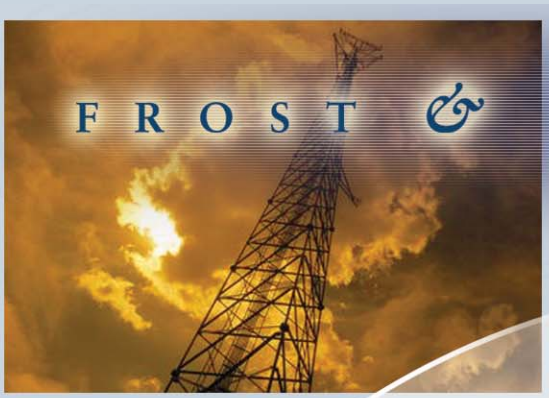


ESSENTIAL SECURITY AGAINST EVOLVING THREATS

A Frost & Sullivan White Paper

INTRODUCTION

Security is no longer optional and has become an absolute need for the successful running of today's businesses. However, the selection of the right partner is crucial to ensure complete protection from current and future threats.

Traditionally, security solutions follow a tedious process whereby a new vulnerability is identified by the vendor, a new signature to neutralise that vulnerability is created and tested, and finally relies on end users to deploy these signature updates on a regular basis. This process, despite being partially automated in most cases, introduces an unacceptable time lag and can be prone to errors as even signatures can be flawed and expose the system to new threats.

This approach has proven to be insufficient in today's environment due to its reactive nature and its lack of protection from threats unknown to the vendor. Therefore, businesses cannot rely on this reactive approach and need more proactive measures in place for total protection against evolving threats, such as modern viruses, spyware and phishing attacks.

Security vendors track the time between the discovery of a vulnerability and the release of attacks exploiting that vulnerability. Most vendors and clients are secretly terrified of a phenomenon know as a "zero day exploit." A zero day exploit is an attack that is released into the wild as soon as, or before, the vulnerability it exploits is publicly identified. The time between vulnerability discovery and exploit release has been rapidly decreasing, and the advent of widespread zero day exploits is not far away.

REACTIVE VS. PROACTIVE SOLUTIONS

On one hand, signature-based security solutions are reactive measures as they only react when a known threat tries to compromise the system. The problem is that signature based solutions can only detect known attacks with identification signatures that need to be deployed in the users' system at the time of the attack. Therefore these solutions offer adequate protection from known threats, but are useless when a new threat emerges. Signature-based systems protect well against known threats launched by script kiddies, but in a world of evolving professional hacking, malicious zero day attacks may soon become commonplace.

On the other hand, heuristics-based solutions are proactive security measures, which can protect systems from threats before security vendors identify the threat and build a signature. Heuristic solutions obtain their results using reasoning from past experiences, theoretical reasoning and learn to recognize how the object under examination behaves. However, this term is often misused to refer to solutions that only offer part of the full potential of heuristics analysis, such as enhanced signature analysis. Some of the so-called heuristics solutions are just a poor complement to signature analysis, and buyers should beware of the subtle differences, which are often obscured by marketing.

Table 1 below summarizes the different approaches taken by security vendors for threat protection.

APPROACH	HOW IT WORKS	PROS	CONS
Signatures	Looks for known malware that matches the signature. It is an exact science, that returns a single unambiguous result	• Good protection against known threats, but not their variances	• No protection against any unknown exploits • Time lag signature update process, which opens windows of vulnerability
Generic Signatures	Pattern recognition in variances of known malware. This is a basic form of heuristics that can only give a probability.	• Enhanced protection against polymorphic or evolved forms of known threats • Provide more accurate identification at an earlier stage	• No protection against totally new threats • Prone to false positives
Sandboxing	Execution of the file in an isolated environment either in a virtual or a live machine	• Satisfactory identification of new threats	• Could be fooled by smart code when executing the suspicious file • Large overhead in terms of performance and size
Passive Heuristics	String search of files	• Good complement to signatures and especially to code emulation.	• Defeated by polymorphism, encryption and runtime packers • If used alone it is prone to false positives
Advanced Heuristics	Simulation of specific parts of the code performed in a secure virtual environment using elements of different methods (generic signatures, emulation, passive heuristics, algorithmic analysis)	• Best protection against new threats • Zero day protection • Very low false positives • Fast, secure and best performance	• Will eventually require updates to algorithms

Source: Frost & Sullivan

ESET'S APPROACH TO THREAT PROTECTION

ESET's Distinctive Approach

ESET's NOD32 offers a truly distinctive approach in the way content threats are combated. The application of advanced heuristics to detect new threats is the key differentiator, but, NOD32 also includes signature-based scanning capabilities to enhance its protection against known threats. The combination of techniques unified in a single engine called ThreatSense™ gives NOD32 an edge, maximizing protection from existing and future threats, including viruses, spyware and even phishing attacks.

ThreatSense™ acts as a virtual malware researcher in the software by applying multiple and complementary methods for threat detection. Amongst the techniques it applies is a hybrid of heuristic-based methods including emulation, passive heuristics, algorithmic analysis and generic signatures. One of NOD32's key strengths is its ability to utilize its different techniques in a parallel fashion to maximize performance.

Proven Zero Day Protection

Zero day protection is becoming a catch phrase that several vendors use inappropriately to catch-up in the market. However, this concept is generally misused and misunderstood. Zero day protection means user protection from known and emergent threats from the very moment. This means real-time proactive protection. Instead, some of these so-called zero day protection solutions take hours to be deployed and all updates need to be installed before they are effective.

ESET is a truly proactive vendor that delivers on the concept of zero day protection. Its proven ThreatSense™ proactive technology uses a combination of heuristics techniques that allow NOD32 to stop new threats from day one of deployment.

"We tested 13 products and evaluated each on its ability to not only identify viruses and Trojans, but to block them. We found that ESET's NOD32 had the highest success ratio. It is an outstanding product with excellent support, and in our opinion the best antivirus solution out there."

Scott Brown
Information Security Analyst
Colby-Sawyer College

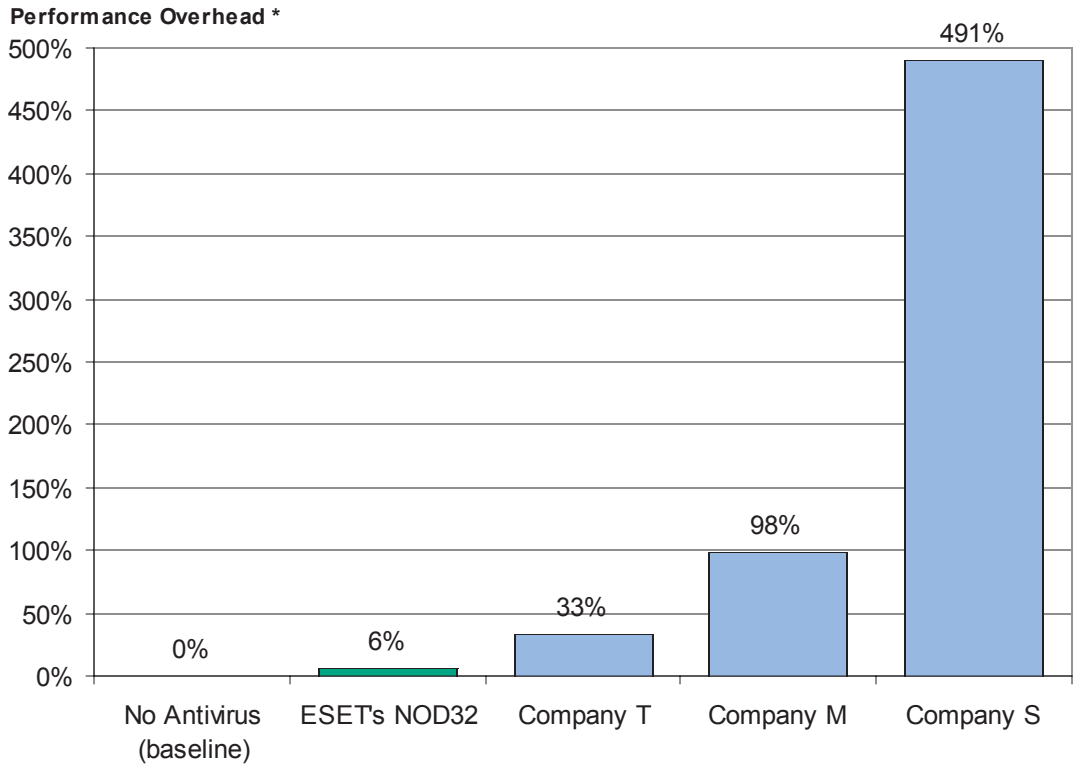
Key Strengths

NOD32 is in essence a very effective product, which offers one of the best detection rates in the industry. According to Virus Bulletin, a leading independent testing organization, NOD32 has not missed a single In-the-Wild virus in the past seven years.

NOD32 is also easy to install, use and maintain. Installation is very fast and can be performed within minutes for average size networks from one centrally managed console.

One of the most important strengths of the product is its low impact on performance. Due to its low resource utilization, especially for memory and CPU usage, the presence of NOD32 is barely noticeable. As an example, Chart 1 shows NOD32's low overhead compared to its leading competing vendors.

Chart 1 Performance of Antivirus Solutions



* Excel file open/close with active On-Access Scanner (average of 200 repeated operations)

Source: Canon System Solutions Inc testing

"Overall, no other security product could match NOD32 in terms of ease of use, speed, detection and cost. It's exciting to see ESET's advanced approach to this ongoing problem and witness firsthand the results of their heuristics as well as signature based technology".

Matt Marchione
Data Security Specialist
Burlington Coat Factory

"It finds stuff previous corporate Anti-virus software hasn't, on the client computers it takes far less time to load on boot-up, and it runs complete system scans in a fraction of the time that our previous solution takes. The amount of system resources it consumes is minimal which is always handy in a Windows environment. Again, I applaud your company on its superior and most excellent software and we are thus far very happy. I will recommend NOD32 to all IT professionals I deal with".

Eric Beckman
Regional Desktop Coordinator
Select Group

In addition, NOD32 offers centralized deployment, management and reporting, which makes it easily configurable across different platforms and layers. This is increasingly important given the hybrid nature of today's networks.

ESET operates globally distributed research labs, which enable the company to be at the forefront of new threat identification. This intelligence is then incorporated into the ThreatSense™ engine for improved effectiveness. In addition, ThreatSense.Net facilitates the automated submission of suspicious code to ESET's labs for further anlaysis. It also acts as an early warning system to notify clients of impending outbreaks and protective measures, as well as the timely notification of clients.

Key differentiating factors

NOD32 is different from the rest of solutions Frost & Sullivan has come across in the market. ESET's use of its unique ThreatSense™ technology has several benefits in terms of product performance, speed and effectiveness, derived from years of evolution. Ultimately, this translates into important benefits to its customers.

Table 2 below summarizes NOD32's key differentiating factors, implications and benefits to its customers, which make NOD32 such an advanced alternative:

"NOD 32's low system resource usage, quick and easy updating and detection accuracy could not be matched"

IT Manager
Top Global 5 Telecommunications company

Table 2: ESET's key differentiating factors, implications and customer benefits

KEY DIFFERENTIATING FACTORS	IMPLICATIONS	CUSTOMER BENEFITS
• ThreatSense™: unified engine including ThreatSense technology giving advanced heuristic detection of new threats • ThreatLabs: research lab that feeds intelligence into ESET's products and services •ThreatSense.Net:system to alert customers of new malicious code detected by ThreatSense heuristics •Free Worldwide technical support	• Immediate protection against all types of threats –Does not rely on known threats or identification • Protection from future threats –Its techniques apply to future malware • Improved protection against: – Spyware, Adware, Riskware – Potentially dangerous applications – Most common threat families – Generic Archive Unpacker – Alternate Data Streams – Automated cleaning of System Restore Points • Improved performance via "Smart" application of Advanced Heuristics • Low False Positives – Well balanced scoring based on code analysis and signatures • Early warning of new threats for other customers – Cleaners provided faster – Analysis available earlier	• Higher level of data integrity with guaranteed protection against all types of threats • Greater uptime and productivity savings for employees – less downtime through scanning speed, and fewer malware infections • Cost savings for IT budget and personnel, due to lower acquisition and maintenance costs • Higher Return on Investment (ROI) as a result of increased user compliance, decreased downtime, and higher productivity • Lower Total Cost of Ownership (TCO) as a result of savings in license acquisition, product maintenance and support

Source: Frost & Sullivan

CONCLUSION

Due to the evolving nature of content threats, it is no longer sufficient to rely on reactive security solutions that leave unacceptable windows of vulnerabilities. This approach is totally ineffective against evolving threats that can easily fool traditional security solutions.

The use of proactive security solutions that fully utilize the capabilities of heuristic techniques is highly recommended for efficient protection against all types of threats. Ideally, a combination of different heuristic techniques coupled with a traditional signature based scanning approach, gives users the best possible weapon to fight against known and evolved threats. However, performance cannot be compromised and that is why code emulation appears to be the safest and lowest impact option. This is effectively ESET's approach and why its NOD32 product stands out from the crowd.

Frost & Sullivan believes that ESET's proactive approach meets the needs of today's businesses. The company's track record and its unique approach to this market make it the ideal partner to beat current and future content threats.

CONTACT US

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

Sao Paulo

London

Oxford

Frankfurt

Paris

Israel

Beijing

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapore

Sydney

Tokyo

Cape Town

ABOUT ESET

Founded in 1992, ESET is one of the longest established players in the anti-virus and threat protection market. The company's flagship product is called NOD32, an increasingly popular product amongst businesses. With offices in North America, and Europe, ESET is distributed and supported in more than 80 countries worldwide. The company has experienced fast growth over the last few years as shown by Deloitte's Technology Fast 500 award, which ESET has received for three consecutive years.

ABOUT FROST & SULLIVAN

Frost & Sullivan, a global growth consulting company, has been partnering with clients to support the development of innovative strategies for more than 40 years. The company's industry expertise integrates growth consulting, growth partnership services and corporate management training to identify and develop opportunities. Frost & Sullivan serves an extensive clientele that includes Global 1000 companies, emerging companies, and the investment community, by providing comprehensive industry coverage that reflects a unique global perspective and combines ongoing analysis of markets, technologies, econometrics, and demographics. For more information, visit http://www.frost.com.