# McAfee Network Threat Behavior Analysis

## Visibilité complète sur le comportement sur le réseau et les menaces

McAfee® Network Threat Behavior Analysis fait partie intégrante de McAfee Network Security Platform, qui offre une visibilité en temps réel sur l'infrastructure réseau et la protège contre les menaces. En analysant le trafic provenant des commutateurs et routeurs, McAfee Network Threat Behavior Analysis est capable de détecter les comportements à risque sur le réseau et de bloquer efficacement les attaques furtives. La solution évalue dans leur globalité les menaces au niveau du réseau, identifie le comportement général de chaque élément du réseau et permet une abstraction instantanée du type d'anomalie ou d'attaque potentiel, notamment les logiciels malveillants (*malware*), les attaques de type « jour zéro », les réseaux de robots (*botnets*) et les vers. McAfee Network Threat Behavior Analysis héberge également plusieurs des moteurs avancés de McAfee Network Security Platform, dont le moteur d'émulation en temps réel qui identifie les logiciels malveillants sans utiliser de signatures.

### Principaux avantages

**Visibilité pour une sécurité efficace du réseau**

- Surveillance des comportements inhabituels sur le réseau et génération de rapports connexes grâce à l'analyse du trafic réseau
- Détection des menaces proactive basée sur le comportement
- Détection efficace des menaces inconnues
- Détection des anomalies, permettant d'identifier notamment les attaques de type « jour zéro », le spam, les réseaux de robots et les tentatives de sondage

**Protection antimalware complète**

- Blocage des logiciels malveillants grâce à l'émulation en temps réel des fichiers malveillants
- Corrélation avancée sur l'ensemble du réseau de manière à détecter l'activité des réseaux de robots
- Informations sur les postes clients et corrélation de celles-ci aux flux et événements réseau

### Une visibilité intelligente pour contrer les attaques furtives actuelles

Votre réseau est la cible d'attaques furtives avancées qui contournent les méthodes de détection traditionnelles, le laissant ainsi exposé à des compromissions et à des périodes d'indisponibilité qui paralysent votre entreprise. McAfee Network Threat Behavior Analysis exerce une surveillance intelligente pour signaler tout comportement inhabituel. Il analyse pour ce faire le trafic émanant de vos commutateurs et routeurs, ce qui permet d'identifier les attaques lancées contre votre réseau et d'y réagir rapidement.

L'appliance McAfee Network Threat Behavior Analysis exploite les données de flux NetFlow et J-Flow pour identifier les menaces au-delà du périmètre du système de prévention des intrusions (IPS). Elle inclut des processeurs quadricœurs, une baie de disques RAID et la connectivité Ethernet multigigabit. Elle offre également la connectivité à un SAN (Storage Area Network) hors ligne. Avec sa fonction de différenciation des flux, elle peut gérer de gros volumes de trafic réseau, en permettant une analyse plus rapide de celui-ci.

### Informations pertinentes et visibilité inégalée à l'échelle du réseau

McAfee Network Threat Behavior Analysis vous aide à prendre des décisions éclairées concernant les applications et protocoles de votre réseau. Il surveille et signale tout comportement inhabituel sur le réseau, et identifie les menaces à l'aide d'algorithmes basés sur le comportement.

En analysant tant le comportement des hôtes que celui des applications, il détecte les anomalies liées aux attaques de type « jour zéro », au spam, aux réseaux de robots et aux tentatives de sondage. Grâce à son analyse globale des flux, la solution décèle toute utilisation non autorisée d'applications et identifie les segments problématiques du réseau.

### Contrôle et prévention des attaques de logiciels malveillants

Opérant de concert avec McAfee Network Security Platform, McAfee Network Threat Behavior Analysis offre une émulation en temps réel qui garantit une inspection minutieuse et le blocage des fichiers suspects. Les moteurs d'émulation en temps réel analysent les fichiers suspects afin de détecter tout comportement malveillant et d'y mettre fin. Grâce à une corrélation avancée entre plusieurs appliances IPS et périphériques réseau, McAfee Network Threat Behavior Analysis détecte les réseaux de robots furtifs qui échappent à la vigilance des systèmes de protection traditionnels basés sur les signatures. En conjonction avec McAfee Endpoint Intelligence Agent, la solution identifie et bloque les postes clients compromis qui transmettent le trafic malveillant dissimulé sous la forme de trafic réseau légitime. L'analyse de l'activité des postes clients basée sur la réputation limite l'exfiltration de données et met en échec les attaques de logiciels malveillants.

## Rationalisation des opérations de sécurité et économies sur les coûts

McAfee Network Threat Behavior Analysis fournit les informations exploitables dont vous avez besoin pour gérer votre sécurité de manière rentable. L'appliance écourte les délais de réaction aux incidents et optimise les performances du réseau tout en bloquant les exploits et les menaces réseau afin d'éviter à votre entreprise les interruptions d'activité.

## Fonctionnalités supplémentaires

- Sécurité optimisée grâce à l'intégration avec McAfee Global Threat Intelligence (McAfee GTI)
- Edition virtuelle pour des implémentations rentables
- Visibilité étendue et corrélation grâce à l'intégration avec McAfee ePolicy Orchestrator® (McAfee ePO™), McAfee Enterprise Security Manager et McAfee Vulnerability Manager
- Tri et analyse aisés du trafic réseau
- Tableau de bord des métadonnées par flux (ID d'application, fichiers, URL)
- Renforcement de la sécurité grâce à des options de mise en quarantaine complètes
- Visibilité sur les hôtes externes, avec évaluations détaillées des facteurs de menace sur l'hôte
- Compatibilité avec les commutateurs et routeurs Cisco (NetFlow versions 5 et 9) et Juniper (J-Flow versions 5 et 9)

| | NTBA T-600 | NTBA T-1200 |
|---|---|---|
| **Spécifications** | | |
| Flux par seconde | Jusqu'à 60 000 | Jusqu'à 100 000 |
| Cisco NetFlow | Versions 5 et 9 | Versions 5 et 9 |
| Juniper J-Flow | Versions 5 et 9 | Versions 5 et 9 |
| Processeur | 1 processeur Xeon E5-2658 | 2 processeurs Xeon E5-2658 |
| Mémoire | 46 Go | 96 Go |
| Stockage utilisable | 4,4 To / Raid 10 | 8,8 To / Raid 10 |
| Interfaces réseau | 4 interfaces réseau cuivre 10/100/1000 | 4 interfaces réseau cuivre 10/100/1000 |
| **Environnement** | | |
| Format | 1U | 2U |
| Largeur | 43,8 cm | 43,8 cm |
| Profondeur | 70,94 cm | 70,78 cm |
| Hauteur | 4,32 cm | 8,76 cm |
| Poids maximal | 14,96 kg | 21,6 kg |
| Consommation électrique estimée (maximale) | 402 W | 667 W |
| Alimentation électrique redondante | 750 W | 750 W |
| Conditions de refroidissement du système (nombre de BTU/h générés) | 1 370 | 2 280 |
| Température de fonctionnement | +10 à +35 °C avec une variation maximale inférieure à 10 °C par heure | |

| Spécifications de l'appliance NTBA virtuelle | T-VM | T-100VM | T-200VM |
|---|---|---|---|
| Mémoire RAM recommandée | 16 Go | 8 Go | 16 Go |
| Nombre de processeurs recommandé | 4 | 4 | 4 |
| Flux par seconde | Jusqu'à 25 000 | Jusqu'à 10 000 | Jusqu'à 25 000 |

McAfee
An Intel Company

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr


60839ds_ntba_0214_ETMG