

# Norman SandBox

## Pro-active virus protection

Norman SandBox stops viruses, worms and Trojans, before you get infected; without the need for updated signature files. The race between creators of new viruses and those that hunt them down, is getting tougher and new viruses use increasingly sophisticated methods to avoid detection and have the ability to spread faster. The goal of a virus author is to be able to operate freely as long as possible before the hunters slow down the spreading of the virus through the release of a new signature file. The chances of us getting less dependant upon our PCs and systems are miniscule and the expense associated with lack of system availability will continue to rise. Norman SandBox assists you in having a continually updated virus protection to ensure system availability.

” Norman SandBox stops viruses, worms and Trojans, before you get infected ”

### The challenge – Traditional methods are too sluggish

The threat posed by computer viruses, is something that most knowledgeable users now know of and a considerable amount of resources, both time and money, have been invested to protect networks and PCs from such attacks. Earlier, a good virus defence consisted of a system that pulled down updated virus signature files once a week. As things intensified, these solutions were set up to get updates several times each day. The current challenge is that irrespective of how frequent updates are made, the PCs will remain unprotected anywhere from 6 to 24 hours from the release of a new virus. No matter how often the virus defence is updated with new signature files, solutions based on signature files alone will always have a period where it cannot protect the user against new threats.

Norman SandBox provides pro-active virus protection, ensuring system availability and protection, even prior to new signature files being available.

### Norman SandBox – Pro-active virus protection

Norman SandBox detects infected files based on the actual action performed by the specific file. All files are expected to execute certain tasks or behave in certain ways. If a file suddenly starts performing tasks beyond a defined framework, this will be detected as non-standard behaviour and Norman SandBox will make the file inoperable.

In conjunction with the virus being stopped, SandBox will inform the user of the type of malicious software and suggested further action.

Norman SandBox emulates a real PC network and runs “the emulator” within a contained environment on the PC. This facilitates both testing files and stopping virus before it can disrupt critical processes.

### Virtual PC and network environment

Emulation of operating environments has been in use since the mid 70s and represents a proven method to predict programs and files behaviour prior to putting them into a production environment. Put another way, you get a preview of what would happen when the program is run in a real environment and Norman SandBox controls this process.

### The process – with Norman SandBox

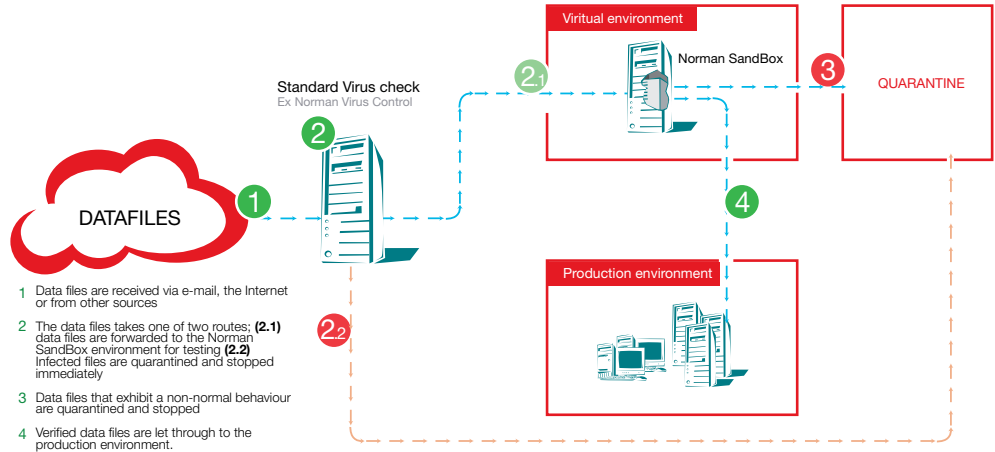
The following takes place in a system with Norman SandBox and Norman Virus Control as a file is received:

1. Data files are received via e-mail, the Internet or from other sources
2. Initially, the files are scanned using the most updated signature files in Norman Virus Control
3. Infected code is stopped
4. All other data is passed on to Norman SandBox for execution within the virtual environment
5. Data files that exhibit a non-normal behaviour are quarantined and stopped
6. Verified data files are let through to the production environment.

” Norman SandBox assists you in having a continually updated virus protection to ensure system availability, even before new signature files are released. ”



Figure 1 Norman SandBox



- 1 Data files are received via e-mail, the Internet or from other sources
- 2 The data files takes one of two routes: (2.1) data files are forwarded to the Norman SandBox environment for testing (2.2) Infected files are quarantined and stopped immediately
- 3 Data files that exhibit a non-normal behaviour are quarantined and stopped
- 4 Verified data files are let through to the production environment.

» There are no special requirements to the operational platform for SandBox and most PCs and servers running modern operating systems, will be sufficiently powerful to use Norman SandBox. »

Thus, infected files are stopped prior to reaching the production environment irrespective of the availability of a signature file identifying the virus. There are no special requirements to the operational platform for SandBox and most PCs and servers running modern operating systems, will be sufficiently powerful to use Norman SandBox.

### Norman SandBox – a part of the Norman Virus Control product suite

Norman SandBox is an integrated part of all Norman Virus Control products.

Norman SandBox ensures pro-active virus protection as new viruses can be stopped even before signature files are released. The solution does not need to be tailored in any way and comes as part of the package when you select one of the market leading anti-virus products from Norman ASA.

Is there any good excuse for not using Norman SandBox?

### System requirements

Norman SandBox is an integrated part of the Norman Virus Control products

#### Norman Virus Control v5 single-user or any other Norman Virus Control Product

- Pentium 133 Mhz, 64 Mb RAM, 100 Mb available disk space
- Windows 95/98/98SE/ME or Windows NT/2000/XP
- Internet Explorer 4 or higher
- Service Pack 4 or higher for Windows NT

System requirements are subject to change. Updated system requirements plus information on other Norman Virus Control products can be found at <http://www.norman.com/>



Norman Virus Control  
Powered by Norman SandBox™

#### Norman ASA - Peace of Mind

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, personal firewall, encryption, data recovery, certified data erasure and computer forensics, the company plays an important role in the data industry.

**NORMAN**  
[www.norman.com](http://www.norman.com)



Statistics



Unread email



Scan content