

# bitdefender® CLIENT SECURITY

## BAZA SECURITĂȚII INFORMATICE

Cerințele de securitate informatică trebuie să fie aceleași pentru toate companiile, indiferent de mărimea acestora. Protejarea proprietății intelectuale și securizarea datelor despre clienți sunt decizii de business inspirate. Totodată, trebuie punctat că infectarea rețelei informatice cu virusi poate duce la scăderea eficienței operaționale și a productivității, ceea ce poate însemna falimentul unei companii de mici dimensiuni.

## SOLUȚIILE ANTIVIRUS DE BAZĂ NU SUNT DE AJUNS

Amenințările informatice evoluează, pentru a "păcăli" bariere organizaționale de securitate. Soluțiile antivirus reprezintă doar baza unei politici de securitate sănătoase, și nu o variantă completă de apărare împotriva codurilor periculoase. Între amenințările ce pot întrerupe activitatea organizației dumneavoastră se numără:



**Virusii:** pot fi transmiși prin infectarea fișierelor executabile, ascunși în arhive sau având forma unor micro-uri în documente aparent legitime. Printre efectele lor regăsim ștergerea de fișiere, a hard disk-ului sau criptarea datelor.



**Adware/Spyware:** aproape la fel de periculoase ca virusii, programele spion sunt greu de identificat și îndepărtat. Urmările infectării cu programe spyware sunt: scurgerea de informații din organizație către exterior, încetinirea stației de lucru, instalarea de software nesolicitat sau redirecționarea activității browser-ului de Internet. Stațiile grav infectate pot necesita reinstalarea completă a sistemului de operare, irosind resurse IT și timp.



**Viermii:** sunt programe ce se automultiplică, folosind rețeaua informatică pentru a se propaga. Viermii încetinesc rețele și infectează sisteme de operare. Ei pot șterge sau cripta fișiere, trimite mailuri neautorizate, instala de backdoor-uri și troieni.



**Troienii și rootkit-urile:** sunt programe ce par legitime, care urmăresc permiterea accesului de la distanță pe o stație de lucru. După instalarea unui troian sau rootkit, un potențial atacator poate să acceseze computerul dumneavoastră, furând date confidențiale. Detectarea și prevenirea manuală a acestor amenințări poate dura mult timp și poate conduce la reinstalarea sistemului de operare, dacă identificarea și îndepărtarea lor se face necorespunzător.



**Spam și Phishing:** mesajele comerciale distribuite cu ajutorul poștei electronice sunt deranjante. Ele ajung să consume foarte mult din timpul dumneavoastră dacă nu sunt gestionate corespunzător. Unele mesaje spam sau tentative de fraudare conțin programe malware ca atașament sau link-uri către site-uri ce vă pot solicita date având caracter personal. Phishing-ul folosește tehnici asemănătoare, trimițând utilizatorul către site-uri ce par a fi legitime, în încercarea de a colecta date personale despre acesta (informații despre cartea sa de credit ori despre contul bancar). Companiile pot fi fraudate prin instalarea nesolicitată de keylogger-e (în vederea identificării parolelor de acces în rețea) și culegerea de informații vitale.

Programele malware pot afecta întreaga dumneavoastră organizație. Cel mai "încercat" de efectele post-infectare este departamentul IT. Administratorii IT care știu ce înseamnă îndepărtarea unui vierme sau virus ce s-a propagat rapid într-un număr mare de stații de lucru sunt conștienți de faptul că o astfel de activitate le va consuma foarte mult timp. Din păcate, o astfel de situație are prioritate în fața altora, în caz contrar putându-se înregistra pierderi de proporții în ceea ce înseamnă date vitale.

## PROTEJAȚI-VĂ STAȚIILE DE LUCRU CU BITDEFENDER

Pentru a contracara pierderea de date și productivitatea scăzută în cadrul companiei dumneavoastră trebuie să apelați la protecție proactivă. Organizațiile își pot proteja în mod real stațiile de lucru de posibile amenințări, folosindu-se de capacitatea produselor Bitdefender de a detecta și preveni atacuri din partea virusilor noi sau cunoscuți, dar și de a coordona și respecta politica de securitate a companiilor utilizând cât mai puține resurse IT cu putință.



## PRINCIPALELE CARACTERISTICI ȘI BENEFICII

- Tehnologia de detectare, dezinfectare și trimitere în carantină a virusilor, programelor spion de tip adware, spyware, troienilor și rootkit-urilor recunoscute și premiate internațional
- Programarea scanării imediate sau la cerere pentru a evalua starea sistemului
- Scanare optimizată prin amprentarea fișierelor, o dată pe sesiune și reluarea procesului la debutul altei sesiuni, după efectuarea unei actualizări sau după o eventuală infectare a sistemului
- Izolarea fișierelor infectate sau suspecte în vederea minimizării daunelor și analizării în siguranță a stării sistemului
- Management și configurare respectând politica de securitate a companiei
- Protecție firewall individuală pentru utilizatorii de la distanță și cei mobili
- Protecție antispam la nivelul sistemului și actualizarea constantă a filtrului Bayesian și a whitelist-urilor/blacklist-urilor, astfel încât noile tipuri de spam să fie identificate
- Filtrare adaptabilă, pe bază de conținut, pentru identificarea datelor vitale și reducerea scurgerii acestora
- Reducerea costurilor de administrare a rețelei IT și administrarea centralizată a clienților printr-o consolă principală
- Configurarea, evaluarea, instalarea sistemului și ștergerea aplicațiilor inutile de la distanță, la nivelul oricărui client și server din rețea.

## TEHNOLOGII BITDEFENDER:

**b-have** Produsele BitDefender conțin B-HAVE. Aceasta este o tehnologie în curs de înregistrare ce analizează comportamentul codurilor potențial periculoase într-un mediu virtual. B-HAVE elimină răspunsurile fals pozitive și crește simțitor rata de detecție a programelor malware noi sau cunoscute.

**NeuNet** Pentru a contracara mai bine noile modalități de transmitere ale mesajelor spam, BitDefender Lab a creat un filtru antispam deosebit de eficient, denumit NeuNet. Produsul este pretestat pe mesaje spam pentru a învăța să recunoască noile tipuri de spam identificând similaritățile dintre acestea și mesajele cîiite deja.

## CERINȚE DE SISTEM

BitDefender Client Security conține două componente de bază: Business Client for Windows și Management Agent.

## BitDefender Business Client for Windows

**Procesor:** procesor compatibil Intel Pentium de minim 800 MHz

**Memorie RAM:**

- minim 256 MB de RAM pentru Windows 2000, Windows XP
- minim 512 MB de RAM pentru Window Vista, Windows 7

**Spațiu minim pe disc:** 200MB (400MB pentru instalare)

**Sistem de operare:**

- Windows 2000 Professional + SP 4 și Update Rollup 1 v. 2
- Windows XP cu Service Pack 2
- Windows Vista
- Windows 7

## BitDefender Management Agent

**Procesor**

- Procesor compatibil Intel Pentium

**Memorie RAM:**

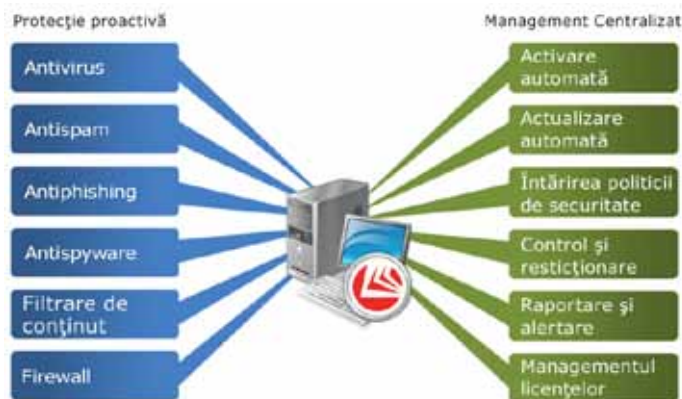
- minim 256 MB de RAM pentru Windows 2000, Windows XP, Windows 2003
- minim 512 MB de RAM pentru Windows Vista, Windows 2008, Window 7

**Spațiu minim pe disc:** 100MB

**Sistem de operare:**

- Windows 2000 Professional + SP 4 și Update Rollup 1 v. 2
- Windows 2000 Server cu Service Pack 4
- Windows XP cu Service Pack 2
- Windows Server 2003 cu Service Pack 2
- Windows Vista, Windows 2008 Server
- Windows 7
- Linux 2.4.x sau 2.6.x cu glibc 2.3.1 sau mai recent și libstdc++5 de la gcc 3.2.2 sau mai recent

Toate mărcile și denumirile de produse la care se face referire sunt mărci înregistrate ale companiilor proprietare. Toate drepturile asupra acestui document aparțin © 2010 BitDefender.



BitDefender Client Security oferă multiple niveluri de protecție și funcționalitate

## DETECȚIE PROACTIVĂ, INOVATIVĂ

Multipremiatele motoare de scanare BitDefender au fost recunoscute de organisme internaționale de certificare precum ICSA Labs, Virus Bulletin sau West Coast Labs pentru capacitatea lor de a oferi protecție împotriva programelor malware. Ele furnizează multiple niveluri de protecție precum: Antivirus, Antispam, Antispyware, Antiphishing, filtrare de conținut, detectarea troienilor, rootkit-urilor și Firewall.



## SCANARE AMĂNUNȚITĂ ȘI MANAGEMENT

BitDefender Client Security oferă numeroase posibilități de scanare în vederea detectării codurilor periculoase, astfel încât să protejeze integritatea tuturor stațiilor de lucru din rețeaua dumneavoastră

**La accesarea fișierului** - scanarea în timp real detectează virușii chiar în momentul în care utilizatorul adaugă sau extrage un document dintr-o librărie de documente.

**La cerere** - permite programarea scanării sistemului în afara orelor în care acesta este solicitat la maxim, pentru a evita încărcarea sa ori o eventuală cădere.

**Configurarea scanărilor programate** - permite planificarea scanării punctuale sau actualizării sarcinilor, evitând supraîncărcarea serverului sau o eventuală cădere a sistemului în timpul orelor de vârf.

**Trimiterea în carantină a fișierelor infectate sau suspecte** - fișierele suspecte sunt izolate în carantină. Ele pot fi curățate, ținute în carantină pentru a fi analizate, trimise în locația originală după ce au fost validate sau trimise direct către BitDefender Antivirus Lab pentru evaluare.

## ACTUALIZĂRI AUTOMATE

Baza de date ce conține semnături de viruși este actualizată din oră în oră. Astfel, produsele BitDefender pot fi și ele actualizate de la distanță în mod constant, protejând rețeaua dumneavoastră de ultimile amenințări informatice

## INTEGRARE ÎN PLATFORMA DE MANAGEMENT CENTRALIZAT BITDEFENDER

Un număr mare de stații de lucru poate fi rapid și ușor de administrat cu ajutorul platformei de management centralizat BitDefender, dând astfel posibilitatea administratorilor IT să verifice întreaga rețea atunci când aceasta este amenințată de viruși. BitDefender Management Server reprezintă un punct central din care se pot administra toate produsele dedicate clienților, serverelor și gateway-urilor active din cadrul organizației. În acest fel, administratorii IT sunt alertați în legătură cu eficiența scanării, gradul de infectare al rețelei sau stadiul proceselor de actualizare ale produselor.

## PROTECȚIE RIGUROASĂ

BitDefender Client Security este parte integrantă a unei game complete de soluții ce oferă protecție întregii dumneavoastră rețele informatice, de la nivel de gateway, până la stațiile de lucru. Tehnologia proactivă BitDefender, compatibilă cu cele mai importante sisteme de operare, detectează și oprește virușii, programele spion, programele de tip adware și troienii ce pot amenința integritatea rețelei dumneavoastră informatice.