McAfee Command Line Scanners and VirusScan for UNIX

When Only a Command Line Scanner Will Do

McAfee® VirusScan® is trusted by millions of enterprises to provide effective defense from virus attacks. In most cases, of course, this means continuous background protection under various versions of Microsoft® Windows.® However, there are occasions when it's useful to have a command line scanner at your disposal. Perhaps you need to use a command line scanner alongside another application—for example, in tandem with a third-party content filter at the Internet gateway. Or perhaps you wish to integrate a command line scanner into your own custom business application or process. McAfee command line scanners are perfect for such situations. They combine comprehensive detection and cleaning with the granular control that you can get only by using a command line scanner.

Scanning Under DOS and Windows

When SCAN.EXE is run, it checks to see if you're running Windows. If you are, it uses the McAfee 32-bit Windows scan engine. If you're running DOS, it calls SCANPM.EXE, which switches the PC into protected mode and scans using the McAfee 32-bit DOS scan engine. SCANPM.EXE will run in a Windows environment if it's launched explicitly from the command line. However, this isn't recommended since it is not optimized for this environment.

Scanning UNIX File Systems

McAfee provides command line scanners for a wide range of UNIX platforms—AIX, FreeBSD, HP-UX, Linux v2.x kernels, SCO UNIX, and Solaris (SPARC). Our UNIX scanners provide more than just search-and-destroy scanning capability for the growing number of native UNIX viruses. They scan for all viruses that may be stored on any UNIX systems operating as file stores for Windows desktops across your enterprise.

Comprehensive Scanning for Today's Threats

There are now in excess of 85,000 threats, and more than 275 new threats appear each month. Alongside "traditional" virus threats, there are now e-mail worms, Internet worms, DDoS (Distributed Denial of Service) attacks, backdoor and remote access Trojans, and zombies. Many of these threats combine multiple-attack mechanisms to maximize their chances of spreading quickly through corporate networks worldwide. Blended threats, in particular, have had a marked effect, combining the use of system exploits, formerly associated with hacking activities, with the spreading capabilities of viruses and worms. An increasing number of threats are designed to cash in on vulnerabilities in operating systems and applications. McAfee command line scanners, using the superior scanning technology of the McAfee scan engine, detect all of these threats.

Advance Protection from Tomorrow's Threats

New threats appear all the time, and many of today's viruses and worms travel at Internet speed—they strike fast and move quickly. So a scanner's ability to flag new, unknown threats is more important than ever. McAfee command line scanners harness the McAfee scan engine's proactive detection technologies to isolate new threats.

Heuristic Detection

The McAfee advanced heuristic analysis lets us look through the code in a file to determine if the actions it takes are typical of a virus. The more virus-like code that's found, the more likely the file is to be infected. To reduce the risk of false alarms—identifying a virus when there isn't one—we combine positive heuristics with negative heuristics to search for those things that are distinctly non-virus like.

Generic Detection and Cleaning

Generic detection involves using a single virus definition to detect and clean many variants of the same virus family. This is especially useful today when a successful threat is often followed by a host of variants. Of course, all threats must be detected, but it is much less efficient to build individual signatures for each one as they appear. Piecemeal detection isn't just less efficient—it also means that a new variant has the opportunity to spread before the scanner is able to detect it.

McAfee's generic detection capability, developed over several years, has brought enormous benefits to McAfee customers, who have been protected—in advance—from threats such as Anna Kournikova, Homepage, Badtrans.b, Fbound.c, Klez.h, W32/Frethem, Bugbear.b, Sobig.e, W32/Mimail, Lovsan, and many others.

The Hidden Threat

When a file is compressed or archived, the original bytes of the file are rearranged as part of the space-saving process. If the file is infected, the bytes belonging to the virus are also rearranged, and the characteristic string that an anti-virus scanner looks for may no longer exist. So there could be a hidden threat lurking within any compressed, archived, or packed file. McAfee command line scanners are able to drill down into multiple layers of compression to seek out the hidden threat within.

The threat isn't confined just to common archive utilities like WinZip. Windows applications can be packed to reduce the size of the program. Such packers may be used legitimately, so they can't all simply be branded as a potential threat. However, many of today's Trojans arrive in packed format, so McAfee command line scanner's ability to identify hostile code within the packing is essential.

Maintain Business Continuity

The McAfee command line scanners make full use of the scan engine's ability to clean infected files. This is very important. If a scanner simply flags an infection, the system administrator must replace the file—either from an original master disk or CD (in the case of EXE files) or from a backup (for documents and spreadsheets)—if a backup even exists. If the scanner is able to clean the infected file, business continuity is maintained, downtime is minimized, and costs are reduced.

Key Features

- 32-bit command line scanner for Windows environments
- 32-bit command line scanners for a range of UNIX environments—AIX, FreeBSD, HP-UX, Linux v2.x kernels, SCO UNIX, and Solaris (SPARC)
- Comprehensive detection for today's and tomorrow's threats
- Detects viruses, e-mail worms, Internet worms, DDoS attacks, backdoor and remote access Trojans, and zombies
- Uses heuristic analysis to flag new threats, without a false-alarm problem
- Includes generic detection and cleaning for new variants of existing threats
- Scans compressed, archived, and packed files
- Maintains business continuity by cleaning infected files

System Requirements

VirusScan Command Line

An IBM-compatible PC with an Intel 80386 processor or equivalent. VirusScan Command Line supports the following platforms:

- SCANPM.EXE
  - MS-DOS 6.22
- SCAN.EXE
  - MS-DOS 6.22 (requires SCANPM.EXE)
  - Windows 9x
  - Windows ME
  - Windows NT 3.51
  - Windows NT 4
  - Windows 2000
  - Windows XP
- Minimum 4MB of free hard-drive space
- Minimum 4MB of RAM

VirusScan for UNIX

VirusScan for UNIX supports the following platforms:

- IBM AIX 4.2.1, 4.3.x, and 5.0L, with all recommended patches installed
- FreeBSD 3.2 and 4.3
- Hewlett-Packard HP-UX 10.20, 10.30, 11.x, and 11.I, with all recommended patches installed
- Linux v2.x kernels up to, and including, v2.4 kernels with libc6 (glibc) and the stdc++ library v2.8*
- Santa Cruz Operation (SCO) OpenServer Release 5 and SCO UnixWare 7.1.1**
- Sun Microsystems Solaris for SPARC architecture v2.5.1, 2.6, 7, and 8, with all recommended patches
- Minimum 10MB of free hard-drive space

McAfee recommends that you have root-account permissions to install VirusScan for UNIX software and perform on-demand scan operations on your file system.

* McAfee does not recommend the use of VirusScan for UNIX in conjunction with any Linux development kernel (v2.1.x and 2.3.x). These kernels are built for testing purposes only and are not supplied with any major Linux distribution.

** The use of VirusScan for UNIX with SCO OpenServer requires installation of the SCO UnixWare Binary Compatibility Module (BCM).

McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 888.VIRUSNO (888.847.8766), www.mcafeesecurity.com

Network Associates® products denote years of experience and commitment to customer satisfaction. The PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission critical projects—all with service levels to meet the needs of every customer organization. McAfee® Research, a world leader in information systems and security, continues to spearhead innovation in the development and refinement of all our technologies.