sarcini BitDefender importante. De asemenea, puteți înregistra produsul şi afla data expirării licenței.

6.1.1. Sarcini rapide

BitDefender permite acces rapid la sarcini esențiale privind securitatea sistemului dumneavoastră. Utilizând aceste sarcini puteți actualiza produsul dumneavoastră BitDefender, puteți scana sistemul sau bloca traficul.

Pentru a scana întreg sistemul faceți clic pe **Scanează acum**. Fereastra de scanare va apărea şi va fi inițiată o scanare completă a sistemului.

Important

Este recomandată o scanare completă a sistemului cel puțin o dată pe săptămână. Pentru mai multe detalii privind sarcinile şi procesul de scanare consultați secțiunea Scanare a acestui manual de utilizare.

Înainte de a executa o scanare a sistemului, este recomandat să actualizați BitDefender pentru a fi protejat împotriva celor mai recente amenințări. Pentru a actualiza BitDefender faceți clic pe **Actualizează acum**. Aşteptați câteva secunde pentru ca procesul de actualizare să fie finalizat sau, mai bine, verificați în secțiunea Actualizare starea acestuia.

Notă

Pentru mai multe detalii privind procesul de actualizare consultați secțiunea Actualizare a acestui manual de utilizare.

6.1.2. Nivel de securitate

Puteți alege nivelul de securitate care satisface cel mai bine nevoile dumneavoastră de protecție. Mutați cursorul pentru a seta nivelul de securitate adecvat.

Există trei niveluri de securitate:

Nivel de securitate	Descriere
Întreținere	Nu oferă niciun fel de protecție. Doar **Actualizarea automată** este activată. Doar actualizează BitDefender. Deşi nu oferă niciun fel de protecție acest nivel de securitate poate fi util administratorilor de sistem.

Nivel de securitate	Descriere
Local System	Oferă protecție antivirus, recomandat în mod special calculatoarelor fără acces la rețea sau Internet. Consumul de resurse este foarte scăzut. Fişierele accesate sunt scanate împotriva viruşilor.
Sistem local plus	Oferă protecție antivirus&antispyware; recomandat în mod special calculatoarelor fără acces la rețea sau Internet. Consumul de resurse este scăzut. Fişierele accesate sunt scanate împotriva viruşilor şi aplicațiilor spyware.

BitDefender Antivirus v10 este recomandat calculatoarelor fără acces la rețea sau Internet.

Puteți personaliza nivelul de securitate făcând clic pe **Nivel personal**. În fereastra care va apărea, selectați opțiunile de protecție BitDefender pe care doriți să le activați şi faceți clic pe **OK**.

Faceți clic pe **Nivel implicit** pentru a seta cursorul la nivelul implicit.

6.1.3. Stare înregistrare

Puteți vedea informații despre starea licenței BitDefender. Aici puteți să înregistrați produsul şi puteți afla data expirării licenței.

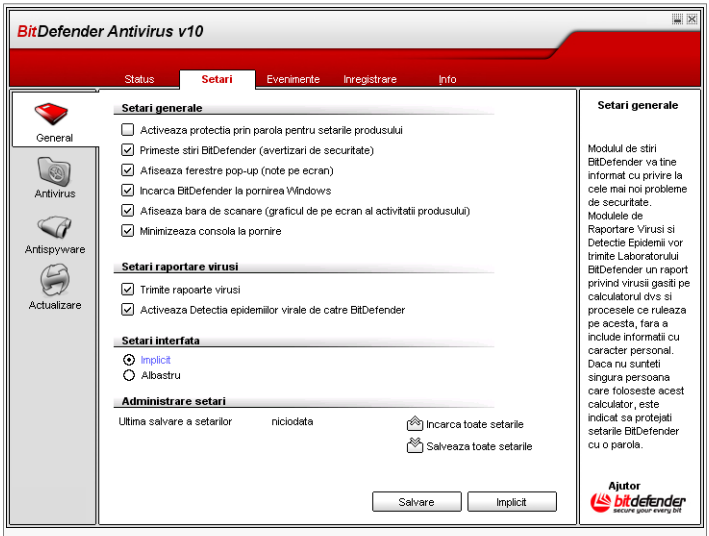
Pentru a introduce o nouă serie de înregistrare faceți clic pe **Introduceți seria nouă**. Urmați paşii asistentului de înregistrare pentru a înregistra cu succes BitDefender.

Notă

Pentru mai multe detalii privind procesul de înregistrare consultați secțiunea Înregistrare produs a acestui manual de utilizare.

6.2. Setări consola de administrare

Pnetru a accesa această secțiune faceți clic pe tabul **Setări** din modulul**General**.



Setări consola de administrare

Aici puteți seta comportamentul general al produsului. BitDefender se încarcă la pornirea Windows iar apoi rulează minimizat în bara de sistem.

Există patru categorii de opțiuni: **Setări generale**, **Setări raportare viruşi**, **Setări interfață** şi **Administrare setări**.

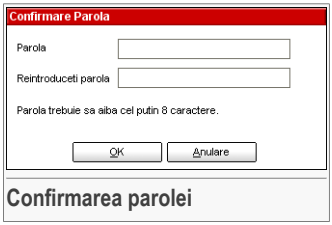
6.2.1. Setări generale

- **Activează protecția prin parolă pentru setările produsului** - permite setarea unei parole pentru a proteja configurația consolei de administrare a BitDefender.

Notă

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

Dacă selectați această opțiune, va apărea următoarea fereastră:



Confirmarea parolei

Introduceți parola în câmpul **Parolă**, reintroduceți-o în câmpul **Reintroduceți parola** şi faceți clic pe **OK**.

Din acest moment, dacă doriți să schimbați opțiunile de configurare ale BitDefender, veți fi rugat să introduceți parola.

Important

Dacă uitați parola va fi nevoie să reparați produsul pentru a schimba configurarea BitDefender.

- **Primeşte ştiri BitDefender (avertizări de securitate)** - afişează din când în când notificări de securitate referitoare la noi viruşi descoperiți, trimise de serverul BitDefender.
- **Afişează ferestre pop-up (note pe ecran)** - afişează ferestre de informare cu privire la starea produsului.
- **Încarcă BitDefender la pornirea Windows** - lansează BitDefender automat, la pornirea sistemului de operare.

Notă

Această opțiune este recomandată.

- **Afişează bara de scanare (graficul de pe ecran al activității produsului)** - activează/dezactivează bara de scanare.
- **Minimizează consola la pornire** - minimizează consola de administrare BitDefender după ce a fost încărcat la pornirea sistemului. Doar icoana BitDefender va apărea în bara de sistem.

6.2.2. Setări raportare viruşi

- **Trimite rapoarte viruşi** - trimite Laboratorului BitDefender rapoarte referitoare la viruşii identificați în calculatorul dumneavoastră. Astfel ne ajutați să ținem evidența noilor viruşi.

Rapoartele nu conțin date confidențiale, precum numele dumneavoastră, adresa IP sau altele, şi nu vor fi folosite în scopuri comerciale. Informațiile trimise vor conține doar numele viruşilor şi vor fi folosite doar pentru a crea rapoarte statistice.

- **Activează Detecția epidemiilor virale de către BitDefender** - trimite Laboratorului BitDefender rapoarte referitoare la potențiale epidemii virale.

  Rapoartele nu conțin date confidențiale, precum numele dumneavoastră, adresa IP sau altele, şi nu vor fi folosite în scopuri comerciale. Informațiile trimise vor conține doar potențialul virus şi vor fi folosite doar pentru a detecta noi viruşi.

6.2.3. Setări interfață

Vă permite să selectați culoarea consolei de administrare. Skin-ul reprezintă imaginea de fundal a interfeței. Pentru a selecta un nou skin, faceți clic pe culoarea corespunzătoare.

6.2.4. Administrare setări

Folosiți butoanele **Salvează toate setările** / **Încarcă toate setările** pentru a salva setările BitDefender într-o anumită locație sau pentru a le încărca dintr-o anumită locație. Astfel, puteți folosi aceleaşi setări şi după ce ați reinstalat sau ați reparat produsul BitDefender.

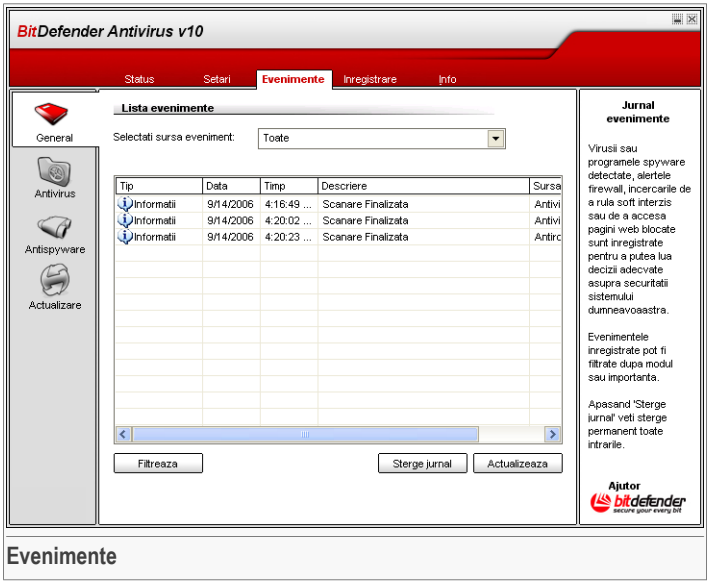
Important

Doar utilizatorii cu drepturi administrative pot salva sau încărca setări.

Faceți clic pe **Salvare** pentru a salva modificările făcute. Dacă faceți clic pe **Implicit** veți reveni la setările implicite.

6.3. Evenimente

Pnetru a accesa această secțiune faceți clic pe tabul **Evenimente** din modulul **General**.



Evenimente

În această secțiune sunt afişate toate evenimentele generate de către BitDefender.

Există 3 tipuri de evenimente: **Informații**, **Avertisment** şi **Critic**.

Exemple de evenimente:

- **Informații** - când a fost scanat un e-mail;
- **Avertisment** - când a fost detectat un fişier suspect;
- **Critic** - când a fost detectat un fişier infectat.

Pentru fiecare eveniment sunt oferite următoarele informații: data şi momentul apariției evenimentului, o scurtă descriere şi sursa lui (**Antivirus**, **Firewall**, **Antispyware** sau **Actualizare**).Faceți dublu-clic pe un eveniment pentru a-i vedea proprietățile.

Puteți filtra aceste evenimente în două moduri (după tip şi după sursă):

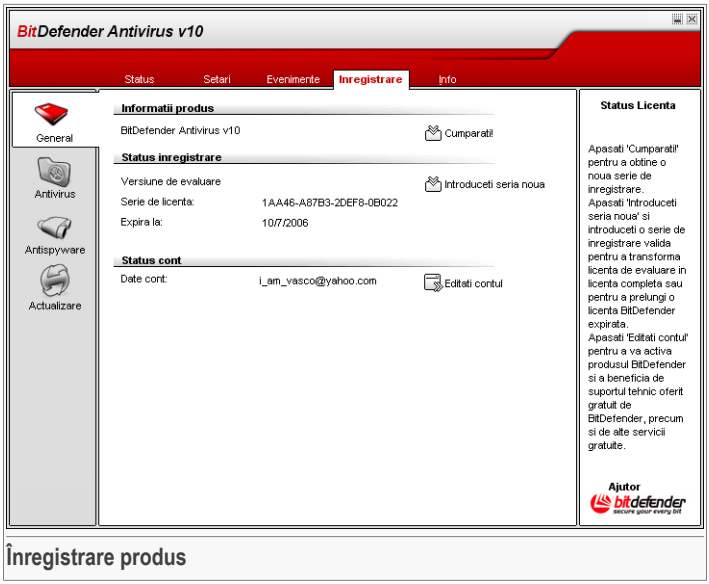
- Faceți clic pe **Filtrează** pentru a selecta ce tipuri de evenimente să fie afişate.
- Selectați evenimentul sursă din meniul drop-down.

În cazul în care consola de administrare este deschisă la secțiunea **Evenimente** şi în acelaşi timp apare un eveniment trebuie să faceți clic pe **Actualizează** pentru a vedea evenimentul respectiv.

Pentru a şterge toate evenimentele din listă faceți clic pe **Şterge jurnal**.

6.4. Înregistrare produs

Pnetru a accesa această secțiune faceți clic pe tabul **Înregistrare** din modulul **General**.



Înregistrare produs

Această secțiune conține informații despre produsul BitDefender (starea licenței, ID-ul produsului, data expirării) şi despre contul BitDefender. Aici puteți să înregistrați produsul şi să configurați contul BitDefender.

Faceți clic pe butonul **Cumpărați!** pentru pentru a obține o nouă serie de înregistrare din magazinul on-line BitDefender.

Puteți înregistra produsul şi modifica seria de înregistrare sau informațiile contului BitDefender făcând clic pe **Introduceți seria nouă**. Pentru a vă configura contul BitDefender faceți clic pe **Editați contul**. În ambele cazuri va apărea asistentul de înregistrare.

6.4.1. Asistentul de înregistrare

Asistentul de înregistrare este o procedură constituită din cinci paşi.

Pasul 1/5 - Bine ați venit în asistentul de înregistrare

Fereastra de întâmpinare

Faceți clic pe **Înainte**.

Pasul 2/5 - Înregistrați BitDefender

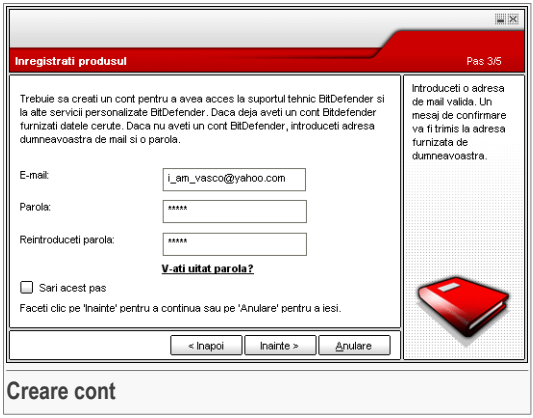
Înregistrare

Selectați **Înregistrează produsul** pentru a înregistra **BitDefender Antivirus v10**. Introduceți seria de înregistrare în câmpul **Introduceți seria nouă**.

Pentru a evalua produsul în continuare selectați **Continuă evaluarea produsului**.

Faceți clic pe **Înainte**.

Pasul 3/5 - Creați un cont BitDefender



Nu am un cont BitDefender

Pentru a beneficia de suport tehnic gratuit şi alte servicii BitDefender gratuite trebuie să creați un cont.

Introduceți o adresă de mail validă în câmpul **E-mail**. Alegeți o parolă şi introduceți-o în câmpul **Parolă**. Confirmați parola în câmpul **Reintroduceți parola**. Utilizați adresa de mail şi parola pentru a accesa contul dumneavoastră la http://myaccount.bitdefender.com.

Notă

Parola trebuie să conțină minim patru caractere.

Pentru a crea un cont trebuie mai întâi să vă activați adresa de mail. Verificați-vă adresa de mail şi urmați instrucțiunile din e-mailul trimis de serviciul de înregistrare BitDefender.

Important

Vă rugăm să vă activați contul înainte de a trece la pasul următor.

Dacă nu doriți să creați un cont BitDefender, selectați **Sari acest pas**. Veți sări, de asemenea, şi peste pasul următor.

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

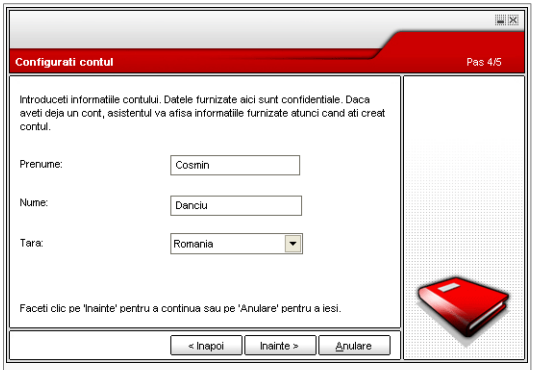
Deja am un cont BitDefender

Dacă aveți deja un cont activ, introduceți adresa de mail şi parola contului dumneavoastră. Dacă parola introdusă este incorectă, vi se va cere să o reintroduceți când faceți clic pe **Înainte**. Faceți clic pe **Ok** pentru a reintroduce parola sau pe **Anulare** pentru a părăsi programul asistent.

Dacă v-ați uitat parola, faceți clic pe **V-ați uitat parola?** şi urmați instrucțiunile.

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

Pasul 4/5 - Introduceți informațiile contului



Informații cont

Notă

Nu veți urma acest pas dacă ați selectat **Sari acest pas** în al treilea pas.

Introduceți numele şi prenumele dumneavoastră şi selectați țara în care locuiți.

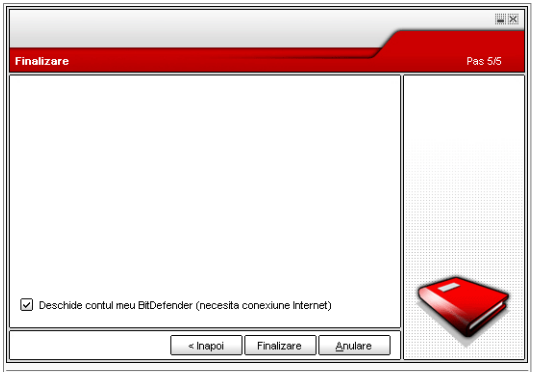
Dacă deja aveți un cont, asistentul va afişa informațiile furnizate anterior, dacă acestea există. Aici puteți, de asemenea, modifica aceste informații dacă doriți acest lucru.

Important

Informațiile furnizate aici vor rămâne confidențiale.

Faceți clic pe **Înainte**.

Pasul 5/5 - Examinați rezumatul



Finalizare

Acesta este ultimul pas al programului asistent. Puteți face orice modificări doriți, revenind la paşii anteriori (faceți clic pe **Înapoi**).

Dacă nu doriți să faceți nicio modificare, faceți clic pe **Finalizare** pentru a închide programul asistent.

Selectați **Deschide contul meu BitDefender** pentru a vă accesa contul BitDefender. Este necesară o conexiune la Internet.

6.5. Info

Pentru a accesa această secțiune faceți clic pe tabul **Info** din modulul **General**.

Informații generale

În această secțiune puteți afla datele de contact precum şi detalii privind produsul.

BitDefender™ este un furnizor global important de soluții de securitate care satisfac nevoia de protecție a mediului informațional contemporan. Compania oferă una dintre cele mai rapide şi eficiente linii de soft de securitate, stabilind noi standarde în ceea ce priveşte prevenirea amenințărilor, detecția rapidă a acestora şi diminuarea efectelor negative produse. BitDefender furnizează produse şi servicii unui număr de peste 41 de milioane de utilizatori din peste 180 dețări.

BitDefender™ este certificat de toate organismele de certificare independente- **ICSA Labs**, **CheckMark** şi **Virus Bulletin** şi este singurul produs de securitate care a primit **Premiul IST**.

Mai multe informații despre BitDefender pot fi obținute vizitând http://www.bitdefender.ro.

7. Modulul Antivirus

Secțiunea **Antivirus** a acestui ghid de utilizare conține următoarele subiecte:

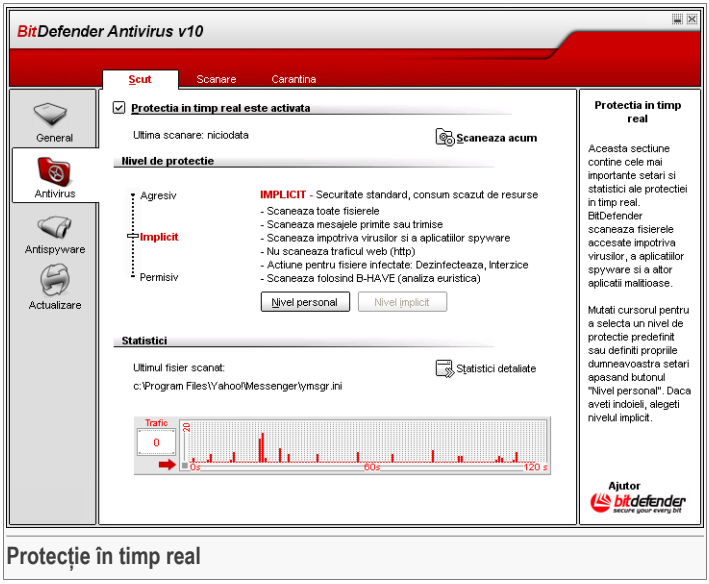
- Scanare la acces
- Scanare la cerere
- Carantină

Notă

Pentru mai multe detalii privind modulul **Antivirus** module consultați "*Modulul Antivirus*" (p. 27).

7.1. Scanare la acces

Pentru a accesa această secțiune faceți clic pe tabul **Scut** din modulul **Antivirus**.



Protecție în timp real

În această secțiune puteți configura **Protecția în timp real** şi puteți vedea informații cu privire la activitatea sa. **Protecția în timp real** vă protejează calculatorul scanând mesajele e-mail şi fişierele descărcate sau accesate.

Important

Pentru a preveni infectarea calculatorului personal cu viruşi, păstrați **Protectia in timp real** activată.

În partea de jos a secțiunii sunt afişate statisticile **Protecției în timp real** privind fişierele şi mesajele e-mail scanate. Faceți clic pe **Statistici detaliate** dacă doriți deschiderea unei ferestre cu informații detaliate despre aceste statistici.

7.1.1. Nivel de protecție

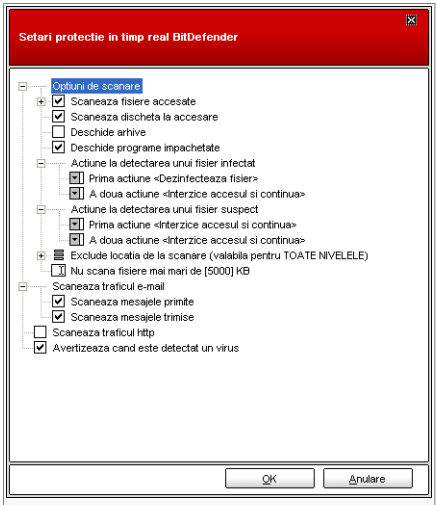
Puteți alege nivelul de protecție adecvat nevoilor dumneavoastră de securitate. Mutați cursorul pentru a seta nivelul de protecție dorit.

Există trei nivele de protecție:

Nivel de protecție	Descriere
Permisiv	Acoperă nevoile elementare de securitate. Consumul de resurse este foarte scăzut. Aplicațiile şi mesajele e-mail primite sunt scanate doar împotriva viruşilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acțiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.
Standard	Oferă protecție standard. Consumul de resurse este scăzut. Toate fişierele şi mesajele e-mail sunt scanate împotriva viruşilor şi a aplicațiilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acțiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.
Agresiv	Oferă protecție avansată. Consumul de resurse este moderat. Toate fişierele şi mesajele e-mail, precum şi traficul web, sunt scanate împotriva viruşilor şi a aplicațiilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acțiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.

Utilizatorii avansați pot folosi şi modifica opțiunile de scanare oferite de BitDefender. Motorul de scanare poate fi setat să sară peste fişierele cu anumite extensii, directoare sau arhive despre care ştiți că sunt inofensive. Aceasta poate reduce cu mult timpul de scanare, precum şi viteza de reacție a sistemului pe durata scanării.

Puteți personaliza **Protecția în timp real** făcând clic pe **Nivel personal**. Va apărea următoarea fereastră:



Setări Scut

Opțiunile de scanare sunt organizate intr-un meniu expandabil similar celor din Windows.

Faceți clic pe semnul “+” pentru a deschide o opțiune sau pe semnul “-” pentru a închide o opțiune.

Puteți observa că, deşi semnul “+” apare, unele opțiuni de scanare nu pot fi deschise. Motivul este că aceste opțiuni nu au fost selectate încă.Dacă veți selecta aceste opțiuni, ele vor putea fi deschise.

- **Opțiuni de scanare a fişierelor şi a transferurilor P2P** - scanează fişierele accesate şi comunicația prin programe de mesagerie instantă (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). În continuare, selectați tipurile de fişiere care doriți să fie scanate.

Opțiune		Descriere
Scanează fişiere accesate	**Scanează toate fisierele**	Vor fi scanate toate fişierele accesate, indiferent de tipul lor.
	Programe	Nu vor fi scanate decât fişierele program, şi anume fişierele cu următoarele extensii: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif;

Opțiune		Descriere
		.prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml şi .nws.
	Extensiile definite de utilizator	Nu vor fi scanate decât fişierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
	Exclude extensiile de la scanare: [ ]	Fişierele cu extensiile specificate de utilizator NU vor fi scanate. Aceste extensii trebuie separate prin ";".
	Scanează după soft cu risc	Scanează împotriva aplicațiilor de risc (riskware). Aceste fişiere vor fi considerate fişiere infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată. Selectați **Nu scana aplicații si programe dialer** dacă doriți să excludeți aceste fişiere de la scanare.
Scanează discheta la accesare		Scanează discheta atunci când aceasta este accesată.
Deschide arhive		Vor fi scanate şi arhivele accesate. Selectând această opțiune, performanțele calculatorului vor scădea.
Deschide programele împachetate		Programele împachetate accesate vor fi scanate.
Prima acțiune		Selectați din meniu prima acțiune ce va fi luată asupra fişierelor infectate sau suspecte.
	Interzice accesul şi continuă	În caz că un fişier este infectat, accesul la acesta va fi interzis.
	Dezinfectează fişier	Dezinfectează fişierul infectat.
	Şterge fişier	Şterge imediat fişierele infectate, fără niciun avertisment.
	Mută fişier în carantină	Mută fişierele infectate în carantină.
A doua acțiune		Selectați din meniu a doua acțiune pentru fişierele infectate sau suspecte, în caz că prima acțiune eşuează.

Opțiune		Descriere
	Interzice accesul şi continuă	În caz că un fişier este infectat, accesul la acesta va fi interzis.
	Şterge fişier	Şterge imediat fişierele infectate, fără niciun avertisment.
	Mută fişier în carantină	Mută fişierele infectate în carantină.
Nu scana fişiere mai mari de [x] Kb		Introduceți dimensiunea maximă a fişierelor ce vor fi scanate. Dacă dimensiunea este de 0 Kb, toate fişierele vor fi scanate, indiferent de mărimea lor.
Exclude locație de la scanare (aplicată la toate nivelele)		Faceți clic pe semnul "+" corespunzător acestei opțiuni pentru a specifica un director care va fi exclus de la scanare. Prin această setare o nouă opțiune, `Obiect nou`, va apărea. Faceți clic pe căsuța corespunzătoare noului obiect, iar din fereastra de explorare selectați directorul pe care doriți să-l excludeți de la scanare. Obiectele selectate aici vor fi excluse de la scanare, indiferent de nivelul de protecție ales (nu doar pentru **Nivelul personal**).

- **Scanează traficul e-mail** - scanează traficul e-mail.

  Următoarele opțiuni sunt disponibile:

Opțiune	Descriere
Scanează mesajele primite	Scanează toate mesajele primite.
Scanează mesajele trimise	Scanează toate mesajele trimise.

- **Scanează traficul http** - scanează tot traficul web.
- **Avertizează când este detectat un virus** - afişează o fereastră de avertizare la descoperirea unui virus într-un fişier sau mesaj e-mail.

  Pentru fişierele infectate fereastra de avertizare va conține calea şi numele virusului, acțiunea luată de BitDefender şi un link către site-ul BitDefender, unde puteți afla

mai multe informații despre virus. Pentru mesajele infectate fereastra de avertizare va conține şi informații despre expeditor şi destinatar.

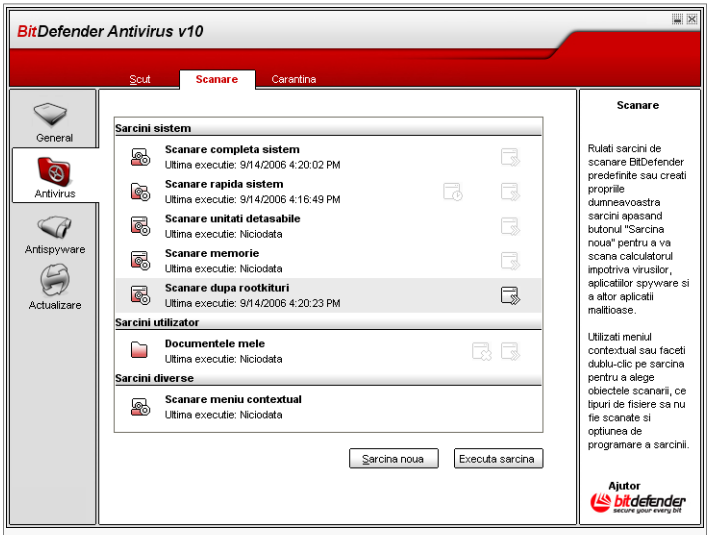
Dacă este detectat un fişier suspect, din fereastra de alertă puteți lansa un program asistent ce vă va ajuta să trimiteți acest fişier Laboratorului BitDefender pentru analiză aprofundată. Pentru a primi informații despre acest fişier introduceți adresa dumneavoastră de e-mail.

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

Dacă doriți să vă întoarceți la nivelul implicit, faceți clic pe **Nivel implicit**.

7.2. Scanare la cerere

Pentru a accesa această secțiune faceți clic pe tabul **Scanare** din modulul **Antivirus**.



Sarcini de scanare

În această secțiune puteți configura BitDefender pentru a vă scana calculatorul.

Principalul obiectiv BitDefender este protejarea calculatorului dumneavoastră de viruşi. Aceasta se face în primul rând nepermițând viruşilor noi să pătrundă în sistem, prin scanarea mesajelor e-mail şi a fişierelor 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 viruşi după instalarea BitDefender. Şi este, de asemenea, recomandat să vă scanați sistemul periodic.

7.2.1. Sarcini de scanare

Scanarea la cerere se bazează pe sarcini de scanare. Utilizatorul poate scana calculatorul folosind sarcinile implicite sau creând propriile sarcini de scanare (sarcini definite de utilizator).

Există trei categorii de sarcini de scanare:

- **Sarcini sistem** - conține lista sarcinilor implicite de sistem. Următoarele sarcini sunt disponibile:

Sarcină implicită	Descriere
Scanare profundă sistem	Scanează întregul sistem, inclusiv arhivele, împotriva viruşilor şi aplicațiilor spion (spyware).
Scanare completă sistem	Scanează întregul sistem, cu excepția arhivelor, împotriva viruşilor şi aplicațiilor spion (spyware).
Scanare rapidă sistem	Scanează programele împotriva viruşilor.
Scanare unități detaşabile	Scanează unitățile detaşabile împotriva viruşilor şi aplicațiilor spyware.
Scanare memorie	Scanează memoria după aplicații spion cunoscute.
Scanare după rootkituri	Scanează memoria împotriva aplicațiilor malițioase ascunse.

- **Sarcini utilizator** - conține sarcinile definite de utilizator.

  O sarcină numită `Documentele mele` este furnizată. Utilizați această sarcină pentru a vă scana documentele din directorul `Documentele mele`.

- **Sarcini diverse** - conține o listă de sarcini de scanare diverse. Aceste sarcini de scanare se referă la tipuri alternative de scanare ce nu pot fi rulate din această fereastră. Puteți doar să modificați setările acestora şi să examinați rapoartele de scanare.

În partea dreaptă a fiecărei sarcini sunt disponibile trei butoane:

- **Planificare sarcină** - indică faptul că sarcina selectată este planificată să ruleze mai tarziu. Faceți clic pe acest buton pentru a accesa secțiunea Planificare din fereastra de **Proprietăți** unde puteți modifica această setare.
- **Şterge** - şterge sarcina selectată.

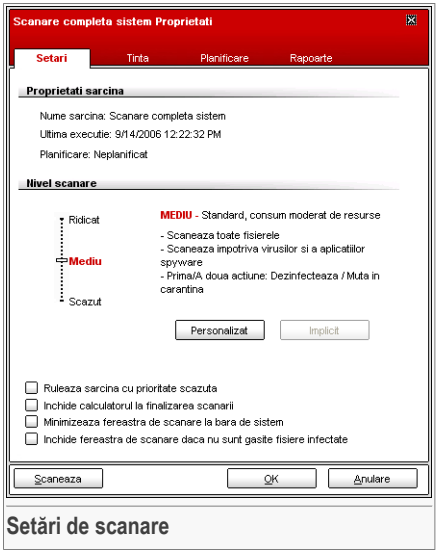
  Notă
  Nu este disponibil pentru sarcinile de sistem. Nu puteți şterge o sarcină de sistem.

- **Scanare** - execută sarcina selectată, pornind o scanare imediată.

7.2.2. Proprietăți sarcină de scanare

Fiecare sarcină de scanare are propria fereastră de **Proprietăți**, unde puteți configura opțiunile de scanare, puteți alege obiectele ce vor fi scanate, puteți planifica sarcina sau examina rapoartele. Pentru a accesa această fereastră faceți dublu-clic pe sarcină. Va apărea următoarea fereastră:

Setări de scanare



Setări de scanare

Aici puteți vedea informații cu privire la sarcină (nume, când a rulat ultima dată şi programul de rulare) şi puteți configura setările de scanare.

Nivel de scanare

În primul rând, trebuie să alegeți nivelul de scanare. Mutați cursorul pentru a seta nivelul de scanare dorit.

Există trei nivele de scanare:

Nivel de protecție	Descriere
Scăzut	Oferă o rată de detecție moderată. Consumul de resurse este scăzut. Doar programele sunt scanate împotriva virușilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acțiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.
Mediu	Oferă o rată de detecție bună. Consumul de resurse este moderat.

Nivel de protecție	Descriere
	Toate aplicațiile sunt scanate împotriva viruşilor şi a aplicațiilor spyware. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acțiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.
Ridicat	Oferă o rată de detecție ridicată. Consumul de resurse este şi el ridicat. Toate aplicațiile şi arhivele sunt scanate împotriva viruşilor şi a aplicațiilor spyware. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acțiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.

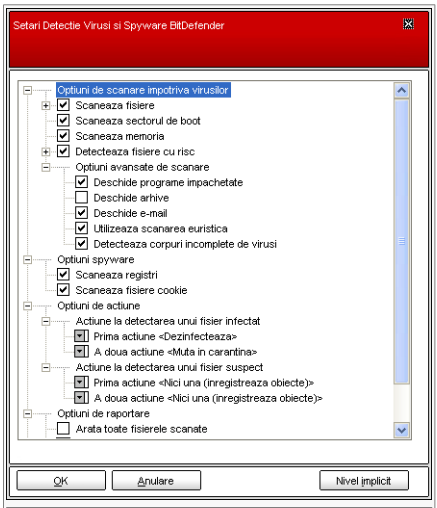
Important

Sarcina **Scanează după rootkituri** prezintă aceleaşi nivele de scanare. Totuşi, opțiunile sunt diferite:

- **Scăzut** - Doar procesele sunt scanate. Nicio acțiune nu va fi aplicată fişierelor detectate.
- **Mediu** - Fişierele şi procesele sunt scanate în căutare de obiecte ascunse. Nicio acțiune nu va fi aplicată fişierelor detectate.
- **Ridicat** - Fişierele şi procesele sunt scanate în căutare de obiecte ascunse. Obiectele detectate sunt redenumite.

Utilizatorii avansați pot folosi şi modifica opțiunile de scanare oferite de BitDefender. Motorul de scanare poate fi setat să sară peste fişierele cu anumite extensii, directoare sau arhive despre care ştiți că sunt inofensive. Aceasta poate reduce cu mult timpul de scanare, precum şi viteza de reacție a sistemului pe durata scanării.

Faceți clic pe **Personalizat** pentru a vă seta propriile opțiuni de scanare. Va apărea următoarea fereastră:



Setări de scanare

Opțiunile de scanare sunt organizate intr-un meniu expandabil similar celor din Windows.

Opțiunile de scanare sunt grupate în cinci categorii:

- **Opțiuni de scanare împotriva viruşilor**
- **Opțiuni spyware**
- **Opțiuni de acțiune**
- **Opțiuni de raportare**
- **Alte opțiuni**

Faceți clic pe semnul “+” pentru a deschide o opțiune sau pe semnul “-” pentru a închide o opțiune.

Important

Pentru sarcina **Scanare după rootkituri** doar trei categorii sunt disponibile: **Opțiuni de detecție rootkit**, **Opțiuni de raportare** şi **Alte opțiuni**. În prima categoria puteți specifica ce obiecte să fie scanate (fişiere, memorie, sau ambele) şi acțiunea aplicată obiectelor detectate (**Niciuna (înregistrează obiecte)/Redenumeşte**). Ultimele două categorii sunt identice celor prezentate mai jos.

- Specificați tipurile de fişiere ce vor fi scanate (arhive, mesaje e-mail şi altele) şi alte opțiuni. Aceasta se face prin selectarea unor opțiuni din categoria **Opțiuni de scanare împotriva viruşilor**.

Opțiune		Descriere
Scanează fişiere	**Scanează toate fisierele**	Vor fi scanate toate fişierele accesate, indiferent de tipul lor.
	Programe	Nu vor fi scanate decât fişierele program, şi anume fişierele cu următoarele extensii: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` şi `nws`.
	Extensiile definite de utilizator	Nu vor fi scanate decât fişierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
	Extensii excluse de la scanare	Fişierele cu extensiile specificate de utilizator NU vor fi scanate. Aceste extensii trebuie separate prin ";".
Scanează sectorul de boot		Scanează sectorul de boot al sistemului.
Scanare memorie		Scanează memoria împotriva viruşilor şi a altor aplicații malițioase.
Detectează fişiere cu risc		Scanează împotriva altor ameninţări decât viruşii, cum ar fi dialer-ele şi aplicațiile adware. Aceste fişiere vor fi considerate fişiere infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată. Selectați **Sări aplicații şi programe dialer** dacă doriți să excludeți aceste tipuri de fişiere de la scanare.
Opțiuni avansate de scanare	**Deschide programe impachetate**	Scanează programele împachetate.
	Deschide arhive	Scanează în interiorul arhivelor.
	Deschide e-mail	Scanează în interiorul arhivelor de e-mail.
	Activează scanarea euristică	Pentru a activa scanarea euristică a fişierelor. Scopul scanării euristice este de a identifica noi viruşi pe baza anumitor elemente şi

Opțiune	Descriere
	algoritmi, înainte ca definiția acestor viruşi să fie cunoscută. Pot apărea şi alarme false. Când este detectat un fişier de acest gen, el este clasificat ca suspect. În aceste cazuri, este recomandat să trimiteți fişierul la analiză către laboratorul BitDefender.
Detectează corpuri incomplete de viruşi	Detectează corpuri incomplete de viruşi.

- Specificați locațiile ce vor fi scanate împotriva aplicațiilor spyware (regiştri, cookie). Aceasta se face prin selectarea unor opțiuni din categoria **Opțiuni spyware**.

Opțiune	Descriere
Scanează regiştri	Scanează intrările din regiştri.
Scanează fişiere cookie	Scanează fişierele cookie.

- Specificați acțiunea pentru fişierele infectate sau suspecte. Deschideți categoria **Opțiuni de acțiune** pentru a vedea toate acțiunile posibile pentru fişierele infectate.

  Selectați acțiunile ce trebuie realizate când este detectat un fişier infectat sau suspect. Puteți specifica acțiuni diferite pentru fişierele infectate şi pentru cele suspecte. Puteți, de asemenea, să selectați o a doua acțiune în caz că prima eşuează.

Acțiune	Descriere
Niciuna (înregistrează obiecte)	Nici se va efectua nicio acțiune în legătură cu fişierelor infectate. Aceste fişiere vor apărea în fişierul de raport.
Întreabă utilizatorul	De fiecare dată când este detectat un virus, va apărea o fereastră de alertă şi utilizatorul va vea posibilitatea de a selecta acțiunea ce va fi realizată. În funcție de importanța fişierului, puteți alege să-l dezinfectați, să-l izolați în zona de carantină sau să-l ştergeți.
Dezinfectează	Dezinfectează fişierul infectat.

Acțiune	Descriere
Şterge	Şterge imediat fişierele infectate, fără niciun avertisment.
Mută în carantină	Mută fişierele infectate în carantină.
Redenumeşte	Schimbă extensia fişierelor infectate. Noua extensie a fişierelor infectate va fi .vir. Prin redenumirea fişierelor infectate, posibilitatea executării lor şi prin urmare a răspândirii infecției este exclusă. De asemenea, acestea pot fi salvate pentru examinare şi analiză detaliată.

Important

Redenumeşte are un efect similar asupra fişierelor ascunse (rootkituri). Noua extensie a fişierelor detectate va fi `.bd.ren`. Prin redenumirea fişierelor detectate, posibilitatea executării lor şi prin urmare a răspândirii infecției este exclusă. De asemenea, acestea pot fi salvate pentru examinare şi analiză detaliată.

- Specificați opțiunile pentru fişierele de raport. Deschideți categoria **Opțiuni de raportare** pentru a vedea toate opțiunile posibile.

Opțiune	Descriere
Arată toate fişierele scanate	Listează toate fişierele scanate (infectate sau nu) şi starea acestora în fişierul de raport. Selectând această opțiune, performanțele calculatorului vor scădea.
Şterge rapoartele mai vechi de [x] zile	Acest este un câmp editabil care vă permite să specificați pentru cât timp poate fi un raport stocat în secțiunea Rapoarte. Selectați această opțiune şi introduceți un nou interval. Intervalul implicit este de 180 de zile.

Notă

Fişierele de raport pot fi examinate în secțiunea Rapoarte din fereastra de **Proprietăți**.

- Specificați celelalte opțiuni. Deschideți categoria **Alte opțiuni** de unde puteți selecta următoarele opțiuni:

Opțiune	Descriere
Trimite fişierele suspecte la laboratorul BitDefender	Vi se va cere să trimiteți toate fişierele suspecte laboratorului BitDefender după încheierea procesului de scanare.

Dacă faceți clic pe **Nivel implicit** veți încărca setările standard.

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

Alte opțiuni

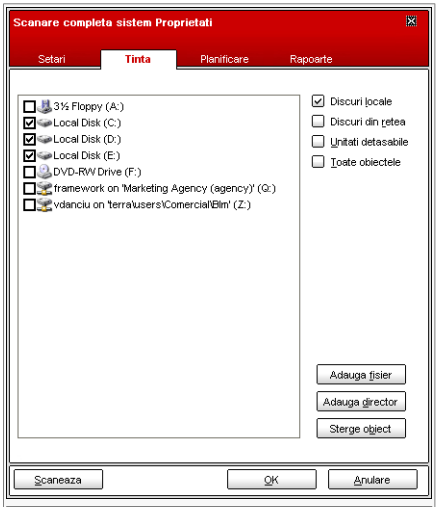
Sunt de asemenea disponibile şi o serie de opțiuni generale privind procesul de scanare:

Opțiune	Descriere
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 creşte.
Închide calculatorul la finalizarea scanării	Închide calculatorul la finalizarea procesului de scanare.
Trimite fişierele suspecte la laboratorul BitDefender	Vi se va cere să trimiteți toate fişierele suspecte laboratorului BitDefender după încheierea procesului de scanare.
Minimizează fereastra de scanare la bara de scanare	Minimizează fereastra de scanare bara de sistem. Faceți dublu-clic pe simbolul BitDefender pentru a o deschide.

Faceți clic pe **OK** pentru a salva modificările şi închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

Locație scanare

Faceți dublu-clic pe o sarcină selectată şi apoi clic pe tabul **Țintă** pentru a accesa această secțiune.



Locație scanare

Aici puteți selecta obiectele ce vor fi scanate.

Secțiunea conține următoarele butoane:

- **Adaugă fişiere** - deschide o fereastră de explorare în care puteți selecta fişierele pe care doriți să le scanați.
- **Adaugă directoare** - deschide o fereastră de explorare în care puteți selecta directoarele care doriți să fie scanate de BitDefender.

Notă

Puteți folosi drag & drop pentru a adăuga fişiere/directoare în listă.

- **Şterge obiect** - şterge fişierele / directoarele care au fost selectate anterior din lista de obiecte de scanat.

Notă

Numai fişierele / directoarele adăugate de utilizator pot fi şterse, nu şi cele care au fost “văzute” automat de BitDefender.

Pe lângă butoanele explicate mai sus există şi unele opțiuni ce permit selectarea rapidă a locațiilor pentru scanare.

- **Discuri locale** - pentru scanarea partițiilor locale.
- **Discuri din rețea** - pentru scanarea partițiilor din rețea recunoscute.
- **Unități detaşabile** - pentru scanarea unităților mobile de disc (unitățile de CD-ROM şi discheta).
- **Toate obiectele** - pentru scanarea tuturor partițiilor, indiferent dacă sunt locale sau de rețea, precum şi a unităților detaşabile.

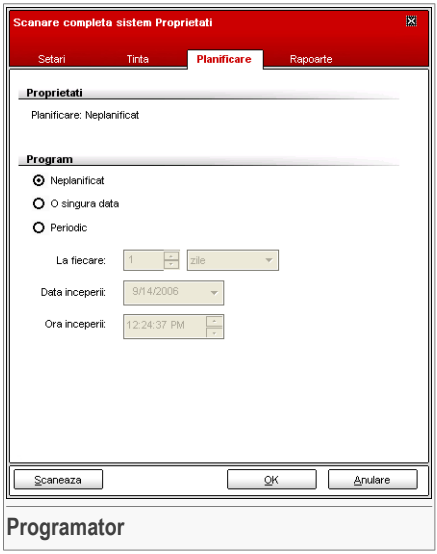
Notă

Dacă doriți să vă scanați tot sistemul, selectați opțiunea **Toate obiectele**.

Faceți clic pe **OK** pentru a salva modificările şi închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

Programator

Faceți dublu-clic pe o sarcină selectată şi apoi clic pe tabul **Planificare** pentru a accesa această secțiune.



Programator

Aici puteți vedea dacă sarcina este planificată să ruleze la un anumit moment sau nu şi puteți modifica această proprietate.

Important

Pentru sarcini complexe procesul de scanare durează mai mult şi este mai eficient dacă închideți toate programele. Din acest motiv este bine să programați astfel de sarcini să ruleze atunci când nu utilizați sistemul.

Când planificați o sarcină trebuie să alegeți una dintre următoarele opțiuni:

- **Neplanificat** - sarcina rulează doar atunci când utilizatorul cere acest lucru.
- **O singură dată** - scanarea se face o singură dată, la un anumit moment. Specificați data şi timpul lansării în execuție în câmpurile **Data începerii/Ora începerii**.
- **Periodic** - scanarea se realizează periodic, la anumite intervale de timp(ore, zile, săptămâni, luni, ani), începând de la un anumit moment.

  Dacă doriți ca scanarea să se repete la anumite intervale de timp, selectați opțiunea **Periodic** şi introduceți în câmpul de editare **La fiecare** numărul de minute / ore / zile / săptămâni / luni / ani la care doriți să se repete scanarea. De asemenea, trebuie să specificați data şi timpul lansării în execuție în câmpurile **Data începerii/Ora începerii**.

Faceți clic pe **OK** pentru a salva modificările şi închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

Rapoarte

Faceți dublu-clic pe o sarcină selectată şi apoi clic pe tabul **Rapoarte** pentru a accesa această secțiune.

Rapoarte

Aici puteți examina rapoartele generate de fiecare dată când sarcina a fost executată. Fiecare fişier conține informații privind rezultatele scanării, data şi timpul la care a fost executată sarcina precum şi un scurt rezumat (scanare finalizată).

Sunt disponibile două butoane:

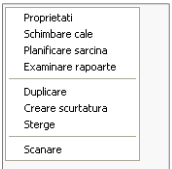
- **Afişează jurnal** - deschide fişierul de raport selectat.
- **Şterge jurnal** - şterge fişierul de raport selectat.

De asemenea, pentru a deschide sau şterge un fişier de raport, faceți clic dreapta pe fişier şi selectați opțiunea corespunzătoare din meniu.

Faceți clic pe **OK** pentru a salva modificările şi închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

7.2.3. Meniu contextual

Un meniu contextual este disponibil pentru fiecare sarcină. Faceți clic dreapta pe o sarcină selectată pentru a-l deschide:



Meniu contextual

Următoarele opțiuni sunt disponibile pe meniul contextual:

- **Proprietăți** - deschide fereastra de **Proprietăți**, la tabul **Setări** unde puteți modifica setările pentru sarcina selectată;
- **Schimbare cale** - deschide fereastra de **Proprietăți**, la tabul **Țintă** unde puteți modifica ținta de scanare pentru sarcina selectată;
- **Planificare sarcină** - deschide fereastra de **Proprietăți**, la tabul **Planificare** unde puteți programa sarcina selectată să ruleze la un moment dat sau doar la cererea utilizatorului;
- **Examinare rapoarte** - deschide fereastra de **Proprietăți**, la tabul **Rapoarte** unde puteți examina rapoartele generate de fiecare dată când sarcina selectată a rulat;
- **Duplicare** - creează o copie a sarcinii selectate;

Notă
Acest lucru este util în crearea de noi sarcini, deoarece puteți modifica setările duplicatului unei sarcini.

- **Creare scurtătură** - creează o scurtătură (shortcut) pe desktop a sarcinii selectate;
- **Şterge** - şterge sarcina selectată.

Notă
Nu este disponibil pentru sarcinile de sistem. Nu puteți şterge o sarcină de sistem.

- **Scanare** - rulează sarcina selectată, lansând o scanare imediată.

Important
Datorită caracterului lor special, pentru sarcinile din categoria **Sarcini diverse** doar opțiunile **Proprietăți** şi **Examinare rapoarte** sunt disponibile.

7.2.4. Tipuri scanări la cerere

BitDefender permite trei tipuri de scanare la cerere:

- Scanare imediată - când este rulată o sarcină de sistem sau definită de utilizator;

- Scanare contextuală - când faceți clic-dreapta pe un fişier sau director şi selectați opțiunea BitDefender Antivirus v10;
- Scanare drag&drop - când aduceți un fişier sau director deasupra Barei de scanare;

Scanare imediată

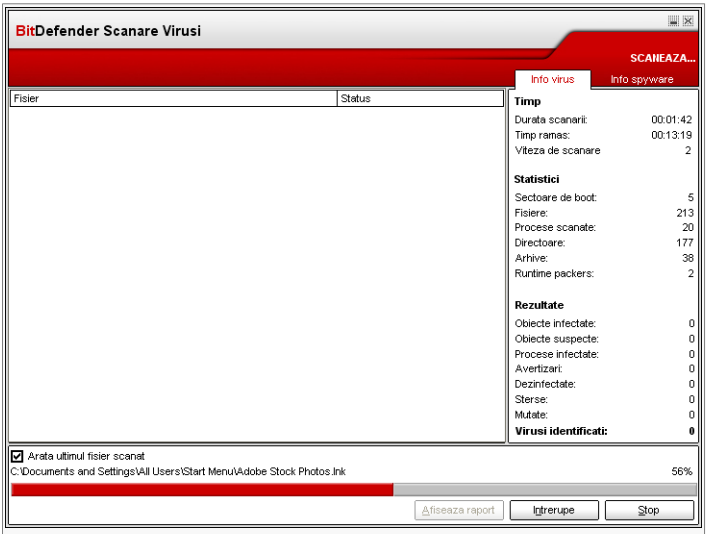
Pentru a vă scana sistemul sau o parte din el puteți utiliza sarcinile de scanare implicite sau puteți crea propriile sarcini de scanare. Există două metode de a crea sarcini de scanare:

- Duplicați o sarcină existentă, redenumiți-o şi faceți modificările necesare în fereastra de Proprietăți;
- Faceți clic pe **Sarcină nouă** pentru a crea o nouă sarcină şi a o configura.

Pentru ca BitDefender să facă o scanare completă, este necesar să închideți toate programele. Este important să închideți în primul rând clientul de e-mail (i.e. Outlook, Outlook Express sau Eudora).

Înainte de a începe scanarea este necesar să vă asigurați că BitDefender este la zi cu semnăturile de viruşi, având în vedere că în fiecare zi se descoperă şi se identifică viruşi noi. Puteți verifica data la care a fost făcută ultima actualizare în partea de jos a modulului Update.

Pentru a lansa scanarea, selectați din listă sarcina dorită şi faceți clic pe butonul **Scanare** din dreapta. Puteți de asemenea să faceți clic pe **Execută sarcina**. Va apărea fereastra de scanare:



Fereastra de scanare

Pe parcursul procesului de scanare, va apărea o icoană în bara de sistem.

În timpul scanării, BitDefender va afişa progresul scanării şi vă va alerta dacă descoperă vreo ameninţare. În dreapta puteţi vedea statisticile procesului de scanare. În funcţie de obiectele scanate pot fi disponibile informaţii despre scanarea împotriva viruşilor sau împotriva aplicaţiilor spyware sau amândouă. Daca amândouă sunt disponibile, faceţi clic pe tabul corespunzător pentru a afla detalii despre scanarea împotriva viruşilor sau aplicaţiilor spyware

Selectaţi opţiunea **Arată ultimul fişier scanat** şi nu va fi vizibilă decât informaţia despre ultimul fişier scanat.

Notă

Procesul de scanare poate dura destul de mult, în funcţie de complexitatea scanării.

Sunt disponibile trei butoane:

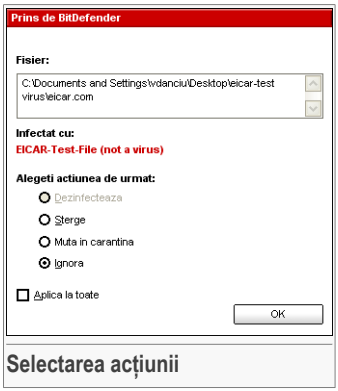
- **Stop** - deschide o fereastră nouă care vă permite oprirea verificării sistemului. Faceţi clic pe **Da&Închide** pentru a închide fereastra de scanare.
- **Întrerupe** - întrerupe temporar procesul de scanare - îl puteţi relua apăsând butonul **Reia**.

- **Afişează raport** - deschide raportul de scanare.

Notă

Dacă faceți clic-dreapta pe o sarcină ce se află în execuție, un meniu contextual va apărea permițându-vă să administrați fereastra de scanare. Opțiunile (**Întrerupe / Reia**, **Opreşte** şi **Opreşte&Închide**) sunt similare butoanelor din fereastra de scanare.

Dacă în fereastra de Proprietăți este setată opțiunea **Întreabă utilizatorul**, atunci când un fişier infectat este detectat va apărea o fereastră de alertă care vă va cere să selectați acțiunea ce va fi luată asupra fişierului infectat.



Selectarea acțiunii

Puteți afla numele fişierului infectat, precum şi numele virusului.

Selectați una dintre următoarele acțiuni pentru fişierul infectat:

- **Dezinfectează** - dezinfectează fişierul infectat;
- **Şterge** - şterge fişierul infectat;
- **Mută în carantină** - mută fişierul infectat în carantină;
- **Ignoră** - ignoră fişierele infectate. Nicio acțiune nu va fi aplicată fişierelor infectate.

Dacă scanați un director şi doriți ca acțiunea să fie la fel pentru toate fişierele infectate, selectați opțiunea **Aplică tuturor**.

Notă

Dacă opțiunea **Dezinfectează** nu poate fi selectată, înseamnă că tentativa BitDefender de a dezinfecta fişierul a eşuat. Cea mai bună soluție este izolarea virusului în carantină si trimiterea pentru analiză la Laboratorul BitDefender.

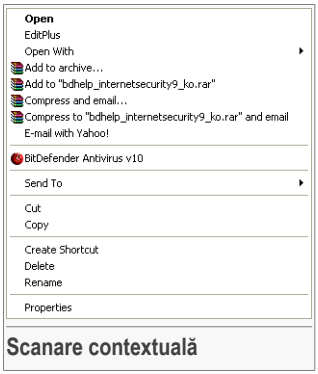
Faceți clic pe **OK**.

Notă

Fişierul de raport este salvat automat în secțiunea Rapoarte din fereastra de **Proprietăți** a sarcinii respective.

Scanare contextuală

Faceți clic-dreapta pe fişierul sau directorul pe care doriți să-l scanați şi selectați opțiunea **BitDefender Antivirus v10**.

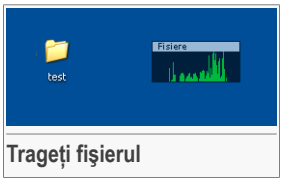


Scanare contextuală

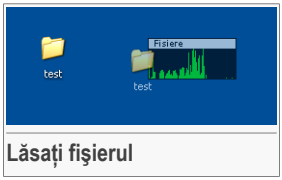
Puteți modifica opțiunile de scanare şi examina fişierele de raport accesând fereastra de Proprietăți a sarcinii **Scanare meniu contextual**.

Scanare prin drag&drop

Trageți fişierul sau directorul pe care doriți să îl scanați peste **Bara de scanare**, ca în imaginile de mai jos.



Trageți fișierul



Lăsați fișierul

Dacă un fișier infectat este detectat, va apărea o fereastră de alertă care vă va cere să selectați acțiunea ce va fi aplicată fișierului infectat.

În ambele cazuri (scanare contextuală sau prin drag&drop) va apărea fereastra de scanare.

7.2.5. Scanare după rootkituri

BitDefender caută să rezolve cele mai noi amenințări de securitate prin introducerea unui detector de rootkituri alături de eficientele sale motoare antivirus&antispyware. Bitdefender este acum capabil să detecteze rootkituri căutând după fişiere, directoare şi procese ascunse. Mai mult, BitDefender vă poate proteja sistemul redenumind aplicațiile malițioase ce utilizează rootkituri.

Pentru a scana calculatorul după rootkituri, rulați sarcina **Scanare după rootkituri**. Va apărea o fereastră de scanare.

Important

Este recomandat ca atunci când căutați rootkituri să setați BitDefender să nu ia nicio acțiune asupra fişierelor ascunse.

La sfârşitul scanării puteți vedea rezultatele. Dacă au fost detectate fişiere ascunse verificați-le cu atenție: prezența fişierelor ascunse poate indica o posibilă intruziune.

Dacă ştiți cu siguranță că fişierele detectate aparțin unor aplicații malițioase, vă recomandăm să setați acțiunea **Redenumeşte** şi să executați din nou sarcina **Scanare după rootkituri**. Astfel vor fi blocate fişierele ascunse.

Avertisment

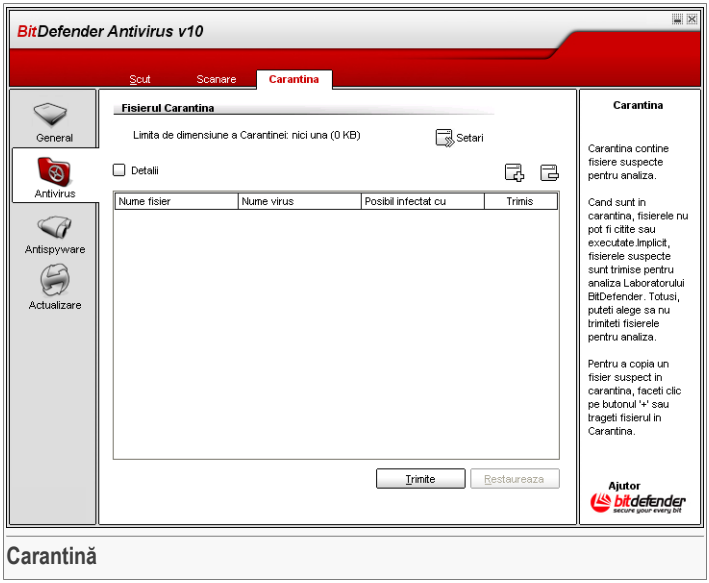
NU TOATE FIŞIERELE ASCUNSE SUNT APLICAȚII MALIȚIOASE!Înainte de a redenumi fişierele ascunse, asigurați-vă că ele nu aparțin unor aplicații valide sau sistemului. Redenumirea unor astfel de fişiere poate provoca instabilitatea sistemului dumneavoastră.

Important

Dacă sistemul dumneavoastră a fost atacat de un hacker, există o singură metodă sigură de a scăpa de agresor: reinstalarea sistemului.

7.3. Carantină

Pentru a accesa această secțiune faceți clic pe tabul **Carantină** din modulul **Antivirus**.



Carantină

BitDefender permite izolarea fişierelor infectate sau suspecte într-o zonă sigură, numită carantină. Izolând aceste fişiere în carantină, riscul răspândirii infecției dispare, iar în plus, aveți posibilitatea să trimiteți aceste fişiere Laboratorului BitDefender pentru analiză aprofundată.

Componenta BitDefender care asigură administrarea fişierelor izolate este modulul **Carantina**. Acest modul a fost creat cu posibilitatea de a trimite automat fişierele infectate la Laboratorul BitDefender.

După cum puteți observa, secțiunea **Carantină** conține o listă cu toate fișierele care au fost izolate până acum. Fiecărui fișier i se poate afla numele, dimensiunea, data izolării şi data trimiterii. Dacă doriți mai multe informații despre fişierele din carantină faceți clic pe **Detalii**.

Notă

Atunci când sunt în carantină viruşii sunt inofensivi, pentru că nu pot fi executați sau citiți.

Faceți clic pe butonul **Adaugă** pentru a aduce în carantină fişiere pe care le suspectați că sunt infectate. Se va deschide o fereastră în care puteți selecta fişierul din locația în care se află pe disc. În acest fel fişierul va fi copiat în carantină. Dacă doriți să mutați fişierul în zona de carantină selectați opțiunea **Şterge din locația originală**. O metodă mai rapidă prin care puteți adăuga fişiere în carantină este folosirea drag&drop pentru a le aduce în listă.

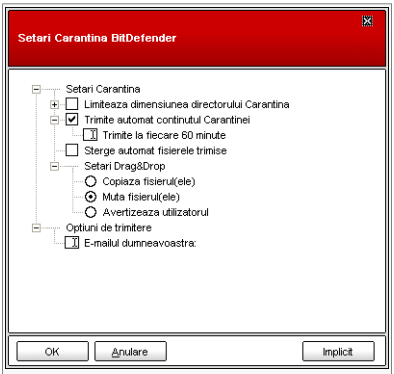
Pentru a şterge un fişier selectat din carantină faceți clic pe butonul **Şterge**. Dacă doriți să mutați fişierul selectat la locația originală faceți clic pe **Restaurează**.

Puteți trimite fişierele selectate la Laboratorul BitDefender pentru o analiză detaliată făcând clic pe **Trimite**.

Important

Înainte de a trimite fişierele trebuie să specificați anumite informații. Pentru aceasta faceți clic pe **Setări** şi completați câmpurile din secțiunea **Opțiuni de trimitere** conform indicațiilor de mai jos.

Faceți clic pe **Setări** pentru a deschide opțiunile avansate pentru zona de carantină. Va apărea următoarea fereastră:



Setări Carantină

Opțiunile carantinei sunt grupate în două categorii:

- **Setări Carantină**
- **Opțiuni de trimitere**

Notă

Faceți clic pe semnul “+” pentru a deschide o opțiune sau pe semnul “-” pentru a închide o opțiune.

Setări Carantină

- **Limitează dimensiunea directorului Carantină** - păstrează dimensiunea carantinei sub control. Această opțiune implicit activată având dimensiunea setată la 12000 KB. Dacă doriți să modificați această valoare puteți introduce valoarea dorită în câmpul corespunzător.Dacă bifați căsuța corespunzătoare opțiunii **Şterge automat fişierele vechi**, atunci când nu mai există spațiu în zona de carantină şi adăugați un nou fişier, cele maie vechi fişiere vor fi şterse automat pentru a se crea spațiul necesar introducerii de noi fişiere.
- **Trimite automat conținutul Carantinei** - trimite automat fişierele din carantină Laboratorului BitDefender pentru analiză aprofundată. Puteți seta frecventa cu care se realizează acest proces în câmpul **Trimite la fiecare x minute**.
- **Şterge automat fişierele trimise** - şterge automat fişierele din carantină după ce au fost trimise la Laboratorul BitDefender.

- **Setări Drag&Drop** - dacă folosiți metoda Drag&Drop pentru a adăuga fişiere în carantină, aici puteți specifica acțiunea pe care doriți să o realizați: copiază fişierele, muta fişierele sau avertizează utilizatorul.

Opțiuni de trimitere

- **E-mailul dumneavoastră** - introduceți adresa de e-mail dacă doriți să primiți informații despre fişierele suspecte pe care le-ați trimis la analiză.

Faceți clic pe **OK** pentru a salva modificările. Dacă faceți clic pe **Implicit** veți încărca setările implicite.

8. Modulul Antispyware

Secțiunea **Antispyware** a acestui ghid de utilizare conține următoarele subiecte:

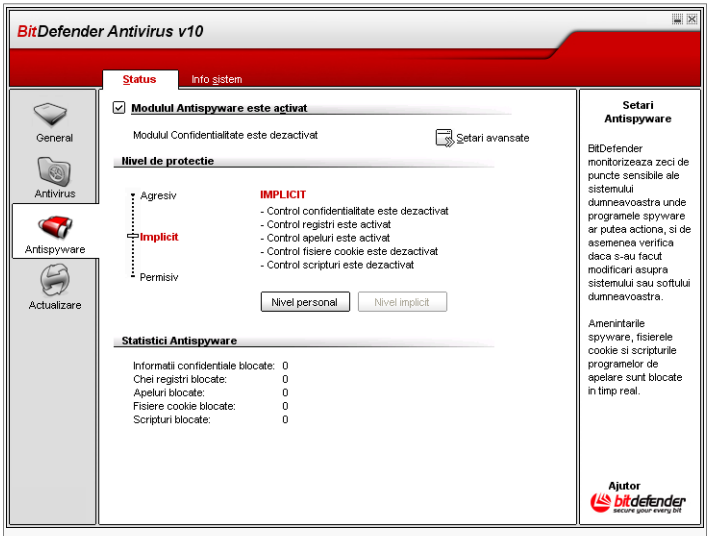
- Status Antispyware
- Setări avansate - Control confidențialitate
- Setări avansate - Control regiştri
- Setări avansate - Control apeluri
- Setări avansate - Control cookie
- Setări avansate - Control scripturi
- Informații sistem

Notă

Pentru mai multe detalii privind modulul **Antispyware** consultați "*Modulul Antispyware*" (p. 27).

8.1. Status Antispyware

Pentru a accesa această secțiune faceți clic pe tabul **Status** din modulul **Antispyware**.



Status Antispyware

În această secțiune puteți configura modulul **Antispyware comportamental** şi puteți vedea informații legate de activitatea sa.

Important

Pentru a preveni infecțiile cu programe spyware țineți activat **protecția Antispyware comportamentală**.

În partea de jos a acestei secțiuni puteți vizualiza **statisticile Antispyware**.

Modulul **Antispyware** vă protejează calculatorul împotriva aplicațiilor spyware prin cinci controale ale protecției:

- Controlul confidențialității - vă protejează datele confidențiale filtrând traficul HTTP(la ieşire) şi SMTP potrivit regulilor create de dumneavoastră în secțiunea Confidențialitate.
- Controlul regiştrilor - vă cere permisiunea de fiecare dată când un program încearcă să modifice informațiile din regiştri astfel încât să fie lansat la pornirea Windows.
- Controlul apelurilor - vă cere permisiunea de fiecare dată când un dialer încearcă să acceseze un modem de calculator.

- Controlul fişierelor cookie - vă cere permisiunea de fiecare dată când un site încearcă să seteze un cookie.
- Controlul scripturilor - vă cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ.

Pentru a configura setările pentru aceste controale faceți clic pe Setări avansate.

8.1.1. Nivel de protecție

Puteți alege nivelul de protecție adecvat nevoilor dumneavoastră de securitate. Mutați cursorul pentru a seta nivelul de protecție dorit.

Există trei nivele de protecție:

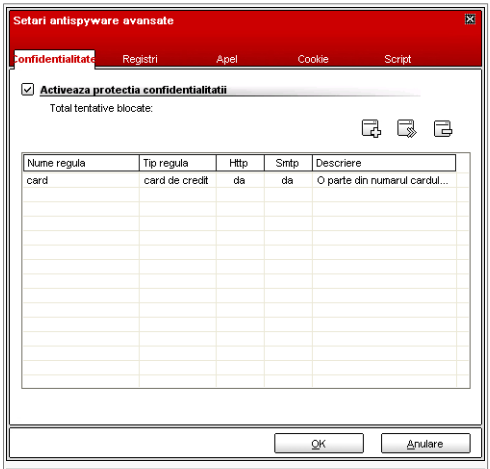
Nivel de protecție	Descriere
Permisiv	Doar **Controlul regiştrilor** este activat.
Standard	**Controlul regiştrilor** şi **Controlul apelurilor** sunt activate.
Agresiv	**Controlul regiştrilor**, **Controlul apelurilor** şi **Controlul confidențialității** sunt activate.

Puteți personaliza nivelul de protecție făcând clic pe **Nivel personal**. În fereastra care va apărea, selectați controalele Antispyware pe care doriți să le activați şi faceți clic pe **OK**.

Faceți clic pe **Nivel implicit** pentru a seta cursorul la nivelul implicit.

8.2. Setări avansate - Control confidențialitate

Pentru a accesa această secțiune faceți clic pe butonul **Setări avansate** din modulul **Antispyware**, secțiunea Status.



Control confidențialitate

Păstrarea datelor confidențiale în siguranță este o problemă importantă ce ne preocupă pe toți. Furtul de date a ținut pasul cu dezvoltarea comunicațiilor pe Internet şi se foloseşte de noi metode de a păcăli oamenii să cedeze informațiile private.

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.

Controlul confidențialității vă ajută să păstrați informațiile confidențiale în siguranță. Acesta scanează traficul HTTP sau SMTP, sau pe amândouă, în căutare de şiruri de caractere definite de dumneavoastră. Dacă este găsită o concordanță, site-ul sau mesajul respectiv este blocat.

Regulile trebuie introduse manual (faceți clic pe butonul **Adaugă** şi alegeți parametrii regulei). Va apărea asistentul de configurare.

8.2.1. Asistentul de configurare

Asistentul de configurare este o procedură constituită din trei paşi.

Pasul 1/3 - Furnizați tipul şi argumentul regulei

Furnizați tipul şi argumentul regulei

Introduceți numele regulei în câmpul editabil.

Trebuie setați parametrii următori:

- **Tip regulă** - alegeți tipul regulei (adresă, nume, card de credit, PIN, etc.).
- **Argument regulă** - introduceți argumentul regulei.

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

Faceți clic pe **Înainte**.

Pasul 2/3 - Selectați traficul

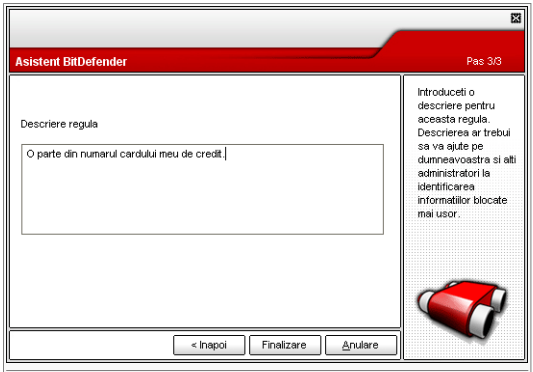
Selectați traficul

Selectați traficul pe care doriți ca BitDefender să îl scaneze. Sunt disponibile următoarele opțiuni:

- **Scanează HTTP** - scanează traficul HTTP (web) şi blochează la ieşire toate datele ce corespund unei reguli.
- **Scanează SMTP** - scanează traficul SMTP (mail) şi blochează la ieşire toate mesajele e-mail ce corespund unei reguli.

Faceți clic pe **Înainte**.

Pasul 3/3 - Descrieți regula



Descrieți regula

Introduceți o scurtă descriere a regulei în câmpul editabil.

Faceți clic pe **Finalizare**.

Puteți vedea regulile listate în tabel.

Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a dezactiva o regulă temporar, fără a o şterge, debifați căsuța corespunzătoare.

Pentru a modifica atributele unei reguli, selectați-o şi faceți clic pe butonul **Editează** sau faceți dublu-clic pe ea. Va apărea următoarea fereastră:

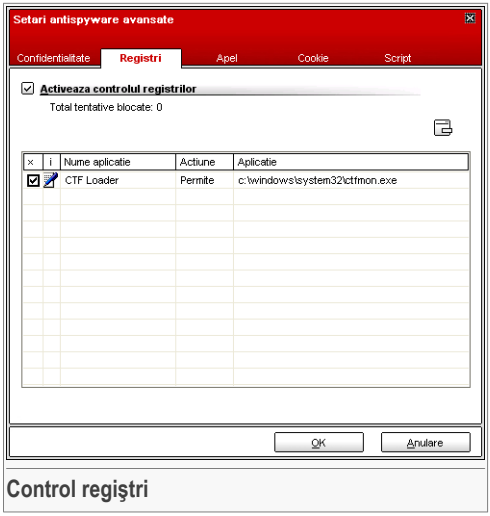
Editează regula

Aici puteți modifica numele, descrierea şi parametrii regulei (tip, argument şi trafic). Faceți clic pe **OK** pentru a salva modificările.

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

8.3. Setări avansate - Control regiştri

Pentru a accesa această secțiune deschideți fereastra **Setări antispyware avansate** (mergeți la modulul **Antispyware**, secțiunea Status şi faceți clic pe **Setări avansate**) şi faceți clic pe tabul **Regiştri**.



Control regiştri

Una dintre părțile importante ale sistemului de operare Windows sunt **regiştrii**. Aici îşi păstrează Windows configurația şi setările, programele instalate, informații despre utilizator şi alte date.

Tot în **regiştri** sunt definite programele care sunt lansate la pornirea Windows. Viruşii folosesc des această caracteristică Windows pentru a se lansa automat atunci când utilizatorul îşi reporneşte calculatorul.

Controlul Regiştrilor supraveghează regiştrii Windows – în acest fel BitDefender poate detecta troienii. BitDefender vă va alerta de fiecare dată când un program încearcă să modifice informațiile din regiştri astfel încât să fie lansat la pornirea Windows.

Alertă regiştri

Puteți interzice această modificare făcând clic pe **Nu** sau puteți să o permiteți făcând clic pe **Da**.

Dacă doriți ca BitDefender să rețină răspunsul selectați opțiunea **Reține acest răspuns**.

Notă

Răspunsurile dumneavoastră vor sta la baza listei de reguli.

Pentru a şterge o intrare în regiştri, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a dezactiva temporar o intrare în regiştri fără să o ştergeți, debifați căsuța corespunzătoare.

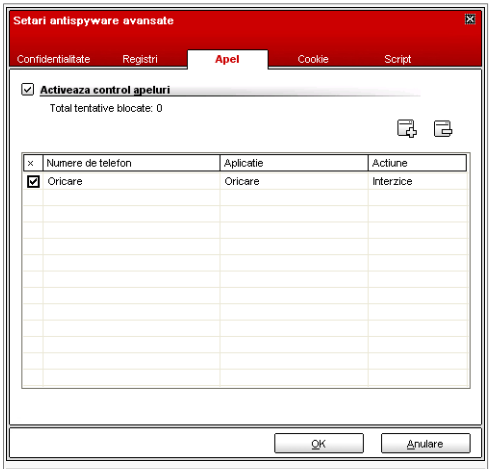
Notă

BitDefender vă va alerta atunci când instalați programe pentru care este necesară lansarea la pornirea Windows. În cele mai multe cazuri, aceste programe sunt de încredere.

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

8.4. Setări avansate - Control apeluri

Pentru a accesa această secțiune deschideți fereastra **Setări antispyware avansate** (mergeți la modulul **Antispyware**, secțiunea Status şi faceți clic pe **Setări avansate**) şi faceți clic pe tabul **Apeluri**.



Control apeluri

Dialer-ele sunt aplicații care se folosesc de modemurile calculatoarelor pentru a forma diferite numere de telefon. De obicei dialer-ele sunt folosite pentru a accesa diferite locații formând numere de telefon cu taxă foarte mare.

Controlul apelurilor vă va permite să specificați ce conexiuni la diferite numere de telefon permiteți sau blocați. Această funcție monitorizează toate dialer-ele care încearcă să acceseze un modem de calculator, alertând imediat utilizatorul şi solicitându-i să blocheze sau să permită operația:

Alertă apeluri

Puteți vedea numele aplicației şi numărul de telefon.

Selectați opțiunea **Reține acest răspuns** şi faceți clic pe **Da** sau **Nu** şi o regulă va fi creată, aplicată şi afişată în lista de reguli. Nu veți mai fi notificat când aplicația va încerca să formeze acelaşi număr de telefon.

Fiecare regulă care a fost creată poate fi accesată în secțiunea **Apel** pentru modificări ulterioare.

Important

Regulile sunt listate în ordinea priorității începând de sus, adică prima regulă are cea mai mare prioritate. Mutați regulile în sus sau în jos pentru a le schimba prioritatea.

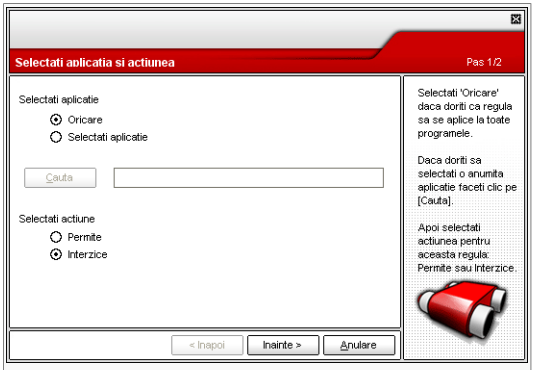
Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a modifica parametrii unei reguli, faceți dublu-clic pe câmpul corespunzător şi faceți modificările dorite. Pentru a dezactiva temporar o regulă fără a o şterge, deselectați căsuța corespunzătoare.

Regulile pot fi introduse automat (prin fereastra de alertă) sau manual (faceți clic pe butonul **Adaugă** şi selectați parametrii regulei). Va apărea asistentul de configurare.

8.4.1. Asistentul de configurare

Asistentul de configurare este o procedură constituită din doi paşi.

Pasul 1/2 - Selectați aplicația şi acțiunea



Selectați aplicația şi acțiunea

Puteți seta parametrii:

- **Aplicație** - selectați aplicația pentru regulă. Puteți alege doar o singură aplicație (faceți clic pe **Selectați aplicație**, apoi pe **Caută** şi selectați aplicația) sau toate aplicațiile (doar faceți clic pe **Oricare**).
- **Acțiune** - selectați acțiunea regulei.

Acțiune	Descriere
Permite	Acțiunea va fi permisă.
Interzice	Acțiunea va fi interzisă.

Faceți clic pe **Înainte**.

Pasul 2/2 - Selectați numerele de telefon

Selectați numerele de telefon

Faceți clic pe **Specifică număr de telefon**, introduceți numerele de telefon pentru care creați regula şi faceți clic pe **Adaugă**.

Notă

Puteți bloca si conexiunile către o întreaga gamă de numere de telefon. De exemplu: 89* înseamnă ca toate conexiunile la numerele de telefon începând cu 89 vor fi blocate.

Selectați **Oricare** dacă doriți ca această regulă să se aplice tuturor numerelor de telefon. Pentru a şterge un număr de telefon, selectați-l şi faceți clic pe **Şterge**.

Notă

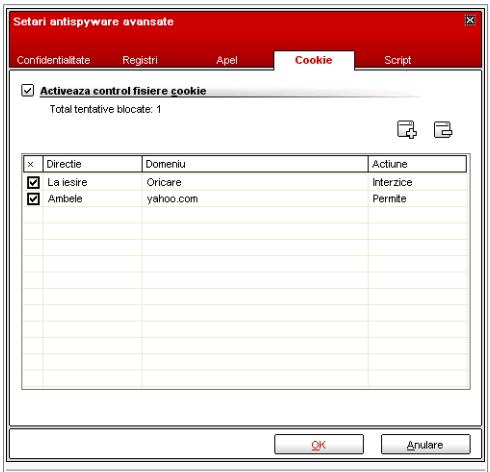
Puteți de asemenea să creați o regulă care permite unui anumit program să formeze anumite numere (cum ar fi cel al operatorului dumneavoastră de servicii Internet şi fax).

Faceți clic pe **Finalizare**.

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

8.5. Setări avansate - Control cookie

Pentru a accesa această secțiune deschideți fereastra **Setări antispyware avansate** (mergeți la modulul **Antispyware**, secțiunea Status şi faceți clic pe **Setări avansate**) şi faceți clic pe tabul **Cookie**.



Control cookie

Fişierele cookie sunt foarte comune pe Internet. Ele sunt fişiere mici salvate pe calculatorul dumneavoastră. Paginile web creează aceste fişiere pentru a vă monitoriza activitatea pe Internet şi a salva informații specifice despre dumneavoastră.

În general, fişierele cookie vă fac viața mai uşoară. De exemplu ele ajută site-urile să vă rețină numele şi preferințele, pentru a nu trebui să le introduceți la fiecare vizită.

Dar ele pot fi folosite şi pentru a vă compromite intimitatea, urmărindu-vă obiceiurile de navigare pe Internet.

Aici vă ajută **Controlul fişierelor cookie**. Când este activat, **Controlul fişierelor cookie** vă va cere permisiunea de fiecare dată când un site încearcă să seteze un cookie:

Alertă cookie

Puteți vedea numele aplicației care încearcă să trimită fişierul cookie.

Selectați opțiunea **Reține acest răspuns** şi faceți clic pe **Da** sau **Nu** şi o regulă va fi creată, aplicată şi afişată în lista de reguli. Data viitoare când vă veți conecta la acelaşi site nu veți mai fi notificat.

Aceasta vă va ajuta să alegeți paginile web în care aveți încredere şi pe cele în care nu aveți.

Notă

Din cauza numărului mare de fişiere cookie de pe Internet, **Controlul fişierelor cookie** poate fi la început. Inițial, vă va pune foarte multe întrebări despre pagini web care încearcă să seteze cookie-uri pe calculatorul dumneavoastră. După ce adăugați paginile web pe care le folosiți frecvent în lista de reguli, navigarea va deveni la fel de uşoară ca la început.

Fiecare regulă care a fost creată poate fi accesată în secțiunea **Cookie** pentru modificări ulterioare.

Important

Regulile sunt listate în ordinea priorității începând de sus, adică prima regulă are cea mai mare prioritate. Mutați regulile în sus sau în jos pentru a le schimba prioritatea.

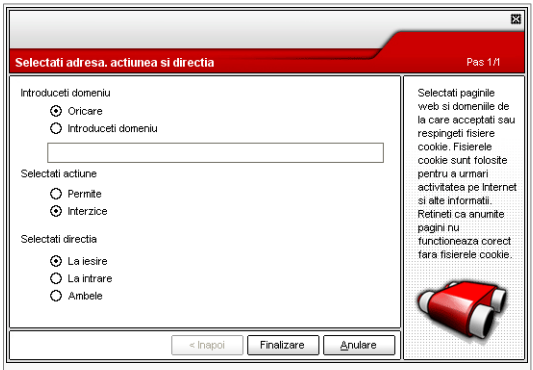
Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a modifica parametrii unei reguli, faceți dublu-clic pe câmpul corespunzător şi faceți modificările dorite. Pentru a dezactiva temporar o regulă fără a o şterge, deselectați căsuța corespunzătoare.

Regulile pot fi introduse automat (prin fereastra de alertă) sau manual (faceți clic pe butonul **Adaugă** şi selectați parametrii regulei). Va apărea asistentul de configurare.

8.5.1. Asistentul de configurare

Asistentul de configurare este o procedură constituită dintr-un singur pas.

Pasul 1/1 - Selectați adresa, acțiunea şi direcția



Selectați adresa, acțiunea şi direcția

Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulei.

Acțiune	Descriere
Permite	Fişierele cookie de la domeniul respectiv vor fi acceptate.
Interzice	Fişierele cookie de la domeniul respectiv vor fi blocate.

- **Direcție** - selectați direcția traficului.

Tip	Descriere
La ieşire	Regula se aplică fişierelor cookie trimise.
La intrare	Regula se aplică fişierelor cookie recepționate.
Ambele	Regula se va aplica în ambele direcții.

Faceți clic pe **Finalizare**.

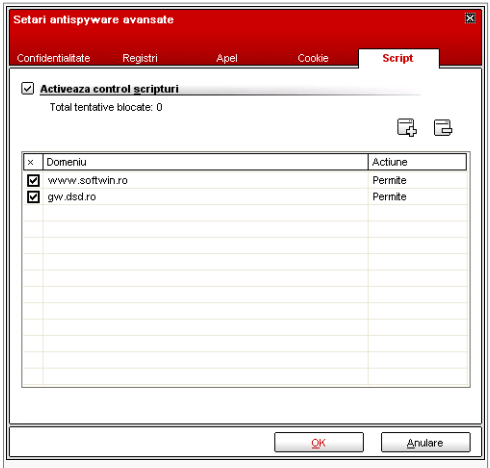
Notă

Puteți accepta fişiere cookie fără a le returna: setați acțiunea **Interzice** şi direcția **La ieşire**.

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

8.6. Setări avansate - Control scripturi

Pentru a accesa această secțiune deschideți fereastră **Setări antispyware avansate** (mergeți la modulul **Antispyware**, secțiunea Status şi faceți clic pe **Setări avansate**) şi faceți clic pe tabul **Script**.



Control scripturi

Scripturile şi alte coduri cum ar fi elementele ActiveX şi Applet-urile Java, care sunt folosite pentru a crea pagini web, pot fi programate astfel încât să aibă efecte dăunătoare. Elemente de tipul ActiveX, de exemplu, pot avea în întregime acces la datele dumneavoastră şi le pot citi sau şterge de pe calculatorul dumneavoastră, pot captura parole şi intercepta mesaje cât timp sunteți conectați la Internet. Este recomandat să acceptați conținutul activ doar de la paginile web pe care le cunoaşteți foarte bine şi care sunt de încredere.

BitDefender vă permite să alegeți să permiteți sau să blocați execuția acestor elemente.

Având **Controlul scripturilor** activat, veți monitoriza adresele web în care aveți încredere şi pe cele în care nu aveți. BitDefender vă va cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ:

Alertă script

Puteți vedea numele resursei.

Selectați opțiunea **Reține acest răspuns** şi faceți clic pe **Da** sau **Nu** şi o regulă va fi creată, aplicată şi afişată în lista de reguli. Nu veți mai fi notificați data viitoare când acelaşi domeniu încearcă să va trimită conținut activ.

Fiecare regulă care a fost creată poate fi accesată în secțiunea **Script** pentru modificări ulterioare.

Important

Regulile sunt listate în ordinea priorității începând de sus, adică prima regulă are cea mai mare prioritate. Mutați regulile în sus sau în jos pentru a le schimba prioritatea.

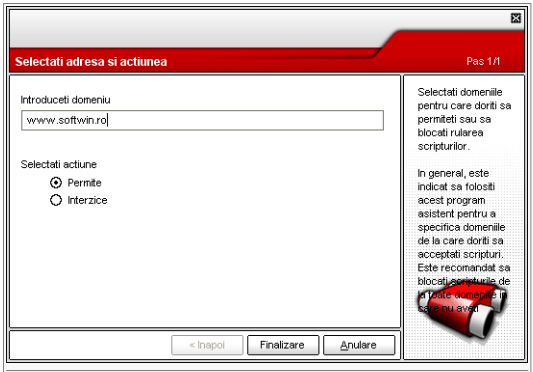
Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a modifica parametrii unei reguli, faceți dublu-clic pe câmpul corespunzător şi faceți modificările dorite. Pentru a dezactiva temporar o regulă fără a o şterge, deselectați căsuța corespunzătoare.

Regulile pot fi introduse automat (prin fereastra de alertă) sau manual (faceți clic pe butonul **Adaugă** şi selectați parametrii regulei). Va apărea asistentul de configurare.

8.6.1. Asistentul de configurare

Asistentul de configurare este o procedură constituită dintr-un singur pas.

Pasul 1/1 - Selectați adresa şi acțiunea



Selectați adresa şi acțiunea

Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulei.

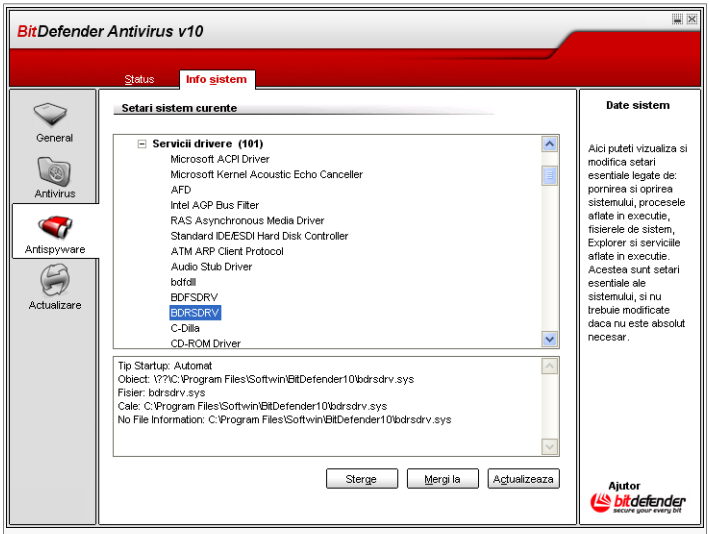
Acțiune	Descriere
Permite	Rularea scripturilor este permisă.
Interzice	Rularea scripturilor este interzisă.

Faceți clic pe **Finalizare**.

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

8.7. Informații sistem

Pentru a accesa această secțiune faceți clic pe tabul **Info sistem** din modulul **Antispyware**.



Informații sistem

Aici puteți vizualiza şi modifica importante setări ale sistemului.

Lista conține toate obiectele încărcate la pornirea sistemului precum şi obiectele încărcate de diverse aplicații.

Sunt disponibile trei butoane:

- **Şterge** - şterge obiectul selectat.
- **Mergi la** - deschide o fereastră unde obiectul selectat este plasat (de exemplu, **Regiştrii**).
- **Actualizează** - redeschide secțiunea **Info sistem**.

9. Modulul Actualizare

Secțiunea **Actualizare** a acestui ghid de utilizare conține următoarele subiecte:

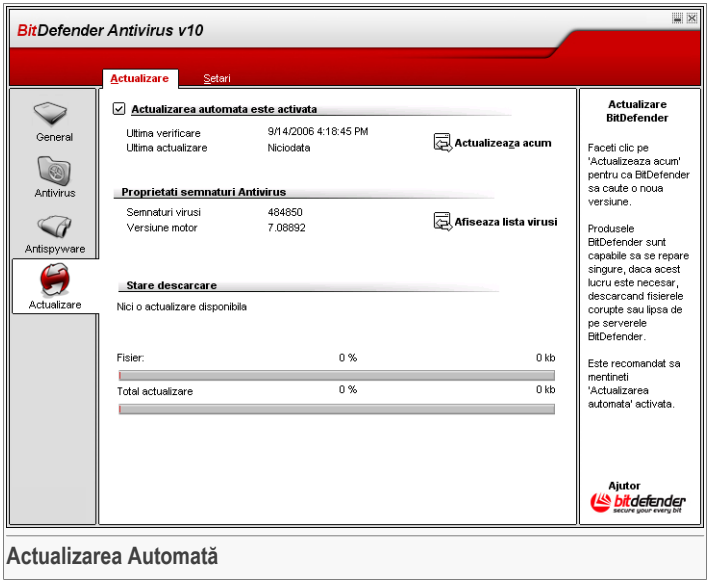
- Actualizare automată
- Actualizare manuală
- Setări actualizare

Notă

Pentru mai multe detalii privind modulul **Actualizare** consultați "*Modulul Actualizare*" (p. 28).

9.1. Actualizarea Automată

Pentru a accesa această secțiune faceți clic pe tabul **Actualizare** din modulul **Actualizare**.



Actualizarea Automată

În această secțiune puteți vedea informații legate de procesul de actualizare şi puteți actualiza produsul.

Important

Pentru a fi protejat împotriva celor mai noi amenințări, mențineți **Actualizarea automată** activată.

Dacă sunteți conectat la Internet prin bandă largă sau ADSL, BitDefender se actualizează singur. BitDefender caută noi actualizări când deschideți calculatorul şi apoi la fiecare **oră**.

Dacă o actualizare este disponibilă, în funcție de opțiunile setate în secțiunea Setări actualizare automată vi se va cere să confirmați actualizarea sau ea va fi realizată automat.

Actualizarea automată poate fi realizată oricând făcând clic pe **Actualizează acum**. Acest tip de actualizare este cunoscut şi ca **Actualizare la cererea utilizatorului**.

Modulul **Actualizare** se va conecta la serverul de actualizare BitDefender şi va verifica dacă sunt disponibile noi semnături. Dacă sunt detectate noi semnături, în funcție de opțiunile setate în secțiunea Setări actualizare la cerere, vi se va cere să confirmați actualizarea sau ea 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.

Notă

Dacă vă conectați la Internet prin dial-up, este o idee bună să faceți un obicei din a actualiza BitDefender manual.

Puteți obține semnăturile aplicațiilor malițioase deținute de produsul dumneavoastră BitDefender făcând clic pe **Afişează listă viruşi**. Va fi creat un fişier HTML care conține toate semnăturile disponibile. Faceți clic din nou pe **Afişează listă viruşi** pentru a vedea lista. Puteți căuta prin baza de date după o anumită semnătură sau puteți face clic pe **Lista de viruşi BitDefender** pentru a accesa baza de semnături online a BitDefender.

9.2. Actualizare manuală

Această metodă vă permite să instalați ultimele definiții de viruşi. Pentru a instala o actualizare de produs folosiți Actualizarea automatică.

Important

Utilizați actualizarea manuală atunci când nu poate fi realizată actualizarea automată sau când calculatorul nu este conectat la Internet.

Există două modalități de a realiza actualizarea manuală:

- Cu fişierul `weekly.exe`;
- Cu `arhive zip`.

9.2.1. Actualizarea manuală cu fişierul `weekly.exe`

Pachetul de actualizare `weekly.exe` este lansat în fiecare vineri şi include toate actualizările definițiilor de viruşi şi ale motoarelor de scanare disponibile la data lansării.

Pentru a actualiza BitDefender folosind `weekly.exe`, urmați paşii:

1. Descărcați fişierul weekly.exe şi salvați-l pe hard discul dumneavoastră.
2. Localizați fişierul descărcat şi faceți dublu-clic pe el pentru a lansa programul asistent de actualizare.
3. Faceți clic pe **Înainte**.
4. Selectați **I accept the terms in the License Agreement** şi faceți clic pe **Next**.
5. Faceți clic pe **Install**.
6. Faceți clic pe **Finalizare**.

9.2.2. Actualizarea manuală cu `arhive zip`

Există două arhive zip pe serverul de actualizare, ce conțin actualizările motoarelor de scanare şi a definițiilor de viruşi: `cumulative.zip` şi `daily.zip`.

- `cumulative.zip` este lansat în fiecare luni şi include toate actualizările motoarelor de scanare şi a definițiilor de viruşi până la data lansării.
- `daily.zip` este lansat zilnic şi include toate actualizările motoarelor de scanare şi a definițiilor de viruşi existente de la ultima arhivă cumulative lansată şi până la data curentă.

BitDefender foloseşte o arhitectură bazată pe servicii. Din această cauză, procedura de înlocuire a definițiilor de viruşi diferă în funcție de sistemul de operare:

- Windows NT-SP6, Windows 2000, Windows XP.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP

Paşi de urmat:

1. **Descărcați actualizarea potrivită.** Dacă este luni, descărcați cumulative.zip şi salvați arhiva undeva pe hard discul dumneavoastră atunci când vi se va cere acest lucru. Altfel, descărcați daily.zip şi salvați arhiva pe hard discul dumneavoastră. Dacă este prima oară când utilizați actualizarea manuală, descărcați ambele arhive.
2. **Opriți protecția antivirus BitDefender.**
   - **Ieşiți din consola de administrare.** Faceți clic-dreapta pe icoana BitDefender din Bara de sistem şi selectați **Exit**.
   - **Deschideți Servicii.** Faceți clic pe **Start**, apoi pe **Control Panel**, dublu-clic pe **Administrative Tools** şi clic pe **Services**.
   - **Opriți serviciul BitDefender Virus Shield.** Selectați serviciul **BitDefender Virus Shield** din listă şi faceți clic pe **Stop**.
   - **Opriți serviciul BitDefender Scan Server.** Selectați serviciul **BitDefender Scan Server** din listă şi faceți clic pe **Stop**.
3. **Extrageți conținutul arhivei.** Începeți cu `cumulative.zip` când ambele arhive sunt disponibile. Extrageți conținutul în directorul `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` şi acceptați înlocuirea fişierelor existente.
4. **Reporniți protecția antivirus BitDefender.**
   - **Porniți serviciul BitDefender Scan Server.** Selectați serviciul **BitDefender Scan Server** din listă şi faceți clic pe **Start**.
   - **Porniți serviciul BitDefender Virus Shield.** Selectați serviciul **BitDefender Virus Shield** din listă şi faceți clic pe **Start**.
   - **Deschideți consola de administrare BitDefender.**

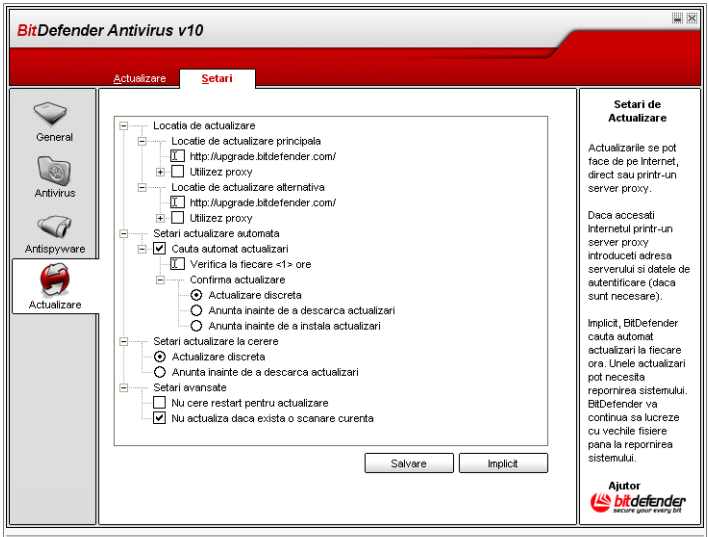
Windows 98, Windows Millennium

Paşi de urmat:

1. **Descărcați actualizarea potrivită.** Dacă este luni, descărcați cumulative.zip şi salvați arhiva undeva pe hard discul dumneavoastră atunci când vi se va cere acest lucru. Altfel, descărcați daily.zip şi salvați arhiva pe hard discul dumneavoastră. Dacă este prima oară când utilizați actualizarea manuală, descărcați ambele arhive.
2. **Extrageți conținutul arhivei.** Începeți cu `cumulative.zip` când ambele arhive sunt disponibile. Extrageți conținutul în directorul `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` şi acceptați înlocuirea fişierelor existente.
3. **Reporniți calculatorul.**

9.3. Setări actualizare

Pentru a accesa această secțiune faceți clic pe tabul **Setări** din modulul **Actualizare**.



Setări actualizare

Actualizările pot fi realizate din rețeaua locală, de pe Internet, direct sau printr-un server proxy.

Fereastra de configurare a modulului Actualizare conține patru categorii de opțiuni (**Locația de actualizare**, **Setări actualizare automată**, **Setări actualizare la cerere** şi **Setări avansate**) organizate într-un meniu expansibil, similar celor din Windows.

Notă

Faceți clic pe semnul “+” pentru a deschide o categorie sau pe “-” pentru a închide categoria.

9.3.1. Locația de actualizare

Pentru o actualizare mai sigură şi mai rapidă, puteți configura două locații de actualizare: o **Locație de actualizare principală** şi o **Locație de actualizare alternativă**. Pentru ambele este necesară configurarea următoarelor opțiuni:

- **Locația de actualizare** - Dacă sunteți conectat la o rețea care are semnăturile de viruşi BitDefender plasate local, aici puteți modifica locația de actualizare. Implicit aceasta este: http://upgrade.bitdefender.com.
- **Utilizez proxy** - În cazul în care compania foloseşte un server proxy selectați această opțiune. Următoarele informații trebuiesc specificate:
  - **Setări proxy** - introduceți adresa IP sau numele serverului proxy precum şi portul pe care îl foloseşte BitDefender pentru a se conecta la serverul proxy.

    Important
    Sintaxă: `nume:port` sau `ip:port`.

  - **Utilizator proxy** - introduceți un nume de utilizator recunoscut de proxy.

    Important
    Sintaxă: `domeniu\utilizator`.

  - **Parolă proxy** - introduceți o parolă validă pentru numele de utilizator introdus.

9.3.2. Setări actualizare automată

- **Caută actualizări automat** - BitDefender verifică automat serverele noastre în căutarea actualizărilor disponibile.
- **Verifică la fiecare x ore** - Setează intervalul la care BitDefender caută actualizări. Perioada setată implicit este de o oră.
- **Actualizare discretă** - BitDefender descarcă şi realizează actualizarea automat.
- **Anunță înainte de a descărca actualizări** - de fiecare dată când o actualizare este disponibilă, veți fi întrebat înainte de a o descărca.
- **Anunță înainte de a instala actualizări** - de fiecare dată când o actualizare a fost descărcată, veți fi întrebat înainte de a o instala.

Important
Dacă selectați **Anunță înainte de a descărca actualizări** sau **Anunță înainte de a instala actualizări** şi ieşiți din consola de administrare actualizarea automată nu va fi realizată.

9.3.3. Setări actualizare manuală

- **Actualizare discretă** - BitDefender descarcă şi realizează actualizarea automat.
- **Anunță înainte de a descărca actualizări** - de fiecare dată când o actualizare este disponibilă, veți fi întrebat înainte de a o descărca.

Important

Dacă selectați **Anunță înainte de a descărca actualizări** şi ieşiți din consola de administrare actualizarea la cerere nu va fi realizată.

9.3.4. Opțiuni avansate

- **Nu cere restart pentru actualizare** - Dacă o actualizare necesită repornirea sistemului, produsul işi va continua funcționarea folosind fişierele vechi până când utilizatorul va reporni calculatorul din proprie inițiativă. Utilizatorului nu i se va cere repornirea calculatorului şi astfel actualizarea BitDefender nu va interfera cu activitatea utilizatorului.
- **Nu actualiza dacă o scanare este în progres** - BitDefender nu se va actualiza dacă o scanare este în desfăşurare. Astfel, procesul de actualizare BitDefender nu va interfera cu sarcinile de scanare.

Notă

Dacă BitDefender este actualizat în timpul unei scanări, procesul de scanare va fi anulat.

Faceți clic pe **Salvare** pentru a salva modificările sau pe **Implicit** pentru a încărca setările standard.

Recomandări de utilizare

10. Recomandări de utilizare

Secțiunea **Recomandări de utilizare** a acestui ghid de utilizare conține următoarele subiecte:

- Cum să vă protejați calculatorul împotriva aplicațiilor malițioase
- Cum să configurați o sarcină de scanare

10.1. Cum să vă protejați calculatorul de aplicații malițioase

Urmați aceşti paşi pentru a vă proteja calculatorul de viruşi, aplicații spyware şi alte aplicații malițioase:

1. **Finalizați asistentul inițial de configurare.** În timpul procesului de instalare va apărea un asistent de configurare. Acesta vă va ajuta să înregistrați BitDefender şi să creați un cont BitDefender pentru a beneficia de suport tehnic gratuit. De asemenea, vă va ajuta să setați BitDefender să execute importante sarcini de securitate.

   Important
   Dacă dețineți un BitDefender Rescue CD, scanați-vă sistemul pentru a vă asigura că nu aveți aplicații malițioase rezidente în sistemul dumneavoastră.

2. **Actualizați BitDefender.** Dacă nu ați finalizat asistentul inițial de configurare în timpul instalării, actualizați BitDefender (mergeți la modulul **Actualizare**, secțiunea Actualizare şi faceți clic pe **Actualizează acum**).
3. **Realizați o scanare completă a sistemului.** Accesați modulul **Antivirus**, secțiunea Scut şi faceți clic pe **Scanează acum**.

   Notă
   Puteți să inițiați o scanare completă a sistemului şi din secțiunea Scanare. Selectați sarcina **Scanare completă sistem** şi faceți clic pe **Execută sarcina**.

4. **Preveniți infectarea.** În secțiunea **Scut**, mențineți protecția în timp real activată pentru a fi protejat împotriva viruşilor, a aplicațiilor spyware şi a altor aplicații malițioase. Setați nivelul de protecție dorit. Îl puteți personaliza oricând doriți, făcând clic pe **Nivel Personal**.

Important

Programați BitDefender Antivirus v10 să vă scaneze sistemul cel puțin o dată pe săptămână, planificând sarcina **Scanare completă sistem** din secțiunea Scanare.

5. **Mențineți BitDefender actualizat.** În modulul **Actualizare**, secțiunea Actualizare, mențineți **Actualizarea automată** activată pentru a fi protejat împotriva celor mai noi amenințări.
6. **Planificați o scanare completă a sistemului.** Mergeți la secțiunea **Scanare** şi programați BitDefender să vă scaneze sistemul cel puțin o dată pe săptămână planificând sarcina **Scanare completă sistem**.

10.2. Cum să configurați o sarcină de scanare

Urmați aceşti paşi pentru a crea şi configura o sarcină de scanare:

1. **Creați o sarcină nouă.** Mergeți la secțiunea Scanare şi faceți clic pe **Sarcină nouă**. Va apărea fereastra de Proprietăți.

Notă

De asemenea, puteți crea o sarcină nouă duplicând una deja existentă. Pentru a face acest lucru, faceți clic-dreapta pe o sarcină şi selectați **Duplicare** din meniu. Faceți dublu-clic pe copie pentru a deschide fereastra de **Proprietăți**.

2. **Setați nivelul de scanare.** Mergeți la secțiunea **Setări** pentru a seta nivelul de scanare. Dacă doriți, puteți personaliza setările de scanare făcând clic pe **Personalizat**.
3. **Setați ținta scanării.** Mergeți la secțiunea **Țintă** şi selectați obiectele care doriți a fi scanate.
4. **Planificați sarcina.** Dacă sarcina de scanare este complexă, ar putea fi nevoie să o programați să ruleze mai târziu, când computerul nu este utilizat. Acest lucru va spori acuratețea scanării. Mergeți la secțiunea **Planificare** pentru a planifica sarcina.

BitDefender Rescue CD

BitDefender Antivirus v10 este furnizat cu un CD de boot (bazat pe LinuxDefender) capabil a scana şi dezinfecta tot calculatorul fără a fi necesară pornirea sistemului de operare.

Este indicat să utilizaţi BitDefender Rescue CD oricând sistemul dumneavoastră de operare nu funcţionează corect din cauza infecţiei cu viruşi. Aceasta se întâmplă în general când nu folosiţi un produs antivirus.

Actualizarea definiţiilor de viruşi se face automat, fără intervenţia utilizatorului de fiecare dată când este pornit BitDefender Rescue CD.

LinuxDefender este o distribuţie Knoppix aplicată BitDefender, care integrează cea mai nouă soluţie de securitate BitDefender pentru Linux într-un CD GNU/Linux Knoppix Live, oferind o protecţie antivirus/antispam a traficului SMTP instantanee şi un antivirus pentru desktop care este capabil să scaneze şi să dezinfecteze hard discurile existente (incluzând partiţiile Windows NTFS) sau partiţii Samba/Windows remote de tip share. De asemenea, este inclusă şi o interfaţă de configuraţie bazată pe web a soluţiilor BitDefender.

11. Descriere generală

Caracteristici importante

- Protecție e-mail instantanee (Antivirus & Antispam)
- Soluții Antivirus pentru hard discul dumneavoastră
- NTFS write support (folosind Captive project)
- Dezinfectarea fişierelor infectate de pe partițiile Windows XP

11.1. Ce este KNOPPIX?

Citat din http://knopper.net/knoppix:

“ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. ”

11.2. Cerințe de sistem

Înainte de a porni LinuxDefender, trebuie să vă asigurați că sistemul dumneavoastră îndeplineşte următoarele cerințe.

Tip procesor

Procesor compatibil cu x86, minimum 166 MHz, dar nu aşteptați performanțe ridicate în acest caz. Un procesor de generație i686, la 800MHz, constituie o alegere mai bună.

Memorie RAM

Valoarea minimă acceptată este de 64MB, iar valoarea recomandată este de 128MB, pentru o performanță crescută.

CD-ROM

LinuxDefender rulează de pe un CD-ROM, de aceea sunt necesare un CD-ROM şi un BIOS capabil să-l pornească.

Conexiune Internet

Deşi LinuxDefender va rula fără conexiune Internet, procedurile de actualizare vor necesita un link HTTP activ, chiar şi printr-un server proxy. De aceea, pentru o protecție actualizată, conexiunea Internet este o CERINȚĂ.

Rezoluție grafică

Este recomandată o rezoluție de cel puțin 800x600 pentru o administrare bazată pe web.

11.3. Soft inclus

BitDefender Rescue CD include următoarele pachete soft.

- BitDefender SMTP Proxy (Antispam & Antivirus)
- BitDefender Remote Admin (configurație bazată pe web)
- BitDefender Linux Edition (motor de scanare antivirus) + Interfață GTK
- Documentatie BitDefender (format PDF & HTML)
- BitDefender Extras (design, Leaflet-uri)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Unelte pentru recuperarea datelor şi repararea sistemelor, chiar şi pentru alte sisteme de operare
- Unelte pentru analiza rețelei şi a securității pentru administratorii de rețea
- Soluția de rezervă Amanda
- thttpd
- Ethereal - analizator trafic rețea, IPTraf IP LAN Monitor
- Nessus - verificator securitate rețea
- Soluția de repartiționare, salvare şi recuperare Parted&QTParted
- Adobe Acrobat Reader
- Browserul web Mozilla Firefox

11.4. Soluțiile de securitate BitDefender pentru Linux

LinuxDefender CD include BitDefender SMTP Proxy Antivirus/Antispam pentru Linux, BitDefender Remote Admin (o interfață bazată pe web pentru configurarea BitDefender SMTP Proxy) şi motorul antivirus de scanare la cerere BitDefender Linux Edition.

11.4.1. BitDefender SMTP Proxy

BitDefender pentru servere de mail Linux - SMTP Proxy este o soluție de inspectare a securității conținutului, care oferă protecție antivirus şi antispam la nivel de gateway,

prin scanarea tot traficului de mesaje după programe virale cunoscute sau necunoscute. Ca rezultat al unei tehnologii unic brevetate, BitDefender pentru servere de mail este compatibil cu majoritatea platformelor de mail existente şi certificate "RedHat Ready".

Această soluție Antivirus şi Antispam scanează, dezinfectează şi filtrează traficul email pentru orice server de mail, indiferent de platformă sau sistem de operare. BitDefender SMTP Proxy este pornit la inițializare şi scanează toate e-mailurile care sosesc. Pentru a configura BitDefender SMTP Proxy, folosiți BitDefender Remote Admin, utilizând instrucțiunile de mai jos.

11.4.2. BitDefender Remote Admin

Puteți configura şi administra serviciile BitDefender de la distanță (după ce v-ați configurat rețeaua) sau local, urmând paşii:

1. Porniți browser-ul Firefox şi încărcați URL-ul BitDefender Remote Admin: https://localhost:8139 (sau faceți dublu-clic pe icoana BitDefender Remote Admin aflată pe desktop)
2. Identificați-vă cu numele de utilizator "bd" şi parola "bd"
3. Alegeți "SMTP Proxy" din meniul stâng
4. Setați serverul real SMTP şi portul de ascultare
5. Adaugați domeniile de mail pentru retransmitere
6. Adaugați domeniile de rețea pentru retransmitere
7. Alegeți "AntiSpam" din meniul stâng pentru a configura opțiunile antispam
8. Alegeți "AntiVirus" pentru a configura acțiunile BitDefender Antivirus (acțiunea la detectarea unui virus, locația carantinei)
9. În plus, puteți configura "Mail notifications" şi opțiunile de raport ("Logger")

11.4.3. BitDefender Linux Edition

Scanerul antivirus inclus în LinuxDefender este integrat direct în desktop. Această versiune conține şi o interfață grafică+GTK.

Doar căutați prin hard discul dumneavoastră (sau prin cele în regim share), faceți clic-dreapta pe oricare fişier sau director şi selectați "Scan with BitDefender". BitDefender Linux Edition va scana obiectele selectate şi va afişa un raport asupra situației lor. Pentru opțiuni mai detaliate urmăriți documentația BitDefender Linux Edition (în directorul BitDefender Documentation sau în manual) şi programul **/opt/BitDefender/lib/bdc**.

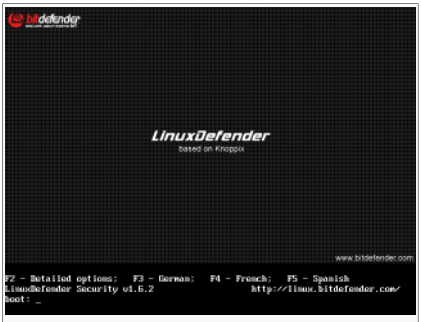
12. Recomandări de utilizare LinuxDefender

12.1. Pornire şi oprire

12.1.1. Porniți LinuxDefender

Pentru a porni cd-ul, setați BIOS-ul calculatorului dumneavoastră să demareze de pe cd, aşezați cd-ul în drive şi reporniți calculatorul. Asigurați-vă că poate fi pornit calculatorul dumneavoastră de pe cd.

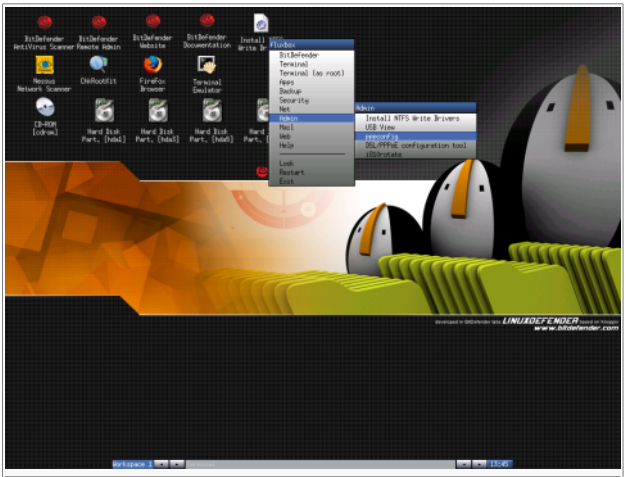
Aşteptați până apare următorul ecran şi urmați instrucțiunile pentru a porni LinuxDefender.



Ecran la pornirea sistemului

Apăsați `F2` pentru opțiuni detaliate. Apăsați `F3` pentru opțiuni detaliate în germană. Apăsați `F4` pentru opțiuni detaliate în franceză. Apăsați `F5` pentru opțiuni detaliate în Spaniolă. Pentru o pornire rapidă, cu opțiunile implicite, apăsați `ENTER`.

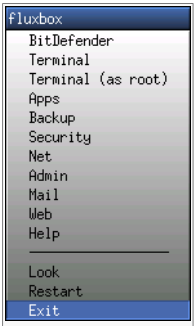
La finalizarea procesului de pornire veți vedea următorul desktop. Acum puteți începe să utilizați LinuxDefender.



Desktopul

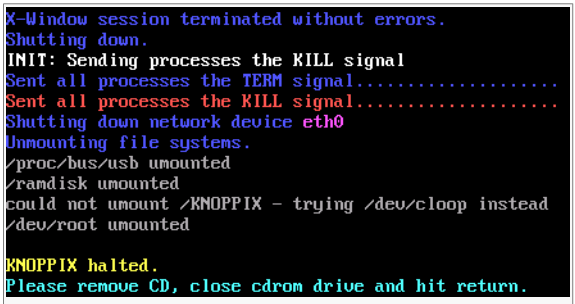
12.1.2. Opriți LinuxDefender

Pentru a ieşi în mod corect din LinuxDefender este recomandat să aduceți partițiile la starea inițială folosind comanda **umount** sau făcând clic-dreapta pe icoanele partițiilor de pe desktop şi selectând **Unmount**. Apoi puteți opri calculatorul selectând **Exit** din meniul LinuxDefender (clic-dreapta pentru a-l deschide) sau utilizând comanda **halt** pe un terminal.



Alegeți "EXIT"

Atunci când LinuxDefender a terminat de închis cu succes toate problemele va apărea un ecran ca cel din imagine. Puteți scoate cd-ul pentru a porni sistemul direct de pe hard drive. Acum puteți opri sau reporni calculatorul.



Aşteptați acest mesaj înainte de oprire

12.2. Configurarea conexiunii Internet

Dacă sunteți într-o rețea DHCP şi aveți un card de rețea ethernet, conexiunea Internet ar trebui să fie deja detectată şi configurată. Pentru configurare manuală, urmați paşii de mai jos.

1. Deschideți meniul LinuxDefender (clic-dreapta) şi selectați **Terminal** pentru a deschide o consolă.
2. Tastați **netcardconfig** în terminalul deschis pentru a deschide unealta de configurare a rețelei.
3. Dacă rețeaua dumneavoastră foloseşte DHCP, selectați **yes** (dacă nu sunteți sigur, întrebați administratorul rețelei). Altfel, priviți mai jos.
4. Conexiunea rețelei ar trebui să fie configurată automat acum. Puteți vizualiza IP-ul şi setările cardului de rețea folosind comanda **ifconfig**.
5. Dacă aveți un IP static (nu utilizați DHCP), selectați **No** la întrebarea DHCP.
6. Urmați instrucțiunile de pe ecran. Dacă nu ştiți ce să scrieți, contactați administratorul sistemului sau rețelei dumneavoastră pentru detalii.

Dacă totul merge bine, puteți testa conexiunea Internet trimițând un ping la `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Dacă aveți conexiune dial-up, alegeți **pppconfig** din meniul LinuxDefender / Admin. Apoi urmați instrucțiunile de pe ecran pentru seta o conexiune Internet prin PPP.

12.3. Actualizare BitDefender

Pachetele BitDefender pentru LinuxDefender utilizează memoria RAM a sistemului pentru fişierele de actualizare. În acest fel, puteți actualiza toate semnăturile de viruşi, motoarele de scanare sau baza de date antispam, chiar dacă rulați sistemul de pe un dispozitiv disponibil doar pentru citire(read-only), cum este LinuxDefender CD.

Asigurați-vă că aveți o conexiune Internet funcțională. Mai întâi deschideți BitDefender Remote Admin şi selectați **Live! Update** din meniul stâng. Apăsați **Update Now** pentru a verifica dacă există noi actualizări.

Ca alternativă, puteți introduce următoarea comandă pe un terminal:

```
# /opt/BitDefender/bin/bd  update
```

Toate procesele de actualizare sunt adunate într-un jurnal implicit BitDefender. Îl puteți vizualiza cu următoarea comandă:

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Dacă utilizați un proxy pentru conexiuni la ieşire, configurați setările Proxy în meniul **Live! Update**, tabul **Configuration**.

12.4. Scanare viruşi

12.4.1. Cum îmi accesez datele de pe Windows?

NTFS Write Support

NTFS write support este disponibil utilizând Captive NTFS write project. Aveți nevoie de două fişiere driver de la instalarea Windows: `ntoskrnl.exe` şi `ntfs.sys`. Momentan, doar driver-ele Windows XP sunt suportate. Puteți să le folosiți de asemenea pentru accesarea partițiilor Windows 2000/NT/2003.

Instalare drivere NTFS

Pentru a accesa partițiile NTFS şi a putea scrie pe ele, trebuie să instalați mai întâi driverele NTFS. Dacă nu folosiți NTFS pentru partițiile dumneavoastră de Windows, ci FAT, sau aveți nevoie doar de acces de tip read-only la datele dumneavoastră, puteți configura direct drive-ele şi accesa drive-ele Windows ca orice drive Linux.

Pentru a avea suportul necesar partițiilor NTFS, trebuie să instalați mai întâi driverele NTFS, de pe hard discurile dumneavoastră, alte partiții în regim share, stick-urile USB sau prin Windows Update. Este recomandat să utilizați driverele de pe o locație sigură deoarece driverele locale de pe gazda Windows pot fi deja afectate.

Faceți dublu-clic pe icoana **Install NTFS Write Drivers** de pe desktop pentru a rula **BitDefender Captive NTFS Installer**. Selectați prima opțiune dacă doriți să instalați driverele de pe hard discul local.

Dacă driverele se găsesc pe o locație obişnuită, folosiți **Quick search** pentru a găsi driverele.

Alternativ, puteți specifica unde se găsesc driverele dumneavoastră. Sau puteți descărca driverele de pe Windows Update SP1.

Driverele nu sunt instalate pe hard disc, ci sunt folosite temporar de LinuxDefender pentru a accesa partițiile Windows NTFS. Dacă programul instalează driverele NTFS, puteți face dublu-clic pe iconițele de pe desktop ale partițiilor NTFS şi căuta prin conținut. Dacă doriți un administrator de fişiere puternic, folosiți Midnight Commander din meniul LinuxDefender (sau introduceți **mc** într-o consolă).

12.4.2. Cum realizez o scanare antivirus?

Navigați printre fişiere, faceți clic-dreapta pe fişierul sau directorul dorit şi selectați **Send to**. Apoi alegeți **BitDefender Scanner**.

Sau puteți inițializa următoarea comandă de la un terminal. **BitDefender Antivirus Scanner** va începe cu fişierul sau directorul selectat ca locație implicită de scanare.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Faceți apoi clic pe **Start Scan**.

Dacă doriți să configurați opțiunile antivirus, selectați **Configure Antivirus** din tabloul stâng al programului.

12.5. Creați un filtru de mail ad-hoc

Puteți utiliza LinuxDefender pentru a crea o soluție ad-hoc de filtrare a mesajelor, fără a instala niciun soft sau a modifica serverul de mail. Ideea este de a aşeza sistemul LinuxDefender înaintea serverului dumneavoastră de mail, permițând BitDefender să scaneze după spam şi viruşi tot traficul SMTP şi să-l retransmită adevăratului server de mail.

12.5.1. Condiții esențiale

Este nevoie de un calculator personal cu un procesor compatibil cu Pentium 3 sau mai nou, având memoria RAM de cel puțin 256MB şi un drive de CD/DVD de pe care să porniți sistemul. Sistemul LinuxDefender va primi traficul SMTP în locul serverului real de mail. Sunt mai multe mijloace de a realiza acest lucru.

1. Schimbați IP-ul serverului dumneavoastră de mail şi atribuiți-l pe cel vechi sistemului LinuxDefender
2. Schimbați înregistrările DNS astfel încât intrarea MX pentru domeniile dumneavoastră să indice sistemul LinuxDefender
3. Setați clientul dumneavoastră de mail pentru a utiliza noul sistem LinuxDefender ca server SMTP
4. Schimbați setările din Firewall pentru a îndrepta / redirecționa toate conexiunile SMTP către sistemul LinuxDefender în loc serverului de mail real

În acest capitol vi se vor explica toate opțiunile de mai sus. Pentru mai multe informații puteți consulta ghidurile Linux Networking şi documentația Netfilter.

12.5.2. Filtrul de mail

Porniți cd-ul LinuxDefender şi aşteptați până sistemul X Windows este încărcat şi funcțional.

Pentru a configura BitDefender SMTP Proxy, faceți dublu-clic pe icoana **BitDefender Remote Admin** de pe desktop. Va apărea următoarea fereastră. Folosiți numele de utilizator `bd` şi parola `bd` pentru a fi identificat de BitDefender Remote Admin.

După ce v-ați identificat, veți putea configura BitDefender SMTP Proxy.

Alegeți **SMTP Proxy** pentru a configura serverul real de mail pe care doriți să-l protejați de viruşi şi spam.

Selectați **Email domains** pentru a introduce toate domeniile de la care vreți să acceptați e-mailuri.

Apăsați **Add Email Domain** sau **Add Bulk Domains** şi urmăriți instrucțiunile pentru a seta domeniile de mail redirecționate.

Selectați **Net domains** pentru a introduce toate rețelele pentru care doriți să retransmiteți mesajele.

Apăsați **Add Net Domain** sau **Add Bulk Net Domains** şi urmăriți instrucțiunile pentru a seta domeniile de rețea redirecționate.

Selectați **Antivirus** din meniul din stânga, pentru a alege acțiunea ce trebuie realizată la detectarea unui virus şi pentru configurarea altor opțiuni antivirus.

Acum, tot traficul SMTP este scanat şi filtrat de BitDefender. Implicit, toate mesajele virusate sunt dezinfectate sau şterse şi toate mesajele spam detectate de BitDefender sunt marcate `[SPAM]` în subiect. Un header de mail (`X-BitDefender-Spam: Da/Nu`) este adăugat tuturor mesajelor pentru a uşura filtrarea lor de către client.

12.6. Realizați un audit asupra securității rețelei

În afara posibilităților de a lupta împotriva programelor răuvoitoare, de a recupera datele şi a filtra poşta electronică, LinuxDefender vine cu un set de unelte care realizează un audit asupra securității gazdei şi a rețelei. De asemenea, este posibilă analiza sistemelor compromise folosind uneltele incluse în LinuxDefender. Citiți acest mic tutorial pentru a învăța cum să porniți un audit rapid asupra securității gazdelor sau rețelelor.

12.6.1. Căutați rootkituri

Înainte de a începe căutarea problemelor de securitate pe calculatoarele aflate în rețea, verificați mai întâi ca gazda LinuxDefender să nu fie compromisă. Puteți realiza o scanare după viruşi a hard discurilor instalate, aşa cum este arătat în tutorialul **Scan for viruses** sau puteți scana după rootkit-uri Unix.

Mai întâi, pregătiți toate partițiile hard discului pentru a putea fi utilizate de sistem, făcând dublu-clic pe icoanele lor de pe desktop sau utilizând comanda **mount** din consolă. Apoi faceți dublu-clic pe icoana **ChkRootKit** pentru a verifica conținutul cd-ului sau lansați comanda **chkrootkit** în consolă, folosind parametrul `-r NEWROOT` pentru a specifica directorul nou / (rădăcină) al gazdei.

```
# chkrootkit -r /dev/hda3
```

Dacă este descoperit un rootkit, chkrootkit va arăta ce a găsit folosind caractere **aldine** şi majuscule.

12.6.2. Nessus - scanerul de rețea

> Nessus este cel mai cunoscut scaner de vulnerabilitate de tip "open source" din întreaga lume, fiind folosit în peste 75 000 de organizații la nivel global. Multe dintre cele mai mari organizații ale lumii obțin reduceri de costuri semnificative folosind Nessus pentru verificarea unor dispozitive şi aplicații critice pentru afacere ale intreprinderii.
>
> *—www.nessus.org*

Nessus poate fi folosit pentru a scana de la distanță calculatoarele dumneavoastră din rețea împotriva vulnerabilităților. De asemenea, recomandă unele măsuri pentru a diminua riscurile de securitate şi a preveni incidentele.

Faceți dublu-clic pe icoana **Nessus Security Scanner** de pe desktop sau rulați de pe un terminal **startnessus**. Asteptați până apare următoarea fereastră. În funcție de resursele hardware, poate dura până la 10 minute ca Nessus să se încarce, împreună cu cele mai mult de 5000 plugin-uri conținând baza de date privind vulnerabilitățile. Folosiți numele de utilizator `knoppix` şi parola `knoppix` pentru a vă identifica.

Faceți clic pe **Target selection** şi introduceți IP-ul calculatorului sau numele gazdelor a căror vulnerabilitate vreți să o scanați. Aveți grijă să setați toate opțiunile de scanare în conformitate cu configurația sistemului sau a rețelei înainte de a începe scanarea pentru a folosi cât mai puține resurse şi pentru un rezultat cât mai precis. Faceți clic apoi pe **Start the scan**.

La finalizarea procesului de scanare, Nessus afişează rezultatele şi recomandările. Puteți salva rapoartele în diverse formate, inclusiv HTML cu diagrame. Rapoartele salvate pot fi vizualizate în browser-ul dumneavoastră favorit.

12.7. Verificați integritatea memoriei RAM a sistemului

De obicei, când un sistem are un comportament ciudat (se blochează sau se reporneşte din când în când), poate fi vorba de o problemă legată de memorie. Puteți testa modulele RAM ale sistemului dumneavoastră cu programul **memtest**, prezentat mai jos.

Porniți calculatorul şi demarați LinuxDefender de pe cd. Tastați **memtest** pornirea sistemului LinuxDefender şi apăsați Enter.

Programul Memtest va porni imediat şi va rula câteva teste pentru a verifica situația memoriei RAM. Puteți alege ce teste să rulați şi alte opțiuni ale programului Memtest apăsând `c`.

Un Memtest complet poate dura până la 8 ore, în funcție de capacitatea RAM şi viteza sistemului. Este recomandat să lăsați Memtest să ruleze toate testele pentru o verificare completă a memoriei RAM. Puteți renunța oricând apăsând `ESC`.

Dacă doriți un nou hardware (un sistem complet sau doar unele componente) este recomandat să utilizați LinuxDefender şi memtest pentru a verifica dacă sunt erori sau probleme de compatibilitate.

Obținere ajutor

13. Suport

13.1. Departamentul de suport tehnic

SOFTWIN se străduieşte să ofere clienților săi un nivel cât mai ridicat în ceea ce priveşte rapiditatea şi calitatea suportului tehnic. Centrul de suport (cu care puteți lua legătura prin adresa indicată mai jos) este actualizat continuu. Aici vă sunt oferite răspunsurile la întrebările dumneavoastră în cel mai scurt timp.

La SOFTWIN, preocuparea pentru economisirea timpului şi banilor clienților prin oferirea celor mai avansate produse la prețuri rezonabile a fost dintotdeauna o prioritate. Mai mult, considerăm că o afacere de succes se bazează pe o bună comunicare şi dedicare în suportul acordat clienților.

Sunteți binevenit oricând să cereți ajutor la <suport@bitdefender.ro>. Pentru un răspuns prompt, includeți în e-mail cât mai multe detalii despre produsul BitDefender pe care-l dețineți, despre sistemul dumneavoastră şi descrieți cât mai exact problema.

13.2. Ajutor online

13.2.1. BitDefender Knowledge Base

BitDefender Knowledge Base este o bază online de informații despre produsele BitDefender. Stochează, într-un format accesibil, rapoarte ale echipelor de suport şi dezvoltare cu privire la rezultatele suportului tehnic continuu şi ale activităților de eliminare a bug-urilor BitDefender împreună cu articole mai generale despre prevenția viruşilor, administrarea soluțiilor BitDefender şi explicații detaliate, şi multe alte articole.

BitDefender Knowledge Base este pusă la dispoziția publicului. Această multitudine de informații reprezintă încă o cale de a oferi clienților BitDefender asistența tehnică de care au nevoie. Toate cererile valide de informații sau rapoarte despre bug-uri venind de la clienții BitDefender ajung în cele din urmă în BitDefender Knowledge Base, ca rapoarte asupra eliminării bug-urilor, fişe de lucru sau articole informative pentru a suplimenta fişierele de suport ale produsului.

BitDefender Knowledge Base este disponibilă oricând la adresa http://kb.bitdefender.com.

13.3. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 10 ani SOFTWIN a câştigat o reputație indisputabilă în depăşirea aşteptărilor clienților şi partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

13.3.1. Adrese Web

Departament de vânzări: <sales@bitdefender.ro>
Suport tehnic: <suport@bitdefender.ro>
Documentație: <documentation@bitdefender.com>
Programe de Parteneriat: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Relații Media: <pr@bitdefender.com>
Cariere: <jobs@bitdefender.com>
Subscrieri viruşi: <virus_submission@bitdefender.com>
Subscrieri spam: <spam_submission@bitdefender.com>
Raportare abuz: <abuse@bitdefender.com>
Site produs: http://www.bitdefender.ro
Arhive ftp ale produsului: ftp://ftp.bitdefender.com/pub
Distribuitori locali: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

13.3.2. Filiale

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

Germany

Softwin GmbH
Sediul pentru Europa de Vest
Karlsdorferstrasse 56
88069 Tettnang
Germany
Telefon: +49 7542 9444 44
Fax: +49 7542 9444 99
Email: <info@bitdefender.com>
Vânzări: <sales@bitdefender.com>

Pagină web: http://www.bitdefender.com
Suport tehnic: <support@bitdefender.com>

Marea Britanie şi Irlanda

One Victoria Square
Birmingham
B1 1BD
Telefon: +44 207 153 9959
Fax: +44 845 130 5069
Email: <info@bitdefender.com>
Vânzări: <sales@bitdefender.com>
Pagină web: http://www.bitdefender.co.uk
Suport tehnic: <suport@bitdefender.ro>

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Suport tehnic:
Email: <support@bitdefender.com>
Servicii clienți: 954-776-6262
http://www.bitdefender.com

Romania

SOFTWIN
Str. Fabrica de Glucoză nr. 5
CP 52-93
Bucureşti
Suport tehnic: <suport@bitdefender.ro>

Vânzări: <sales@bitdefender.ro>
Telefon: +40 21 2330780
Fax: +40 21 2330763
Pagină web produs: http://www.bitdefender.ro

Vocabular

ActiveX

ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe şi sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini Web interactive care se comportă ca nişte aplicaţii şi nu ca nişte simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane şi să interacţioneze şi 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 securităţii; experţii în securitatea calculatoarelor descurajează utilizarea lui pe Internet.

Adware

Aplicaţia adware este adesea combinată cu o aplicaţie gazdă care este oferită gratuit dacă utilizatorul acceptă aplicaţia adware. Deoarece aplicaţiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licenţiere care explică scopul aplicaţiei, nu este comisă nicio infracţiune.

Totuşi, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanţele sistemului. De asemenea, informaţiile pe care unele dintre aceste aplicaţii le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licenţiere.

Arhivă

Un disc, o casetă sau un director care conţine fişiere de rezervă.

Un fişier care conţine unul sau mai multe fişiere într-un format comprimat.

Backdoor

Reprezintă o gaură de securitate realizată în mod deliberat. Motivaţia acestor "găuri" nu este întotdeauna maliţioasă: unele sisteme de operare, de exemplu, sunt puse în circulaţie cu conturi privilegiate pentru tehnicienii din service sau de responsabilii cu mentenanţă produsului din partea vânzătorului.

Sector de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului şi altele). În cazul discurilor de startup, sectorul de boot conţine un program care încarcă sistemul de operare.

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.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza şi încărca pagini de Web. Două din cele mai populare browsere sunt Mozilla Firefox şi Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afişa atât grafice cât şi text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet şi animație.

Linie de comandă

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

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 şi care este actualizat de fiecare dată când utilizatorul accesează din nou site-ul. Serverul, la fel ca şi browserul, salvează informațiile despre utilizator conținute în cookie. Aceste informații sunt stocate sub forma unui fişier text în directoarele de sistem ale browserelor Netscape şi Explorer;nu toate browserele suportă cookie. Fişierele cookie stochează informații cum ar fi numele utilizatorului şi parola, cât şi 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 fişiere cookie sunt programate cu dată de expirare, astfel încât ele vor fi şterse automat după o anumită perioadă de timp.

Drive de disc

Este un dispozitiv care citeşte date de pe un disc şi scrie date pe un disc.

Un drive de hard disc citeşte / 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).

Download

Reprezintă copierea (de obicei a unui întreg fişier) de pe o sursă principală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fişier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi şi la copierea unui fişier de pe un server de rețea pe un calculator din rețea.

E-mail

Se referă la poşta electronică. Acesta este un serviciu care transmite mesaje prin intermediul rețelei locale sau globale.

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.

Fals pozitiv

Apare atunci când un analizator detectează un fişier ca fiind infectat când de fapt acesta nu este infectat.

Extensie de fişier

Reprezintă porțiunea dintr-un nume de fişier ce urmează după caracterul punct, şi care indică tipul de date pe care le stochează fişierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fişiere. 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 fişierele text oarecare, "c" pentru fişierele sursă scrise în limbajul C, etc.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruşi noi. Această metodă de scanare nu se bazează pe semnături de viruşi cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuşi ocazional poate raporta un cod suspicios în programe normale, generând aşa-numitul "fals pozitiv".

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât şi reasamblarea pachetelor IP.

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 şi mărimea acestuia. Când este accesată o pagină web, browser-ul descarcă applet-ul de pe un server şi îl rulează pe maşina utilizatorului (clientul). Applet-urile diferă de aplicații prin aceea că sunt guvernate de un protocol de securitate strict.

Astfel că, deşi 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 priveşte scrierea şi citirea datelor.

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 şi Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente şi execută aceste macro-uri de fiecare dată când este deschis documentul.

Client de mail

Un client de mail este o aplicație care vă permite să trimiteți şi să recepționați mesaje.

Memorie

Reprezintă arii de stocare a datelor din interiorul calculatorului. Termenul de memorie desemnează locul de stocare a datelor pe chipuri şi 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 ne-euristică

Această metodă de scanare se bazează pe semnături specifice de viruşi. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus şi din acest motiv nu generează fals pozitiv.

Programe împachetate

Reprezintă un fişier în format comprimat. Multe din sistemele de operare şi aplicații conțin comenzi care vă dau posibilitatea de a împacheta un fişier astfel încât să ocupe mai putină memorie. De exemplu, să presupunem că aveți un fişier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați.

Totuşi, un program care împachetează fişiere 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.

Cale

Reprezintă direcția exactă către un fişier de pe un calculator. Această direcție este specificată utilizând sistemul ierarhic de organizare a fişierelor de sus în jos.

Ruta între două puncte, cum ar fi de exemplu canalul de comunicație între două computere.

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 şi numere de card de credit, de asigurări sociale şi de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals şi folosit pentru a fura informațiile despre utilizator.

Virus polimorf

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

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului, şi a altor dispozitive periferice.

În rețelele TCP / IP şi 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.

Fişier de raport

Reprezintă un fişier care listează acțiunile care au avut loc. BitDefender menține un fişier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fişierelor, numărul de arhive şi fişiere scanate, câte fişiere infectate şi suspecte au fost găsite.

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 şi se referea la unelte recompilate ce furnizau intruşilor drepturi administrative, permițându-le să îşi ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fişiere, loginuri şi 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 şi chiar unele aplicații ascunde fişiere critice utilizând rootkituri. Totuşi, ele sunt folosite în general pentru a ascunde aplicații malițioase sau prezența intruşilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea şi integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fişiere şi jurnale şi evita detecția.

Script

Un alt termen pentru fişiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

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 ştirea 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; totuşi, trebuie ştiut că majoritatea aplicațiilor de tip shareware şi freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet şi transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail şi chiar parole şi numere de carduri de credit.

Asemănarea dintre spyware şi un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obişnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fişiere care sunt disponibile astăzi.

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

Elemente din startup

Orice fişier 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, şi nu direct fişierul.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în taskbar-ul de Windows (situat lângă ceas) şi conține iconițe pentru accesul rapid la aplicații sistem cum ar fi cele legate de fax, imprimantă, modem, volum, şi altele. Executați dublu-clic cu mouse-ul pe o iconiță pentru a vizualiza şi accesa elementele.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul Internet şi care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware şi sisteme de operare

diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât şi convenţii folosite în conectarea reţelelor şi rutării traficului.

Troian

Este un program distructiv care este mascat sub forma unei aplicaţii benigne. Spre deosebire de viruşi, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascaţi troieni este acela care pretinde că elimină viruşii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruşi pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă duşmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul oraşului lor, din interiorul calului ies o mulţime de soldaţi greci, care deschid porţile cetăţii, permiţându-le celorlalţi soldaţi greci să pătrundă în oraş şi să captureze Troia.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiaşi produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteţi instala actualizarea.

BitDefender dispune de modulul său propriu care realizează actualizarea automatică sau manuală.

Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără ştirea dumneavoastră şi rulează independent de voinţa dumneavoastră. Cea mai mare parte a viruşilor se pot şi înmulţi. Toţi viruşii informatici sunt creaţi de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar şi un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus şi mai periculos este acela care este capabil să se răspândească în reţea şi poate să treacă de sistemele de securitate.

Semnătură de virus

Reprezintă tiparul binar al unui virus, utilizat de un program antivirus pentru detecţia şi eliminarea virusului.

Vierme

Reprezintă un program care se autopropagă în interiorul unei reţele, reproducându-se pe măsură ce se răspândeşte. Nu se poate ataşa la alte programe.