Trend Micro

VISION ONE™

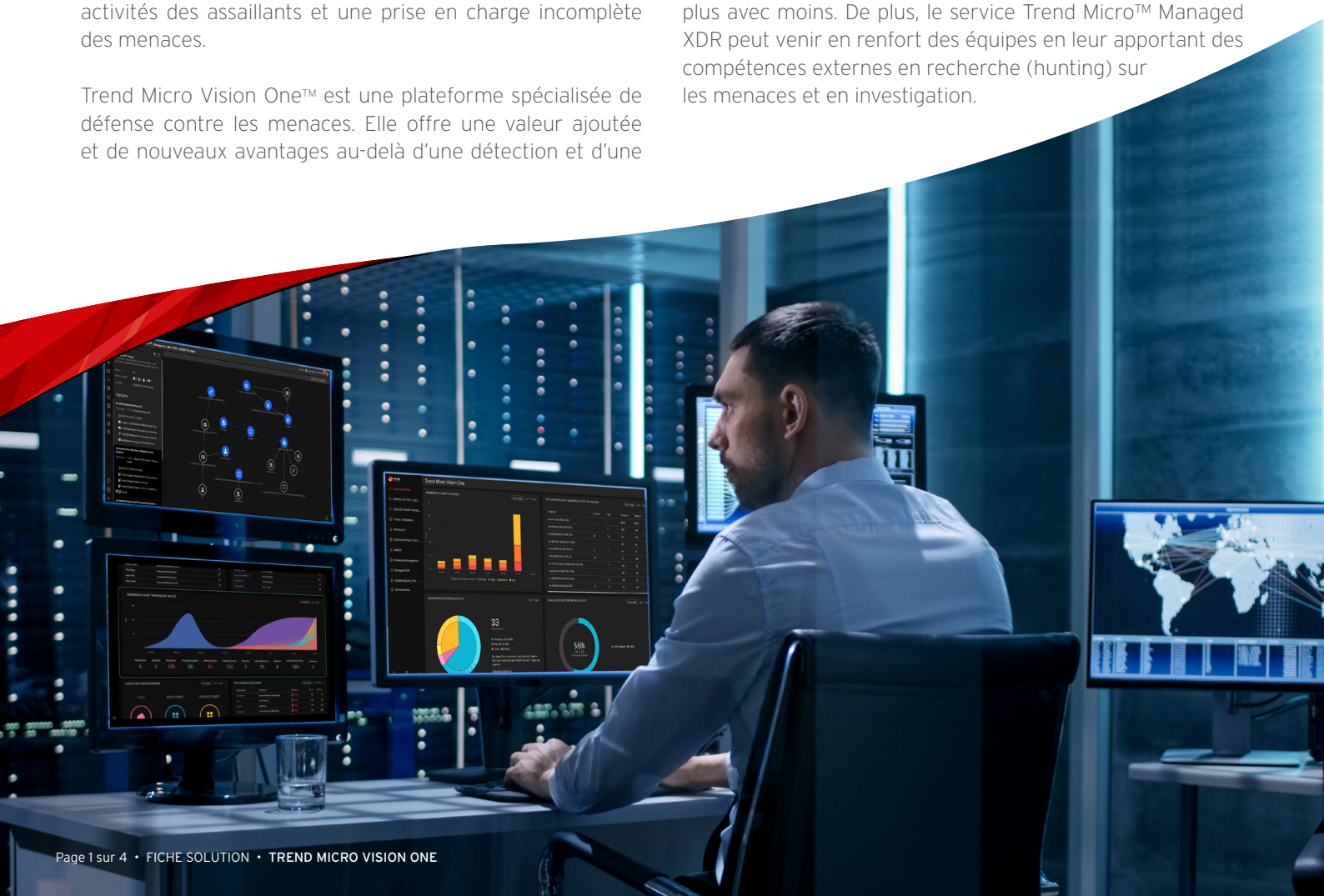
Voir plus. Réagir plus vite.

Avec un paysage de menaces en évolution constante, vous devez disposer des leviers pour détecter et réagir rapidement aux menaces qui compromettent vos lignes de défense en place. Aujourd'hui, de nombreuses entreprises utilisent des couches de sécurités distinctes pour détecter les menaces ciblant l'email, les endpoints, les serveurs et les services Cloud : les informations sur les menaces sont alors cloisonnées et donnent lieu à une prolifération d'alertes non corrélées.

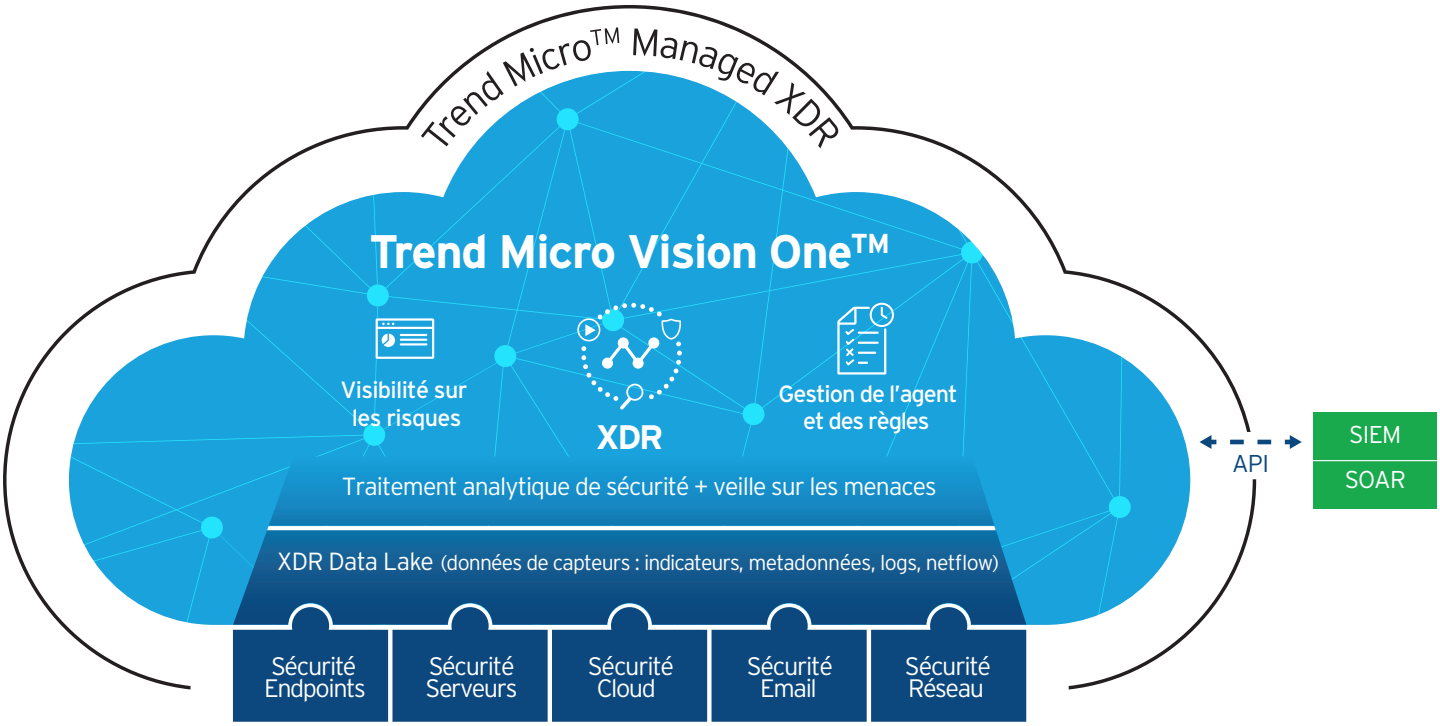
Les investigations sur les menaces portent sur un ensemble de solutions et de couches disparates et doivent être réalisées manuellement. En l'absence d'une visibilité globale et de corrélation, il est probable que tous les risques ne sont pas identifiés. Nombre d'outils de détection et de réponse aux menaces ne s'intéressent qu'aux endpoints et ne tiennent pas compte des menaces qui passent par les emails des utilisateurs, les serveurs, les workloads du Cloud et les différents réseaux. Il en résulte une visibilité limitée sur les activités des assaillants et une prise en charge incomplète des menaces.

Trend Micro Vision One™ est une plateforme spécialisée de défense contre les menaces. Elle offre une valeur ajoutée et de nouveaux avantages au-delà d'une détection et d'une réponse étendues et approfondies (XDR) aux menaces, vous permettant de voir plus et de réagir plus rapidement. Trend Micro Vision One™ offre les fonctionnalités XDR qui recueillent et corrèlent automatiquement les données de sécurité en provenance de différents vecteurs d'attaque potentiels : email, endpoints, serveurs, instances Cloud et réseau. La solution prévient ainsi la majorité des attaques grâce à une protection automatisée.

Les senseurs et des dispositifs de protection natifs, couplés aux capacités XDR qui collectent l'activité des menaces sur différentes couches, permettent de détecter rapidement les attaques complexes qui échappent à la surveillance. Il en résulte une parfaite compréhension des données d'activité au sein de votre environnement et une approche pondérée à la sécurité. Les équipes de sécurité peuvent suivre l'historique d'une attaque et y répondre plus rapidement, avec plus de précision. L'efficacité et la visibilité qu'offre Trend Micro Vision One™ dopent les performances, permettant d'en faire plus avec moins. De plus, le service Trend Micro™ Managed XDR peut venir en renfort des équipes en leur apportant des compétences externes en recherche (hunting) sur les menaces et en investigation.



UNE PLATEFORME DE DÉFENSE QUI DÉPASSE LES OUTILS XDR CLASSIQUES



PROBLÉMATIQUES MÉTIERS

- Les menaces furtives continuent à contourner les meilleures défenses.
- Des couches de sécurité déconnectées, avec des outils et ensembles de données cloisonnés, ne facilitent en rien la corrélation des informations de sécurité et la détection des menaces critiques.
- Des alertes trop nombreuses et des équipes IT déjà surchargées ne permettent pas de consacrer le temps et les ressources nécessaires aux investigations.
- Une visibilité consolidée sur le statut de sécurité d'une entreprise et sur les tendances à venir est difficile à concrétiser : impossible de savoir sur quoi se focaliser et les actions à mettre en place.

"Il est désormais plus simple pour mon équipe d'expliquer une attaque et sa séquence d'événements. C'est aussi **facile que de lire un livre** et d'une parfaite clarté."

Frank Bunton
CISO, MedImpact

AVANTAGES

Voir plus

- **Protection intégrale** - La détection et la prévention de Trend Micro (réputation Web, contrôle applicatif, IPS...) neutralisent proactivement et automatiquement les attaques.
- **Données plus complètes** - Les senseurs natifs intégrés fournissent des données d'activité complètes, et pas seulement des détections, sur les e-mails, les endpoints, les serveurs, les charges de travail Cloud et les réseaux.
- **Détection accélérée et précoce** – Le système XDR corrèle automatiquement une série d'activités mineures pour détecter des attaques en cours, donnant lieu à des alertes moins nombreuses, hiérarchisées et présentant un historique graphique des attaques.
- **Plus de contexte, moins de bruit** - L'intégration des informations sur les menaces de Trend Micro avec MITRE ATT&CK permet d'enrichir la détection et rend les investigations plus pertinentes.
- **Visibilité élargie sur les risques** - Une visibilité holistique basée sur les rôles indique les risques et les tendances les plus significatives pour votre équipe. Un tableau de bord intuitif offre une visibilité centralisée et étendue sur vos évènements réseau et sur la situation dans votre pays : synthèse des détections, cibles des techniques d'attaque, liste des dispositifs et utilisateurs à risque, visibilité sur les applications Cloud légitimes ou pas et risques associés.

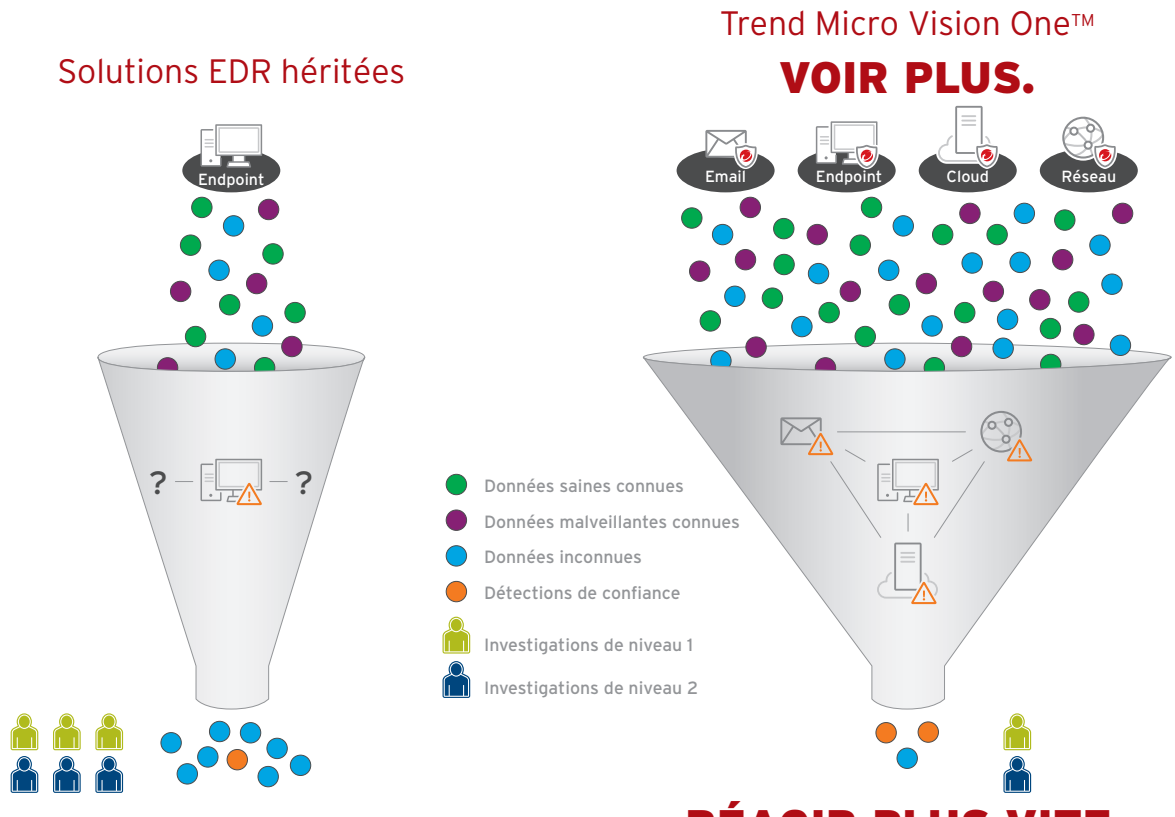
Réagir plus vite

- **Règles de détection actualisées** - De nouvelles règles expertes de détection sont rajoutées régulièrement, à chaque nouvelle menaces identifiée par les experts de Trend Micro. Ceci favorise la recherche automatique de nouveaux indicateurs de compromission (IoC).
- **Investigation accélérée** - La visibilité sur l'historique des attaques. XDR associe automatiquement différents fragments d'une activité malveillante et dresse une image globale couvrant l'ensemble des couches de sécurité.
- **Automatisation** - Les fonctions de remédiation traitent des menaces comme le ransomware (auto-restauration de fichiers endommagés) ou suppriment automatiquement les malware.
- **Prise en charge complète des menaces** - Luttez plus efficacement et simplement contre les menaces, évaluez leur impact, et neutralisez-les sur l'email, les endpoints, les serveurs et les instances Cloud.
- **Gestion proactive des règles** - Avec la visibilité fournie par XDR, les analystes peuvent moduler les règles pour optimiser les fonctions de défense. Ils peuvent également assurer le provisioning de l'agent logiciel.

Des équipes de sécurité plus efficaces

Avec Trend Micro Vision One™, vous disposez d'une seule plateforme pour une réponse rapide aux menaces et qui mobilise moins de ressources.

- **Une seule source** d'alertes prioritisées pour corréler et analyser les données de manière pertinente.
- **Un seul lieu** d'où mener des investigations centralisées, visualiser rapidement la chaîne des évènements sur toutes les couches de sécurité et connaître les étapes d'exécution d'une attaque.
- **Un espace centralisé** pour assurer la prise en charge des menaces véhiculées par email, endpoints, instances Cloud, serveurs et réseau.



LES AVANTAGES CLÉS DE XDR AVEC TREND MICRO VISION ONE™

Hiérarchisation des alertes :

Les entreprises sans XDR ignorent jusqu'à deux fois plus d'alertes de sécurité que celles utilisant XDR[1]. Cette technologie corrèle des indicateurs faibles, déclenche des alertes fiables en cas d'attaque et restitue l'historique d'une attaque. Les équipes de sécurité savent ainsi où focaliser leurs efforts.

Des analyses plus efficaces :

En s'intégrant nativement avec l'email, les endpoints, les serveurs et les environnements cloud et les réseaux, les capteurs de Trend Micro XDR affinent la compréhension des sources de données. Ceci aboutit à un traitement analytique plus efficace, associé à des règles de détection actualisées en permanence et à une veille mondiale sur les menaces proposée par Trend Micro Research. Une vraie alternative à une intégration avec des applications tierces via des API. Les entreprises qui ont adopté XDR subissent deux fois moins d'attaque réussies[1].

Une visibilité contextuelle et claire sur les menaces :

Avec des alertes contextuelles plus nombreuses sur plus de vecteurs d'attaque, des évènements en apparence bénins peuvent soudainement devenir des indicateurs de compromission. Avec cette visibilité décisionnelle, vous accédez à toute la chaîne d'événements liée à une attaque, sur l'ensemble des couches de sécurité, et vous pouvez centraliser les actions correctives nécessaires. Vos investigations sont plus pertinentes et vous pouvez détecter les menaces en amont.

Neutraliser davantage d'attaques, plus rapidement :

La ligne de défense qu'offre XDR améliore la protection de votre entreprise, grâce à une détection et à une remédiation accélérées. Selon ESG, les entreprises adeptes de XDR ont 2,2 fois plus de chances de détecter un piratage ou une attaque réussie dans un délai de quelques jours, contre plusieurs semaines ou mois pour les autres[2].

Détection accélérée des menaces :

Soyez plus prompts à détecter, isoler et prendre en charge les menaces : vous minimisez ainsi leur impact et leur périmètre. ESG constate que les entreprises utilisant XDR assurent une prise en charge plus complète des attaques et ont 60% moins de chance de subir à nouveau cette attaque.

Une investigation plus efficace sur les menaces :

En corrélant automatiquement les données sur les menaces à partir de sources multiples, XDR accélère et automatise les processus d'investigation et permet aux analystes en sécurité d'accéder à l'historique des attaques. Les entreprises utilisatrices de XDR estiment qu'il leur faudrait l'équivalent de 8 personnes à temps plein pour réaliser les fonctions de corrélation de données qu'offre XDR. D'autre part, elles sont 2,6 fois moins nombreuses à déclarer que leur équipe est surchargée par leur travail.

Intégration avec des systèmes tiers :

Vous disposez sans doute d'autres outils et technologies de sécurité déployés au sein de votre environnement. Nous proposons des API et intégrations avec ces systèmes tiers de type SIEM et SOAR. Trend Micro Vision One s'adapte à ces écosystèmes et aux workflows opérationnels de sécurité, en recueillant des données pertinentes à partir de votre infrastructure pour enrichir davantage vos fonctionnalités XDR.

TREND MICRO™ MANAGED XDR

Déchargez vos équipes en charge de la sécurité

Managed XDR offre, en 24/7, un monitoring et une hiérarchisation des alertes, ainsi que des fonctions d'investigation et de recherche de menaces, sous forme de services managés à disposition des clients. Les clients tirent parti des ressources et du savoir-faire des experts en sécurité de Trend Micro pour accélérer la détection et la réponse aux menaces. Grâce à des techniques propriétaires, ce service offre un monitoring efficace des alertes, des investigations sur les menaces évoluées identifiées, ainsi que des fonctions de recherche de menaces. Avec ce service managé, nos chercheurs peuvent répondre à vos menaces. Ils établissent un plan d'actions par étape pour répondre aux menaces, ainsi que des outils de nettoyage lorsqu'une restauration post-incident s'avère nécessaire.

Le service Managed XDR s'applique à l'email, aux endpoints, aux réseaux, ainsi qu'aux instances de serveur et Cloud.

1 - L'atout XDR : une meilleure posture de sécurité, Sept 2020
2 - L'atout XDR, ESG Research
3 - L'atout XDR, ESG Research

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