

Debate» Enterprises should deploy a multi-engine anti-virus approach to combat malware.

FOR



David Vella
product manager
for GFI MailSecurity,
GFI Software

There is no single engine which is the fastest at reacting to all viruses and the best at identifying all threats, all companies using a single anti-virus engine are leaving themselves open to viruses and other malware.

Using multiple anti-virus engines provides three primary security benefits.

First, each anti-virus engine has different reaction times. No one comes out on top every time!

Additionally, multiple proactive and heuristic engines working in parallel *are* the most effective. McAfee was the first to detect the Win32/Blackmal.E through its proactive and heuristic engine; however, it did not detect the Win32/MyDoom.BB. It was caught first by Kaspersky.

Finally, anti-virus engines have strengths and weaknesses. Some engines excel at identifying certain type of malware, while others are stronger at detecting viruses, trojans and backdoors.

A multiple anti-virus engine approach provides the most holistic approach for protecting a network against infection with no extra taxation on performance.

AGAINST



Bob Hansmann
senior product
marketing manager,
Trend Micro

Due to response times measured in 'days' during the 1990s, multi-engine anti-virus techniques increased the likelihood that at least one of them would be among the earliest to detect a new threat. Nevertheless, this improved response time came with increased 'false positive' disruptions.

With so many major outbreaks, the trade-off was in favor of the multi-engine approach, sometimes protecting systems a day or more ahead of many single solution systems.

But today's typical anti-virus response is under an hour, eliminating the 'value' of this approach, while the 'false positive' problem has remained steady for many vendors. This year alone, updates from major AV vendors have shut down QuickTime, killed Microsoft Excel, and even identified core operating system files as threats, thereby interrupting operations.

So, if you are using four or five anti-virus engines, you have essentially increased the likelihood of a false positive by up to 500 percent. Not a smart trade-off for potentially faster detection.



GFI Software

15300 Weston Parkway Suite 104
Cary, NC 27513 USA
Tel: +1 (888) 243-4329
Fax: +1 (919) 379-3402
www.gfi.com • sales@gfiusa.com