

# Network Box 'Sentinel AV' Antivirus Engine Launched

New antivirus engine focuses on developing signatures for emerging threats in less than one minute.



A new virus detection and signature service launched by Network Box, the premier managed security service company, aims to reduce the time it takes to respond to serious new internet threats by cutting response times down from hours, which is common throughout the anti-virus industry, to less than one minute.

Network Box's Sentinel AV anti-virus engine focuses on developing its own signatures to protect against emerging viruses within one minute of a threat being seen rather than waiting for the antivirus industry to release a new signature which can often take several hours.

The new Sentinel AV anti-virus engine works with Network Box's existing anti-virus technology and award winning automatic PUSH update systems to provide the fastest protection against new threats available on the market.

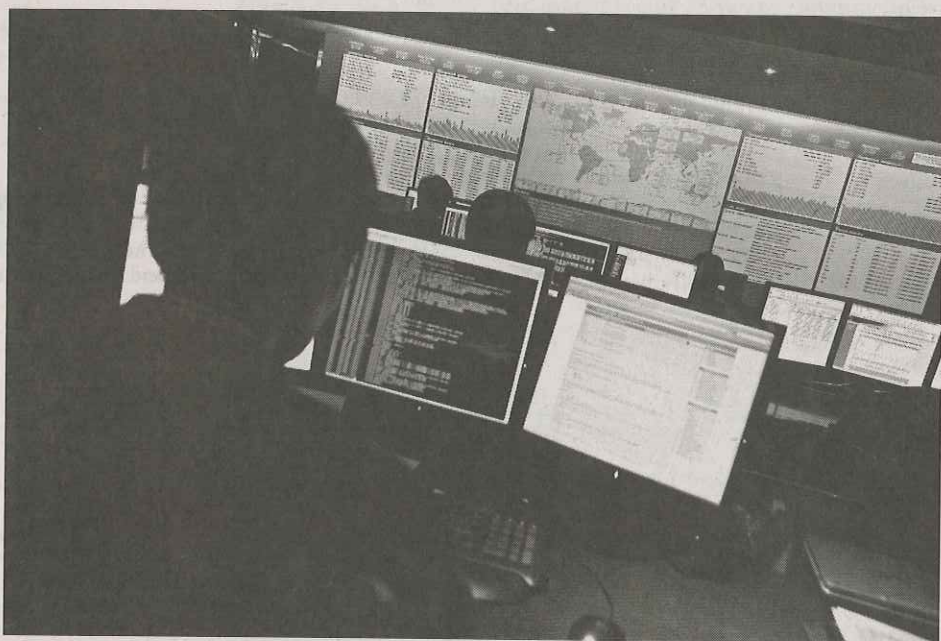
While heuristic, reputation, and relationship technologies continue to improve and are very important tools in the fight against malware, signature-based systems remain the primary technology used in malware protection today.

August 2010 saw another huge increase in the number of malicious viruses spreading via email, up 296.6% from July. The sheer volume of malware and the work that needs to be done to protect against each - obtaining samples, analysis, producing and validating signatures, and then releasing updates - means that the process of protecting against an emerging threat using traditional technology can take several hours.

The Network Box Sentinel AV anti-virus engine was designed to reduce this time to less than one minute by producing its own signatures in addition to the existing process of releasing millions of antivirus signatures from the top antivirus software manufacturers to each Network Box system.

Response times during testing were less than 30 seconds for a signature to deal with a single new suspicious sample; and less than 15 seconds for multiple samples. Signature release time globally is less than 3 seconds, including thorough validation.

The Network Box Sentinel AV anti-virus engine operates by continually analysing all the threat information that is received by the company's proprietary Network Box Security Response system which includes spam-traps,



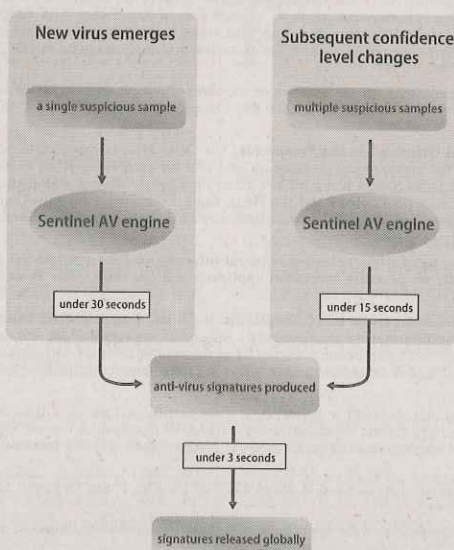
virus-traps, in-house submissions, customer submissions, mail statistics, http statistics, and suspect samples. This is done 24 hours a day, seven days a week, 365 days a year.

This information is used to determine that a particular object may be malicious and the system maintains a confidence level for the

likelihood of an object being malicious. Security managers can set that level to whatever they want. The default block is 50% but it can be adjusted according to each company's individual security requirements.

For more information, please see [www.network-box.com.hk](http://www.network-box.com.hk).

## The Flowchart of Sentinel AV Engine



## About Network Box:

Network Box Corporation, is a multi-award winning managed security services company, specialising in Unified Threat Management (UTM). It continuously defends the networks of its customers using PUSH technology to instantaneously update protection, from 12 Security Operations Centres spread across the globe. Network Box Corporation has been named one of the world's Top 100 Strategic IT Vendors by MIS Asia Magazine for three years. The company's customers across the globe, include many of the world's best known corporations, organisations, and government departments.

Website:  
[www.network-box.com.hk](http://www.network-box.com.hk)