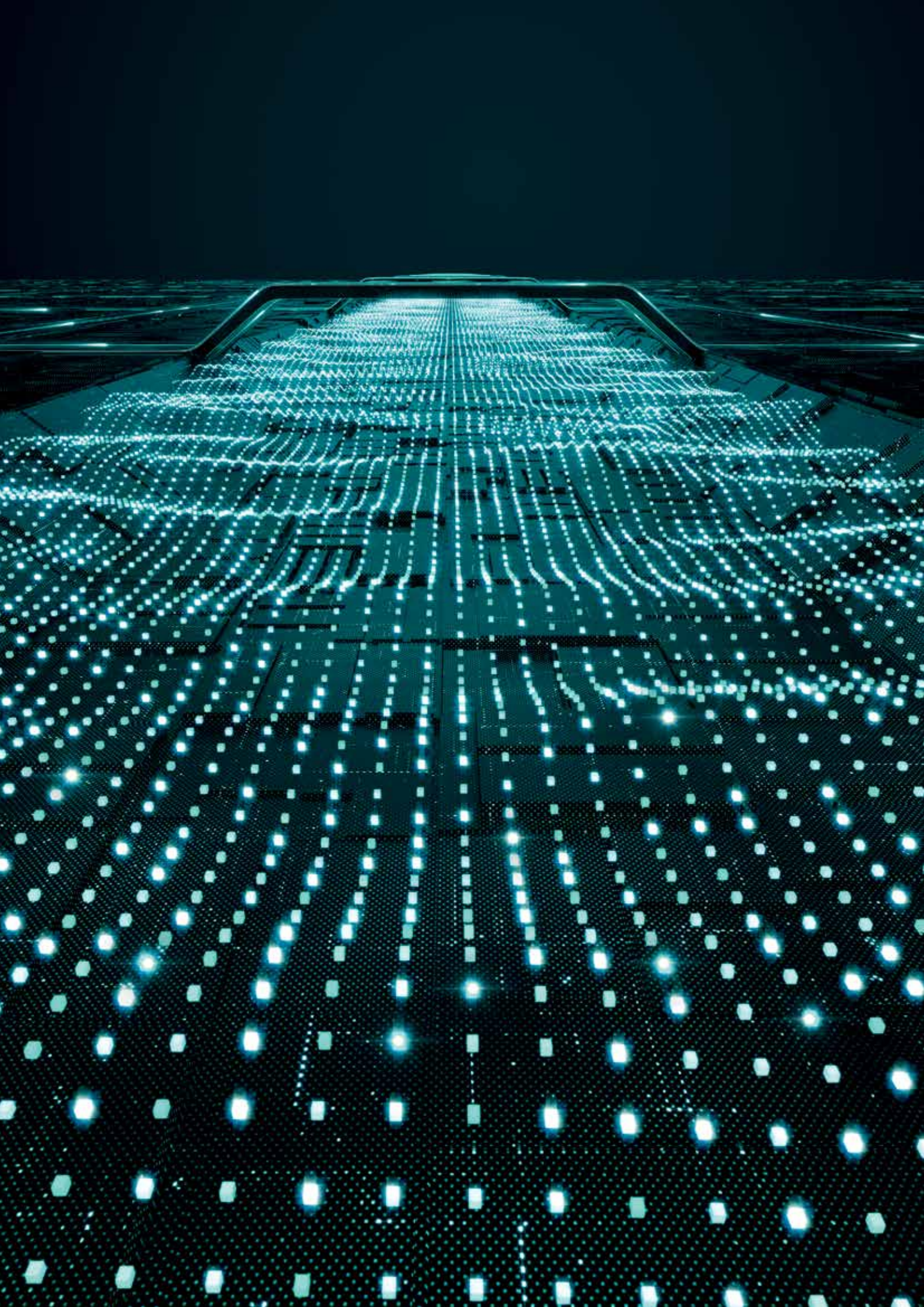
FICHE PRODUIT

ENTERPRISE INSPECTOR

Assurez une visibilité exceptionnelle et
une intervention synchronisée avec notre solution EDR

**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 déterminer qu'une violation de données s'est produite, mais également la limiter et l'éliminer. Tout cela doit être fait avec la plus grande efficacité et sans aucune interruption des activités. La plupart des entreprises ne sont pas prêtes à effectuer ce type d'enquête complète et font plutôt appel à un prestataire extérieur pour les aider. Aujourd'hui, les entreprises ont besoin de plus de visibilité sur leurs ordinateurs pour veiller à ce que les nouvelles menaces, les comportements à risque des collaborateurs et les applications indésirables ne mettent pas en danger les profits et la réputation.

Les principaux secteurs d'activité concernés par les violations de données sont traditionnellement ceux qui détiennent des données précieuses, tels que les secteurs de la finance, du commerce de détail, de la santé, et le secteur public. Cela ne signifie pas pour autant que les autres secteurs sont à l'abri, mais simplement que les pirates pèsent généralement le pour et le contre.

MENACES PERSISTANTES AVANCÉES (APT) ET ATTAQUES CIBLÉES

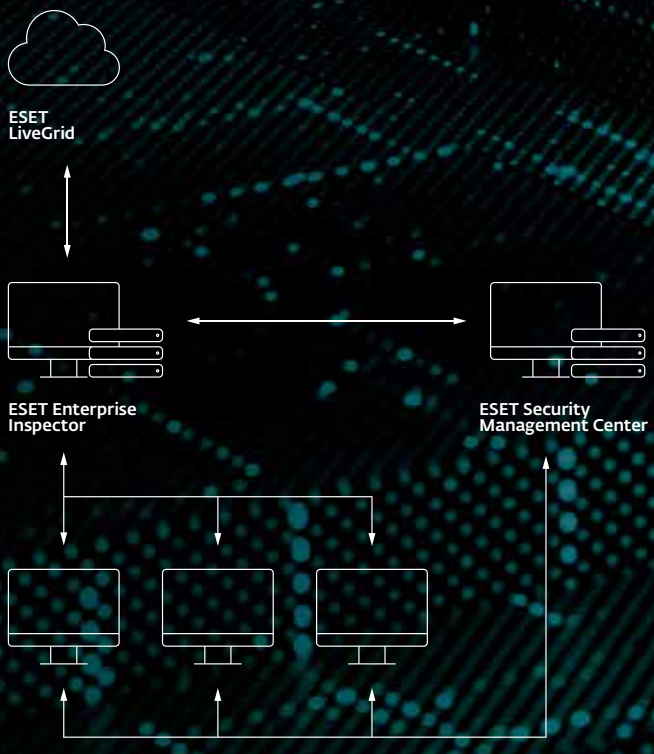
Les systèmes EDR sont couramment utilisés pour identifier les APT et les attaques ciblées via Threat Hunting, réduire le délai d'intervention sur les incidents, et stopper les attaques futures de manière proactive. La découverte des APT en particulier est importante pour les entreprises car la plupart d'entre elles ne se sentent pas prêtes à affronter les nouvelles attaques qui peuvent passer inaperçues sur le réseau pendant des jours, voire des mois.

Fournit une détection unique s'appuyant sur la réputation et les comportements, qui est totalement transparente pour les équipes de sécurité et qui leur fournit un feedback en temps réel alimenté par plus de 100 millions de terminaux dans notre LiveGrid..

MEILLEURE VISIBILITÉ

Les menaces internes et les attaques d'hameçonnage sont des problèmes majeurs pour les entreprises. Les attaques d'hameçonnage sont couramment utilisées contre les entreprises en raison du grand nombre de collaborateurs à cibler. Il y a de fortes chances qu'un seul collaborateur morde à l'hameçon et finisse par compromettre l'ensemble de l'entreprise. Les attaques internes constituent une autre menace pour les entreprises, là encore parce que le grand nombre de collaborateurs augmente les chances que l'un d'entre eux nuise aux intérêts de l'entreprise.

Les systèmes EDR offrent une meilleure visibilité aux entreprises pour découvrir, comprendre, bloquer et corriger tout problème sur l'ensemble de leurs appareils. ESET Enterprise Inspector peut par exemple identifier et bloquer rapidement les scripts malveillants qui se font passer pour des documents inoffensifs, tels que des fichiers Word.



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

INTERVENTION SYNCHRONISÉE

Conçu à partir de l'offre existante de sécurité des terminaux d'ESET, il crée un écosystème cohérent qui permet le recoupement de tous les objets pertinents et une intervention synchronisée sur les incidents. Les équipes de sécurité peuvent stopper des processus, télécharger le fichier qui a déclenché une détection, ou simplement lancer le redémarrage d'un ordinateur, l'éteindre, l'analyser ou isoler l'appareil du réseau directement depuis la console.

ARCHITECTURE OUVERTE

Fournit un comportement unique et une détection s'appuyant sur la réputation, qui est totalement transparente pour les équipes de sécurité. Toutes les règles sont rédigées dans un format XML courant et peuvent être facilement personnalisées et créées pour répondre aux besoins d'environnements d'entreprise spécifiques, y compris les intégrations avec des solutions de SIEM.

ACCÈS À DISTANCE

ESET Enterprise Inspector est doté de fonctionnalités PowerShell qui permettent aux ingénieurs en sécurité d'inspecter et de configurer les ordinateurs de leur entreprise à distance, afin qu'une intervention sophistiquée puisse être réalisée sans interrompre le flux de travail de l'utilisateur.

MULTIPLATFORME

ESET Enterprise Inspector fonctionne sur Windows et MacOS, ce qui en fait le choix idéal pour les environnements multiplateformes.

API PUBLIQUE

ESET Enterprise Inspector comprend une API qui permet d'accéder aux détections et de les exporter, et d'accéder à leurs interventions pour permettre une intégration efficace avec des outils de SIEM, de SOAR, de tickets et bien d'autres.

SENSIBILITÉ RÉGLABLE

Supprimez facilement les détections en ajustant la sensibilité des règles pour différents groupes d'ordinateurs ou d'utilisateurs. Combinez des critères tels que le nom du fichier, le chemin d'accès, le hachage, la ligne de commande et le signataire, pour affiner les conditions de déclenchement.

MITRE ATT&CKTM

Les détections d'ESET Enterprise Inspector s'appuient sur le cadre MITRE ATT&CK™ (Adversarial Tactics, Techniques, and Common Knowledge), qui fournit des informations complètes en un clic, même sur les menaces les plus complexes.

SYSTÈME DE RÉPUTATION

Le filtrage étendu d'ESET permet aux ingénieurs en sécurité d'ignorer toutes les applications connues à l'aide du système de réputation robuste d'ESET. Notre système de réputation intègre une base de données de centaines de millions de fichiers bénins afin de garantir que les équipes de sécurité puissent se consacrer à des fichiers inconnus, et potentiellement malveillants, et non sur des faux positifs.

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.

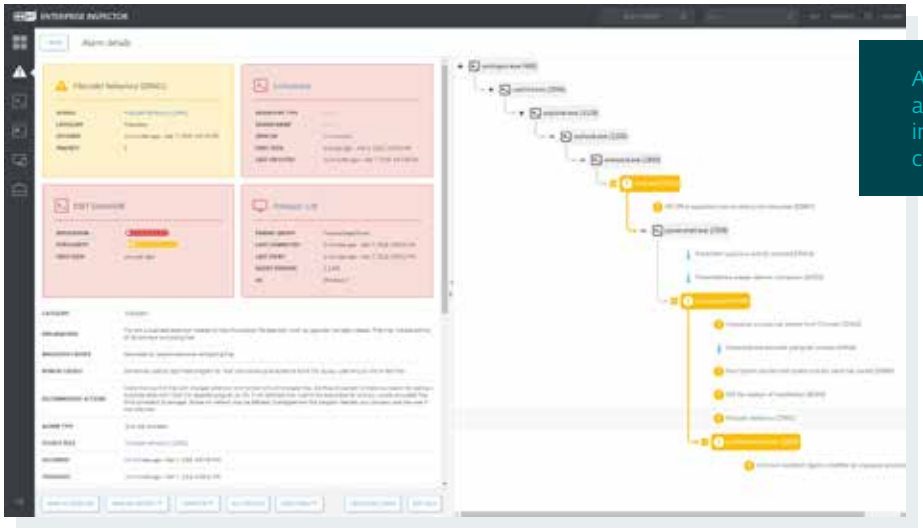
ESET Enterprise Inspector permet à votre équipe de sécurité de détecter ces comportements, d'identifier les éléments affectés, de déterminer l'emplacement et le moment où l'exécutable, le script ou l'action ont été lancés, et enfin d'analyser la cause profonde de l'incident en quelques clics seulement.

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

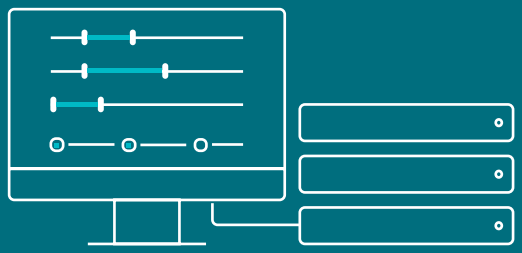
Certaines entreprises se méfient des logiciels que leurs utilisateurs exécutent dans leur système. Vous devez non seulement tenir compte des applications classiques, mais également surveiller les solutions portables qui ne nécessitent pas forcément d'installation pour fonctionner. Mais comment faire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

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.

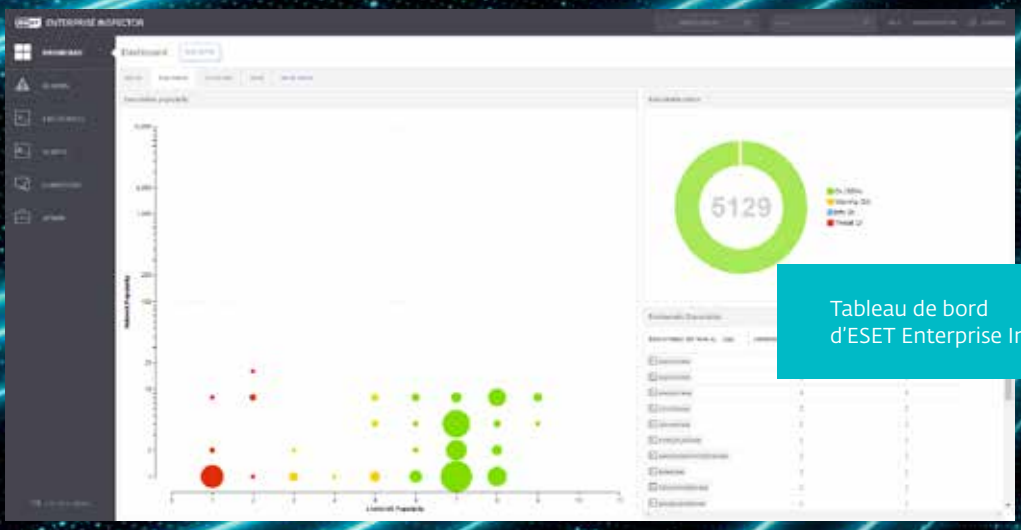


Tableau de bord
d'ESET Enterprise Inspector

Possibilités

RECHERCHE DES MENACES

Appliquez des filtres de données pour les trier en fonction de la popularité des fichiers, de leur réputation, leur signature numérique, leur comportement ou des informations contextuelles. L'utilisation de plusieurs filtres permet de trouver facilement des menaces de manière automatisée, notamment les menaces persistantes avancées et les attaques ciblées, et peut être personnalisée en fonction de l'environnement de chaque entreprise. En ajustant les règles de comportement, ESET Enterprise Inspector peut également être personnalisé pour rechercher des menaces antérieures et relancer l'analyse de l'ensemble de la base de données des événements.

DÉTECTION DES INCIDENTS (ANALYSE DES CAUSES PROFONDES)

Visualisez rapidement et facilement tous les incidents de sécurité dans la section des détections. En quelques clics, les équipes de sécurité peuvent consulter une analyse complète des causes profondes, notamment ce qui a été affecté, où et quand l'action ou le script exécutable a été lancé.

ENQUÊTE ET INTERVENTION

Utilisez un ensemble de règles intégrées et créez vos propres règles pour intervenir sur les incidents détectés. Chaque détection déclenchée comprend des conseils pour l'intervention. La fonctionnalité d'intervention rapide permet de bloquer des fichiers spécifiques par hachage, de stopper des processus et les mettre en quarantaine, et d'isoler ou d'éteindre certaines machines à distance. La réactivité de cette fonctionnalité veille à ce qu'aucun incident isolé ne passe entre les mailles du filet.

ISOLEMENT EN UN CLIC

Définissez des politiques d'accès au réseau pour stopper rapidement les mouvements latéraux des malwares. Isolez un appareil compromis du réseau en un seul clic via l'interface d'EEI. Vous pouvez également facilement retirer des appareils de la quarantaine.

NOTATION

Hiérarchisez la gravité des alarmes grâce à une fonctionnalité de notation qui attribue une valeur de gravité aux incidents, et permet à l'administrateur d'identifier facilement les ordinateurs présentant une probabilité plus élevée d'incident potentiel.

BALISAGE

Attribuez et retirez des balises pour un filtrage rapide des objets EEI tels que les ordinateurs, les alarmes, les exclusions, les tâches, les exécutables, les processus et les scripts. Les balises sont partagées entre les utilisateurs, et peuvent être attribuées en quelques secondes une fois qu'elles sont créées.

COLLECTE DE DONNÉES

Consultez des données complètes sur un processus nouvellement exécuté, y compris le temps d'exécution, l'utilisateur qui l'a lancé, la durée de temporisation et les appareils concernés.

CONNEXION SÉCURISÉE

Activez l'authentification à deux facteurs : une couche de sécurité supplémentaire pour votre compte administrateur qui empêche un adversaire de s'y connecter, même s'il possède votre mot de passe.

DÉTECTION DES INDICATEURS DE COMPROMIS

Consultez et bloquez des modules en fonction de plus de 30 indicateurs différents, y compris le hachage, les modifications de la base de registre, les modifications de fichiers et les connexions réseau.

DÉTECTION DES ANOMALIES ET DES COMPORTEMENTS

Vérifiez les actions qui ont été effectuées par un exécutable et utilisez le système de réputation LiveGrid® d'ESET pour déterminer rapidement si les processus exécutés sont fiables ou suspects. La surveillance des incidents anormaux liés aux utilisateurs est possible grâce à des règles conçues pour être déclenchées par un comportement, et non par de simples détections de malwares ou des signatures. Le regroupement des ordinateurs par utilisateurs ou par services permet aux équipes de sécurité de déterminer si un utilisateur est autorisé à effectuer une action spécifique ou non.

DÉTECTION DES VIOLATIONS DE LA POLITIQUE DE SÉCURITÉ

Bloquez l'exécution de modules malveillants dans votre réseau. Détectez les violations des politiques de sécurité concernant l'utilisation de logiciels spécifiques tels que les applications de téléchargement de torrents, de stockage dans le Cloud, de navigation via Tor ou d'autres logiciels indésirables.

À propos d'ESET

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

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

QUELQUES-UNS DE NOS CLIENTS

MITSUBISHI MOTORS
Drive your Ambition

Protégé par ESET depuis 2017
Plus de 14 000 endpoints

Canon

Protégé par ESET depuis 2016
Plus de 9 000 endpoints

Allianz Suisse

Protégé par ESET depuis 2016
Plus de 4 000 boites mails

Partenaire de sécurité FAI depuis 2008
2 millions d'utilisateurs

ESET est conforme à ISO/IEC 27001:2013, une norme de sécurité internationalement reconnue et applicable dans la mise en œuvre et la gestion de la sécurité de l'information. La certification est accordée par l'organisme de certification tiers accrédité SGS. Elle démontre la conformité totale d'ESET aux meilleures pratiques du secteur.

ESET est un contributeur dévoué du cadre MITRE ATT&CK. En faisant partie des fournisseurs les plus référencés et des contributeurs les plus actifs, ESET confirme son engagement à fournir la meilleure protection à la communauté et à nos clients.

NOS RÉCOMPENSES LES PLUS PRESTIGIEUSES

RECONNAISSANCE PAR LES SPÉCIALISTES

ESET est le seul Challenger du Magic Quadrant 2019 de Gartner, « Endpoint Protection Platforms », pour la deuxième année consécutive.

ESET est classé comme Strong Performer dans Forrester Wave (TM), « Endpoint Security Suites », Q3 2019.

ESET est classé comme Top Player dans le rapport Radicati « Endpoint Security » de 2019 en raison des fonctionnalités offertes et de sa vision stratégique.

Gartner Inc, Magic Quadrant « Endpoint Protection Platforms », Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, 20 août 2019. 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. Gartner Peer Insights est une plateforme gratuite d'évaluation et de notation par des pairs conçue pour les décideurs en matière de logiciels et de services d'entreprise. Les évaluations sont soumises à un strict processus de validation et de modération pour garantir l'authenticité des informations. Les évaluations de Gartner Peer Insights sont des opinions subjectives d'utilisateurs finaux individuels qui s'appuient sur leurs propres expériences, et ne représentent pas les opinions de Gartner ou de ses affiliés.

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