FICHE PRODUIT

POURQUOI MOBILE THREAT DEFENSE

- **Sécurité mobile globale :** défense multicouche contre les attaques connues, inconnues et ciblées sur tous les vecteurs d'attaques.
- **Technologie prédictive :** identification et protection contre les réseaux suspects, les développeurs malveillants et leurs applications, avant qu'ils ne puissent provoquer des dégâts.
- **Productivité et discrétion :** l'application mobile publique protège la confidentialité et la productivité des utilisateurs sans peser sur l'expérience mobile ni la durée de vie des batteries.
- **Déploiement sans effort :** intégration rapide avec des applications iOS et Android natives faciles à gérer et à entretenir.
- **Défense adaptée aux entreprises :** application automatisée de politiques IT par le biais de l'intégration aux systèmes UEM ou MDM et VPN existants de l'entreprise. La solution MTD peut être déployée sur des milliers d'appareils en quelques minutes.[1]
- **Efficacité et transparence :** visibilité optimale sur les vulnérabilités, menaces et attaques affectant les appareils mobiles, avec détection et remédiation automatisées.
- **Intelligence collective considérable :** défense contre les attaques exploitant les failles de sécurité grâce à une communauté d'informations sur la sécurité mobile extrêmement efficace et exhaustive et au réseau Global Intelligence Network (GIN) de Symantec.
- **Expertise exceptionnelle en cybersécurité :** les technologies et le personnel de Symantec sont pleinement dédiés à l'identification et au signalement de très nombreuses vulnérabilités et menaces inédites, au moins une vulnérabilité signalée et corrigée dans chacune des quatre dernières versions d'iOS.

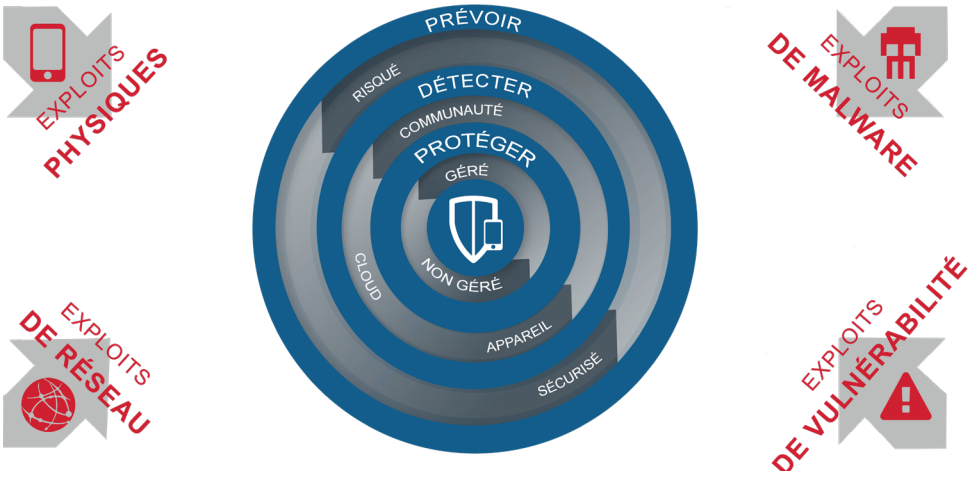
1. D'après les déploiements client réels

Mobile Threat Defense de Symantec Endpoint Security

Présentation

La solution de défense contre les menaces mobiles de Symantec® Endpoint Security, Mobile Threat Defense (MTD), fait partie des solutions complètes pour entreprise de la gamme Symantec Endpoint Security. Elle offre la solution de sécurité mobile la plus exhaustive, précise et efficace, et fournit une intelligence approfondie pour prédire et détecter tout un éventail de menaces existantes et inconnues. La technologie prédictive de MTD s'appuie sur une approche multicouche qui associe une intelligence collective hors norme à une analyse basée à la fois sur les serveurs et les appareils. Elle protège ainsi les appareils mobiles de manière proactive contre les malwares, les menaces réseau et les exploits de vulnérabilités des applications et des systèmes d'exploitation, avec ou sans connexion Internet.

Illustration 1 : Sécurité multicouche de MTD



Optimisez votre solution UEM

MTD s'intègre directement aux solutions de gestion unifiée des terminaux (UEM) les plus puissantes au monde. Grâce à MTD, vous bénéficiez d'une visibilité en temps réel sur les menaces et les attaques provenant des réseaux Wi-Fi et mobiles publics, les exploits de vulnérabilité des systèmes d'exploitation ou des applications, les applications malveillantes et le comportement des utilisateurs susceptibles de compromettre les appareils appartenant à l'entreprise et les appareils BYOD.

Cette approche multicouche de la sécurité mobile est essentielle pour devancer les pirates informatiques modernes, qui sont organisés en groupes et disposent de financements importants. Enfin, grâce à l'intégration des solutions MTD et UEM, vous pouvez centraliser la gestion de la sécurité et de la conformité en appliquant des politiques basées sur des niveaux de risque en temps réel. Optez pour la mobilité sans compromis, améliorez les informations analytiques sur la sécurité mobile et excellez sans entraves dans le monde basé sur les applications et les données.

Composants de la solution

Notre plate-forme de défense contre les menaces mobiles pour les entreprises réunit les composants suivants :

Application mobile publique

- Déploiement, adoption, maintenance et mise à jour faciles.
- Préservation de la productivité, de l'expérience et de la confidentialité (sur la base des témoignages clients).
- Protection en temps réel contre un certain nombre d'applications et de réseaux suspects.
- Protection automatisée des ressources de l'entreprise en cas d'attaques.
- Contribution à la base de données d'intelligence collective sur les menaces de MTD.

Serveurs Cloud

- Analyse secondaire approfondie des applications suspectes.
- Moteur de réputation avec Machine Learning pour les applications, les réseaux et les systèmes d'exploitation.
- Immense base de données d'intelligence collective sur les menaces.
- Application de politiques via un système UEM, un VPN, un serveur Exchange et d'autres intégrations.
- Journaux d'activité complets pour l'intégration avec toute solution SIEM.

Protection étendue

Défense contre les malwares

- Défense proactive contre les applications repackagées malveillantes de type Zero Day.
- Analyse incrémentielle des applications en fonction de la signature, d'une analyse statique/dynamique, du comportement, de la structure, des autorisations, de la source, etc.
- Réponse et protection en temps réel contre divers malwares connus, inconnus et ciblés.

Défense des réseaux

- Bouclier efficace contre les réseaux Wi-Fi malveillants.
- Détection, blocage et remédiation des profils iOS malveillants.
- Technologie brevetée de leurre actif pour identifier les attaques de type Man-in-the-Middle, de déclassement SSL et de manipulation de contenu, sans porter atteinte à la confidentialité.

Défense contre les vulnérabilités

- Surveillance des appareils pour détecter les vulnérabilités connues non corrigées.
- Sensibilisation des utilisateurs et notifications aux équipes de sécurité IT.
- Mise au jour des vulnérabilités existantes (Zero Day) dans les applications et systèmes d'exploitation, et notification aux éditeurs concernés.
- Détection des vulnérabilités connues et inconnues.

Intelligence approfondie

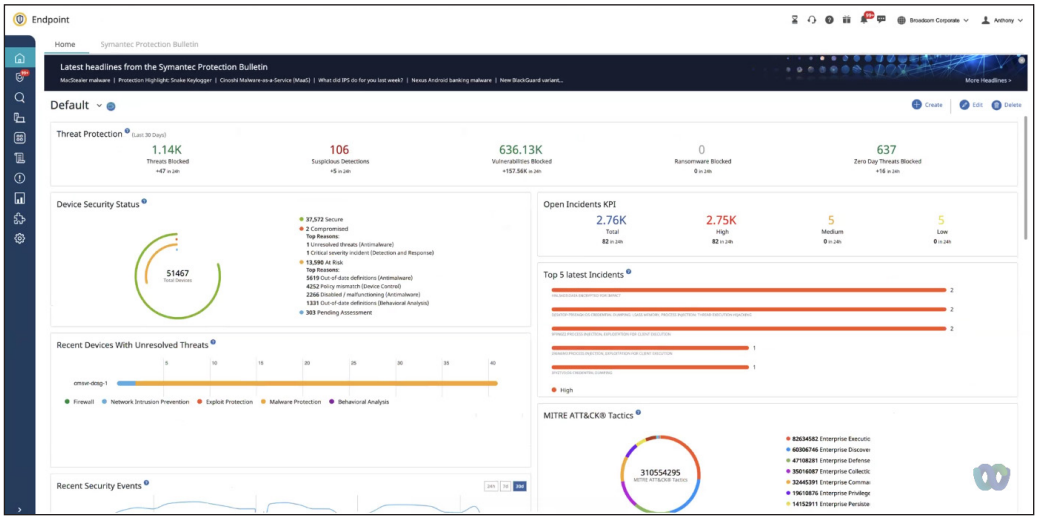
Appareil

- Cette première ligne de défense permet d'identifier les applications et réseaux suspects.
- L'analyse incrémentielle des applications repose sur un large éventail de caractéristiques.
- Les réseaux légitimes et suspects sont immédiatement reconnus.
- Une corrélation est établie entre le type de l'appareil, la version OS et d'autres propriétés du système par rapport à la base de données des risques.

Communauté

- Chaque application MTD utilisée dans le monde constitue un détecteur et un collecteur de données.
- Les caractéristiques des applications et réseaux malveillants et bienveillants sont cataloguées.
- Les versions d'OS et les types d'appareils sont évalués pour déterminer si une mise à niveau est possible.
- La communauté est essentielle pour réaliser une détection Zero Day des applications et autres types de malware.

Illustration 2 : Console SES Management



BROADCOM
connecting everything®

Pour plus d'informations, visitez notre site web à l'adresse suivante : www.broadcom.com

SES-Mobile-PB101_FR 14 avril 2023