

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 attack. 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's VirusScan command line scanners are perfect for such situations. They combine comprehensive detection and cleaning with the granular control that you can only get 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 McAfee's 32-bit Windows scan engine. If you're running DOS, it calls SCANPM.EXE, which switches the PC into protected mode and scans using McAfee's 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 a file-store for Windows desktops across your enterprise.

Comprehensive Scanning for Today's Threats

Today there are more than 60,000 threats and alongside "traditional" viruses there are now mass-mailers, Internet worms, DDoS (distributed denial-of-service) attacks, and backdoor Trojans and zombies. McAfee's command line scanners, using the superior scanning technology built into the McAfee scan engine, detect all of these threats.

Proactive Security for Tomorrow

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's command line scanners harness the McAfee scan engine's proactive detection technologies to isolate new threats.

Heuristic Detection

McAfee's 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 it is to be infected. To reduce the risk of false alarms—identifying a virus when there isn't one—this "positive" heuristics approach is combined with "negative" heuristics—a 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, they must all be detected, but it is a lot less efficient to build individual signatures for each one as they appear. Piecemeal detection is not 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 AnnaKournikova, Homepage, Badtrans.b, Fbound.c, Klez.h, and many others.

The Hidden Threat

When a file is compressed or archived, the original bytes of the file are re-arranged as part of the space-saving process. If the file is infected, the bytes belonging to the virus are also re-arranged 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's command line scanners are able to drill-down into multiple layers of compression, to seek out the hidden threat within.

McAfee Command Line Scanners and VirusScan for UNIX

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 the McAfee command line scanner's ability to identify hostile code within the packing is essential.

Maintain Business Continuity

McAfee's 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, down-time 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 threats and tomorrow's

- Detects viruses, Internet worms, DDoS (distributed denial-of-service) attacks, backdoor 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 of 4MB free hard disk space

Minimum of 4MB RAM

System Requirements— 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 11i, 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 of 10MB free hard disk 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).

All Network Associates products are backed by our PrimeSupport® program and Network Associates Laboratories. Tailored to fit your company's needs, PrimeSupport® service offers essential product knowledge and rapid, reliable technical solutions to keep you up and running. Network Associates Laboratories, a world leader in information systems and security, is your guarantee of the ongoing development and refinement of all our technologies.

3965 Freedom Circle | Santa Clara, CA 95054 | 888.847.8766 main

networkassociates.com



YOUR NETWORK. OUR BUSINESS.