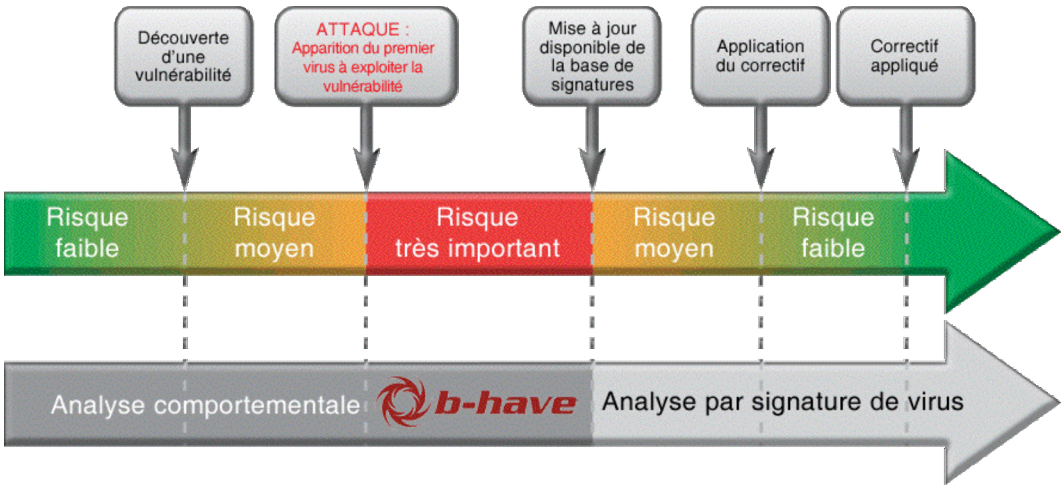
Pourquoi choisir les solutions de protection BitDefender ?

Des technologies innovantes 100% propriétaires

Acteur européen incontournable de la sécurité informatique depuis 10 ans, BitDefender concentre particulièrement ses efforts de développement sur les technologies proactives contre les codes encore inconnus et la protection contre les attaques de type « Zero-Day », une démarche primée par la Commission Européenne pour l'Innovation Technologique (IST Prize).
BitDefender développe 100% des technologies utilisées dans ses produits, assurant ainsi sa réactivité face à l'évolution des menaces, une intégration parfaite des technologies et l'optimisation de leur prise de ressources.

1. Détection proactive des programmes malveillants avec B-HAVE

B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) émule un ordinateur virtuel interne sur l'ordinateur, exécutant des fragments de programme pour rechercher un comportement signalant un logiciel malveillant. Cette technologie BitDefender brevetée représente une nouvelle couche de sécurité qui préserve le système d'exploitation des virus inconnus en détectant des bouts de code malveillants n'ayant pas encore fait l'objet de publication de signatures.
Contrairement aux autres logiciels d'analyse comportementale, la technologie B-HAVE de BitDefender traite non seulement les fichiers auxquels accède l'utilisateur (à l'accès), mais aussi les fichiers analysés manuellement (sur demande).
Avec d'autres logiciels d'étude comportementale, l'utilisateur n'est protégé contre les virus inconnus que lorsqu'il ouvre et exécute le fichier infecté, ce qui signifie que le système subit un certain degré d'infection. Etant donné que l'analyse basée sur B-HAVE est réalisée dans un environnement virtuel, le risque d'infection est pratiquement nul.
L'intérêt incontestable de B-HAVE a été confirmé par l'équipe indépendante allemande de recherche antivirus AV-Test (www.av-test.org), qui a fait apparaître que BitDefender était capable de détecter six variantes sur six du virus Zotob sans nécessiter de mise à jour des signatures.
L'efficacité de B-HAVE a été une nouvelle fois confirmée lors d'un test rétrospectif/proactif (mai 2006) mené par l'organisme de test indépendant www.av-comparatives.org, dans lequel les moteurs d'analyse antivirus BitDefender ont obtenu le plus haut niveau de certification : advanced+.



Fenêtre de vulnérabilité à l'apparition d'une nouvelle menace virale

Pour en savoir plus, télécharger le document B-HAVE, la route du succès.

B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) combine différentes techniques pour détecter les codes malveillants de manière proactive. B-Have se base sur :

- L'heuristique comportementale,
- Des procédures de détection générique,
- Une machine virtuelle pour les VB scripts,
- Une machine virtuelle pour les scripts BAT/CMD,
- L'émulateur VB script,
- Une machine virtuelle pour les fichiers exécutables (PE, MZ, COM, SYS, Boot Images).

La technologie B-HAVE agit également en tant que «multiplicateur de force» pour les lignes de défenses plus traditionnelles. Par exemple, les fichiers émanant de l'environnement virtuel B-HAVE (composants OLE, exécutables) sont ensuite filtrés par les autres modules, et même de manière récursive (ils peuvent alors être retournés au module B-HAVE pour une seconde opinion ou bien ils sont dirigés directement vers les filtres heuristiques classiques).

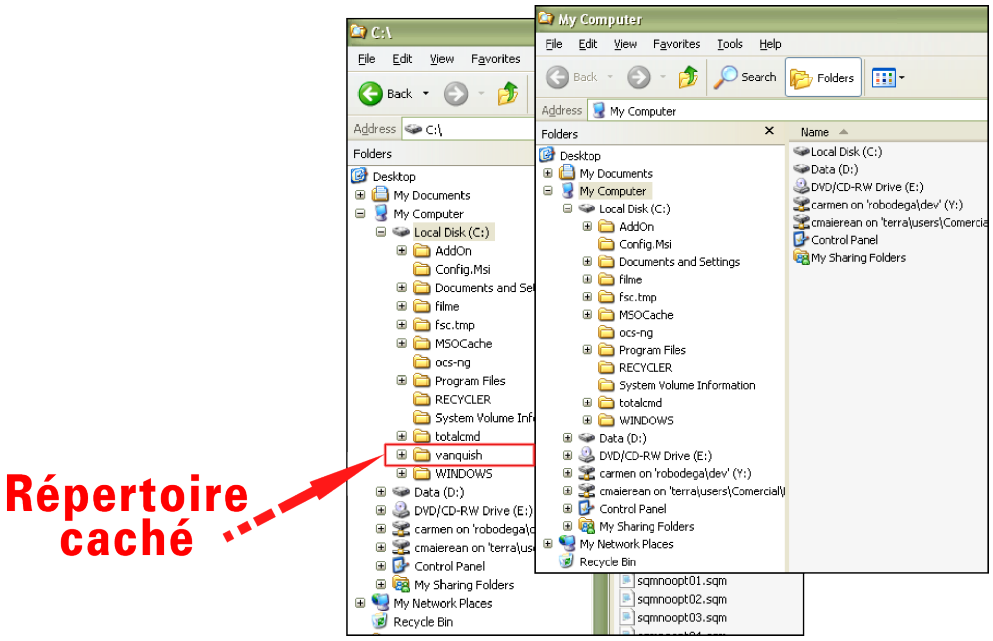
En plus des techniques heuristiques classiques basées sur le contenu, qui sont maintenant largement utilisées y compris parmi nos concurrents, B-HAVE implémente la technique heuristique basée sur le comportement, ce qui réduit considérablement les faux positifs et augmente le taux de détection des nouveaux malwares.

Détection des failles :

Des processus spéciaux de détection ont été ajoutés dans BitDefender pour traquer les codes "exploit". Des routines de détection spéciales peuvent être (et ont été) ajoutées à BitDefender pour traquer des exploitations de failles, comme la récente faille WMF. Cela permet notamment la détection d'attaques de type «zero-day» (exploitant des failles non-encore corrigées) en bloquant pro-activement des codes qui essaieraient d'exploiter ces failles.

2. Détection des rootkits grâce à la technologie RootkitUNCOVER

RootkitUNCOVER est un moteur d'analyse conçu pour détecter et supprimer les rootkits cachés dans les systèmes Windows.



La technologie est en fait une comparaison de deux listes de fichiers. L'une d'elles est faite en utilisant les fonctions API régulières, tandis que l'autre est faite par les drivers Antirootkit de BitDefender.
Si les deux listes ont des résultats différents, cela veut dire que certains fichiers ont été cachés. Bien que ces fichiers puissent avoir été cachés par des applications légitimes, habituellement ce comportement est typique de rootkits.

3. SID et Neunet, deux technologies innovantes dans la lutte contre le spam

La technologie Neunet est un système d'intelligence artificielle basé sur un réseau neuronal artificiel, système de traitement de l'information s'inspirant de la façon dont des systèmes nerveux biologiques, tels que le cerveau, traitent des informations.
La technologie Neunet est un processus automatique apprenant rapidement et sans intervention humaine les caractéristiques du nouveau spam sans nuire à la précision de la détection du spam moins récent. L'approche fondée sur les réseaux neuronaux est plus élaborée, plus mathématique et potentiellement beaucoup plus précise et fiable dans la réalisation de cette tâche.
En complément de ce système, la technologie SID (Spam Image Distance) de lutte contre les spams-images vient enrichir l'arsenal de la solution antispam BitDefender.
Alors que le « spam image » représente désormais 30 à 40% du total des spams en circulation, leur capacité à se modifier légèrement et de manière aléatoire à chaque envoi rend presque impossible leur détection par les techniques antispam traditionnelles.
Intégrée aux produits pour serveurs Linux, aux produits pour postes de travail BitDefender v10 et aux versions 2 de BitDefender for Mail Servers Windows, cette dernière génération d'antispam BitDefender a reçu la certification Checkmark Antispam Premium car elle atteint un taux de détection du spam supérieur à 97% avec un taux de faux positifs inférieur à 0.07%.

En savoir plus sur la technologie SID

En savoir plus sur Neunet

4. Support d'un grand nombre d'archives

Les moteurs de détection BitDefender analysent les fichiers au sein de la plupart des archives et fichiers empaquetés, incluant les formats suivants :

Types d'archives supportées :

7zip	ACE	Alz	Arc
Arj	Bzip2	Cab	CPIO
GZIP	Ha	Imp	Jar
Lha	MS Compress	Zip	Zoo

Archiveurs d'installation :

Inno (Inno Installer)	Instyler	VISE (viza.xmd)
InstallShield (ishield.xmd)	Nullsoft Installer (NSIS)	Wise Installer

Types de packs supportés :

Support for generic unpacking ("GenPack:" detections)	ACProtect/UltraProtect	AHPack	Armadillo
ASPack	AsProtect	Bat2Exec	BePac
Beria	Cexe	CryExe	Diet
Doompack	DotFix	DxPack	Dza Patcher
ECLIPSE	EPack	Exe32Pack	ExePack
ExeStealth	Expressor	Ezip	FakeNeo
Fsg	Ice	JdPack	JdProtect
Kcuf	Krypton	Lamecrypt	Lzexe
Mew	Molebox	Molebox	Momma
Morphine	NakedPack	Neolite	Ntpacker
Nspack	Obsidium	Packlite	Packman
PC/PE Shrinker	PcGuard	PCPEC	PE Crypt 32
PE PACK\CRYPT	PeBundle	PeCompact	PeCrypt.Kcuf
PeCrypt.Sqr	PeCrypt.Sue	PeCrypt.Wonk	PeDiminisher
Pelock	PELock NT	Pencrypt	Penguin
PENinja	PePack	PePatch.DotFix	Perplex
Perplex	PeShield	PeSpin	Petite
Pex	PhrozenCrew PE Shrinker	PkLite	PKLITE32
PolyCrypt-PE	Polyene	RelPack	Rjcrush
SecuPack	Shrinker	SoftComp	SoftDefender
StarDust	Stpe	T-pack	Telock
Ucexe	Upack	Upc	Upolyx
UPX	VgCrypt	Wincrypt	Wwpack
WWPACK32	Xcomor	Yoda Cryptor	Yoda Protector
Yoda's Cryptor			

Archives Messagerie :

DBX	MBX	PST	Mime
MBOX	HQX	Uudecode	TNEF

Autres :

Chm (contient des fichiers html qui peuvent être infectés	Iso (images CD)	pdf	Rtf
Mso (contient des fichiers comprimés OLE2, ainsi les macros sont sauvegardés quand un document est enregistré en html)	Swf (extrait certains champs contenant diverses commandes ; elles sont analysées par d'autres plug-ins, par ex : SDX	Bach (extrait les scripts debug.exe utilisant les méthodes heuristiques)	OMF (Object File)

5. Récompenses & références

BitDefender est la solution qui a obtenu le plus de reconnaissance au niveau international à la fois pour sa capacité de détection des virus en circulation, sa capacité de détection proactive des codes malveillants inconnus, ses performances de lutte contre le spam et sa capacité d'innovation.

BitDefender est régulièrement plébiscité par la presse internationale

Pour ne donner que quelques exemples parmi les plus récents, BitDefender est arrivé premier d'un comparatif réalisé sur l'édition du mois de mai 2007 de PC Answers, magazine informatique de référence en Grande Bretagne.
En conclusion générale, BitDefender est plébiscité : « Une protection puissante, doublée d'une licence avantageuse, fait de BitDefender un gagnant incontestable », « De tous les programme antivirus, BitDefender est celui que nous installerions sur nos PC ».

BitDefender a été élu « Produit d'exception 2006-2007 » par PC Expert (janvier 2007) qui le décrit comme : « un excellent compromis entre efficacité et ressources machine ».

Dans le même temps, BitDefender est « Choix du labo PC Mag », le magazine ne tarit pas d'éloges : « Efficace, rapide, léger et complet », « le produit idéal pour équiper son domicile. »

BitDefender obtient par ailleurs, la médaille d'argent dans la catégorie sécurité lors de la remise des prix des Produits de l'année 2006 par le site « SearchWindowsSecurity » pour le logiciel BitDefender Client Protection Professional.

BitDefender Internet Security est une fois de plus élu Choix de la Rédaction de « Online PC Zeitung » en Suisse.

Dans le magazine roumain Chip, BitDefender est élu meilleur produit de l'année 2006, par les lecteurs de ce magazine, donc en utilisation réelle.

De plus, BitDefender s'est vu décerner la première place lors d'un des plus importants tests de détection des spywares mené par l'organisme indépendant Malware-test.org. BitDefender Internet Security v 10 obtient le meilleur taux de détection en comparaison avec les 30 autres logiciels de sécurité testés dont des logiciels antispywares purs.

Enfin, le test réalisé par PC World en Janvier 2006 a déterminé que BitDefender était le meilleur antivirus en ce qui concerne la détection de virus nouveaux ou inconnus.

Références

Parmi les clients BitDefender en France, on compte Cegetel, NetStream, Ornis, STMicroelectronics, Meilleurstaux.com, Hama, ComExpo, plus de 5000 Collectivités locales, des Ministères, des Académies, des CHU et de nombreux centres de formation.
BitDefender protège des dizaines de millions d'utilisateurs dans 180 pays, directement ou via des applications tierces telles que celles d'IBM Internet Security Systems, GFI, Software602, IPSwitch, Laplink, etc.

6. Services

PushUpdate sur les serveurs de messagerie pour des mises à jour « en temps réel », mises à jour automatiques toutes les heures sur les stations et serveurs, assistance technique 7j/7 – 24h/24, accès aux BitDefender Labs pour la soumission de fichiers suspects, possibilité d'intervention par prise de contrôle à distance sont autant de services qui font de BitDefender une solution performante.

Les laboratoires BitDefender sont reconnus pour être les plus réactifs du marché. Une étude réalisée par l'organisme indépendant Av-Test, réalisée une première fois en 2004 puis en 2006 sur 8 mois a mesuré le temps de réponse des éditeurs antivirus face à l'apparition de nouvelles menaces, et BitDefender est arrivé chaque fois en première position face à ses principaux concurrents avec un temps moyen de mise à jour de ses signatures virales inférieur à heures, contre une moyenne de 8 heures sur le total des éditeurs ayant participé au test.
Ce service est un élément clé de la performance d'une solution de protection.

7. BitDefender, des solutions pour chaque besoin

Les solutions de protection BitDefender sont disponibles sur plate-formes Windows, Linux et FreeBSD et sont administrables de façon centralisée avec des fonctions avancées de gestion de la politique de sécurité du réseau. BitDefender dispose de modules de protection spécifiques pour MS Exchange, Postfix, Sendmail, QMail, Communigate Pro, Exim et protège tout autre serveur de messagerie via sa solution relais SMTP. Il s'intègre dans les serveurs MS ISA, MS Sharepoint, Samba ou Windows Server, et protège les plate-formes mobiles sous Symbian et Windows Mobile.

Pour protéger la plupart des configurations réseau, des packs solutions existent également :

Packs BitDefender	BitDefender Network Protection Pro	BitDefender Corporate Suite	BitDefender Gold SBS
BitDefender Professional Plus Client	√	√	√
BitDefender Security for Mail Servers (Windows)		√	
BitDefender Security for Exchange			√
BitDefender Security for File Servers		√	√
BitDefender Security for Sharepoint			√
BitDefender Security for ISA Servers			√
BitDefender Enterprise Manager (Windows)	√	√	√

Historique BitDefender

1996 : Lancement d'AVX - Antivirus eXpert, destiné au système d'exploitation DOS, le produit peut également être utilisé sous Windows 9x.

Août 1998 : Premier antivirus dans le monde qui possède une mise à jour intelligente, sans intervention de l'utilisateur.

Septembre 1998 : Premier antivirus à s'intégrer à un navigateur Web afin d'analyser tous les fichiers téléchargés.

Juillet 1999 : Première solution de sécurité à utiliser la technologie WAP pour l'administration à distance en environnement réseau.

Août 1999 : Troisième société au monde à fournir une solution antivirus pour dispositifs mobiles (Palm OS, WinCE, Epoc).

Novembre 1999 : Première technologie de blocage comportemental.

Mars 2000 : Première solution antivirus incluant la fonction de firewall personnel.

Avril 2000 : SOFTWIN augmente le niveau des services gratuits en incluant le chat online en plus du Web, de l'e-mail et du support téléphonique. Nouveau service client disponible 7j/7 - 24h/24 via chat on line en plus du web, de l'e-mail et du support téléphonique déjà existant.

Septembre 2000 : AVX reconnu comme la solution antivirus la plus robuste au monde selon VTC (Virus Test Center).

Octobre 2000 : Security Focus nomme AVX parmi les six premières solutions antivirus au monde grâce à la première intégration entre une application firewall et une solution antivirus.

Avril 2001 : Lancement en avant-première mondiale, des solutions antivirus pour toutes les applications de messagerie instantanée existantes (ICQ, MSN Messenger, Yahoo Messenger, NetMeeting, et mIRC), anticipant ainsi les nouvelles menaces émergentes.

Juin 2001 : AVX lance sa 6ème génération et devient le premier produit de sa catégorie à inclure le blocage comportemental. La 6ème génération d'AVX est également le premier produit à intégrer une application firewall.

Novembre 2001 : Changement de nom : AVX devient BitDefender et se positionne sur le marché international.

Mars 2002 : BitDefender lance la première solution antivirus pour MS Sharepoint, au CeBIT 2002.

Février 2003 : MIDAS (Malware Intrusion Detection Advanced System) entre en phase de développement de produit. La technologie propriétaire qui a été récompensée par le « IST Prize » décerné par la Commission Européenne, est créée pour révolutionner la conception de l'antivirus.

Août 2003 : Septième génération de BitDefender – Premier antivirus à intégrer la technologie antidialer.

Novembre 2003 : Première mondiale, BitDefender lance le premier antivirus commercial pour Samba 3.

Janvier 2004 : La première version de LinuxDefender Live! CD est lancée au LinuxConf 2003. LinuxDefender est une distribution Linux complète, directement disponible sur un CD bootable, ce qui en fait le premier kit de secours antivirus.

Avril 2004 : BitDefender développe sa propre technologie antispam.

Juillet 2004 : Le nouveau service de "Push Update" est lancé. Au lieu de dépendre seulement des mises à jour programmées, les clients qui optent pour ce service ont les dernières mises à jour « poussées » directement sur leurs serveurs à la seconde où ces mises à jour sont disponibles, réduisant ainsi la menace causée par les nouveaux virus.

Octobre 2004 : Andreas Marx édite le classement des temps de réaction des produits antivirus. BitDefender est déclaré produit le plus réactif avec moins de 4 heures de temps de réaction.

Mars 2005 : BitDefender introduit HiVE – Heuristic in Virtual Environment, une technologie destinée à réduire la dépendance vis-à-vis des signatures de virus grâce à une analyse proactive des menaces inconnues.

Avril 2005 : BitDefender lance le système de mise à jour toutes les heures.

Août 2005 : En Août, les tests d'Andreas Marx montrent « un zéro seconde » de temps de réaction pour BitDefender contre toutes les menaces majeures. La technologie HiVE aide BitDefender à détecter de manière proactive tous les nouveaux virus ITW (en circulation) durant le mois d'Août 2005.

Septembre 2005 : BitDefender lance sa 9ème génération. BitDefender Internet Security devient l'une des solutions les plus complètes du marché incluant l'antivirus, l'antispyware, l'antispam, le firewall, l'antidialer et le contrôle parental.

Mai 2006 : BitDefender lance B-HAVE (Behavioral Heuristic Analyzer in Virtual Environment), la dernière génération de technologie d'analyse heuristique.

Décembre 2006 : Lancement de la nouvelle technologie S.I.D. (Spam Images Distance) pour lutter contre la prolifération des spams sous forme d'images.