FICHE SOLUTION

La cybersécurité des infrastructures critiques

Sécurité intégrale de la surface d'attaque & gestion des risques avec Trend Vision One™

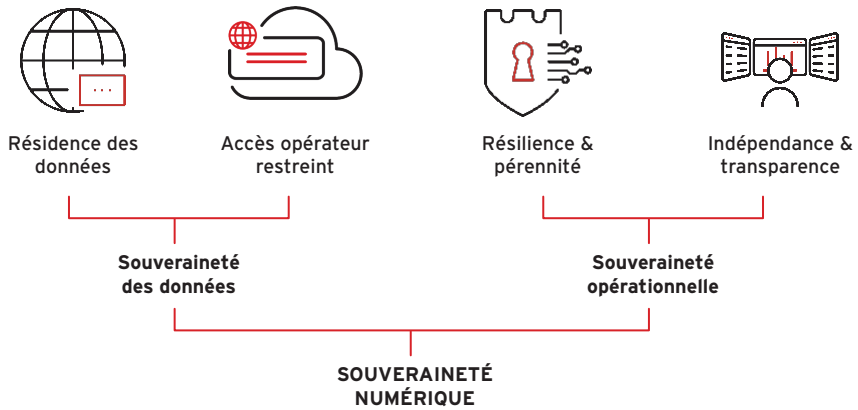
Les infrastructures critiques, cibles privilégiées des cybercriminels

Selon le rapport 2024 de l'ENISA (agence de l'Union européenne de cybersécurité), les infrastructures critiques deviennent plus vulnérables, notamment dans les secteurs des services publics, du transport ou encore de la défense. Elles représentent une part importante des cyberincidents enregistrés de juillet 2023 à juin 2024 :

- Administrations publiques (19 %)
- Transports (11 %)
- Santé (4 %)
- Énergies (3 %)
- Défense et sécurité nationale (2 %)

L'urgence pour des mesures de cybersécurité robustes face aux ransomwares

Les entreprises évoluant dans des secteurs critiques et réglementés sont confrontées à nombre de défis, de la gestion des systèmes hérités à l'adoption de nouvelles technologies émergentes et à l'impératif de protéger des infrastructures nationales sensibles. Alors que ces secteurs évoluent, ils font face à des menaces complexes, avec notamment des attaques sponsorisées par des États-nations. Des cadres réglementaires, à l'instar du Règlement de l'UE sur la cybersécurité et la Directive NIS2 accentuent le besoin pour des mesures de sécurité renforcées et le respect des exigences de souveraineté. Ces exigences dictent comment les données doivent être stockées, traitées et protégées pour se conformer à la législation applicable en matière de protection des informations sensibles, souvent hébergées au sein d'environnements cloisonnés qui assurent leur souveraineté.



> **Nous faisons appel à Trend Vision One pour relever des défis de cybersécurité critiques dans le secteur public. La solution assure la souveraineté de nos ressources numériques et est adaptée aux acteurs du Service public, aux infrastructures critiques et à d'autres secteurs d'activité réglementés.**
>
> Thomas Teitge
> Vice-président, secteur public
> Bechtle GmbH & Co

Sécuriser les écosystèmes critiques avec Trend Vision One

Trend Vision One, notre plateforme de cybersécurité d'entreprise optimisée par IA, dote les équipes en charge d'infrastructures critiques de capacités de détection des menaces, de gestion des risques et de souveraineté des données. Les professionnels de la sécurité sont outillés pour contextualiser les risques et évaluer la probabilité des attaques, ce qui encourage une sécurité proactive.

Notre plateforme propose la technologie XDR (extended detection and response) en natif, ainsi qu'une gestion de l'exposition aux risques cyber, pour offrir à vos équipes la visibilité dont elles ont besoin. Celles-ci disposent d'indicateurs d'activité pertinents, qui vont au-delà de simples données de détection, ainsi que d'une visibilité centralisée sur les différentes couches de sécurité protégeant les endpoints, les serveurs, l'email, les identités, les dispositifs mobiles, les instances cloud et le réseau. Cette approche globale donne lieu à une détection et à une gestion proactive et précise des risques et des menaces, à des investigations plus simples et à une gestion globale des risques de sécurité.

Trend Vision One s'adapte aux environnements cloisonnés sous votre contrôle

Écosystèmes spécifiques à un secteur d'activité

Une sécurité sur mesure pour les administrations, les entreprises de l'énergie ou encore les acteurs de la défense.

Visibilité intégrale sur les risques et les menaces

Bénéficiez de perspectives en temps réel sur les vulnérabilités et les vecteurs d'attaque grâce à une plateforme intégrée qui associe détection des menaces et veille de premier rang.

Protection des systèmes et infrastructures hérités

Protégez vos environnements hétérogènes, pour assurer la continuité des activités et la résilience sur l'ensemble des opérations critiques tout en réduisant la surface d'attaque.

Conformité aux exigences de souveraineté

Avec Trend Vision One, votre entreprise respecte ses contraintes de gouvernance en assurant la localisation des données, la conformité aux lois nationales et le respect des normes sectorielles. Cette capacité est essentielle à la conformité réglementaire et à la protection des données sensibles au sein des secteurs critiques.

2024 MITRE ATT&CK™ Enterprise Security Evaluation

Analyse de toutes les étapes majeures (16/16)

Analyse de toutes les sous-étapes pour Linux et macOS

Analyse de toutes les sous-étapes pour les plateformes de serveur (Windows/Linux)

Analyse de 99 % des sous-étapes (79/80)

Omdia Research: Quantifying the Public Vulnerability Market: 2025 Edition

Trend Zero Day Initiative™ (ZDI), premier programme mondial d'identification de bugs, a divulgué davantage de vulnérabilités confirmées en 2024 que tous les autres éditeurs participants réunis.

Leader dans le Magic Quadrant de Gartner 2025 dédié aux plateformes de protection des endpoints

Trend Micro est de nouveau salué en tant que Leader pour sa protection intégrale des endpoints contre les menaces.

TREND Vision One

Plateforme de cybersécurité d'entreprise optimisée par IA

SaaS | Sur site | GovCloud | Cloud privé | Fournisseurs de services

Cap sur une sécurité proactive

Trend Vision One est la seule plateforme de cybersécurité d'entreprise qui centralise la gestion de l'exposition aux risques cyber, les opérations de sécurité, ainsi qu'une protection robuste et en profondeur. Autant de leviers pour anticiper et prévenir les menaces, mais aussi accélérer les résultats d'une sécurité proactive.

Une seule plateforme de cybersécurité pour sécuriser différentes technologies

Valeur ajoutée de la solution CREM de Trend Vision One™

Une étude de Trend™ Research portant sur 6 588 entreprises utilisatrices de la technologie CREM (Cyber Risk Exposure Management), menée sur la première moitié de 2024, révèle une corrélation étroite entre des indices de risque élevés et une vulnérabilité plus marquée aux ransomwares. Les entreprises ayant souffert d'attaques par ransomware affichent un indice de risque de 52,38 contre 40,25 pour celles qui n'en ont pas subi, ce qui rend la gestion efficace des risques un impératif pour prévenir de telles menaces.

Les conclusions de l'étude révèlent que les entreprises dont l'indice de risque est supérieur à la moyenne sont 12 fois plus susceptibles de subir une infection par ransomware que leurs pairs présentant un indice moindre, soulignant ainsi l'importance d'une gestion proactive des risques. Le CREM identifie les vulnérabilités sur l'ensemble de votre surface d'attaque, priorise les risques et déploie des mesures efficaces. Votre entreprise peut optimiser sa posture globale de sécurité en réduisant son indice de risque (Risk Index) composé de l'indice d'attaque (Attack Index), de l'indice d'exposition (Exposure Index) et de l'indice de configuration de la sécurité (Security Configuration Index).

Ces capacités sont fournies en mode SaaS, à partir du cloud public. Avec Trend Vision One, l'environnement est hébergé sur site.

Pour en savoir davantage, consultez **Vulnerable to Resilient: Cutting Ransomware Risk with Proactive Cyber Risk Exposure Management** sur trendmicro.com/vulnerable-to-resilient-report

Découvrir Trend Vision One en action

Évaluez la plateforme Trend Vision One gratuitement pendant 30 jours. Accédez à ses fonctionnalités XDR robustes, ses outils éprouvés de gestion des risques cyber et sa veille sur les menaces maintes fois récompensée.

Démarrez votre évaluation >

Posture de sécurité renforcée et contextuelle

Trend Vision One vous permet de protéger les technologies utilisées dans nombre de secteurs critiques (service public & administration, énergie, soins de santé, défense), en vous apportant :

- **Des solutions pour l'IT :** protection des endpoints, tablettes, smartphones, instances physiques et virtuelles, serveurs cloud et conteneurs. La sécurité robuste se déploie sur différentes infrastructures IT tout en respectant les exigences de souveraineté des données. Les données sensibles sont stockées et traitées en conformité avec la législation en vigueur.
- **Des solutions pour l'OT :** sécurité des réseaux industriels OT (Operational Technology) présentant des exigences de haute disponibilité, à l'instar des réseaux de distributeurs bancaires. Vous disposez d'une protection intégrale des environnements qui font appel à des technologies OT. La souveraineté des données grâce à une gestion en local des données et la conformité réglementaire.
- **Des solutions pour les TC :** protection des réseaux et des dispositifs sur des réseaux mobiles privés de type 5G et un framework sécurisé et résilient pour les TC (technologies de communication). Les principes de souveraineté des données sont appliqués tandis que le trafic de données est conforme à la réglementation en vigueur.

Des capacités CREM robustes permettent à votre entreprise de maîtriser la complexité de la cybersécurité tout en assurant la conformité réglementaire. Des indicateurs XDR pertinents apportent à vos équipes SOC et de réponse aux incidents une visibilité intégrale pour détecter et répondre aux menaces sur l'ensemble de votre écosystème, chaîne collaborative incluse. La souveraineté des données est assurée tout au long du processus.

Haute disponibilité & productivité opérationnelle maximale

Bénéficiez de capacités CREM au service de votre résilience pour évaluer les risques en permanence, bénéficier de recommandations décisionnelles et automatiser les opérations de remédiation. XDR avec IA permet à vos analystes de prioriser les alertes plus efficacement, pour ainsi neutraliser les nouvelles menaces plus rapidement. L'IA Générative (GenIA) vient au renfort des compétences des analystes SOC qui doivent déjouer des menaces versatiles.

Validation économique de Trend Vision par ESG

Dans cette analyse économique, ESG se penche sur les avantages quantitatifs et qualitatifs auxquels les entreprises peuvent prétendre lorsqu'elles remplacent leur cybersécurité fragmentée par Trend Vision One. Selon cette étude, Trend Vision One allège les coûts de cybersécurité de 70 % et offre de solides avantages :

- **Maîtrise des risques :** selon ESG, les clients de Trend Vision One sont moins exposés aux ransomwares et aux intrusions, mais aussi moins impactés en cas d'incident avéré.
- **Détection et réponse plus efficace aux incidents :** les clients pointent une nette amélioration de leur capacité à détecter les problématiques à haut risque et à les traiter plus rapidement.
- **Productivité opérationnelle renforcée :** les clients constatent qu'ils investissent moins dans la sécurité et dans la réponse aux incidents par rapport à leurs solutions précédentes.

Interrogés sur leur sentiment que leur exposition aux risques est moindre avec Trend Vision One, chaque répondant met en avant une visibilité améliorée, des alertes plus fiables et un délai de présence (*dwell time*) moindre des menaces, ce délai étant, en moyenne, 65 % inférieur comparé à leur environnement précédent.

Principaux défis de sécurité des services d'infrastructure	
Sécurité IT	
Détection et protection contre les ransomwares, le phishing, les malwares, etc.	✓
Analyse de la surface d'attaque et priorisation des tâches pour minimiser les risques de cybersécurité	✓
Protection contre le piratage de données et les accès prohibés, grâce au Zero-Trust	✓
Traitement des indicateurs de compromission et des indicateurs d'attaque sur toutes les couches de défense	✓
Visibilité et contrôle sur les dispositifs, les applications et les données	✓
Restauration des vulnérabilités connues, inconnues et non divulguées sur votre réseau. Restauration des vulnérabilités par virtual patching	✓
Maîtrise des risques de sécurité liés à la chaîne collaborative	✓
Conformité	
Contrôle des risques associés à une mauvaise utilisation de l'IA (Règlement de l'UE sur l'intelligence artificielle)	✓
Microsegmentation des systèmes critiques	✓
Protection des systèmes d'exploitation obsolètes	✓
Tests C5 (norme allemande Cloud Computing Compliance Criteria Catalogue) des services SaaS	✓
Modèle de déploiement sur site, sans dépendance au cloud	✓
Infrastructure commune	
Migration sécurisée vers le cloud et amélioration des opérations dans le cloud	✓
Prévention des accès prohibés, des infections par malware et de leur prolifération sur les réseaux 5G privés	✓
Prise en charge du multi-cloud et du cloud hybride	✓
Accès externe	
Sécurité Zero-Trust des accès et de la maintenance à distance à partir de dispositifs gérés ou non	✓
Acheminement sécurisé des données sensibles au sein des environnements cloisonnés	✓
SOC/CSIRT	
Détection et priorisation des dispositifs, des utilisateurs et des applications cloud à risque au sein de votre environnement	✓
Simplification des opérations de sécurité et visibilité sur la totalité des chaînes d'évènements, sur l'ensemble des couches de sécurité (analyse de causes racines, évaluation des impacts sur les ressources et réponse immédiate)	✓
IA pour mieux comprendre les éléments de contexte	✓
Équipes de sécurité hypersollicitées	
Service managé XDR, disponible en 24/7, au renfort de votre équipe pour détecter et répondre en amont aux incidents*	✓
En option, des simulations de type Red teaming ou Purple teaming	✓
Réponse aux incidents en situations d'urgence.*	✓

* Trend Service One™ est disponible en tant que service SaaS managé pour Trend Vision One SaaS

Copyright © 2025 Trend Micro Incorporated. Tous droits réservés. Trend Micro, le logo Trend Micro, le logo t-ball et Trend Vision One sont des marques déposées de Trend Micro Incorporated. Toutes les autres marques de produit ou d'entreprise sont susceptibles d'être des marques déposées par leurs détenteurs respectifs. Les informations présentées dans ce document sont susceptibles d'être modifiées sans préavis. Données non contractuelles. Trend Micro, le logo Trend Micro et le logo t-ball portent le symbole standard Reg. U.S. Pat. et Tm. TrendMicro.com [SB00_Critical_Sector_Solution_Brief_250903FR]

Pour plus d'informations sur les informations personnelles que nous recueillons et sur la raison pour laquelle nous le faisons, veuillez consulter notre Déclaration de confidentialité sur notre site Web à l'adresse trendmicro.com/privacy

Faites vos premiers pas

RDV sur Trendmicro.fr > Évaluation gratuite