

ESET Is Recognized by Frost & Sullivan for Hybrid
Network Security Technology That Offers Proactive
Threat Protection



ESET Is Recognized by Frost & Sullivan for Hybrid Network Security Technology That Offers Proactive Threat Protection

Adapted from Innovations in Network Security, a Research Service Released by the Technical Insights Unit of Frost & Sullivan, 31 Mar 2006

ESET leverages technology based on active heuristics and traditional malware signatures to protect against unknown and existing threats

A burgeoning increase in blended threats has necessitated the development of sophisticated security techniques and systems that help mitigate threats to networks caused by malicious programs.

A blended threat receives its name from the integration or mixing of different malware components, including trojan horses and worms. Threat detection is challenging due to minor variations associated with each instance of an attack. Malware frequently evades anti-threat solutions for prolonged periods of time, causing significant damage.

Implementing proactive methods is one way to combat attacks. Patent-pending ThreatSense technology developed by ESET leverages an advanced heuristic-approach in combination with a malicious signature-based approach to effectively mitigate existing and unknown future threats.

The technology works by proactively closing the window of vulnerability that is left open by reactive schemes that rely on updating signatures to detect malware, and it offers real-time protection against viruses, trojans, spyware, adware and identity theft.

ESET has developed ESET's NOD32 antivirus software based on its proprietary ThreatSense technology. The software is an optimized engine offering a unified solution to detect and protect against a dizzying array of threats. The key value proposition of NOD32 is the active heuristic technique that is implemented by code emulation to trick malware. This distinguishing feature in conjunction with less utilization of system resources helps maintain better performance and speed of operation.

In marked contrast to existing threat detection systems that rely on either the signature based approach or heuristics, ThreatSense technology offers a bundled solution. The advanced heuristics based approach makes use of traditional malware signatures to detect existing viruses. Attacks by a variant of the malware family are diagnosed using next generation generic signatures.

Detection of malware that is unspecified in the signature is handled by proactive handling and analysis of code. Attacks are effectively and immediately detected and the network is protected to prevent future invasion of the system by the same threat. Zero-day attacks normally occur when traditional antivirus vendors develop a new signature, test it, and then push it out to customers; several hours pass while networks remain vulnerable. ESET's integrated technology effectively addresses this problem through the heuristic approach.

ThreatSense implements unpacking and emulation techniques to eliminate issues related to archiving and packing--the two approaches most often followed by virus writers to attack networks and evade signature-based detection.

Speaking to Technical Insights, Andrew Lee, Chief Technical Officer, ESET says, "Every device with an IP address is vulnerable, and therefore requires an antivirus solution. Given this, the technology has wide application and

is not restricted to any particular market or organization. ThreatSense is a newer marketing term which also includes the latest 'stage' known as advanced heuristics and generic signatures. We believe that a security vendor should deliver protection as soon as it is available, not necessarily according to magazine review cycles. So, we recently delivered additional protection from rootkits." Rootkit detection prevents infiltration as it is initiated. It is done using intelligent signatures to prevent users from getting a false notion of security as their systems are updated.

ESET's Program Component Update (PCU) system dynamically updates logic that detects malware, a process similar to updating signatures. The clear benefit of this approach is that customers do not need to buy a new version of the product every year under the guise of adding detection functionality. ESET NOD32 Antivirus also features a single scanning engine so users do not need to rely on additional point solutions for spyware and adware protection. End-users and IT administrators neither suffer from network delays nor are hit by CPU performance issues as the NOD32 uses a small foot print.

The breakthrough idea of integrating defense procedures with a host of techniques to offer full protection has achieved recognition in the form of a recent partnership agreement between Universidad Tecnologica Nacional, the National Technology University of Argentina and ESET. The university aims to offer a security and anti-malware course spanning the areas of virus defense, network and endpoint security, as a part of its computer science degree program, leveraging ESET's technical innovation and intelligence.

About Frost & Sullivan

Frost & Sullivan, a global growth consulting company founded in 1961, partners with clients to create value through innovative growth strategies. The foundation of this partnership approach is our Growth Partnership Services platform, whereby we provide industry research, marketing strategies, consulting and training to our clients to help grow their business. A key benefit that Frost & Sullivan brings to its clients is a global perspective on a broad range of industries, markets, technologies, econometrics, and demographics. With a client list that includes Global 1000 companies, emerging companies, as well as the investment community, Frost & Sullivan has evolved into one of the premier growth consulting companies in the world. For more information, visit www.frost.com,

About ESET

Founded in 1992, ESET is a global provider of security software for enterprises and consumers. ESET's award-winning, anti-threat software system, NOD32, provides real-time protection from known and unknown viruses, spyware and other malware. NOD32 offers the smallest, fastest and most advanced protection available, with more Virus Bulletin 100% Awards than any other antivirus product (www.virusbulletin.com). ESET was named to Deloitte's Technology Fast 500 four years running, and has an extensive partner network, including corporations like Canon, Dell and Microsoft. Eset is headquartered in Bratislava, SK; offices in San Diego, USA; Prague, CZ; Buenos Aires, AR; and is represented worldwide in more than 80 countries. For more information, visit www.eset.com.