McAfee Advanced Threat Defense

Détection des logiciels malveillants avancés

McAfee® Advanced Threat Defense permet de détecter les logiciels malveillants furtifs et avancés, mais aussi de traduire les informations sur les menaces en mesures de protection immédiates. Par rapport aux environnements sandbox conventionnels, la solution présente des fonctionnalités d'inspection supplémentaires qui élargissent le champ de la détection et identifient les menaces appliquant des techniques de contournement. Les solutions de sécurité sont étroitement intégrées, du réseau jusqu'aux terminaux individuels et aux outils d'investigation. Cette intégration favorise l'échange instantané d'informations sur les menaces dans l'ensemble de l'environnement, ce qui améliore à la fois la protection et l'investigation. Des options de déploiement flexibles permettent de prendre en charge tous les types de réseau.

Nos technologies révolutionnent l'art de la détection en reliant des fonctionnalités avancées d'analyse antimalware aux mécanismes de protection existants (du périmètre du réseau jusqu'au terminal) et en partageant une cyberveille sur les menaces avec l'ensemble de l'environnement informatique. Grâce à ce partage d'informations au sein de l'écosystème, les solutions de sécurité intégrées agissent en synergie pour immédiatement interrompre les communications de prise de contrôle, mettre en quarantaine les systèmes compromis, bloquer les instances de menaces identiques ou similaires, établir l'impact du problème et prendre les mesures nécessaires.

McAfee Advanced Threat Defense : détection des menaces avancées

McAfee Advanced Threat Defense recourt à une approche multiniveau innovante pour détecter les logiciels malveillants « jour zéro » furtifs. La solution combine des méthodes d'analyse à faible empreinte, telles que les signatures de virus, l'analyse de la réputation et l'émulation en temps réel avec des fonctions d'analyse dynamique (sandboxing) pour décortiquer le comportement réel des logiciels malveillants. L'investigation se poursuit avec une analyse statique approfondie du code : celle-ci examine les attributs et les jeux d'instructions afin de déterminer le comportement furtif ou attendu et évalue les similitudes avec les familles de logiciels malveillants connus.

Principaux avantages distinctifs de McAfee Advanced Threat Defense

Intégration de solutions à grande échelle

- McAfee Advanced Threat Defense s'intègre avec les solutions McAfee déjà présentes, les passerelles de messagerie d'autres fournisseurs et d'autres produits reposant sur des normes ouvertes.
- Le délai entre la phase d'identification et les phases d'endiguement et de protection est réduit à l'échelle de toute l'entreprise.
- Les workflows sont optimisés pour une réponse et une correction plus rapides.
- L'intégration permet l'automatisation.

Gardez le contact

Au cours de la dernière étape de l'analyse, McAfee Advanced Threat Defense recherche spécifiquement les indicateurs malveillants identifiés grâce à l'apprentissage automatique via un réseau neuronal. Ensemble, ces fonctionnalités constituent la technologie de protection antimalware de pointe la plus puissante du marché, et offrent le juste compromis entre inspection approfondie et performances. D'une part, les méthodes d'analyse moins intensives telles que les signatures ou l'émulation en temps réel préservent les performances en bloquant les logiciels malveillants facilement identifiables. D'autre part, l'analyse statique approfondie du code et l'ajout des données d'apprentissage automatique à l'analyse sandbox étendent la détection aux menaces dissimulées et furtives. Les indicateurs malveillants qui ne peuvent pas s'exécuter en environnement dynamique peuvent être identifiés grâce à la décompression, à l'analyse statique approfondie du code et aux données d'apprentissage automatique.

Les auteurs de logiciels malveillants utilisent la compression pour modifier la composition du code ou la dissimuler, s'efforçant ainsi d'échapper à la détection. La plupart des produits sont incapables de décompresser correctement l'ensemble du code exécutable d'origine (source) pour analyse. McAfee Advanced Threat Defense comprend des fonctions de décompression étendues qui contrent les techniques de dissimulation et exposent le code exécutable d'origine. Il permet à l'analyse statique approfondie du code de rechercher des anomalies au-delà des attributs de fichiers de haut niveau, en analysant les attributs et jeux d'instructions afin de déterminer le comportement attendu.

Ensemble, l'analyse statique approfondie du code, l'apprentissage automatique et l'analyse dynamique offrent une méthode d'évaluation complète du logiciel malveillant potentiel. Ces résultats d'analyse hors pair sont consignés dans des rapports de synthèse pour vous aider à cerner l'ampleur d'une attaque et à prioriser les actions. Ils sont également renseignés dans des rapports plus détaillés contenant des données d'analyse de niveau professionnel sur les logiciels malveillants.

Protection renforcée

McAfee Advanced Threat Defense s'intègre avec divers équipements de sécurité, du périmètre du réseau jusqu'au terminal, permettant à ceux-ci d'intervenir immédiatement lorsque la solution établit qu'un fichier est malveillant. Cette intégration étroite et automatisée entre les étapes de détection et de blocage est essentielle.

Elle peut s'effectuer de diverses manières : directement avec les solutions de sécurité, via McAfee Threat Intelligence Exchange ou via McAfee Advanced Threat Defense Email Connector.

Avec une intégration directe, les solutions de sécurité sont capables d'intervenir lorsqu'un fichier est identifié comme malveillant par McAfee Advanced Threat Defense. Elles peuvent immédiatement intégrer la cyberveille sur les menaces aux processus existants d'application des stratégies et empêcher d'autres instances de fichiers identiques ou similaires de pénétrer sur le réseau.

Puissantes fonctionnalités d'analyse

- L'association de fonctions d'analyse statique approfondie du code, d'analyse dynamique et d'apprentissage automatique rend la détection plus précise et offre des données d'analyse de qualité.
- Des fonctionnalités avancées viennent en aide au SOC et facilitent l'investigation.

Déploiement centralisé flexible

- Le déploiement centralisé, qui prend en charge plusieurs protocoles, permet de réduire les coûts.
- Des options de déploiement flexibles permettent de prendre en charge tous les types de réseau.

Les menaces identifiées par McAfee Advanced Threat Defense apparaissent dans les journaux et les tableaux de bord des produits intégrés, comme si ces derniers avaient effectué l'analyse complète. Ce partage des informations permet de rationaliser les workflows et d'optimiser la gestion des alertes par les administrateurs.

L'intégration avec McAfee Threat Intelligence Exchange étend les fonctions à des mécanismes de défense supplémentaires, notamment McAfee Endpoint Protection. Elle signifie en outre que de nombreuses solutions de sécurité intégrées ont accès aux résultats d'analyse et indicateurs de compromission. Dès que McAfee Advanced Threat Defense identifie un fichier comme malveillant, McAfee Threat Intelligence Exchange publie cette information via la mise à jour des informations de réputation à l'intention de tous les systèmes de contre-mesures intégrés au sein de l'entreprise.

Les terminaux sur lesquels McAfee Threat Intelligence Exchange est installé peuvent bloquer l'installation de logiciels malveillants « patient zéro » et disposent d'une protection proactive si le même fichier se présente à nouveau. De plus, les passerelles intégrées à McAfee Threat Intelligence Exchange empêcheront le fichier de pénétrer dans l'entreprise. Enfin, les terminaux dotés de McAfee Threat Intelligence Exchange continueront de recevoir les informations d'identification de fichiers malveillants, qu'ils soient connectés ou non au réseau, ce qui élimine les « angles morts » générés par la distribution hors bande des charges actives.

McAfee Advanced Threat Defense Email Connector permet à McAfee Advanced Threat Defense de recevoir des pièces jointes envoyées par une passerelle de messagerie à des fins d'analyse. McAfee Advanced Threat Defense analyse ces fichiers et renvoie un verdict dans l'en-tête du message à toutes les passerelles de messagerie actives. La passerelle de messagerie peut ensuite prendre les mesures adéquates conformément à la stratégie de sécurité en place, par exemple supprimer ou mettre en quarantaine la pièce jointe, afin d'empêcher le logiciel malveillant de se propager au réseau interne et d'infecter les autres terminaux. Un mode hors ligne permet de transmettre à l'utilisateur final les e-mails contenant des pièces jointes alors même que celles-ci sont analysées par McAfee Advanced Threat Defense. Cette passerelle de messagerie n'attend pas d'avoir le verdict concernant la pièce jointe. Les administrateurs voient les résultats de l'analyse des pièces jointes dans McAfee Advanced Threat Defense ou McAfee Threat Intelligence Exchange. Pour une détection renforcée au niveau du serveur de messagerie, McAfee Advanced Threat Defense s'intègre avec McAfee Security for Email Servers par le biais de McAfee Threat Intelligence Exchange.

Solutions intégrées

- McAfee® Active Response
- McAfee® Advanced Threat Defense Email Connector
- McAfee® Enterprise Security Manager
- McAfee® ePolicy Orchestrator®
- McAfee® Network Security Platform
- McAfee® Threat Intelligence Exchange
  - McAfee® Application Control
  - McAfee® Endpoint Protection
  - McAfee® Security for Email Servers
  - McAfee® Server Security
- McAfee® Web Gateway
- Bro Network Security Monitor
- TAXII (Trusted Automated eXchange of Indicator Information)

Partage de cyberveille pour des investigations automatisées et optimisées

Pour analyser et corriger les conséquences d'une attaque, les entreprises ont besoin d'une visibilité totale et d'une cyberveille directement exploitable, leur permettant de prendre les bonnes décisions et de réagir de manière adéquate. McAfee Advanced Threat Defense génère des informations approfondies sur les menaces qui peuvent facilement être diffusées dans l'ensemble de votre environnement, afin d'optimiser et d'automatiser les investigations. La prise en charge des API Data Exchange Layer (DXL) et REST facilite en outre l'intégration avec d'autres produits. De plus, le recours à des normes courantes de partage d'informations sur les menaces, comme STIX (Structured Threat Information eXpression) ou TAXII (Trusted Automated eXchange of Indicator Information), permet aux organisations de mettre en place, renforcer et étendre un écosystème de sécurité collaboratif.

Au sein d'un écosystème McAfee, McAfee Enterprise Security Manager rassemble les événements d'exécution et de réputation de fichiers générés par McAfee Advanced Threat Defense et d'autres systèmes de sécurité. Il les met ensuite en corrélation pour offrir des alertes avancées et des vues historiques qui permettent d'affiner la cyberveille, prioriser les risques et développer une connaissance situationnelle en temps réel. Sur la base des données des indicateurs de compromission reçues de McAfee Advanced Threat Defense, McAfee Enterprise Security Manager peut examiner les six derniers mois de toutes les données réseau ou système conservées pour y rechercher une trace de ces artefacts. Cette analyse permet de déceler les systèmes qui avaient précédemment communiqué avec des sources de logiciels malveillants récemment identifiées. L'intégration étroite avec McAfee Endpoint Protection, McAfee Threat Intelligence Exchange et McAfee Active Response optimise l'efficacité et les interventions des équipes de sécurité. Celles-ci disposent en effet d'une meilleure visibilité et peuvent prendre des mesures telles que créer de nouvelles configurations, implémenter de nouvelles stratégies, supprimer des fichiers ou déployer une mise à jour logicielle, dans un seul et même but : réduire les risques de manière proactive. Les terminaux infectés sont automatiquement identifiés au sein du réseau par McAfee Active Response et répertoriés dans les rapports McAfee Advanced Threat Defense, ce qui permet une prise de décision éclairée. Les analystes peuvent travailler plus efficacement lorsqu'ils peuvent consulter ces rapports détaillés depuis un espace de travail unique, dans McAfee Active Response.

Des capacités avancées pour des investigations plus fines

McAfee Advanced Threat Defense offre de nombreuses fonctionnalités avancées :

- **Prise en charge configurable des systèmes d'exploitation et applications :** Permet de personnaliser les images d'analyse à l'aide de variables d'environnement spécifiques afin de valider les menaces et de faciliter l'investigation.
- **Mode utilisateur interactif :** Permet aux analystes d'interagir directement avec les échantillons de logiciels malveillants.

- **Fonctions de décompression complètes :** Réduisent la durée d'investigation de plusieurs jours à quelques minutes.
- **Chemin logique complet :** Permet une analyse plus approfondie des échantillons en forçant l'exécution de chemins logiques supplémentaires, qui restent inactifs dans les environnements sandbox classiques.
- **Envoi d'échantillons à plusieurs environnements virtuels :** Accélère l'investigation en déterminant les variables d'environnement nécessaires à l'exécution de fichiers.
- **Rapports détaillés :** Offrent des informations critiques pour les investigations, et notamment la mise en correspondance avec le cadre MITRE ATT&CK™, des vues décomposées, des vidages de mémoire, des représentations graphiques des appels de fonction, des informations sur les fichiers incorporés ou injectés, des journaux d'API utilisateur et des données PCAP. Une représentation chronologique des menaces permet de visualiser les étapes d'exécution des attaques.
- **Intégration avec Bro Network Security Monitor :** Déployez un capteur Bro sur un segment suspect du réseau pour surveiller et capturer le trafic et transmettre les fichiers à McAfee Advanced Threat Defense en vue de leur inspection.

Déploiement

Des options de déploiement flexibles des fonctions d'analyse des menaces avancées permettent de prendre en charge tous les types de réseau. McAfee Advanced Threat Defense existe sous la forme d'une appliance sur site ou virtuelle. Disponible sur Azure Marketplace, la solution prend en charge tant les clouds publics que privés.

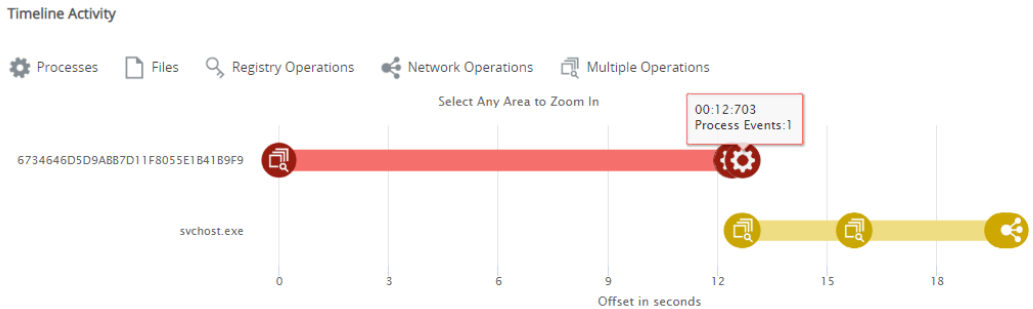

Figure 1. Une représentation chronologique permet de visualiser les étapes d'exécution de la menace analysée.

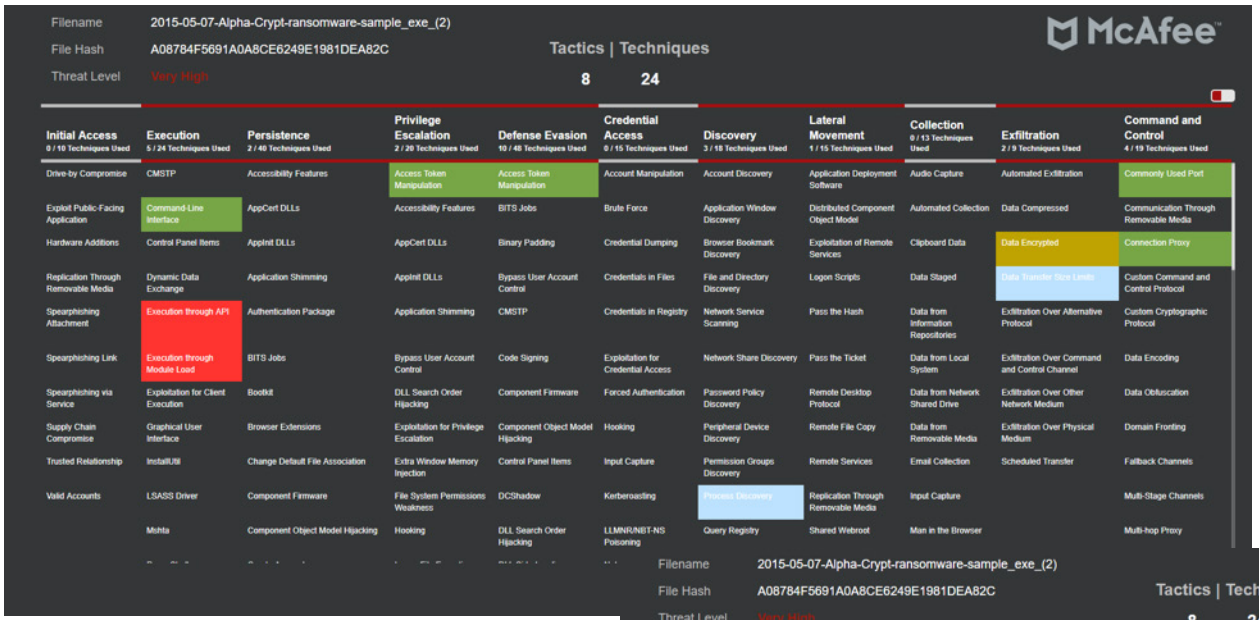

Figure 2. Les résultats sont mis en correspondance avec le cadre MITRE ATT&CK™.

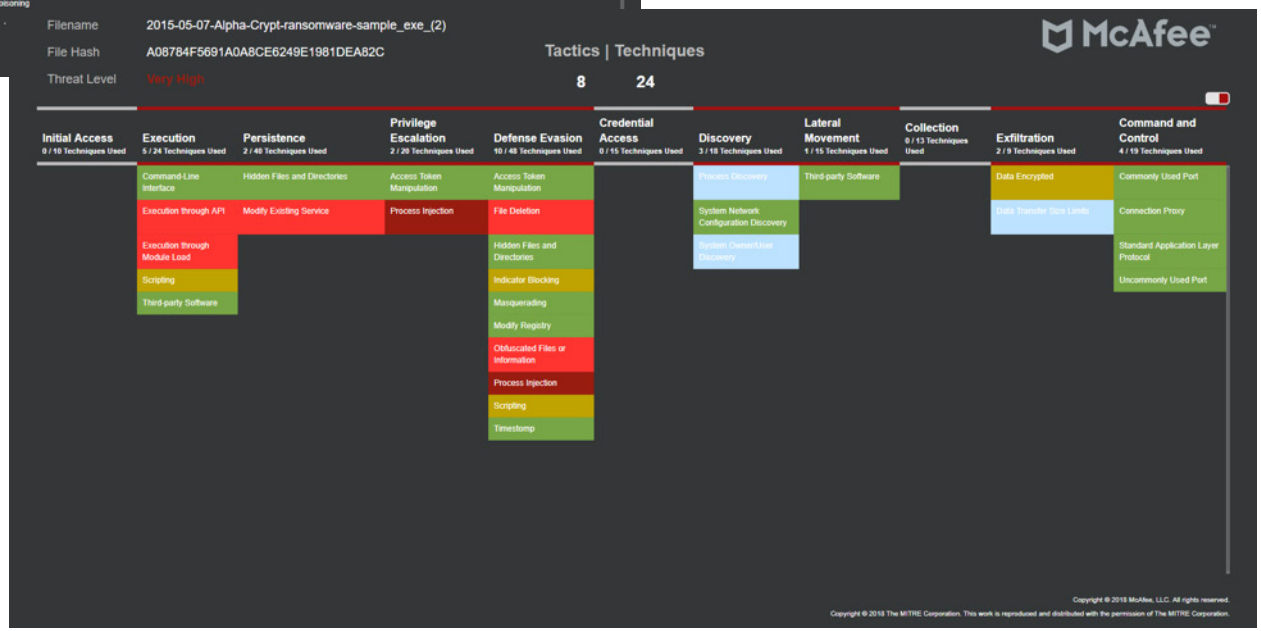

Figure 3. Une vue filtrée des résultats présentés à la figure 2 permet de mettre en évidence les techniques identifiées.

Spécifications de McAfee Advanced Threat Defense		
Déploiement physique	ATD-3100 Montage en baie 1U	ATD-6100 Montage en baie 1U
Déploiement virtuel	v1008 ESXi 5.5, 6.0, 6.5, 6.7 Hyper-V sur Windows Server 2012 R2, Windows Server 2016 Azure Marketplace	
Détection		
Types de formats et fichiers pris en charge	PE, Adobe, suite Microsoft Office, images, archives, Java, Android Application Package, URL	
Méthodes d'analyse	Moteur McAfee Anti-Malware Engine ; analyse de la réputation de McAfee GTI (fichiers, URL, adresses IP) ; moteur Gateway Anti-Malware (émulation et analyse comportementale) ; analyse dynamique (sandboxing) ; analyse approfondie du code ; règles YARA personnalisées ; apprentissage automatique : réseau neuronal pour apprentissage profond	
Systèmes d'exploitation pris en charge	Windows 10 (64 bits), Windows 8.1 (64 bits), Windows 8 (32/64 bits), Windows 7 (32/64 bits), Windows XP (32/64 bits), Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android Toutes les langues des systèmes d'exploitation Windows sont prises en charge.	
Formats de sortie	STIX, OpenIOC, XML, JSON, HTML, PDF, texte	
Méthodes de transmission des données	Intégrations de produits individuels, API RESTful, transmission manuelle et McAfee Advanced Threat Defense Email Connector (SMTP)	

En savoir plus

Pour plus d'informations ou pour réaliser une évaluation de McAfee Advanced Threat Defense, contactez votre représentant ou consultez notre site à l'adresse : **www.mcafee.com/fr/products/advanced-threat-defense.aspx**.

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr