



# "TruPrevent™: perfect antivirus protection without updates."

Andreas Marx, Director of AV-Test

Classic virus engines have become rapidly obsolete. The battle is easier thanks to new techniques such as TruPrevent™ provided by the experts.

## BY VALENTIN PLETZER

"They are one step ahead of viruses" says José María Hernández, Vice-President of International Expansion at Panda Software, describing the new feature of the company's antivirus solution. Under the name of TruPrevent™, the Spanish company remains a step ahead in the fight against the Internet mafia and virus creators. The novelty is that this protection technology works with sophisticated profiles that analyze the behavior of potential threats instead of checking them against the signature file. **Designed as an added value in contrast to traditional antivirus solutions, TruPrevent™ covers the gap of reaction time, which in many cases is several hours, until the signature file is updated.**

The current problem: firstly, when a new virus attacks and its signature can be recorded, the antivirus manufacturer can react and offer the antidote. Consequently, most antivirus manufacturers work intensively to reduce reaction times between the appearance of the virus and creation of the signature (signature file) to a minimum. The heuristic search must help recognize new variants of known viruses, but both methods have their weaknesses: with malware such as the Wity worm, propagated in a few hours, the signature file update is not quick enough. The heuristic scan cannot effectively fight new malware.

Classic antivirus engines can produce errors with false alarms, also known as "false positives". Occasionally therefore an antivirus program recognizes spyware as a virus even though it has the information in the signature file.

**TruPrevent™ blocks viruses without the need for a signature file.** The solution comes from the perimeter of corporate networks. In order to disarm hackers, the so-called "intrusion prevention systems" were developed some time ago. These tools scan all network traffic at protocol level and detect suspicious activities. TruPrevent™ works

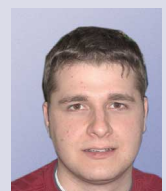
in a similar way with the program observing the behavior of all active processes in the computer. After detecting potentially dangerous applications, TruPrevent™ interrupts and then blocks them. In one of the tests carried out by the antivirus expert Andreas Marx from AV-Test, TruPrevent™ was able to demonstrate its strength by detecting and blocking known worms such as Sobig and Blaster, without the need for a signature file.

### Scanning: Rootkits technique against malware.

In order to observe Windows programs, TruPrevent™ is installed in a central position similar to a Rootkit in the system. The best place for this is the API (Application Programming Interface). Rather than directly attacking Windows hardware, the programs give orders with respect to a port where the Windows API receives the instructions. Here the process is coordinated, the appropriate driver invoked and the instruction completed.

TruPrevent™ is involved in this process and scans each call to the API in order to scan the calls at protocol level. It then compares the call with the rules defined in Panda's software and assesses the danger of the action. If the program tries to break a critical rule, it is passed immediately to virus protection and marked.

*"Traditional antiviruses have serious problems in their limitations. They can only help new technologies such as TruPrevent™."*



Andreas Marx, Director of AV-Test.

### Intelligent scanning discovers hackers and password thieves.

In case a program affects different hard disk data, the Windows API is required for reading and writing. This is how TruPrevent™ finds out which data is affected. For example, if the program opens the executable Adobe Reader file and tries to change or replace it, this will indicate an unusual activity: a virus tries to add its damaging routine to this program so that it can spread itself. However, this may also be a harmless update routine trying to change EXE data for an improved version.

For this reason an action of this type receives a high ratio, but is not finalized immediately. TruPrevent™ observes the program and collects more ratios, with the program being rated as potentially dangerous and its execution halted only when the values set by Panda Software are exceeded.

TruPrevent™ does not only control the API (see image). When a program tries to contact many different ports in a very short period of time, this can be considered as an indication of a hacker attack. Access to the storage of other applications may indicate a password thief attack.

### The special characteristic of TruPrevent™ is intelligent scanning of API protocols.

The ratios for different accesses to the API are calculated and valued among themselves. If they exceed the limits, TruPrevent™ finalizes the process categorized as malware and disables it for subsequent boots (restarts). In certain cases the malware is stopped immediately. The intelligent scanning unit always keeps the rules in full view and immediately interrupts accesses to the API in case of notorious behavior, for example when somebody writes or alters .ini files. This may be an attempt by a hacker to access the system.

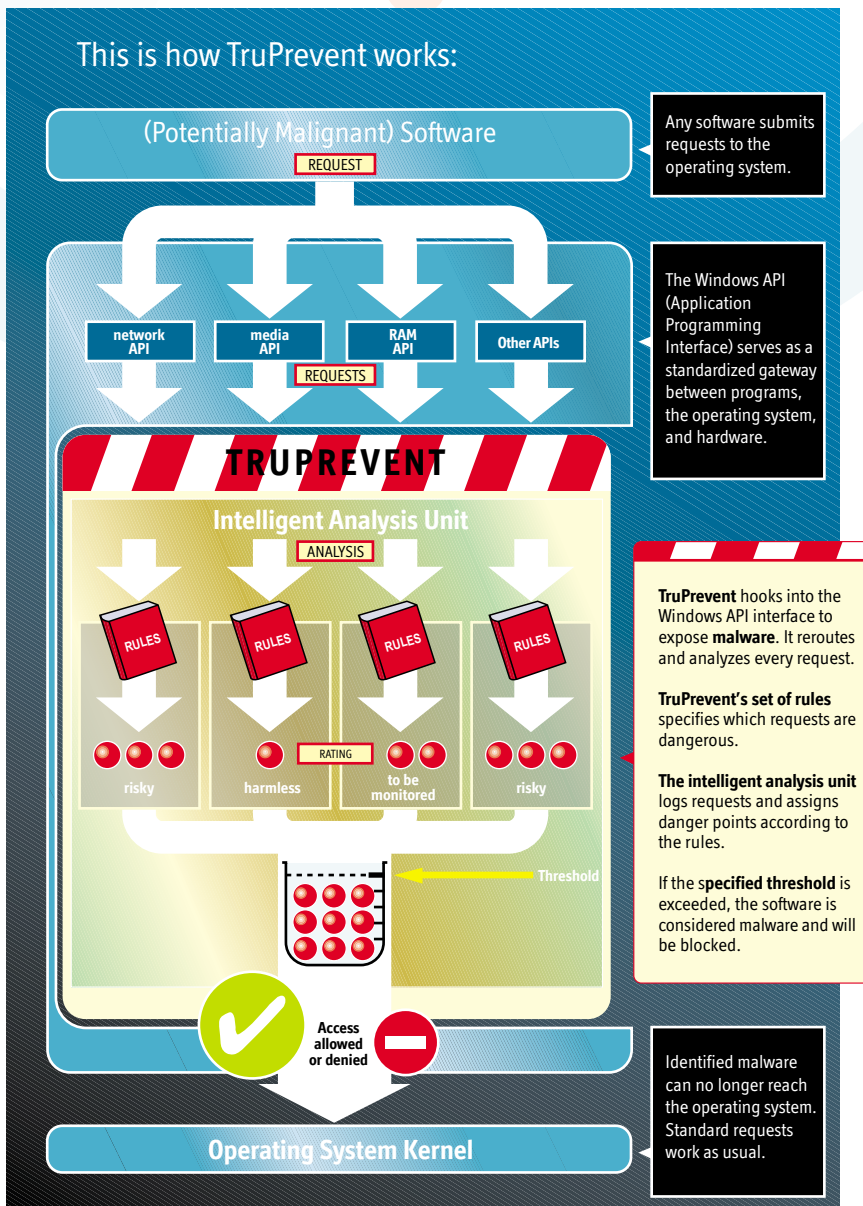
Administrators have to occasionally open and read .ini files with the Windows Notepad, as a result of which TruPrevent™ does not immediately block the opening of the editor, but does so with any change and writing of the .ini files.

Delayed reaction is an additional problem: TruPrevent™ protects far more quickly than conventional signature file updates, but in order to assess a program it has to allow prior access to the API, so that in the worst-case scenario damage has already been caused before reaching the critical valuation (ratio).

### The result: Good initiatives of other manufacturers are already being left behind.

Panda Software is on the right track with these new techniques, since an increasing number of computers are connected and communications ever faster. The gap between virus authors and their hunters is widening. For the first time TruPrevent™ reduces this gap to a minimum.

Other manufacturers such as Kaspersky Labs, Symantec and McAfee have also recognized this. They hope to equip their future versions with similar techniques. This includes wanting to integrate rollback functions (returning to previous situations) which would enable the user to return to situations prior to the damage caused by the malware. Without these types of mechanisms, no security suite will be able to survive in the market.



Originally published in April 2006 in Chip-Magazin, Germany.

