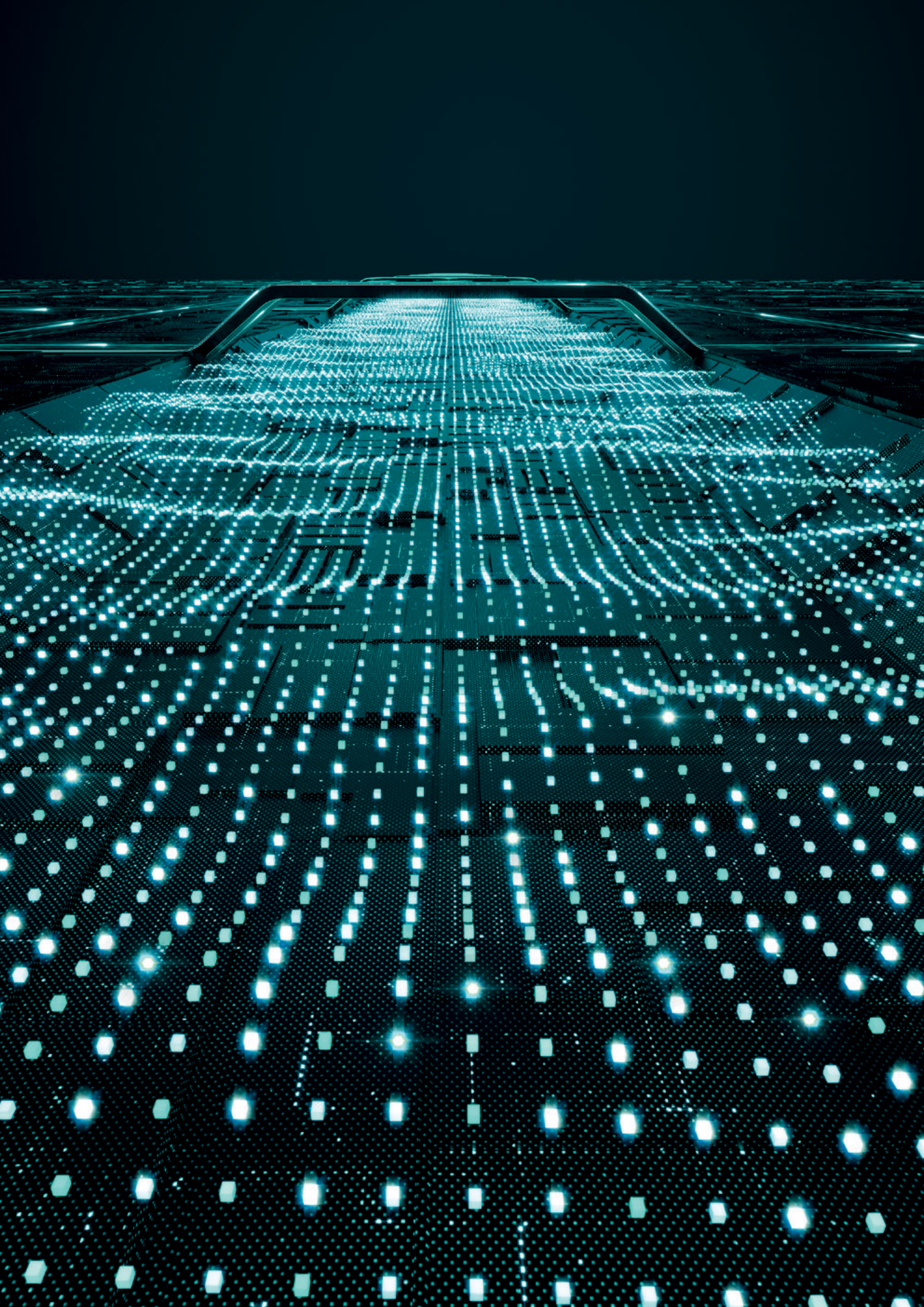
FICHE PRODUIT

ENTERPRISE INSPECTOR

Contrez les attaques ciblées et APT, ainsi que les comportements malveillants avec notre solution EDR développée par des experts de la cybersécurité

DES EXPERTS EN CYBERSÉCURITÉ
À VOS CÔTÉS



Qu'est-ce qu'une **solution EDR ?**

ESET Enterprise Inspector est une solution EDR (Endpoint Detection and Response) sophistiquée permettant de détecter les comportements anormaux et les failles, d'évaluer les risques, de réagir aux incidents, d'enquêter et de résoudre les problèmes.

Elle surveille et évalue toutes les activités au sein de votre du réseau telles que les utilisateurs, les fichiers, les processus, la base de registre, la mémoire et les évènements réseau en temps réel, vous permettant d'agir immédiatement en cas de nécessité.

Pourquoi **déployer une solution EDR ?**

VIOLATIONS DE DONNÉES

Les entreprises doivent non seulement pouvoir détecter les failles de données, mais aussi être en mesure de les limiter et de les éliminer. Dans la plupart des cas, elles ne disposent pas des capacités internes requises pour réaliser ces investigations et font donc appel à des prestataires externes. Les organisations ont aujourd'hui besoin d'une meilleure visibilité sur leurs ordinateurs afin de s'assurer que les menaces émergentes, les comportements utilisateurs à risque et les applications indésirables ne menacent pas les bénéfices et la réputation de leur établissement.

Les secteurs les plus touchés par les violations de données sont traditionnellement ceux qui possèdent des données de valeur, tels que la finance, le commerce de détail, la santé et le secteur public. Cela ne veut pas dire que les autres secteurs sont à l'abri, mais simplement que les pirates calculent généralement le rapport entre efforts requis et bénéfices escomptés.

MENACES PERSISTANTES AVANCÉES (APT) ET ATTAQUES CIBLÉES

Les systèmes EDR permettent d'identifier les APT ou les attaques ciblées, d'accélérer la réactivité face aux incidents et de lutter contre les attaques à venir de manière proactive. Dans le monde de l'entreprise, il est particulièrement important de pouvoir détecter les APT. En effet, les entreprises doivent pouvoir contrer et contenir les attaques susceptibles de passer inaperçues au sein de leur réseau pendant des jours voire des mois.

MEILLEURE VISIBILITÉ ORGANISATIONNELLE

Les menaces internes et les attaques d'hameçonnage s'imposent comme des menaces majeures pour les entreprises. L'hameçonnage est souvent utilisé en entreprise en raison du nombre important de cibles potentielles (les salariés). En effet, il suffit qu'un utilisateur tombe dans le piège pour compromettre l'ensemble de l'organisation. Parallèlement, les menaces internes représentent elles aussi un facteur de risque, car plus l'entreprise emploie de salariés, plus il est probable que l'un d'entre eux œuvre à l'encontre des intérêts de l'organisation.

Les systèmes EDR offrent la visibilité dont les entreprises ont besoin pour identifier, comprendre, bloquer et éliminer les menaces au sein de leurs équipements. Ils permettent notamment de bloquer les pièces jointes malveillantes et de s'assurer que les salariés utilisent uniquement les ressources validées par l'organisation.

Plateforme de protection des terminaux d'ESET
Sécurité des terminaux multicouche : chaque couche envoie ses données à ESET Enterprise Inspector.

+

ESET Enterprise Inspector
Un outil EDR sophistiqué analysant l'ensemble des données en temps réel pour détecter toutes les menaces et les attaques.

=

Une solution de prévention, détection et réponse complète permettant d'analyser et d'éliminer rapidement les problèmes de sécurité au sein de votre réseau.

Les organisations ont aujourd'hui besoin d'une meilleure visibilité sur leurs ordinateurs afin de s'assurer que **les menaces émergentes, comportements utilisateurs à risque et applications indésirables** ne menacent pas les bénéfices et la réputation de leur établissement.

Optez pour l'accompagnement des experts ESET afin de maîtriser de bout en bout les solutions :

ESET Deployment & Upgrade

Les professionnels d'ESET installent et configurent vos produits ESET dans votre environnement, puis forment vos équipes pour garantir la réussite du déploiement dès le premier jour.

ESET Threat Monitoring

Les experts d'ESET surveillent votre réseau et la sécurité de vos terminaux et vous préviennent dès qu'une situation anormale nécessite votre attention.

ESET Threat Hunting

Les experts d'ESET aident les clients à analyser les données, les évènements et les alertes générés par ESET Enterprise Inspector, y compris les analyses des causes, les enquêtes et les conseils utiles pour limiter l'impact des problèmes.

Les avantages ESET

ANALYSE DES MENACES ANTÉRIEURES

ESET Enterprise Inspector assure à la fois l'analyse personnalisée des menaces et l'analyse des menaces antérieures. Vous pouvez facilement modifier les règles comportementales, puis relancer l'analyse de la base de données d'évènements. Cela vous permet d'identifier les nouvelles alertes déclenchées par les modifications que vous avez effectuées. Vous n'avez plus besoin de rechercher d'IOC statiques : le système détecte des comportements dynamiques avec différents paramètres.

DANS LE CLOUD OU SUR SITE

Grâce à son architecture flexible et sécurisée, ESET Enterprise Inspector peut être déployé sur site ou dans le cloud pour offrir une meilleure évolutivité, en fonction de la taille et des besoins de l'entreprise.

ARCHITECTURE OUVERTE

Système de détection unique basé sur le comportement et la réputation, entièrement transparent et paramétrable. Il est facile de modifier ou de créer des règles via XML pour affiner la configuration selon les besoins de l'environnement de l'entreprise, y compris dans le cas des intégrations SIEM.

SENSIBILITÉ AJUSTABLE

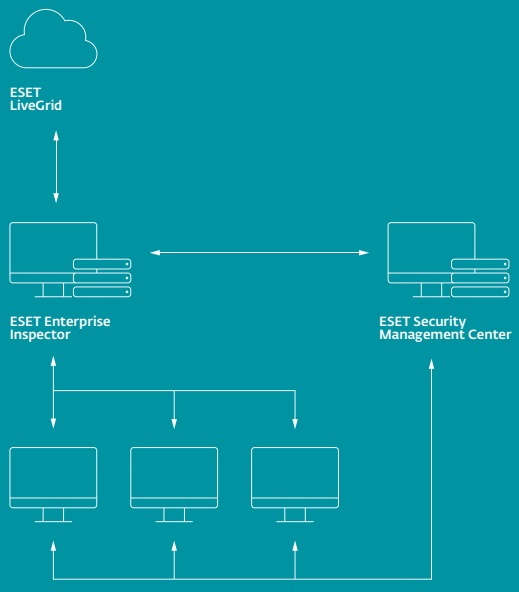
Éliminez facilement les fausses alertes en ajustant la sensibilité des règles de détection pour différents groupes d'équipements ou d'utilisateurs. Combinez plusieurs critères comme le nom des fichiers, l'emplacement, le hash, la ligne de commande et le signataire pour affiner les conditions de déclenchement des alertes.

SYSTÈME DE RÉPUTATION

Le système de filtrage avancé d'ESET permet aux ingénieurs sécurité de filtrer toutes les applications de confiance en s'appuyant sur le système de réputation développé par ESET. Ce dernier inclut une base de données rassemblant des centaines de millions de fichiers vérifiés, pour faire en sorte que les équipes de sécurité se concentrent sur les fichiers inconnus, et non pas sur les faux positifs.

INTERVENTION SYNCHRONISÉE

Reposant sur l'offre de sécurité des terminaux d'ESET, l'intervention synchronisée crée un écosystème cohérent qui lie tous les objets pertinents et permet de résoudre les incidents de manière synchronisée. Les équipes de sécurité peuvent ainsi interrompre les processus, télécharger les fichiers ayant déclenché des alertes, éteindre les ordinateurs ou redémarrer les systèmes directement depuis la console.



Système de détection unique basé sur le comportement et la réputation, entièrement transparent pour les équipes en charge de la sécurité.

Cas d'utilisation

Détection des menaces avancée - Ransomware

Les ransomwares ont pour objectif de passer inaperçus sur le réseau et de se propager sur un plus grand nombre de terminaux possible. Ils s'infiltrent également dans les sauvegardes machines pour rester exécutables même lorsque les équipes restaurent les images sauvegardées.

L'agent d'ESET Enterprise Inspector approfondit les fonctionnalités des solutions de protection des terminaux d'ESET et vous permet de détecter les ransomwares présents sur le réseau de manière proactive. Les ransomwares sont généralement transmis via des pièces jointes d'e-mails. À l'ouverture, le document demande à l'utilisateur d'activer les macros. L'activation des macros déclenche l'enregistrement d'un exécutable dans le système. Ce fichier commence ensuite à chiffrer tous les éléments qu'il trouve, y compris les équipements connectés.

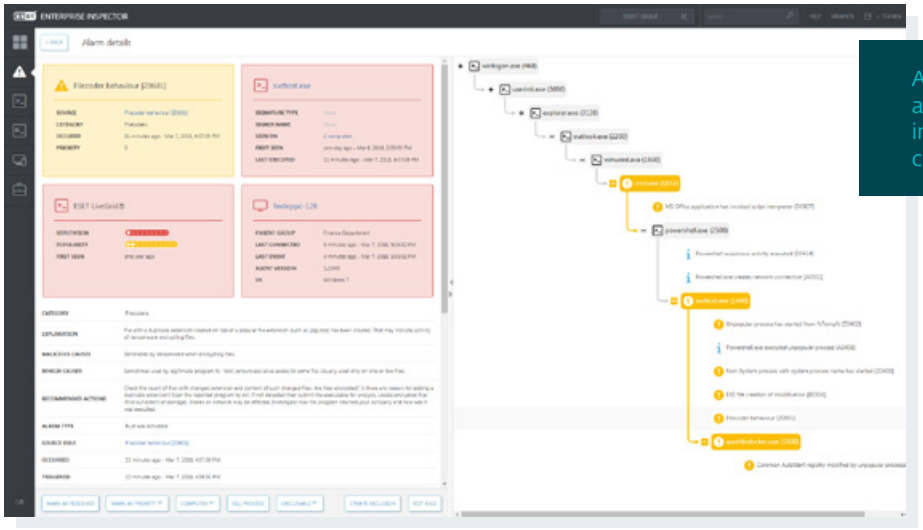
ESET Enterprise Inspector permet à votre équipe de sécurité de détecter ces comportements, d'identifier les éléments affectés, de déterminer l'emplacement et le moment où l'exécutable, le script ou l'action ont été lancés, et enfin d'analyser la cause profonde de l'incident en quelques clics seulement.

CAS D'UTILISATION

Une entreprise a besoin d'outils supplémentaires pour pouvoir détecter les ransomwares et pour recevoir des alertes rapides lorsque des comportements suspects surviennent au sein du réseau.

SOLUTION

- ✓ Configuration de règles pour détecter les applications exécutées depuis des dossiers temporaires.
- ✓ Configuration de règles pour détecter les fichiers Office (Word, Excel, PowerPoint) lorsqu'ils exécutent des scripts ou des exécutables supplémentaires.
- ✓ Envoi d'alertes dès qu'une extension typique des ransomwares est détectée sur un appareil.
- ✓ Les alertes Ransomware Shield des solutions ESET Endpoint Security sont consultables via la console.



Analysez les arborescences et les informations détaillées des comportements Filecoder.

Détection des comportements et des récidivistes

Même les utilisateurs les plus bienveillants peuvent s'imposer comme la principale faiblesse de la sécurité d'entreprise.

ESET Enterprise Inspector identifie facilement ces éléments à risque en classant les ordinateurs selon le nombre d'alertes uniques déclenchées. Lorsqu'un utilisateur déclenche plusieurs alarmes, il faut que ses activités soient surveillées.

CAS D'UTILISATION

Dans votre réseau, vous avez identifié plusieurs utilisateurs qui sont des cibles récurrentes dont les ordinateurs sont régulièrement infectés par des malwares. Est-ce à cause de leur comportement ? Ou sont-ils ciblés plus fréquemment que vos autres salariés ?

SOLUTION

- ✓ Visualisez facilement les utilisateurs et les équipements problématiques.
- ✓ Effectuez rapidement des analyses des causes profondes pour identifier l'origine des infections.
- ✓ Bloquez les vecteurs d'attaque identifiés (e-mail, Web ou appareils USB).

Détection et blocage des menaces

La performance inégalée d'ESET Enterprise Inspector repose sur son approche de détection des menaces avancée.

Grâce à des filtres permettant de trier les fichiers par popularité, réputation, signature digitale, comportement ou informations contextuelles, le système identifie et analyse facilement les activités malveillantes. En paramétrant plusieurs filtres, vous pouvez automatiser les processus de détection des menaces et ajuster les seuils de détection selon votre environnement d'entreprise.

Toutes les activités suspectes peuvent être facilement identifiées et analysées.

CAS D'UTILISATION

Votre système d'alertes proactives ou votre centre de sécurité (SOC) vous envoie une nouvelle alerte. Comment procédez-vous ?

SOLUTION

- ✓ Tirez parti des alertes proactives pour collecter des données sur les nouvelles ou prochaines attaques.
- ✓ Analysez tous les ordinateurs pour détecter cette nouvelle menace.
- ✓ Analysez les ordinateurs pour déterminer si la menace était déjà présente avant l'envoi de l'alerte.
- ✓ Empêchez la menace de s'infiltrer sur votre réseau ou de s'exécuter dans votre environnement.

Visibilité du réseau

ESET Enterprise Inspector est une solution à architecture ouverte qui permet à votre équipe de sécurité d'ajuster les règles de détection des vecteurs d'attaque en fonction de votre environnement informatique.

Grâce à l'architecture ouverte, vous pouvez également paramétrer ESET Enterprise Inspector pour détecter les violations des politiques de votre organisation concernant notamment l'utilisation de certains logiciels comme les applications torrent, les plateformes de stockage Cloud, la navigation sur Tor, les serveurs indépendants et d'autres systèmes indésirables.

CAS D'UTILISATION

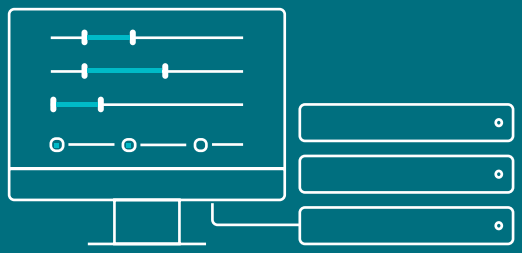
Certaines entreprises se méfient des logiciels que leurs utilisateurs exécutent dans leur système. Vous devez non seulement tenir compte des applications classiques, mais également surveiller les solutions portables qui ne nécessitent pas forcément d'installation pour fonctionner. Mais comment faire ?

SOLUTION

- ✓ Visualisez et filtrez facilement toutes les applications installées sur vos appareils.
- ✓ Visualisez et filtrez tous les scripts sur vos appareils.
- ✓ Bloquez facilement les scripts ou les applications non autorisés.
- ✓ Intervenez en envoyant des alertes aux utilisateurs concernant les applications non autorisées et désinstallez automatiquement les logiciels indésirables.

Vous devez non seulement tenir compte des applications classiques, mais également surveiller les solutions portables qui ne nécessitent pas forcément d'installation pour fonctionner. Mais comment faire ?

Votre équipe de sécurité peut **ajuster les règles de détection** des vecteurs d'attaque en fonction de votre environnement informatique.



Enquête et intervention contextuelles

La « malveillance » des activités dépend de leur contexte.

Les activités réalisées sur les postes des administrateurs réseau sont radicalement différentes de celles du département financier. En regroupant efficacement les ordinateurs, les équipes de sécurité peuvent facilement déterminer si les activités des utilisateurs sont autorisées ou interdites. La synchronisation des groupes de terminaux ESET Security Management Center et des règles ESET Enterprise Inspector offre des informations contextuelles très utiles.

CAS D'UTILISATION

La qualité des données dépend du contexte. Pour prendre les meilleures décisions possibles, vous devez connaître la nature des alertes, les équipements concernés et les utilisateurs qui les ont déclenchées.

SOLUTION

- ✓ Identifiez et triez tous vos ordinateurs en fonction d'Active Directory, des groupes automatiques ou des groupes manuels.
- ✓ Autorisez ou bloquez les applications ou scripts selon vos groupes d'ordinateurs.
- ✓ Autorisez ou bloquez les applications ou scripts selon les utilisateurs.
- ✓ Recevez des notifications pour certains groupes uniquement.

Configuration et intervention simplifiées : pas besoin d'équipe de sécurité

Même quand les entreprises disposent d'une équipe de sécurité dédiée, il peut être difficile de définir rapidement les priorités et de trouver la meilleure approche d'intervention face à la multitude d'alertes reçues.

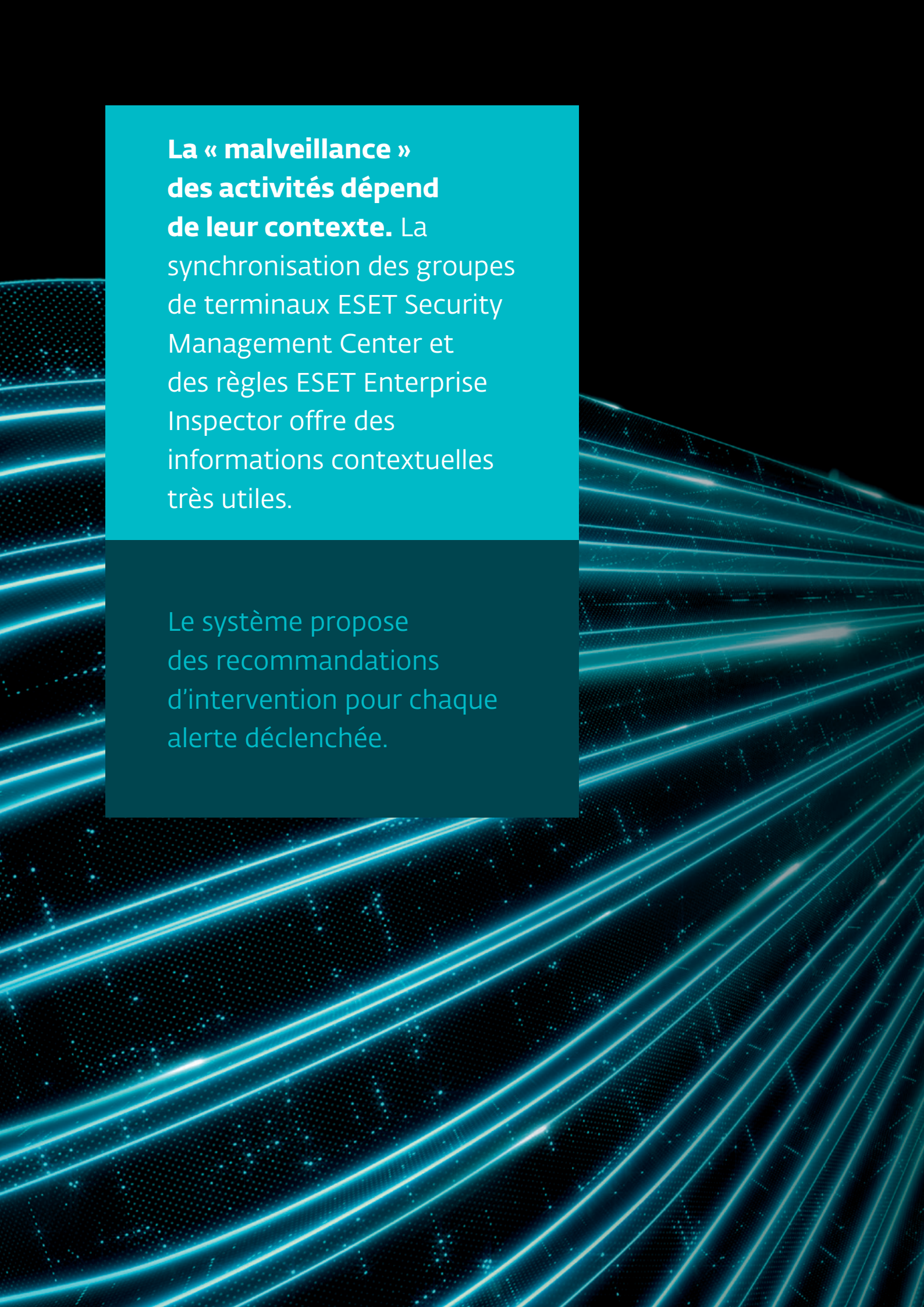
Dans ce contexte, le système propose des recommandations d'intervention pour chaque alerte déclenchée. ESET Enterprise Inspector permet d'intervenir rapidement lorsqu'une alerte est identifiée. Il est également possible de bloquer des fichiers spécifiques par hachage, d'interrompre les processus et de les mettre en quarantaine, ou encore d'isoler ou d'éteindre certaines machines à distance.

CAS D'UTILISATION

Toutes les entreprises ne disposent pas d'équipes de sécurité dédiées : dans cette situation, il peut être difficile de mettre en place des règles de détection avancées.

SOLUTION

- ✓ Plus de 180 règles intégrées et préconfigurées.
- ✓ Intervenez facilement en un clic pour bloquer, interrompre ou mettre en quarantaine les équipements affectés.
- ✓ Intervention suggérée et étapes suivantes intégrées aux alertes.
- ✓ Règles éditables via XML pour modifier ou créer de nouvelles règles.



La « malveillance » des activités dépend de leur contexte. La synchronisation des groupes de terminaux ESET Security Management Center et des règles ESET Enterprise Inspector offre des informations contextuelles très utiles.

Le système propose des recommandations d'intervention pour chaque alerte déclenchée.

Possibilités

DÉTECTION DES MENACES

Appliquez des filtres aux données pour trier les fichiers par popularité, réputation, signature digitale, comportement ou information contextuelle. En paramétrant plusieurs filtres, vous pouvez automatiser les processus de détection des menaces et les personnaliser en fonction de votre environnement d'entreprise. Détection des menaces simplifiée, y compris pour les APT et les attaques ciblées.

DÉTECTION DES INCIDENTS (ANALYSE DES CAUSES PROFONDES)

Consultez facilement et rapidement les incidents de sécurité dans la section alertes. En quelques clics seulement, les équipes de sécurité peuvent accéder à des analyses des causes profondes incluant les équipements affectés, ainsi que l'emplacement et le moment où l'exécutable, le script ou l'action ont été lancés.

ENQUÊTE ET INTERVENTION

Utilisez un ensemble de règles prédéfinies ou créez vos propres règles pour réagir aux incidents détectés. Chaque alarme déclenchée comprend des conseils d'intervention. Grâce à la fonctionnalité d'intervention rapide, il est également possible de bloquer des fichiers spécifiques par hachage, d'interrompre les processus et de les mettre en quarantaine, ou encore d'isoler ou d'éteindre certaines machines à distance. Cette fonctionnalité permet aux équipes de traiter tous les incidents, sans exception.

COLLECTE DE DONNÉES

Consultez des données complètes sur les nouveaux modules exécutés : heure, utilisateur à l'origine de l'exécution, durée d'activité et équipements affectés. Toutes les informations sont stockées localement pour éviter les fuites de données.

DÉTECTION DES INDICATEURS DE COMPROMISSION

Visualisez et bloquez les modules en fonction d'une trentaine d'indicateurs différents, y compris le hachage, les modifications apportées au registre, les modifications de fichiers et les connexions réseau.

DÉTECTION DES ANOMALIES ET DES COMPORTEMENTS

Vérifiez les actions lancées par des exécutables et utilisez le système de réputation LiveGrid® d'ESET pour déterminer rapidement si les processus sont fiables ou suspects. En regroupant les ordinateurs par utilisateurs, services ou d'autres critères, les équipes de sécurité peuvent facilement déterminer si les utilisateurs agissent de manière normale ou inhabituelle.

VIOLATION DES POLITIQUES D'ENTREPRISE

Bloquez l'exécution des modules malveillants au sein des ordinateurs de votre réseau d'entreprise. L'architecture ouverte d'ESET Enterprise Inspector vous permet également de détecter les violations des politiques de votre organisation concernant notamment l'utilisation de certains logiciels comme les applications torrent, les plateformes de stockage Cloud, la navigation sur Tor, les serveurs indépendants et d'autres systèmes indésirables.

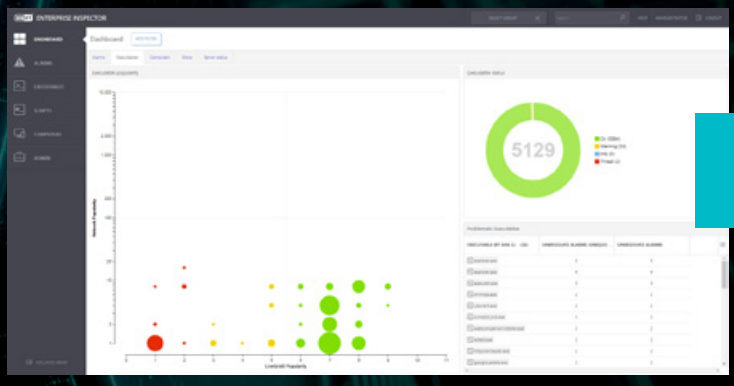


Tableau de bord
d'ESET Enterprise Inspector

À propos d'ESET

ESET, acteur mondial de la sécurité informatique, est désigné comme unique Challenger dans le Gartner Magic Quadrant 2018, « Endpoint Protection »

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe, qui protègent en temps réel les entreprises et les particuliers du monde entier contre des menaces de cybersécurité en constante évolution.

En tant qu'entreprise privée non endettée, nous sommes libres de mener toutes les actions nécessaires pour offrir à nos clients une protection optimale et complète.

ESET EN QUELQUES CHIFFRES

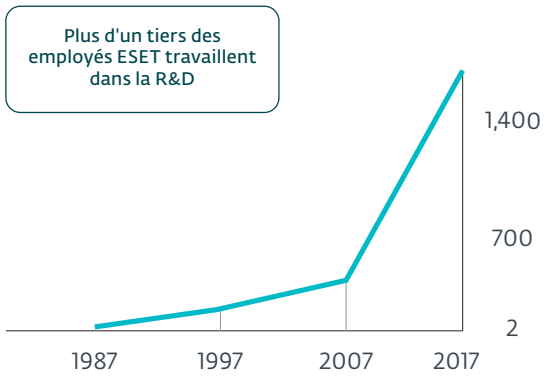
+110 millions
d'utilisateurs partout dans le monde

+ 400 000
Clients Entreprises

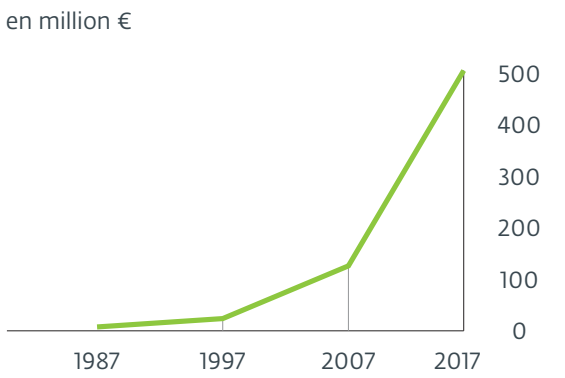
+ 200
pays et territoires couverts

13
centres R&D dans le monde

EMPLOYÉS ESET



CHIFFRE D'AFFAIRES ESET



*Gartner ne recommande aucun fournisseur, produit ou service mentionnés dans ses rapports d'études. Les opinions exprimées par Gartner dans ses publications ne doivent pas être interprétées comme des faits établis. Gartner décline toute responsabilité, expresse ou tacite, relative à cette étude, notamment toute garantie de valeur commerciale ou d'adéquation à un usage particulier.

QUELQUES-UNS DE NOS CLIENTS

HONDA

Protégé par ESET depuis 2011

Licence prolongée 3 fois, étendue 2 fois

GREENPEACE

Protégé par ESET depuis 2008

Licence prolongée/étendue 10 fois

Canon

Protégé par ESET depuis 2016

Plus de 14 000 endpoints

T . .

Partenaire de sécurité FAI depuis 2008

2 millions d'utilisateurs

NOS RÉCOMPENSES LES PLUS PRESTIGIEUSES

SE Labs AAA ENTERPRISE ENDPOINT OCT-DEC 2016

THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE WINNER 2017

AV comparatives Approved Business Product 2017

SC MEDIA RECOMMENDED

" Avec ses excellentes fonctionnalités anti-malware, sa simplicité de gestion et sa présence internationale, ESET fait partie des meilleurs candidats du marché pour les appels d'offres de solutions de sécurité. "

KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018

ENJOY SAFER TECHNOLOGY™

30 ANNÉES D'INNOVATION POUR PROTÉGER VOTRE VIE NUMÉRIQUE

Consultez notre catalogue complet des solutions et services sur :

WWW.ESET.COM/NA/BUSINESS

Besoin de renseignements ? Contactez-nous :

+33 (0)1.72.59.42.01

info.afrique@eset-nod32.fr