# McAfee Endpoint Security

## Une sécurité spécialement conçue pour une gestion proactive des menaces et des contrôles de sécurité éprouvés

### Protection des terminaux : quelles sont vos priorités ?

Les entreprises actuelles confient la gestion de leur sécurité à une ou plusieurs équipes. Dans les grandes structures, la fonction est souvent partagée, avec par exemple une équipe chargée de l'administration informatique et une autre responsable des opérations de sécurité. Quelle que soit l'approche qui reflète le mieux le rôle que vous jouez au sein de votre entreprise, vos priorités influencent forcément les fonctionnalités et les résultats que vous attendez de votre plate-forme de protection des terminaux.

Votre solution de protection des terminaux doit donc s'aligner sur vos priorités. Indépendamment de votre rôle, McAfee® Endpoint Security s'adapte à vos besoins critiques, qu'il s'agisse de bloquer et de traquer les menaces ou de personnaliser les contrôles de sécurité. McAfee® MVISION Insights priorise les menaces afin de vous permettre d'agir avant qu'une attaque ne survienne. La solution vous permet de garantir la disponibilité des systèmes pour les utilisateurs, d'identifier des opportunités d'automatisation supplémentaires et de simplifier les workflows complexes.

### Disponibilité et visibilité

McAfee Endpoint Security permet aux clients de gérer le cycle de défense contre les menaces et de réagir efficacement tout au long de celui-ci grâce à des défenses proactives et à des outils de correction. La correction par restauration automatique rétablit l'intégrité des systèmes afin de préserver la productivité des utilisateurs et des administrateurs, puisqu'elle leur évite d'avoir à attendre l'application de mesures correctives, la reprise après sinistre ou la restauration de l'image d'une machine infectée. La cyberveille mondiale sur les menaces et les informations locales en temps réel sur les événements sont partagées entre les terminaux et McAfee® MVISION EDR afin d'obtenir des détails sur les événements relatifs aux menaces, détecter et bloquer les menaces qui tentent d'échapper à la détection, ainsi que les relier au cadre MITRE ATT&CK pour les soumettre à une analyse plus approfondie. La gestion est simplifiée grâce à une console centralisée permettant le déploiement d'environnements locaux, virtuels ou en modèle SaaS. MVISION Insights offre une visibilité unique sur les menaces potentielles avec une propension à l'attaque élevée, et détermine si le niveau de sécurité d'une organisation est suffisant pour bloquer ces menaces.

### Principaux avantages

- **Une défense de pointe contre les menaces avancées :** Apprentissage automatique, surveillance du vol d'identifiants et correction par restauration qui viennent compléter les fonctions de sécurité de base des postes de travail et serveurs Windows 10.
- **Une simplicité préservée :** Gérez les technologies McAfee, les stratégies antivirus Windows Defender, Defender Exploit Guard et les paramètres du Pare-feu Windows à l'aide d'une seule stratégie et d'une seule console.

Gardez le contact

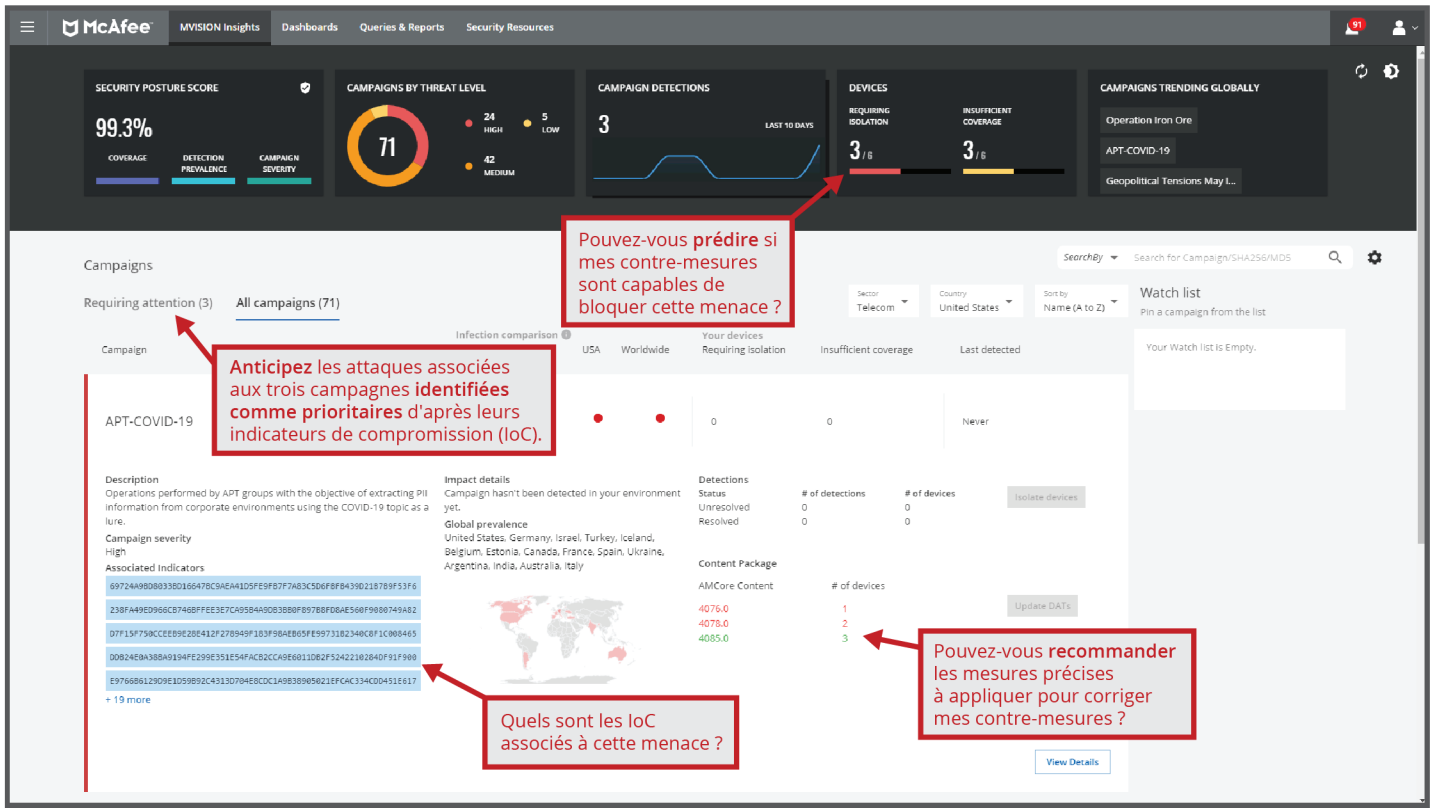


Figure 1. Tableau de bord de MVISION Insights. (Pour que MVISION Insights fonctionne correctement, l'option d'envoi de données de télémétrie de McAfee Endpoint Security doit être activée.)

MVISION Insights offre aux entreprises une visibilité et un contrôle uniques sur les menaces dont elles sont les plus susceptibles de subir les attaques, tout en déterminant si leur niveau de sécurité est suffisant pour les protéger. La solution garantit ainsi un niveau de protection avancé contre les menaces critiques et déjoue les attaques avant qu'elles n'aient lieu.

Grâce à MVISION Insights, les organisations reçoivent des alertes et des notifications concernant des menaces priorisées susceptibles de frapper en fonction du secteur et de la région. En outre, la solution propose une évaluation locale du niveau de sécurité et détermine s'il est suffisant pour bloquer ces menaces. Elle identifie également les terminaux vulnérables à des menaces

## Principaux avantages (suite)

- **MVISION Insights :** Réagissez immédiatement aux campagnes d'attaque les plus susceptibles de vous cibler en fonction de leur activité dans votre secteur ou votre région géographique grâce à cette solution de cyberveille de pointe, dont les informations de sécurité sont directement exploitables. MVISION Insights identifie à l'avance les terminaux dotés d'une protection insuffisante contre ces campagnes particulières et fournit des conseils pour améliorer la détection. Il s'agit de la seule solution de sécurité des terminaux du marché qui établisse de manière prédictive un plan d'action priorisé et prescritif.

particulières et fournit des conseils prescriptifs concernant les mesures à prendre. Elle appuie les efforts proactifs déployés pour prendre une longueur d'avance sur les cybercriminels susceptibles de passer à l'offensive.

McAfee Endpoint Security rassemble des informations sur les menaces provenant de plusieurs niveaux d'engagement à l'aide d'un agent logiciel unique ; l'objectif étant d'éliminer les redondances caractéristiques de la concomitance de produits isolés. Vous bénéficiez ainsi d'une approche intégrée de la sécurité qui élimine les processus manuels de corrélation des menaces. et qui permet de transmettre automatiquement les informations nécessitant une analyse plus approfondie aux équipes de réponse aux incidents. Les données sur les événements de menace sont présentées dans un format simple et clair via la fonctionnalité Story Graph, qui affiche des informations détaillées sur les menaces et permet aux administrateurs de remonter facilement aux sources des attaques et de les analyser.

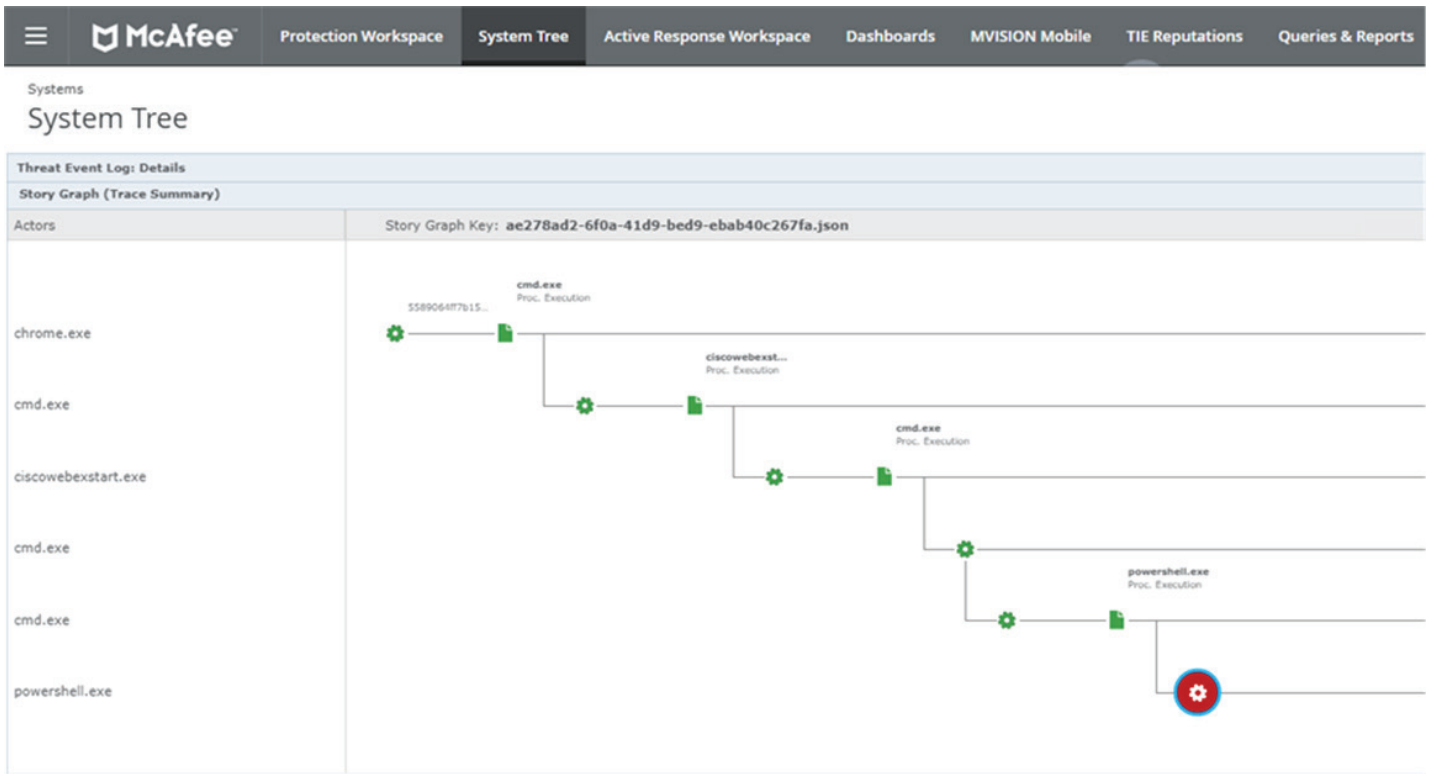


Figure 2. Story Graph

## Une protection intégrée contre les menaces avancées qui automatise les interventions et accélère les temps de réponse

Le cadre intégré McAfee Endpoint Security propose en outre des fonctions supplémentaires de protection pour aider les entreprises à se défendre contre les menaces avancées les plus récentes[1]. À titre d'exemple, la fonction de confinement d'application dynamique analyse les logiciels « gris » (greywares) et d'autres logiciels malveillants émergents et les isole pour éviter la propagation de l'infection.

De même, Real Protect tire parti de la classification des comportements avec apprentissage automatique pour améliorer la détection des logiciels malveillants « jour zéro ». Cette classification sans signatures est effectuée dans le cloud et consomme peu de ressources sur le client, tout en offrant une détection en temps quasi réel. Les informations exploitables fournies permettent, entre autres, de générer des indicateurs de compromission (IoC) et des indicateurs d'attaque (IoA). Ceux-ci sont particulièrement utiles pour détecter les attaques à déplacement latéral, identifier les « patients zéro », attribuer les attaques à des cybercriminels, mener des investigations numériques et appliquer des mesures de correction. Real Protect accélère également les analyses ultérieures en optimisant automatiquement la classification des comportements et en ajoutant des règles pour identifier les attaques futures présentant des caractéristiques similaires, à l'aide de fonctions statiques et dynamiques.

Enfin, en cas de malveillance avérée, pour prévenir toute infection et réduire les temps de réponse des administrateurs de la sécurité informatique, le logiciel client rétablit la dernière bonne configuration connue du terminal.

## Une protection des terminaux intelligente qui vous informe des faits et gestes des cyberattaquants

Avec une meilleure cyberveille, vous ne pouvez obtenir que de meilleurs résultats. La solution McAfee Endpoint Security communique en temps réel ses observations aux différentes technologies de protection des terminaux connectées à son infrastructure. Celles-ci peuvent donc agir de concert et accélérer l'identification des comportements suspects, améliorer la coordination des défenses et renforcer la protection contre les attaques ciblées et « jour zéro ». Des informations telles que la valeur de hachage de fichier, l'URL source, les événements AMSI et PowerShell font l'objet d'un suivi et sont partagées non seulement avec les autres systèmes de protection, mais aussi avec les interfaces clientes et de gestion. Résultat : les utilisateurs peuvent mieux cerner les attaques et les administrateurs disposent de données directement exploitables pour l'investigation numérique.

De plus, grâce à la technologie McAfee® Threat Intelligence Exchange, les défenses adaptatives peuvent collaborer avec d'autres solutions McAfee, notamment les passerelles, les sandbox et notre solution SIEM.

La collecte et la distribution d'informations de sécurité au niveau local, mondial et communautaire permettent de ramener le délai entre la découverte d'une attaque et sa neutralisation de plusieurs semaines ou plusieurs mois, à quelques millisecondes seulement.

Associé à McAfee® Global Threat Intelligence (McAfee® GTI), le cadre McAfee Endpoint Security tire parti du cloud pour surveiller et contrer, en temps réel, tout le spectre des menaces nouvelles et émergentes, sur tous les vecteurs : fichiers, Web, messagerie et réseau. Le système existant de protection et gestion des terminaux est optimisé grâce à une cyberveille à la fois locale et mondiale, de manière à refouler instantanément les logiciels malveillants inconnus et ciblés. De plus, grâce à des actions automatisées sur les applications et processus suspects, les mesures d'intervention sont rapidement appliquées aux nouvelles formes d'attaques émergentes, tandis que les informations sont transmises aux autres mécanismes de défense ainsi qu'à la communauté de cyberveille mondiale.

Les clients qui utilisent le confinement d'application dynamique et Real Protect bénéficient d'informations sur les menaces plus avancées et les comportements qui les caractérisent. Par exemple, le confinement d'application dynamique propose des informations sur les applications confinées et le type d'accès tenté par celles-ci, comme l'accès au registre ou à la mémoire.

Quant à Real Protect, il fournit des renseignements sur les comportements jugés malveillants et classe les menaces. Les entreprises qui cherchent à recueillir des informations sur les processus malveillants affectant les terminaux peuvent s'en servir afin de traquer les logiciels malveillants et de faciliter la tâche des équipes de réponse aux incidents. Ces informations sont tout particulièrement utiles pour découvrir les techniques utilisées par les logiciels malveillants basés sur les fichiers afin d'échapper à la détection : compression, chiffrement ou exploitation abusive d'applications légitimes.

## Les performances au service de la réactivité

Aussi intelligente soit-elle, une solution de sécurité n'a que peu d'intérêt si elle entrave le travail des utilisateurs par des analyses trop lentes, des installations trop longues ou une gestion compliquée. Avec McAfee Endpoint Security, les utilisateurs restent productifs. En effet, une couche de services commune et notre nouveau moteur antimalware réduisent les ressources et la puissance de calcul utilisées par le système d'un utilisateur. Les analyses des terminaux ne s'effectuent que lorsque ceux-ci sont inactifs et reprennent de manière transparente après un redémarrage ou un arrêt du système.

Un processus d'analyse adaptatif permet en outre de limiter les demandes soumises au processeur par un mécanisme d'apprentissage des processus et sources approuvés, afin de concentrer les ressources uniquement sur les processus qui semblent suspects ou dont la source est inconnue. McAfee Endpoint Security intègre également un pare-feu qui utilise McAfee GTI pour protéger les terminaux contre les réseaux de robots (botnets), les attaques par déni de service distribué (DDoS), les menaces APT et les connexions web dangereuses.

## Plus de durabilité, moins de complexité

Avec la multiplication des produits de sécurité aux fonctionnalités redondantes et aux consoles de gestion distinctes, il est devenu très difficile de disposer d'une vision claire sur les attaques potentielles. McAfee Endpoint Security évite tous ces écueils. La solution assure une protection fiable et à long terme grâce à son cadre ouvert et extensible, fondement de la centralisation des solutions pour terminaux actuelles et futures. Ce cadre exploite la couche Data Exchange Layer pour permettre une collaboration avec les technologies d'autres solutions déjà présentes, ce qui préserve les investissements de sécurité de l'entreprise. Cette architecture intégrée vient elle-même s'intégrer de manière transparente avec d'autres produits McAfee, de façon à combler les failles de sécurité, à réduire les cloisonnements de technologies et à éliminer les redondances. De plus, elle améliore la productivité en réduisant les coûts d'exploitation et la complexité d'administration.

McAfee® ePolicy Orchestrator® (McAfee ePO™) simplifie encore la gestion grâce à sa console unique qui permet la surveillance, le déploiement et la gestion des terminaux à partir d'un point central. Des vues personnalisables, mais aussi des workflows faciles à comprendre et à exploiter offrent les outils nécessaires pour évaluer rapidement le niveau de sécurité de l'entreprise, localiser les infections et limiter l'impact des menaces en mettant en quarantaine les systèmes touchés, en arrêtant les processus malveillants et en bloquant l'exfiltration de données. La console offre également un point centralisé de gestion de tous les terminaux, des autres produits et fonctions McAfee et de plus de 130 solutions de sécurité de fournisseurs tiers.

## FICHE TECHNIQUE

| Fonctionnalité | Avantage |
|---|---|
| **Détection et neutralisation proactives des menaces (MVISION Insights)** | ▪ Détecte les menaces potentielles de manière prédictive et préventive en fonction de votre secteur d'activité et de votre région.<br>▪ Évalue localement votre niveau de protection contre les menaces potentielles et propose des mesures correctives.<br>▪ Permet de prendre une longueur d'avance sur les cybercriminels en mettant en place des protections avant qu'une attaque n'ait lieu. |
| **Real Protect** | ▪ Détecte les menaces « jour zéro » en temps quasi réel et génère une cyberveille exploitable grâce à la fonction de classification des comportements basée sur l'apprentissage automatique.<br>▪ Optimise automatiquement la classification des comportements pour les identifier plus facilement et ajoute des règles afin de détecter les futures attaques. |
| **Protection des terminaux contre les attaques ciblées** | ▪ Réduit considérablement le délai entre la détection et la neutralisation de l'attaque : quelques millisecondes au lieu de plusieurs jours.<br>▪ McAfee Threat Intelligence Exchange collecte des informations sur les menaces à partir de plusieurs sources et permet la communication instantanée entre les composants de sécurité pour mieux refouler les attaques avancées émergentes et multiphases.<br>▪ La journalisation des événements AMSI et PowerShell détecte les attaques sans fichier et basées sur des scripts et offre une protection contre celles-ci. |
| **Analyse adaptative et intelligente** | ▪ Améliore les performances et la productivité en contournant l'analyse des processus approuvés et en priorisant les processus et applications suspects.<br>▪ L'analyse adaptative du comportement surveille les activités, cible les événements suspects et transmet les alertes nécessaires. |
| **Correction par restauration** | ▪ Annule automatiquement les modifications effectuées par les logiciels malveillants et rétablit la dernière bonne configuration connue des systèmes, tout en préservant la productivité des utilisateurs. |
| **Sécurité proactive de l'environnement web** | ▪ Garantit une navigation sécurisée grâce à des fonctions de protection et filtrage web spécialement conçues pour les terminaux. |
| **Confinement d'application dynamique** | ▪ Protège contre les ransomwares et les logiciels « gris » (greywares) ; isole le « patient zéro »[2]. |
| **Blocage des attaques réseau** | ▪ Le pare-feu intégré utilise des scores de réputation basés sur McAfee GTI pour protéger les terminaux contre les réseaux de robots (botnets), les attaques DDoS, les menaces APT et les connexions web suspectes.<br>▪ La protection par pare-feu autorise uniquement le trafic en sortie au démarrage du système, de façon à protéger les terminaux lorsqu'ils ne sont pas connectés au réseau d'entreprise. |
| **Story Graph** | ▪ Les administrateurs peuvent identifier immédiatement les systèmes infectés, les causes de l'infection et la durée d'exposition, pour mieux comprendre la menace et réagir plus rapidement. |
| **Gestion centralisée (plate-forme McAfee ePO) avec plusieurs options de déploiement** | ▪ L'administration centralisée grâce à une console unique procure de nombreux avantages : amélioration de la visibilité, simplification des opérations, augmentation de la productivité de l'équipe informatique, sécurité unifiée et réduction des coûts. |
| **Cadre ouvert et extensible pour la sécurité des terminaux** | ▪ Une architecture intégrée permet aux produits de protection des terminaux de collaborer et de communiquer, ce qui renforce la sécurité.<br>▪ Les coûts d'exploitation sont réduits grâce à l'élimination des redondances et l'optimisation des processus.<br>▪ L'intégration avec les produits McAfee et ceux d'autres fournisseurs s'effectue de manière transparente pour réduire les failles dans la protection. |

Tableau 1. Principales fonctionnalités et leurs avantages

## Une longueur d'avance sur les cybermenaces

McAfee Endpoint Security offre aux professionnels de la sécurité tout ce dont ils ont besoin pour prendre l'avantage sur les cybercriminels : des défenses intelligentes et collaboratives, mais aussi un cadre qui simplifie les environnements complexes. Sa capacité de détection des menaces et ses performances exemplaires, démontrées par des tests indépendants, permettent aux entreprises d'assurer à leurs utilisateurs protection, productivité et tranquillité d'esprit.

McAfee, leader du marché de la sécurité des terminaux, propose une gamme complète de solutions de défense en profondeur et proactive grâce à la combinaison de fonctions de protection puissantes et d'un système de gestion d'une grande efficacité. Cette approche permet aux équipes de sécurité de neutraliser les menaces plus rapidement et avec moins de ressources.

## Une migration en toute facilité

Les environnements équipés de versions récentes du logiciel McAfee ePO, de McAfee VirusScan® Enterprise et de McAfee® Agent peuvent tirer parti de notre outil de migration automatique pour migrer toutes les stratégies existantes vers McAfee Endpoint Security en moins de 20 minutes[3].

McAfee Endpoint Security offre en outre les avantages suivants :

- Analyses sans impact sur l'utilisateur pour améliorer la productivité
- Données d'investigation numérique plus complètes reliées à la fonctionnalité Story Graph permettant d'obtenir un aperçu des informations et de simplifier les investigations pour vous aider à renforcer vos stratégies
- Correction par restauration permettant d'annuler automatiquement les modifications effectuées par les logiciels malveillants et de préserver l'intégrité des systèmes
- Renseignements proactifs sur des menaces potentielles priorisées et conseils prescriptifs concernant la prise de contre-mesures contre les menaces avec MVISION Insights
- Moins d'agents à gérer, moins d'analyses à exécuter et moins de saisies manuelles
- Fonctions de protection collaboratives qui fonctionnent de concert pour tenir en échec les menaces avancées
- Cadre de nouvelle génération qu'il est possible d'intégrer avec d'autres solutions de protection contre les menaces avancées et solutions EDR (Endpoint Detection and Response)

## En savoir plus

Pour en savoir plus sur McAfee Endpoint Security, cliquez ici.

Pour plus d'informations sur la manière dont McAfee Endpoint Security complète la gamme de produits McAfee, consultez les pages ci-dessous :

- MVISION Endpoint
- Gamme de produits MVISION
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator
- MVISION Insights

1. Disponible avec la plupart des suites de protection des terminaux McAfee. Pour en savoir plus, contactez votre commercial.
2. Ibid.
3. La durée de la migration dépend de vos stratégies existantes et de votre environnement.

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