

WHY TRADITIONAL ENDPOINT PROTECTION WILL NO LONGER CUT IT.

Symantec Endpoint Protection 12 provides world-class protection for the realities of today.

Malicious code is in a constant state of evolution, finding new forms, disguises, and vectors to reach, penetrate, and compromise its targets. Consider these alarming trends:

- 51% of all malicious code signatures catalogued by Symantec appeared in 2009, a 71% increase over 2008
- 57% of all malware detected by Symantec was new – seen only once

Insight: the power behind Endpoint

Symantec Insight, the foundation that Endpoint Protection 12 is built on, is reputation-based security technology that puts files in context. IT users their age, frequency, location and more to expose threats otherwise missed.

Cyber-criminals use rapid mutation technology to prevent security solutions from identifying the signatures of their code. Insight finds newly mutated programs, detecting threats as they're created and rating their level of risk based on how new and common the program is, as well as its source and other security metrics.

With Insight, malware creators are caught in a Catch-22 – mutate too little and get caught by signature-based protection, mutate too much and get caught by Insight.

Some of Insight's accomplishments to date:

- Directly blocking over 8.7 million attacks.
- Assisted in blocking over 31 million attacks.
- Tracked more than 2.5 billion files.
- Served 2.5 billion Insight ratings each day.

While mass emails and other traditional attacks are still common, years-old malware still finds thousands of unprotected computers to exploit. The trends are clear: its harder than ever for traditional signature-based antivirus software to keep up to the rapid evolution of threats.

Signature-based antivirus software, for its part, is effective against viruses, trojans and worms for which signatures have been catalogued. But signature based defenses are useless in encounters with new malware or malwayre which mutates so that it's more difficult to pick up a signature. Because of this vulnerability, signature-based AV is typically backed by additional lines of defense—often tools that look for so-called generic signatures, and advanced heuristics that look for evidence of malicious behavior. These add substantial protection, but impact performance more than scanning for signatures. They also have lower accuracy and generate more false positives, reducing employee productivity and paradoxically creating incentives for companies to dial back protection.

Another issue with traditional endpoint protection is that it hasn't been optimized for virtual environments. The lack of awareness for the virtual environment leads to performance issues and security risks.

Symantec Endpoint Protection 12 leverages reputation-based state-of-the-art defense (see "Insight: the power behind Endpoint" sidebar for more details) against all types of attacks for both physical and virtual systems. Seamlessly integrating essential security tools into a single, high performance agent with a single management console, Endpoint Protection 12 provides leading protection without compromising efficiency and productivity.

Unrivaled Security: Symantec Endpoint Protection 12 blocks new and unknown threats missed by traditional signature, heuristic, behavioral and HIPS-based security solutions. All of the product's security engines are now reputation-enabled, leveraging Insight's online reputation database to identify and block malware attacks. Symantec's Insight has analyzed the anonymous software adoption patterns from more than 175 million customer computers to automatically derive highly accurate security ratings for more than 2.5 billion unique software files—Insight has ratings for virtually every software file, good or bad in existence.

Built for Virtual Environments: Symantec Endpoint Protection 12 offers comprehensive defense against all types of attacks and is optimized for performance on virtual systems by scanning virtual machines intelligently – for instance, it doesn't scan every virtual machine at the same time, knows which machines have already been scanned and protected from current threats and skips machines it knows are already protected. These innovations dramatically reduce the load on virtual hosts, alleviating 'AV Storms' /concurrent scans from bogging down system resources and allowing for faster, more responsive systems.

Fastest Performance: Symantec Endpoint Protection 12 leverages cloud-based community intelligence to reduce the overhead of virus scanning by as much as 70 percent by using Symantec Insight to automatically identify and whitelist trusted high-reputation files, resulting in fewer, faster and smarter scans. The new, Insight-driven compatible scan engine is also designed to do most of its work while computers are idle.

Ask your Account Manager whether Endpoint Protection 12 is right for your physical and virtual environments.

Need straight talk on security? Softchoice can help.

Softchoice Security Solution Architects are here to help you find the best technology and best fit for your environment. You can connect with us by calling **1-800-268-7638** – and be sure to check out our IT Grok blog at blogs.softchoice.com/itgrok where we share the knowledge, expertise and unbiased IT advice of our 100+ Enterprise Technical Architects. It's like having your own internal technology trends research team at your fingertips!

