Trend Micro™

XDR

Une fenêtre de visibilité sur ce que vous ne voyez pas

Face à des menaces en forte mutation, protéger vos utilisateurs et vos infrastructures reste impératif. Il est néanmoins important d'aller plus loin, en s'appuyant sur des processus et des fonctionnalités éprouvés prenant rapidement en charge les menaces susceptibles de percer vos défenses. Une sécurité en profondeur, aussi évoluée soit-elle, ne peut prévenir 100% des menaces : Il suffit qu'une seule menace s'immisce au sein de votre organisation pour que vous en subissiez les conséquences à 100%. Pour maîtriser les dommages, il est donc vital de continuer à optimiser vos techniques de prévention, tout en maîtrisant la détection des menaces et la remédiation post-incident.

Les entreprises recourent à des couches de sécurité distinctes pour détecter les menaces ciblant leurs Endpoints, leur réseau, leur messagerie ou leur infrastructure Cloud. Or cette approche cloisonne les informations sur les menaces et offre peu de moyens pour les corréler à des fins d'analyse et de hiérarchisation. Lancer des investigations sur les menaces sur l'ensemble de ces solutions disparates, devient complexe : les carences en termes de visibilité et de corrélation impliquent souvent des processus manuels et au coup par coup. De nombreuses solutions de détection et de gestion des menaces se contentent de cibler uniquement les Endpoints, éludant ainsi celles s'immisçant via l'email, le réseau et les serveurs. La visibilité sur un éventuel piratage devient parcellaire, tandis que la prise en charge de l'incident est inadaptée. Pour disposer d'une vision globale des menaces affectant l'intégralité de votre entreprise, il est crucial que les fonctionnalités de détection et de remédiation soient intégrées en natif et opérationnelles sur un périmètre incluant l'email, les serveurs, le réseau, les workloads sur le Cloud, ainsi que les Endpoints.

Toutefois, si les fonctionnalités de détection et de remédiation sont essentielles pour toutes les organisations, ces dernières sont néanmoins confrontées à des contraintes de ressources et de compétences. Les techniques actuelles de détection et de remédiation sont souvent chronophages et exigent des ressources expertes dédiées dont bon nombre d'entreprises sont dépourvues.

La solution XDR de Trend Micro propose une détection et une remédiation au-delà des Endpoints pour une visibilité plus large et un traitement analytique holistique des données de sécurité : la détection des menaces gagne en efficacité, en proactivité et en rapidité. En optant pour XDR, les clients prennent en charge les menaces de manière plus efficace et gardent ainsi la main sur la sévérité et le périmètre des incidents de sécurité.

AVANTAGES

Intelligence Artificielle et traitement analytique expert

L'expertise et la veille mondiale sur les menaces permettent de détecter davantage de menaces :

- Associez les données de détection sur les menaces issues de votre environnement avec la veille mondiale sur les menaces proposée par l'infrastructure Trend Micro™ Smart Protection Network™, pour affiner les alertes.
- La prise en compte du contexte accélère les détections et rend les alertes plus pertinentes.
- Des techniques d'IA et un traitement analytique orienté Big Data assurent une compréhension granulaire des données recueillies par les capteurs intelligents de Trend Micro.
- Tirez parti des règles de détection basées sur les informations et menaces identifiées par les experts de Trend Micro sur le terrain.

Au-delà des Endpoints

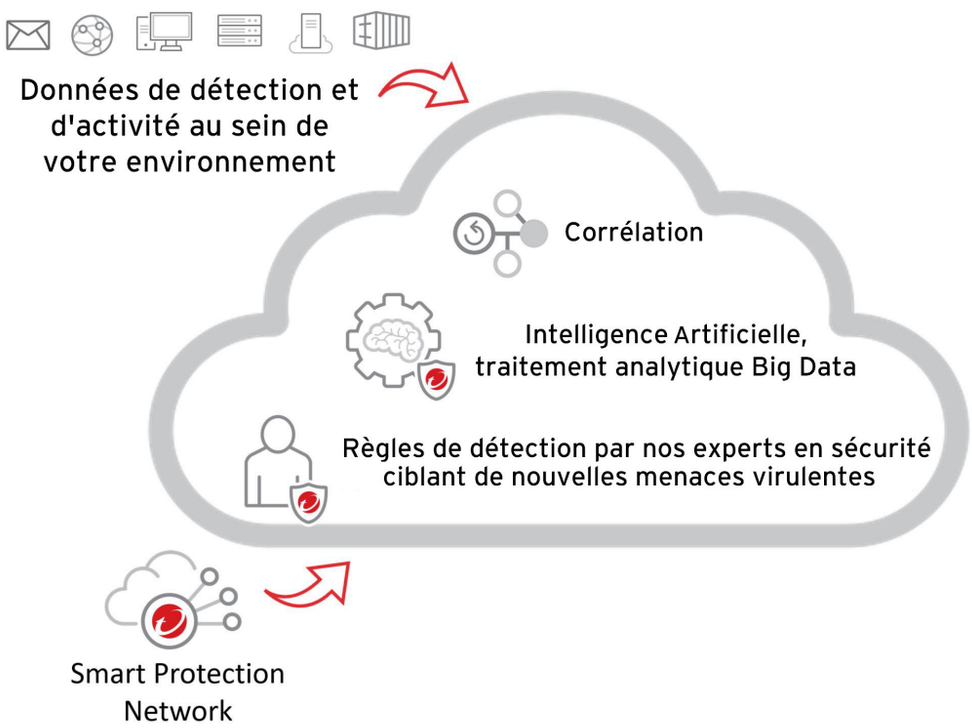
Détectez et neutralisez les menaces sur différentes couches de sécurité et prenez en compte davantage de données contextuelles pour concrétiser les avantages suivants :

- Corrélez automatiquement les données issues des capteurs des solutions Trend Micro recueillant des données de détection et les données d'activité sur différents périmètres : email, réseau, Endpoints et serveurs
- Une activité a priori légitime, mais en réalité malveillante, peut être détectée. Elle déclenche alors une alerte de haute priorité qui vous permet de réagir plus rapidement pour en juguler l'impact.
- Luttez plus efficacement et simplement contre les menaces, évaluez leur impact et assurez la remédiation sur l'email, les Endpoints, les serveurs et les workload sur le Cloud.

Une visibilité intégrale

Une seule plateforme pour une prise en charge plus rapide des menaces, avec moins de ressources :

- **Une seule** source d'alertes priorisées selon un schéma d'alerte pour interpréter les données de manière normalisée et pertinente.
- **Une seule** interface consolidée pour accéder aux alertes et comprendre le cheminement de l'attaque sur l'ensemble des couches de sécurité.
- **Une seule** source pour des investigations guidées, afin d'évaluer l'impact et d'identifier les méthodes de résolution



PROBLÉMATIQUES MÉTIERS

- Des menaces furtives continuent à contourner la ligne de défense en place.
- Des couches de sécurité sans lien entre elles, ainsi que des outils et ensembles de données cloisonnés, ne facilitent pas la corrélation des informations et la détection des menaces critiques.
- La présence d'alertes trop nombreuses, dans un contexte où les équipes IT sont déjà fortement mobilisées, ne permettent pas de consacrer le temps et les ressources nécessaires aux investigations.

LES AVANTAGES DE XDR

Hiérarchisation des alertes sur l'ensemble de l'environnement

Pour des alertes plus fiables, moins nombreuses et hiérarchisées, les informations sont corrélées sur l'ensemble du périmètre organisationnel, pour disposer d'une veille sur les menaces, faire appel à l'intelligence Artificielle et utiliser un traitement analytique expert.

Investigation efficace sur les menaces

En corrélant automatiquement les données sur les menaces à partir de sources multiples, Trend Micro XDR accélère et automatise les processus d'investigation et assure des analyses particulièrement précises.

Visibilité contextuelle et claire sur les menaces

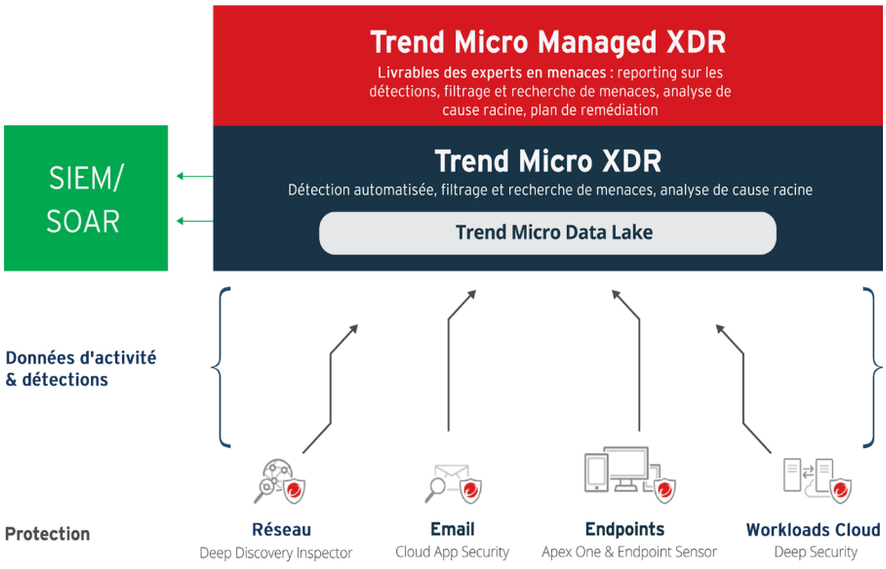
Avec des alertes contextuelles plus nombreuses sur davantage de vecteurs de menaces, des évènements en apparence bénins peuvent soudainement devenir des indicateurs de compromission pertinents. Vous pouvez ainsi tirer les conclusions qui s'imposent à partir d'une visibilité unifiée, mener des investigations plus pertinentes et détecter les menaces en amont.

Détection accélérée des menaces

Soyez plus rapide pour détecter, isoler et prendre en charge les menaces, ce qui minimise leur impact et leur périmètre.

Analyses plus efficaces

S'intégrant nativement avec les Endpoints, les serveurs et les environnements Cloud, les capteurs de Trend Micro XDR affinent la compréhension des sources de données. Le traitement analytique devient plus efficace qu'avec une intégration via des API avec une plateforme tierce.



TREND MICRO™ MANAGED XDR

Soulagez vos équipes de sécurité

Avec Managed XDR, les avantages de la technologie XDR sont à disposition des clients grâce aux ressources et compétences des experts de Trend Micro qui mèneront les investigations sur les menaces avancées.

Ce service managé offre un monitoring des alertes en 24/7, une hiérarchisation des alertes, des fonctionnalités d'investigation et des services de recherche de menaces

Managed XDR recueille des données sur la sécurité des Endpoints, du réseau et des serveurs pour corréler et prioriser les alertes et informations systèmes, tout en réalisant des analyses de cause racine. Nos chercheurs sur les menaces mènent les investigations pour vous et vous offrent un plan de remédiation complet.

Pour toute information sur les données personnelles que nous recueillons et les raisons pour lesquelles nous les recueillons, merci de consulter notre charte de confidentialité sur : https://www.trendmicro.com/privacy

TREND MICRO™

Securing Your Connected World