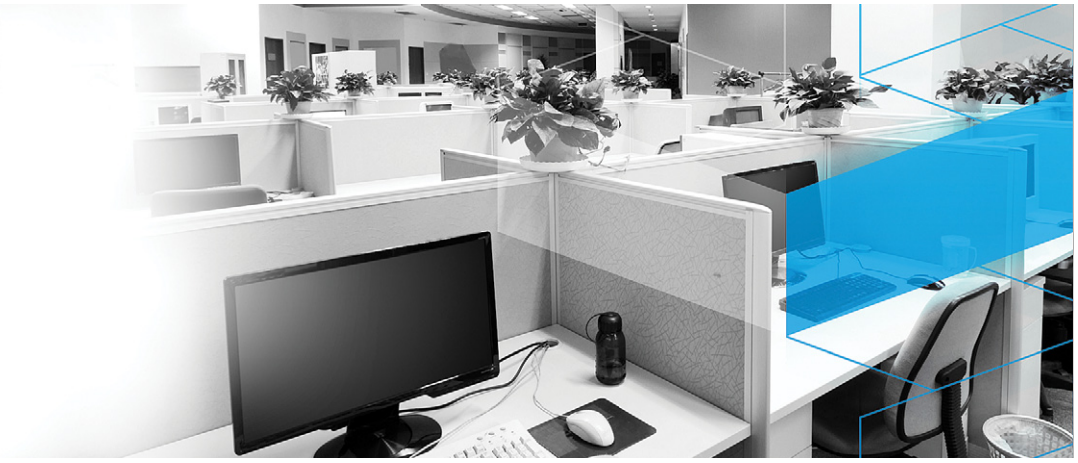
BITDEFENDER CLIENT SECURITY



BAZA SECURITĂȚII INFORMATICE

Cerințele în materie de securitate informatică ar trebui să fie aceleași pentru orice companie, indiferent de mărimea sau vechimea acesteia. Două principii de securitate importante sunt protejarea drepturilor de proprietate intelectuală ale companiei și securizarea datelor despre clienți. Infectarea rețelei informatice a companiei poate conduce la scăderea eficienței operaționale și a productivității. Aceste efecte nedorite pot afecta grav evoluția unei companii mici, având drept efect minor îngreunarea dezvoltării acesteia.

SOLUȚIILE ANTIVIRUS NU MAI SUNT DE AJUNS

Amenințările informatice evoluează constant în încercarea de a „păcăli" barierele de securitate ale companiei dumneavoastră. Soluțiile antivirus reprezintă baza unei politici de securitate sănătoase. Din păcate, ele nu mai reprezintă o variantă completă de apărare împotriva codurilor periculoase. Printre amenințările ce pot întrerupe activitatea organizației dumneavoastră se numără:

Virușii: Se pot propaga infectând fișierele executabile sau ascunzându-se în interiorul arhivelor sau a macro-urilor din documente legitime. Printre urmările infectării cu viruși se numără ștergerea de fișiere, criptarea de date sau ștergerea datelor de pe hard disc etc.

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

Viermi: Sunt programe ce se multiplică singure și care folosesc rețeaua dumneavoastră informatică pentru a se propaga, încetinind rețelele și infectând sistemele de operare, profitând de vulnerabilitățile sistemului și ale aplicațiilor. Efectele adverse pot include ștergerea sau criptarea fișierelor, trimiterea neautorizată de documente prin intermediul poștei electronice, instalarea de backdoor-uri, zombi și troieni.

Troienii și Rootkit-urile: programe care par a fi legitime, dar care permit accesarea de la distanță a calculatorului. Odată ce a fost instalat un troian sau un rootkit, un atacator poate să acceseze respectivul calculator de la distanță si să fure datele confidențiale stocate în sistem. Detecția și prevenția manuală a acestui tip de amenințări pot fi operații consumatoare de timp și pot duce la necesitatea reinstalării complete a sistemului dacă sunt realizate în mod necorespunzător.

Spam și Phishing în cazul poștei electronice: mesajele comerciale nesolicitate primite prin e-mail sunt extrem de deranjante. Mesajele nesolicitate de tip spam ajung să consume foarte mult din timpul dumneavoastră dacă nu sunt gestionate corespunzător. Unele mesaje spam sau tentative de fraudare de tip phishing conțin programe malware ca atașament sau link-uri către site-uri ce vă pot solicita date având caracter personal și pot compromite sistemul dacă sunt executate. 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 cardul de credit ori despre contul bancar). Companiile pot fi fraudate prin instalarea nesolicitată de keylogger-e și culegerea de informații vitale confidențiale.

Programele malware pot afecta viața întregii dumneavoastră organizații. Totuși, cel mai „încercat" de efectele post-infectare este departamentul IT. Administratorii IT care s-au confruntat și știu ce înseamnă îndepărtarea unui vierme sau virus ce s-a propagat cu rapiditate într-un număr mare de stații de lucru sunt conștienți de faptul că o astfel de activitate le va lua foarte mult timp. Din păcate, o astfel de situație trebuie rezolvată cu rapiditate și are prioritate în fața altora, pentru a limita pierderile de date și pentru a restabili eficiența operațiunilor.

PRINCIPALELE CARACTERISTICI ȘI BENEFICII

- Tehnologie premiată de detectare, trimitere în carantină și dezinfectare a virușilor recunoscută și premiată internațional
- Programare flexibilă a scanării imediate sau la cerere pentru a evalua gradul de infectare al sistemului
- Scanare optimizată prin amprentarea fișierelor. Fiecare fișier este scanat o singură dată în timpul aceleiași sesiuni, procesul fiind reluat la începutul unei noi sesiuni, după efectuarea unei actualizări sau dacă sistemul a fost infectat.
- Izolează fișierele infectate sau suspecte în carantină, pentru limitarea daunelor și analiză ulterioară în condiții de siguranță
- Configurare și management pe bază de politici de securitate
- Protecție firewall individuală pentru utilizatorii de la distanță și ocazionali
- Scanare a mediilor de stocare amovibile și politici de control al accesului
- Protecție antispam la nivelul sistemului prin actualizarea constantă a listelor albe/negre și prin folosirea motorului de învățare Bayesian, pentru identificarea noilor tipuri de spam care trec de filtrele tradiționale
- Filtrare adaptabilă, pe bază de conținut, pentru identificarea și evitarea transmiterii de date cu caracter personal
- Securitate folosind profil cu acces restricționat la interfață și dezinstalare protejată prin parolă
- Reducerea costurilor legate de administrarea rețelei IT și administrarea centralizată a clienților prin intermediul unei console principale
- Asigură configurarea, evaluarea, instalarea sistemului și ștergerea aplicațiilor de la distanță, la nivelul oricărui client sau server din rețea.

bitdefender

TEHNOLOGII BITDEFENDER:

AVC BitDefender Active Virus Control constituie o tehnologie de depistare inovatoare proactivă ce folosește metode euristice avansate pentru a detecta potențiale amenințări în timp real. Monitorizează fiecare program ce rulează pe calculatorul dvs. și sesizează activitățile de tip malware în timpul executării. În cazul în care sunt depistate suficiente astfel de activități, programul care le-a efectuat este declarat periculos.

b-have Toate produsele BitDefender conțin B-HAVE. Aceasta este o tehnologie în curs de brevetare 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 necunoscute.

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. Acest produs este pretestat pe o serie de mesaje spam astfel încât să învețe să recunoască noile tipuri de spam identificând similaritățile dintre acestea și mesajele citite deja.

CERINȚE DE SISTEM

Soluția BitDefender Client Security cuprinde componente de management centralizat pe server și de protecție a stației de lucru pe partea dedicată clienților. Aceasta din urmă cuprinde două componente: BitDefender Business Client, destinat protecției și controlului stațiilor de lucru Windows, și BitDefender Agent, destinat activării managementului centralizat. Aceste componente se implementează pe calculatoarele-client cu ajutorul platformei de management centralizat BitDefender.

BitDefender Business Client și Management Agent

Procesor compatibil Intel Pentium:

- 500 MHz pentru Windows 2000
- 800 MHz pentru Windows XP
- 1 GB pentru Windows Vista și Windows 7

Memorie RAM:

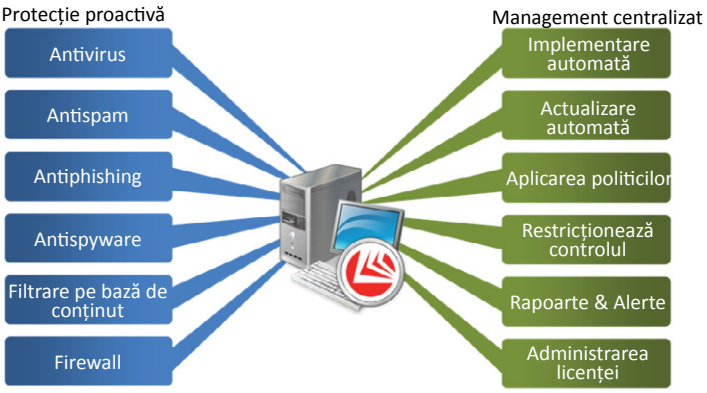
- 512 MB pentru Windows 2000, Windows XP
- 1 GB pentru Windows Vista și Windows 7

Spațiu minim pe disc:

- 300MB (400MB pentru instalare)

Sistem de operare:

- **Business Client și Management Agent** pentru Windows 7, Windows Vista SP1, Windows XP (SP2), Windows Home Server, Windows 2000 Professional (SP4 Rollup 1 v2)
- **Management Agent** de asemenea pentru Windows 2008 / 2008 SBS / 2008 R2, Windows Server 2003 (SP2), Windows 2000 Server (SP4 Rollup 1 v2), Mac OS X 10.4.6 sau o versiune mai recentă, Linux 2.4.x sau 2.6.x cu glibc 2.3.1 sau o versiune mai recentă și libstdc++5 de la gcc 3.2.2 sau o versiune mai recentă



BitDefender Client Security oferă mai multe niveluri de protecție și funcția de management al clienților

DETECȚIE PROACTIVĂ, INOVATIVĂ

Premiate în nenumărate rânduri, motoarele de scanare BitDefender au fost recunoscute de organisme internaționale de certificare precum ICSA Labs, Virus Bulletin și West Coast Labs pentru capacitatea lor de a oferi protecție proactivă fără egal împotriva programelor malware.

BitDefender Client Security asigură niveluri multiple de protecție avansată: antivirus, antispam, antispyware, antiphishing, filtrare conținut, detecție troieni / rootkit și un firewall personal complet. Toate caracteristicile sunt configurabile de la distanță, incluzând politici de securitate avansate destinate controlului accesului utilizatorilor la medii externe portabile, aplicații locale sau limite de timp pentru utilizarea internetului.

CONFIGURARE ȘI MANAGEMENT AL SCANĂRII AMĂNUNȚITE

BitDefender Client Security oferă numeroase posibilități de scanare în vederea detectării codurilor periculoase pentru a proteja integritatea laptop-urilor și a tuturor stațiilor de lucru din rețeaua dumneavoastră. Diferitele opțiuni de scanare ajută la menținerea integrității sistemului, minimizând în același timp impactul asupra utilizatorului.

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

Caracteristicile scanării la cerere permit programarea scanării în afara orelor de lucru de vârf pentru a nu afecta performanța sau disponibilitatea sistemului.

Configurarea scanărilor programate permite planificarea activităților de securitate, cum ar fi scanarea punctuală sau actualizarea sarcinilor, evitându-se, astfel, suprasolicitarea serverului sau o eventuală cădere a sistemului în timpul programului de lucru.

Trimiterea în carantină a fișierelor infectate sau suspecte fișierele suspecte sunt izolate în zone de carantină. Acestea pot fi dezinfectate, ținute în carantină pentru analiză, trimise în locația inițială, după validare, sau direct către BitDefender Antivirus Lab, pentru evaluare.

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 și să protejeze proactiv resursele rețelei. 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.

vb 100 VIRUS virusbtn.com

Compatible with Windows 7

bitdefender

PENTRU INFORMAȚII SUPLIMENTARE: WWW.BITDEFENDER.COM/BUSINESS