

DEEP DISCOVERY

TESTS DE DETECTION DES INTRUSIONS - NSS LABS



Trend Micro™ Deep Discovery

- 1er sur la détection des intrusions
- TCO maîtrisé : 25% plus économique que la moyenne
- Zéro faux-positif

Le benchmark 2014 mené par NSS Labs en matière de détection des intrusions assure un bench mark indépendant de l'efficacité et du coût total de possession (TCO) des produits des acteurs suivants :

- Ahn Labs
- Fidelis
- FireEye
- Fortinet
- SourceFire
- Trend Micro

Ces tests ont soumis les 6 produits à un panel d'attaques sophistiquées menées à l'aide de malware et de manière intensive. L'évaluation du TCO intègre le prix d'achat, la maintenance et les coûts d'exploitation.

NSS Labs a testé Trend Micro™ Deep Discovery Inspector, une appliance réseau qui utilise plusieurs moteurs anti-malware, des environnements personnalisés de sandboxing et le service de veille Trend Micro™ Smart Protection Network, pour détecter les malware sophistiqués, les communications Command & Control (C&C), ainsi que le comportement des assaillants qui n'est que rarement identifié par les outils de sécurité classiques.

Les résultats des tests d'intrusions de NSS Labs

Produit				Détection d'intrusions	Performances testées
Trend Micro Deep Discovery Inspector Model 1000 v3.5				99,1%	1 000 Mbps
Malware HTTP	Malware Email	Exploits	Stabilité and Fiabilité	Evasions	Faux positifs
97%	100%	100%	OK	94%	0%

Trend Micro Deep Discovery : le meilleur score pour la détection d'intrusions

Le score de Deep Discovery Inspector: 99,1% — Le score le plus élevé parmi les outils testés en matière de détection des intrusions. Ces tests ont été menés sur des malware sophistiqués, acheminés par HTTP et SMTP, et qui utilisent différentes techniques d'infiltration et de contournement des outils de détection en place.

Ces tests ont utilisés des canaux HTTP et SMTP standards, mais les assaillants restent

susceptibles d'utiliser des protocoles tiers pour perpétrer leur exaction. Deep Discovery surveille plus de 80 protocoles et applications sur tous les types de ports réseau. Il en résulte une visibilité plus précise, et une détection des attaques à 360 °, qui porte au-delà des canaux HTTP et SMTP.

Zero faux-positifs

Deep Discovery Inspector affiche un taux de faux-positifs de 0% : aucun faux-positif n'a été détecté lors de ces tests.

TCO maîtrisé

Trend Micro s'impose également au second rang de ces tests dans le domaine du coût total de possession (TCO) le plus optimisé, avec des économies supérieures à 25% par rapport au TCO moyen des autres produits testés.

Des performances certifiées

Deep Discovery Inspector a tenu ses performances annoncées de 1 Gbps dans le cadre des tests réalisés par NSS Labs.

Pour accéder au rapport (anglais) du benchmark *NSS Labs Breach Detection System Comparative Analysis Security Value Map (SVM)*, RDV sur www.trendmicro.com/deepdiscovery