

Norman Virus Control v5.8

Corporate edition

New viruses appear on a daily basis and your business could be the next victim. Be prepared to meet these malware threats in a professional way with a professional partner!

Norman Virus Control (NVC) is a collection of antivirus software applications and utilities that protect your workstations, servers and gateways against malicious software. The most prevalent types of malware are computer viruses, worms, and trojans.

The single most important task for antivirus software is to keep computers free from viruses. NVC is based on the advanced core technologies of Norman's Scanning Engine, which accurately detects known and unknown computer viruses, worms and trojans. When infected files are detected, NVC cleans, isolates or deletes them immediately — before the destructive code is activated.

Every administrator knows how important it is to have software that is easy to install, deploy, update, configure, maintain, and manage. A product that is difficult to install and manage is unlikely to succeed in today's market. Norman has taken this into consideration when making the new version of the award-winning Norman Virus Control. NVC v5 is just as easy to install and administer in a small LAN as it is in an enterprise WAN. NVC v5 gives new meaning to TCO («Total Cost of Ownership»).

Key features

Key features

- ✓ On-access and On-demand scanning of files
- ✓ Norman SandBox II – revolutionary way to detect new and unknown malware
- ✓ Automatic updates over the Internet – complete product and incremental updates of definition files
- ✓ Proactive email and newsgroup scanning

Norman SandBox

Norman's SandBox technology detects new and unknown computer viruses, including trojans and worms. Today, an email worm can infect tens of thousands of workstations in a matter of seconds. The antivirus vendors are expected to find the cure, update the virus definition files, and distribute these to its customers immediately.

The need for speed is paramount. Norman's SandBox is a virtual world where everything is simulated. An emulator provides an environment where possible virus infected executables «run» just as they would do on a real system. When execution stops, the SandBox is analyzed for changes. The SandBox is particularly tuned to find new email-, network- and peer-to-peer worms.

Recent test from AV-Test GmbH shows that the Norman SandBox has the best proactive protection of new and unknown viruses. For more details please visit

http://www.norman.com/News/Press_releases/17613/en

On-access scanner

On-access scanning involves constant monitoring of the file system on servers and workstations. For an anti-virus application, it is imperative to detect and block a computer virus before it is activated. Whenever a file is accessed in a read/write operation, or a program is executed, the On-access scanner is notified and scans the file on the fly.

Like the On-demand scanner, Norman Virus Control's On-access scanner detects and repairs many types of malicious code. Whenever possible, an infected file is repaired before the file is handed over to the application. If repair fails, Norman Virus Control denies access to the infected file. There are a number of configuration options for the On-access scanner, and in general it's a good idea to decide upon a strategy when this feature is configured. NVC provides guidelines in the program, help files, and documentation.

Norman is one of the world's leading companies within the field of data security. With products for virus control, spam control, email control, download control and personal firewall, the company plays an important role in the data industry.



NORMAN[®]
www.norman.com

On-demand scanner

This scanner is used for manual scans of selected areas on a machine. Entire drive(s), or certain folders and subfolders - even specific files - can be selected for scanning. From Windows Explorer, for example, any object can be selected and scanned by choosing the Norman Virus Control entry from the right-click menu.

In networks, the system administrator can create scanning tasks to be executed on selected, or on all workstations and servers in the organization. Tasks can be executed immediately, or scheduled for execution later, for example at fixed intervals. The On-demand scanner can use the Norman SandBox technology to further increase protection levels by detecting new and unknown malware before it can cause damage.

Norman Internet Protection

The Norman Internet Protection (NIP) module scans incoming and outgoing email as well as files downloaded from newsgroups. To reduce the risk of virus infection, we have added file attachment blocking. The user can set up rules for attachment blocking according to their security policy.

- ✓ Block all attachments
- ✓ Block any attachment with double extensions
- ✓ Block attachments with CLSID extensions
- ✓ Block all except chosen extensions
- ✓ Accept all except chosen extensions

NIP hooks all applications using Winsock, and scans all traffic on ports for POP3, SMTP, and NNTP.

Automatic updates

Norman Internet Update (NIU) is an integrated part of NVC and can be configured to regularly check for new and updated files on Norman's product servers. NIU provides complete updating and upgrading of the application software and virus definition files to ensure that the latest version of the software is always installed. NIU employs incremental updates of virus definition files to keep the size of the updates as small as possible, thereby reducing download time.

New Internet Update functionality allows separate configuration for attended (user initiated) and unattended (scheduled) update mode. In addition the new update dialogs also enable download of components separately, for example if you want to download signature and scanner engine updates, but don't want to download new versions of other components during regular updates.

Task editor

With the Task editor you can create task files for scans to be performed on a regular basis, or special scans that need to be run in certain situations. For example, if files are downloaded from the Internet to designated areas, a task file can be created to scan these areas only, or run manually by the user after downloads are complete. In addition, the task can be scheduled to run at a pre-defined time. Administrators can create task files and distribute them to all workstations in the network to ensure consistent checking of areas that require special attention.

Utilities

Certain elements can be changed by selecting some of the entries, for example Task files. You can also manually delete, restore or save files that are placed in the quarantine from the Utilities module.

Other functions

- ✓ Messaging (routing/handling)
- ✓ Messaging module for administrators
- ✓ NDesk, Norman Management tool
- ✓ Configuration through Microsoft Management Console

For more information please visit; www.norman.com/Product

System requirements

Pentium processor with Windows 95/98/Me or Windows NT/2000/2003/XP, OS/2, Linux

For Windows 95 Internet Explorer version 4.0 or later is required

For Windows NT Service Pack 4 or later is required

For Linux i386 or compatible architecture, glibc 2.2 or better and Java 1.4 for configuration

System requirements

Norman solutions for clients/workstations: Norman Virus Control for Windows 95, 98, Me, NT4.0, 2000, XP, OS/2, Linux (On-Demand scanning)
• Norman Internet Control for Windows 95, 98, Me, NT4.0, 2000, XP • Norman Personal Firewall • Norman Ad-Aware

Norman solutions for servers: Norman Virus Control for Microsoft Windows NT4.0, 2000, 2003 • Norman Virus Control Firebreak for Novell Netware 4.11 and later • Norman Virus Control for Linux • Norman Virus Control for OS/2

Norman solutions for web/gateways/mailservers: GFI MailEssentials • GFI MailSecurity • GFI DownloadSecurity • NVCnet • Norman Virus Control for Lotus Domino (Win32, OS/2) • Norman Virus Control for Firewall-1 NG • Norman Virus Control for Microsoft Internet Information Server • Norman Virus Control for Microsoft Exchange • Norman Virus Control for Microsoft Exchange 5.5 • Norman Virus Control for MIMESweeper



NORMAN[®]
www.norman.com