



BITDEFENDER ANTIVIRUS TECHNOLOGY

White paper



Introduction

This is an executive summary of the architecture, design and general structure of the BitDefender Antivirus.

The BitDefender Antivirus System presents a pluggable and distributed architecture that is based on distinct scanning engines for different types of files and malware. Its distinct plug-ins can be loaded on-the-fly, one for each kind of malware, without reconfiguring the whole system or restarting it.

Each type of malware is dealt with by a plug-in which can detect and possibly disinfect/clean the given malware type. As an example, the Antispyware modules were integrated into BitDefender Internet Security right alongside the antivirus-specific ones. Plugins function sequentially (i.e. they take turns at checking each file), to detect malware like viruses, worms, trojans, exploits and also spyware. The plugin architecture is such that the plugins can pass messages between themselves.

The modularized architecture used to build BitDefender has contributed to its ability to be used in a variety of environments ranging from embedded systems to workstations and high-end servers, in desktop, dedicated or generic server solutions.

BitDefender antivirus technology is integrated in a diverse range of products from: IBM ISS, GFI, Hauri, Ipswitch, Laplink, Software 602, Bullguard, and others.

BitDefender Antivirus is portable and platform independent, presenting compatibility at binary level for any IA32 based Operating Systems (such as: Windows, Linux, FreeBSD) and at the source code level for other OS's.

An added side-benefit of having portable binaries is that the BitDefender Antivirus is effectively isolated and largely independent from the host OS, which makes the adding of detection routines a relatively straightforward process, which does not have to be repeated for each OS to deal with compatibility issues.

BitDefender Antivirus is differentiated into two main components:

- **The Scanning Engines**
- **The Archive Logic**



The Scanning Engines

The scanning engines are comprised of modules which are continually being developed to offer full protection against all types of malware including, but not limited to: executable viruses, script viruses, macro viruses, backdoors, trojans, spyware, dialers, etc. Every virus family benefits from a dedicated scan engine which was designed in accordance with the class characteristics.

- High speed. Multi - threading architecture
- Low memory consumption.
- 100% disinfection for In The Wild viruses as certified by ICSA Labs and Checkmark
- Proactive detection of viruses including various versions of very well known viruses such as Bagle, Zafi, Sober, Zotob
- Using this technology BitDefender can detect suspicious activity common to P2P worms, E-mail worms, Antivirus Killer programs and many other
- The optimized emulation procedure enables BitDefender to analyze the behavior of all files types in a virtual machine without significant performance impact.

BitDefender Antivirus System

The scanning engines benefit from a number of technologies which have been implemented over time:

Classic antivirus scanning (pattern matching)

In February 2006, BitDefender had in its database over 270 thousand malware signatures (of which "only" 256 thousand were viruses and worms, and the rest as spyware. This is not to say, however, that BitDefender can detect 270 thousand pieces of malware – the addition of generic signatures means that many "related" virus or spyware threats are described with one signature, so the actual number is much higher. The generic signatures can also help to protect against new variants of old malware.

Heuristic Scanning

B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) combines a lot of different techniques to proactively detect malware.

B-HAVE is the basis for:

- Behavior-based heuristics
- Generic detection routines



- Virtual Machine for VB scripts
- Virtual Machine for BAT/CMD scripts
- VB script emulator
- Virtual Machine for executable files (PE, MZ, COM, SYS, Boot Images)

B-HAVE is by now thoroughly proven technology and is responsible for some spectacular results:

- According to independent German testing outfit AV-Test, BitDefender antivirus was capable to detect six out of six variants of the Zotob virus without the need for a signature update.
- The PC World test held in January current nominated BitDefender as the best antivirus where detection of new/unknown viruses is concerned.

The B-HAVE technology also acts as a “force multiplier” for other, more traditional forms of defense. For example, files which emerge from the B-HAVE environment (OLE components, dropped executables, etc) are then filtered by the other modules, possibly even in a recursive manner (where they are afterwards returned to the B-HAVE component for a “second opinion”, or go straight into the more classical heuristic filters.

In addition to content-based heuristics, which is now in wide use even among our competitors, B-HAVE implements behavior-based heuristics, which reduces false positives enormously and increases detection rates for new malware.

Exploit detection code

Special detection routines can (and have been) added to the BitDefender Antivirus to root out exploit code, such as the recent unpatched WMF exploit. Thus sometimes detection is available for worms using a new exploit long before the actual worms are written.



The archive Logic

BitDefender Antivirus archive logic component is built around the concept of “in-depth scanning”, which means that it can be configured to scan embedded archives down to any depth, while still being relatively impregnable against zip bombs or other forms of DoS attack against itself.

- Generic unpacking for executables packed with new packers 80% of new viruses appearing in the wild use some form of packing, but packing apps are legion, and more are created every day. Generic unpacking routines allow for variations in packing format, and so can unpack new/unknown types of packed files.
- Scanning support for over 18 types of archivers and more than 100 packers (including UPX, Neo-Lite, ASPack, PECrypt, pklite and self extractable files SFX) as well as the majority of installation packers and mail archive types.

BitDefender Antivirus has cleaning support for .zip, some mail databases, .gzip and other types of archives. The archives are unpacked, files are checked, cleaned and then repacked.

BitDefender scans inside the most common type of archives and packed files, including, but not limited to the following:

Supported archive types

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

Mail Databases

DBX	MBX	PST	Mime
MBOX	HQX	Uudecode	TNEF



Supported Packers

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			

Installation packers

Inno Installer	Instyler	WISE
InstallShield	Nullsoft Installer (NSIS)	Wise Installer

Others

Chm	ISO	PDF	RTF
MSO	SWF	Bach	OMF

Notes:

malware: A program can be regarded as malware if it does at least one of the following:

- replicates through a network or a file system without users' consent
- allows an unauthorized person control over a remote system
- sends information or files to a remote system without user's consent
- sends data to a system in order to disrupt normal functioning.

B-HAVE: Behavioral Heuristic Analyzer in Virtual Environment (patent pending technology)



About BitDefender®

BitDefender is a leading global provider of security solutions that satisfy the protection requirements of today's computing environment. The company offers one of the industry's fastest and most effective lines of security software, setting new standards for threat prevention, timely detection and mitigation. BitDefender delivers products and services to over 41 million home and corporate users in more than 180 countries. BitDefender has offices in the United States, the United Kingdom, Germany, Spain and Romania. Further information about BitDefender can be obtained by visiting: www.bitdefender.com

Contact Info

Efficient communication is the key to a successful business. For the past 10 years SOFTWIN has established an indisputable reputation in exceeding the expectations of clients and partners, by constantly striving for better communications. Please do not hesitate to contact us regarding any issues or questions you might have.

Country: **North America**
Address: 6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Phone: 954 776 62 62
E-mail: sales@bitdefender.us
Web: www.bitdefender.com

Country: **Central & Eastern Europe, Middle East**
Address: 5 Fabrica de Glucoza St. Bucharest
Phone: +40 21 2330780
E-mail: sales@bitdefender.ro
Web: www.bitdefender.ro

Country: **Asia Pacific, Africa, Latin America**
Address: 5 Fabrica de Glucoza St. Bucharest
Phone: +40 21 2330780
E-mail: sales@bitdefender.com
Web: www.bitdefender.com

Country: **Western Europe**
Address: Karlsdorferstrasse 56, 88069
Tettngang - Germany
Phone: +49 7542 9444 44
E-mail: vertrieb@bitdefender.de
Web: www.bitdefender.de

Country: **Spain**
Address: C/ Balmes 195, 2ª planta, 08006 Barcelona
Phone: +34 932189615
E-mail: comercial@bitdefender-es.com
Web: www.bitdefender-es.com

Country: **UK and Ireland**
Address: One Victoria Square, Birmingham, B1 1BD
Phone: 0845 130 5096
E-mail: Sales@BitDefender.co.uk
Web: www.bitdefender.co.uk