Trend Micro

WORRY-FREE™ SERVICES ENDPOINT SENSOR

Un outil d'investigation intégré et un module complémentaire de Trend Micro Worry-Free Services dédié à l'EDR (Endpoint Detection and Response)

Un malware évolué peut se manifester au sein de vos réseaux d'entreprise, après avoir contourné ses technologies traditionnelles de sécurité. Ce malware peut muter et se propager sur l'ensemble d'une organisation avant de cibler et de détourner vos éléments de propriété intellectuelle. Il peut aussi rester « en sommeil » jusqu'à ce qu'une opportunité se présente pour pirater ou prendre en otage vos données. Trend Micro™ Worry-Free™ Services déploie une sécurité robuste contre les menaces. Cette solution capitalise sur la sécurité XGen™, un panel de techniques cross-générationnelles de protection (machine learning, analyse comportementale, etc.). Lorsqu'une menace est détectée, plusieurs questions émergent : quelle en est l'origine ? Combien d'endpoints ont été infectés ? Quel est le lien avec les autres évènements détectés par l'outil de protection les endpoints ?

Trend Micro™ Worry-Free™ Services Endpoint Sensor répond à ces questions au travers d'une visibilité précise sur les malware détectés. Ce module dote les responsables IT d'une fonction EDR qui leur permet de détecter les menaces et de procéder aux investigations nécessaires.

FONCTIONNALITÉS CLÉS

Un workflow intégré : l'analyse des menaces détectées est réalisée via la console Worry-Free Services et selon un workflow dédié, piloté à partir d'une console unique.

Un enregistrement efficace des activités sur les endpoints : Endpoint Sensor enregistre et stocke des informations relatives aux comportements des systèmes, aux communications et aux utilisateurs. Les méta-données de ces informations sont envoyées vers le serveur Worry-Free Services pour permettre aux responsables IT d'identifier les indicateurs de compromission (IoC).

Recherches des indicateurs IOC côté serveur : le serveur de Worry-Free Services ne stocke que les meta-données essentielles des données enregistrées et relatives à l'utilisateur final (télémétrie). L'équipe IT peut ainsi sonder directement ces données, sans avoir à interroger chaque endpoint individuellement. D'autre part, une recherche approfondie peut être réalisée directement sur chaque endpoint.

De la flexibilité en matière de recherche : les recherches peuvent être menées selon différents paramètres : communications spécifiques, malware spécifique, activités de registre, activités des comptes et processus en cours d'exécution. Les marqueurs au format OpenIOC peuvent également être utilisées ans le cadre de ces investigations.

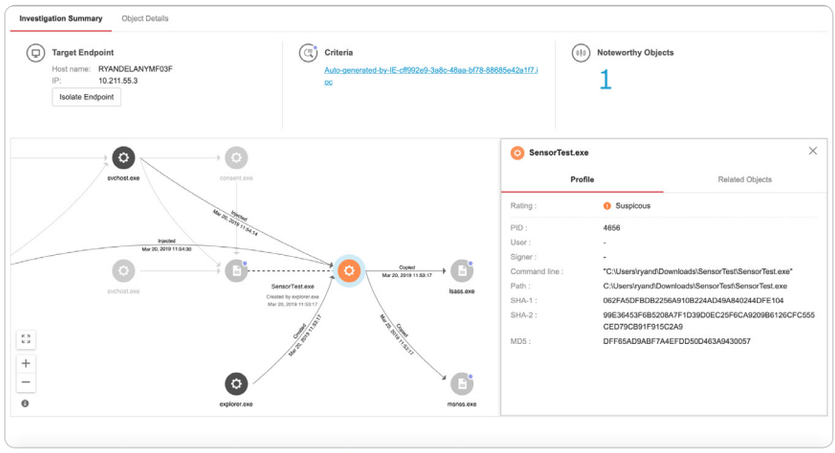
Analyse des causes racines : les responsables IT peuvent explorer un diagramme de processus interactif qui illustre la chaîne de frappe d'une attaque. Grâce à une visibilité sur les activités, les objets et les processus, il devient possible d'analyser comment la menace détectée est arrivée, s'est transformée et s'est propagée. Une prise en charge immédiate est possible pour stopper tout processus malveillant en cours.

Veille et support de la part du constructeur : Trend Micro™ Smart Protection Network™, la plateforme de veille proactive sur les menaces apporte des informations claires et une assistance dans les travaux de recherche. Endpoint Sensor reconnaît les objets et processus légitimes, mais aussi ceux qui sont malveillants. Il est possible d'accéder une analyse des causes racines, restituée sous forme de codes de couleur, pour identifier les processus à risque et inconnus et mener la remédiation.

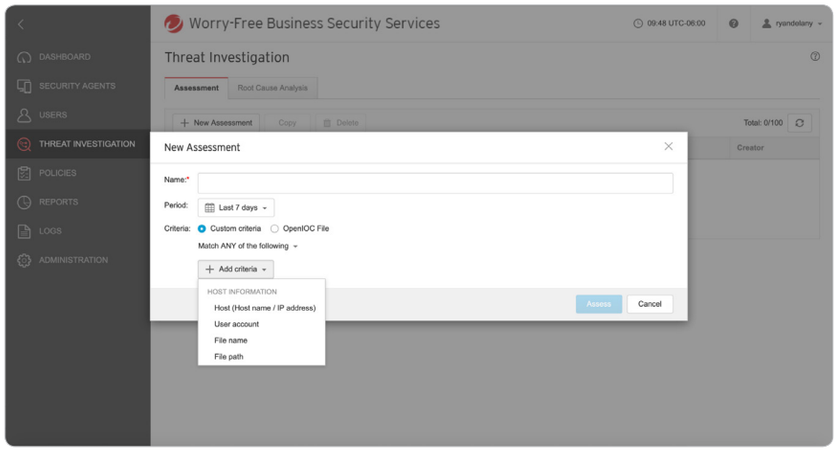
Des options pour une prise en charge immédiate : Worry-Free Services mise sur l'automatisation pour assurer la remédiation des menaces détectées. La solution permet également d'isoler les menaces, de les mettre en quarantaine, d'empêcher leur exécution et de paramétrer les options de rollback (pour les fichiers chiffrés par un ransomware par exemple). Il est aussi possible d'intervenir manuellement lors d'une investigation en isolant les endpoints.

LE MODE OPÉRATOIRE

1. Les endpoints qui disposent de Worry-Free Services Endpoint Sensor enregistrent les comportements systèmes, les comportements des utilisateurs et les communications.
2. Les méta-données des informations enregistrées sont envoyées au serveur Worry-Free Services.
3. Lorsqu'un incident est détecté par Worry-Free Services, il est possible de consulter des méta-données pour mener une analyse d'impact et identifier le périmètre de propagation et d'infection de la menace.
4. Une analyse complète des causes racines permet d'identifier l'origine d'une menace détectée et de réagir immédiatement. Il s'agit de restaurer les systèmes infectés et de mettre à jour Worry-Free Services pour neutraliser toute menace similaire dans le futur.



5. D'autre part, en amont d'une détection, les environnements peuvent être analysés selon différents critères ou selon le standard OpenIoC.



CONFIGURATION REQUISE POUR L'AGENT

Worry-Free Services Endpoint Sensor est proposé en tant que module optionnel qui vient en renfort de la protection des endpoints qu'offre Worry-Free Services. Merci de consulter la configuration requise pour Worry-Free Services.

Worry-Free Services Endpoint Sensor est compatible aux endpoints suivants dans le cadre de Worry-Free Services :

Windows

- Windows 7 SP1 (6.1)
- Windows 8.1 (6.3)
- Windows 10 (10.0)

Matériel :
2Go minimum de RAM, 2Go de disque dur (3Go recommandé)

Périmètre de protection

- Microsoft® Windows®

Fonctionnalités clés

- Recherche des IoC
- Analyse des causes racines d'une menace détectée
- Analyse d'impact suite à une détection
- Prise en charge immédiate

TREND MICRO™

Securing Your Connected World