

F R O S T &

S U L L I V A N

LIVRE BLANC

« PROTECTION EN
TEMPS RÉEL CONTRE
TOUTES LES MENACES »

INTRODUCTION

La sécurité informatique n'est plus une option. Elle est devenue un besoin vital pour le bon fonctionnement des entreprises. Cependant, le choix de « la bonne solution » est crucial pour assurer une protection intégrale face aux menaces actuelles et futures.

Traditionnellement, les solutions de sécurité suivent un processus laborieux : une nouvelle vulnérabilité est identifiée, une signature est créée et testée en conséquence, puis distribuée en téléchargement lors des mises à jour des bases antivirus. Ce processus, en dépit d'être partiellement automatisé dans la plupart des cas, présente un délai inacceptable et peut être enclin aux erreurs. Parfois, les signatures elles-mêmes peuvent être défectueuses et exposer le système à de nouvelles menaces.

Il a été prouvé que cette approche est insuffisante dans l'environnement actuel, notamment en raison de sa nature réactive, et de son manque certain de protection face aux virus inconnus. Par conséquent, les entreprises ne peuvent se limiter à cette approche réactive. Elles ont besoin de mesures proactives en place pour assurer une protection totale contre les menaces évoluées, comme les virus modernes, les Spyware et les attaques de type Phishing.

Les éditeurs d'antivirus misent sur le temps entre la découverte d'une vulnérabilité et la propagation des attaques exploitant cette vulnérabilité. De nombreux éditeurs et utilisateurs craignent un phénomène connu sous le nom de zero day exploit (Exploitation immédiate). En réalité, il s'agit d'une menace propagée dès que, ou même avant que, la vulnérabilité qu'elle exploite soit publiquement identifiée. Le temps entre la découverte d'une vulnérabilité et son exploitation a considérablement diminué, et la prolifération du phénomène zero day exploit est imminente.

SOLUTIONS RÉACTIVES CONTRE PROACTIVES

Il existe des solutions réactives, basées sur un ensemble de signatures, n'agissant que lorsqu'une menace connue tente de compromettre la stabilité du système. Le problème de ce type de solutions est qu'elles ne peuvent détecter que les attaques connues, grâce aux signatures d'identifications qui nécessitent d'être présentes sur le système au moment de l'attaque. Par conséquent, ces solutions offrent une protection adéquate pour les menaces identifiées, mais totalement inutile face aux nouvelles menaces.

D'autre part, les solutions proactives, basées sur un système d'analyse heuristique, protègent votre système avant qu'une menace soit identifiée et signée. Ces solutions utilisent un raisonnement basé sur des expériences antérieures, un raisonnement théorique et apprennent à identifier « comment » l'objet se comporte lors de son examen. Cependant, ce terme est souvent utilisé à mauvais escient pour qualifier des solutions qui n'offrent qu'une partie de la pleine capacité de l'analyse heuristique, comme par exemple une analyse améliorée de signatures. Certaines des prétendues solutions heuristiques sont en réalité un faible complément à l'analyse par signatures, et les utilisateurs devraient prendre garde à ces subtiles différences, souvent obscurcies par le marketing.

Tableau récapitulatif des différentes méthodes choisies par les éditeurs d'antivirus

Technique	Mode de fonctionnement	Avantages	Inconvénients
Signatures	Analyse se référant à une base de donnée de Malware connus. Il s'agit d'une science exacte, le résultat est évident, simple et unique.	<ul style="list-style-type: none"> ■ Bonne protection contre les Malware connus (mais pas leurs variantes). 	<ul style="list-style-type: none"> ■ Aucune protection face à des menaces inconnues. ■ Le temps de latence lors des mises à jour laisse des failles de sécurité importantes.
Signatures Génériques	Identification par "modèle" des variantes de virus déjà connus. Méthode heuristique basique, elle ne peut donner qu'une approximation.	<ul style="list-style-type: none"> ■ Protection efficace contre les vers polymorphes ou les nouvelles variantes de menaces connues. ■ Procure une protection plus efficace et plus précoce que les simples signatures. 	<ul style="list-style-type: none"> ■ Pas de protection contre des menaces totalement nouvelles. ■ Tendance à l'erreur (fichier considéré à tort comme dangereux).
"sand-boxing"	Exécution du fichier dans un environnement isolé, tant sur une machine émulée que sur une machine physique.	<ul style="list-style-type: none"> ■ Identification satisfaisante des nouvelles menaces. 	<ul style="list-style-type: none"> ■ Peut être trompé par certains scripts exploitant un programme dangereux. ■ Très gourmande en matière de ressources systèmes.
Heuristique Passive	Recherche par chaîne de caractères.	<ul style="list-style-type: none"> ■ Bon complément aux signatures et spécialement pour les systèmes d'émulation. 	<ul style="list-style-type: none"> ■ Inutile face aux polymorphes, aux fichiers cryptés et aux archives auto extractibles. ■ A utiliser en complément d'une autre solution pour éviter les erreurs.
Heuristique Avancée ou Proactive	Simulation de certaines parties du code suspect, dans un environnement virtuel sécurisé en utilisant différentes méthodes (heuristique passive, signatures normales et génériques, exploitations d'algorithme)	<ul style="list-style-type: none"> ■ Protection optimale contre les nouveaux vers. ■ Protection de type "Zero Day". ■ Rapide, fiable, obtient les meilleures performances. 	<ul style="list-style-type: none"> ■ Nécessite occasionnellement des mises à jour au niveau de l'algorithme.

APPROCHE D'ESET EN MATIÈRE DE PROTECTION

L'approche distincte d'Eset.

Le NOD32 d'Eset offre une approche réellement distincte dans sa lutte contre les menaces informatiques. L'utilisation d'une analyse heuristique avancée de type Proactive pour détecter de nouvelles menaces en est la clé. Par ailleurs, NOD32 inclut aussi une analyse fondée sur une base de signature virale, assurant parfaitement une protection contre les menaces connues. Cette combinaison, réunie en un seul et même moteur appelé ThreatSense™, procure à NOD32 une protection maximale contre les menaces actuelles et futures tel que les virus, les Spyware et même les attaques de type «Phishing».

ThreatSense™ agit comme un traqueur virtuel de Malware dans un logiciel en appliquant de multiples méthodes de détection complémentaires. Le système exploite alors un mélange hybride de méthodes heuristiques (incluant émulation, heuristique passive et analyse algorithmique) et une base de signature virale. L'un des principaux points forts de NOD32 est sa capacité à utiliser différentes techniques d'analyse en parallèle pour maximiser les performances.

Une protection immédiate (Zero day protection)

Zero day protection* devient un slogan que bon nombres d'éditeurs utilisent souvent de façon inappropriée pour séduire le marché. Par ailleurs, ce concept est souvent incompris et utilisé à mauvais escient. En effet, ce dernier implique une protection des menaces connues, mais aussi de toutes nouvelles menaces et ce, dès leur apparition. Cela implique une protection proactive en temps réel. Au lieu de cela, certaines desdites protections zero day mettent plusieurs heures pour être déployées, et toutes les mises à jour doivent être installées pour rendre la protection effective.

Eset fournit une solution réellement proactive correspondant au concept Zero day protection. Grâce à sa technologie ThreatSense™, reposant sur une combinaison des méthodes heuristiques, NOD32 est capable d'arrêter une menace le jour même de son apparition.

* Protection immédiate et permanente

« Le système de NOD32 est rapide, efficace, faible en consommation de ressource et possède un taux de détection incomparable »

*IT Manager
Top Global 5
Telecommunications
company*

« Nous avons testé 13 produits et évalué chacune de leurs capacités, non seulement pour identifier les virus et Trojans, mais aussi pour les bloquer. Nous avons constaté que NOD32 avait le plus important taux de réussite. C'est un produit exceptionnel avec un excellent support et, à nos yeux, la meilleure solution antivirus existante. »

*Scott Brown
Information Security Analyst
Colby-Sawyer College*

POINTS FORTS

NOD32 est un produit très efficace, qui offre l'un des meilleurs taux de détection de l'industrie antivirus. Conformément au Virus Bulletin, un organisme indépendant et leader dans le test antiviral, NOD32 n'a pas manqué le moindre virus In-the-Wild* (Dans la Nature) ces sept dernières années.

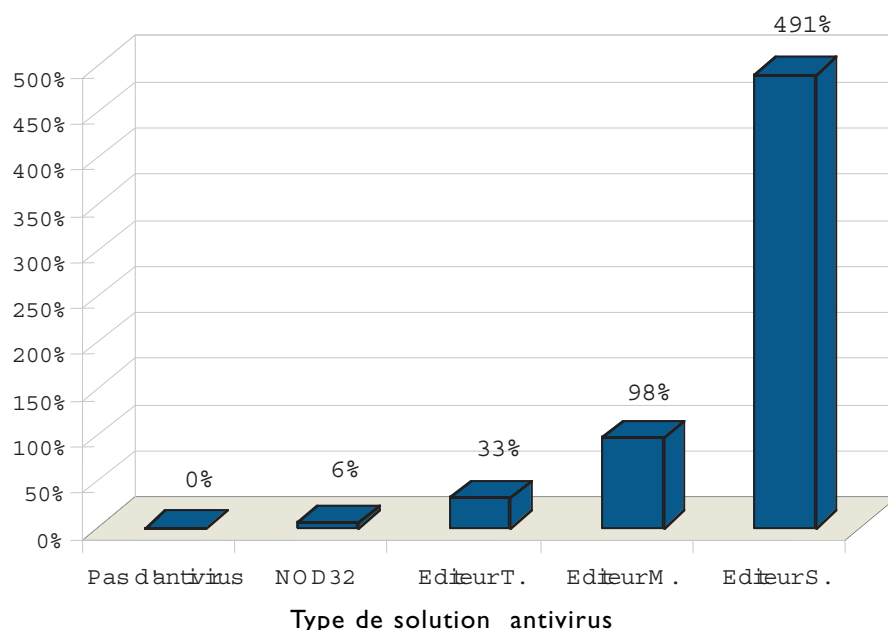
*Virus inconnu non répertorié

De plus, NOD32 est facile à installer, à utiliser et sa maintenance est également aisée. L'installation est très rapide et peut être réalisée en quelques minutes sur un réseau étendu depuis une seule et même console.

L'une des qualités les plus importantes de NOD32 est le faible ralentissement des performances système qu'il occasionne. La présence de NOD32 est à peine perceptible, en raison de sa faible consommation en ressource, notamment au niveau de la mémoire et de l'utilisation du processeur.

Pour exemple, le graphique suivant démontre la faible consommation de NOD32 en comparaison à celle de ses principaux concurrents.

Performance des Solutions Antivirus



Source : Canon System Solutions Inc testing

*Performances réalisées lors de l'ouverture/fermeture d'un fichier Excel, avec module d'analyse à l'accès activé (taux moyen constaté sur 200 opérations)

De plus, NOD32 Entreprise offre un déploiement, une gestion et des rapports centralisés, qui le rendent facilement configurable à travers différentes plateformes. Ceci est de plus en plus important étant donné la nature hétérogène des réseaux actuels.

« D'un point de vue général, aucun concurrent n'a pu rivaliser avec NOD32 en termes de facilité d'utilisation, de vitesse, de qualité de détection et de coût. Il est passionnant de découvrir l'approche avancée d'ESET dans ce domaine et d'être le témoin de leurs résultats en analyse heuristique et base de signatures virales »

*Matt Marchione
Data Security Specialist
Burlington Coat Factory*

« NOD32 détecte des virus que les précédents antivirus ne trouvaient pas sur les ordinateurs clients. Il est bien plus rapide au démarrage et réalise une analyse complète du système en une fraction de seconde par rapport à nos précédentes solutions. La quantité de ressources système consommée est minime, ce qui est toujours utile dans un environnement Windows. J'applaudis encore une fois Eset pour cet excellent antivirus de grande qualité dont nous sommes jusqu'ici très satisfaits. Je recommanderai NOD32 à tous les professionnels IT avec lesquels je travaille. »

*Eric Beckman, Regional
Desktop, Coordinator,
Select Group.*

Eset opère globalement, grâce à différents laboratoires de recherche, ce qui lui permet d'être au premier plan en ce qui concerne l'identification de nouvelles menaces. Cette technologie est intégrée au moteur ThreatSense™ pour une efficacité toujours plus grande. Par ailleurs, ThreatSense.Net facilite la soumission automatique des codes suspects aux laboratoires d'Eset pour une analyse plus approfondie. Son fonctionnement se rapproche de celui d'un système d'alerte préventif qui informe les utilisateurs de menaces imminentes, des mesures de sauvegarde à prendre, tout en recensant des informations émanant des clients.

Principaux facteurs de différenciation

NOD32 est différent des autres solutions testées et présentes sur le marché. L'utilisation par Eset de leur technologie unique ThreatSense™, leur confèrent bon nombre d'avantages en termes de performance, de vitesse et d'efficacité. Très récemment, ceci s'est traduit par d'importants avantages pour l'utilisateur.

Tableau récapitulatif des principaux facteurs de différenciation des implications et des avantages que NOD32 apporte à ses utilisateurs.

Principaux facteurs de différenciation	Implications	Bénéfices pour l'utilisateur
<p>ThreatSense™: moteur unique incluant la technologie ThreatSense, permettant une détection heuristique avancée des nouvelles menaces</p> <p>***</p> <p>ThreatLabs : laboratoire de recherche, à l'origine des produits et services proposés par ESET</p> <p>***</p> <p>ThreatSense.Net : système d'alerte pour les utilisateurs lors de l'apparition d'une nouvelle menace, détectée par l'analyse heuristique avancée du moteur ThreatSense™</p> <p>***</p> <p>Support technique mondial gratuit</p>	<ul style="list-style-type: none"> ▪ Protection immédiate contre tous types de menaces <ul style="list-style-type: none"> - Non basé sur les virus déjà connus ▪ Protection contre des futures menaces <ul style="list-style-type: none"> -Technologie protégeant des futurs Malware ▪ Protection améliorée <ul style="list-style-type: none"> - Contre les Spyware, Adware, Riskware... - Contre la majorité des différentes menaces existantes - Contre les applications potentiellement dangereuses - Contre les archives auto extractibles - Nettoyage automatique des points de restauration système -Flux de données parallèles (alternate data streams) ▪ Performances améliorées par une optimisation de l'utilisation de l'heuristique avancée ▪ Peu de "fausses alertes" <ul style="list-style-type: none"> - Résultats bien équilibrés, basés sur une analyse heuristique et de signatures ▪ Système d'alerte rapide lors de la détection d'une nouvelle menace pour les autres utilisateurs <ul style="list-style-type: none"> - Mesure de nettoyage disponible plus rapidement - Permet une analyse plus précoce 	<ul style="list-style-type: none"> ▪ Meilleure intégrité des données, avec une garantie de protection contre tous types de menaces ▪ Gain de temps et de productivité pour les utilisateurs - en raison d'une analyse plus rapide, et moins d'attaques provenant de menaces diverses ▪ Réduction des coûts, notamment pour le budget IT, en raison d'un prix d'achat plus faible, et d'une baisse des frais de maintenance ▪ Un retour sur investissement plus important, en raison de sa simplicité, de sa fiabilité et du gain de temps/productivité occasionné. ▪ Un coût total plus faible, en raison de l'économie réalisée sur le coût d'acquisition des licences, la maintenance et le support.

Source : Frost & Sullivan

CONCLUSION

En raison de la nature évolutive des menaces actuelles, il est insuffisant de compter sur une simple solution de sécurité de type réactive, qui laisse place à un nombre inacceptable de vulnérabilités. Cette approche est totalement inefficace contre les menaces actuelles, qui se jouent facilement de telles solutions de sécurité.

L'utilisation d'une sécurité de type proactive qui utilise pleinement les capacités de la technologie heuristique est donc très fortement recommandée pour conserver une protection efficace contre toute forme de menace. Idéalement, une combinaison des différentes techniques heuristiques associée à une analyse fondée sur une base de donnée virale, donne à l'utilisateur les meilleures armes disponibles pour lutter contre les menaces connues et inconnues. Par ailleurs, les performances ne peuvent être ignorées et c'est pour cela que la technique « d'émulation de code » semble être l'option offrant le meilleur rapport performance/rentabilité. Ceci est l'approche d'ESET, et c'est pour cela que leur antivirus NOD32, se démarque de ses concurrents.

Frost & Sullivan pense que l'approche proactive d'ESET répond parfaitement aux besoins des entreprises. L'expérience professionnelle d'ESET et son approche unique du marché en font le partenaire idéal pour se protéger des menaces actuelles et futures.

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

CONTACT US

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

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 SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

Paris
24 rue de Londres
75009 Paris, France
Tel 33(0)1 42 81 54 50
Fax 33(0)1 42 81 54 52

A PROPOS D'ESET

Fondé en 1992 et basé à San Diego en Californie, Eset est l'un des acteurs ayant la plus longue expérience dans le domaine de l'anti-virus. Eset édite une solution antivirus globale nommée NOD32 Antivirus. Cette solution a reçu de nombreux prix, notamment la récompense « VBI00% » qui lui a été décernée 32 fois de suite par Virus Bulletin, la prestigieuse revue professionnelle de l'industrie antivirus.

Eset possède des bureaux à San Diego (USA), Londres (UK), Prague (CZ) et à Bratislava (SK). Grâce à cette implantation et une analyse en temps réel de dizaines de millions d'emails qui transitent quotidiennement dans le monde entier, ESET est capable de réagir très rapidement. C'est notamment grâce à cette technologie que l'antivirus NOD32 a détecté le premier la nouvelle variante du ver Bagle. Moins de deux heures après la détection de ce ver, une mise à jour de la base de signature était délivrée, permettant l'identification exacte et la désinfection de cette nouvelle variante qui fut nommée Win32/Bagle.AS par Eset.

Eset et NOD32 en France :

Tel 01 55 89 08 85 - info@eset-nod32.fr - <http://www.eset-nod32.fr>

ESET Software - Californie, USA - <http://www.nod32.com>

A PROPOS DE FROST & SULLIVAN

Frost & Sullivan, une société internationale de conseil en stratégies de croissance fondée en 1961, agit en collaboration avec ses clients pour créer de la valeur à travers des stratégies de croissance novatrices. Ce partenariat est fondé sur notre plateforme Growth Partnership Services par laquelle nous fournissons des études sur les industries, des stratégies de marketing, des conseils et de la formation à nos clients dans le but de les aider à développer leurs affaires. L'avantage essentiel que Frost & Sullivan apporte à ses clients est une perspective globale sur une vaste gamme d'industries, de marchés, et de technologies, et sur des données économétriques et démographiques. Avec une clientèle qui comprend des sociétés parmi les 1000 premières à un niveau mondial, des entreprises émergentes ainsi que la communauté financière, Frost & Sullivan est devenue l'une des plus grandes sociétés de conseil spécialisées en problématiques de croissance dans le monde. Pour plus d'informations consultez: www.frost.com.