PRÉSENTATION

PROTECT

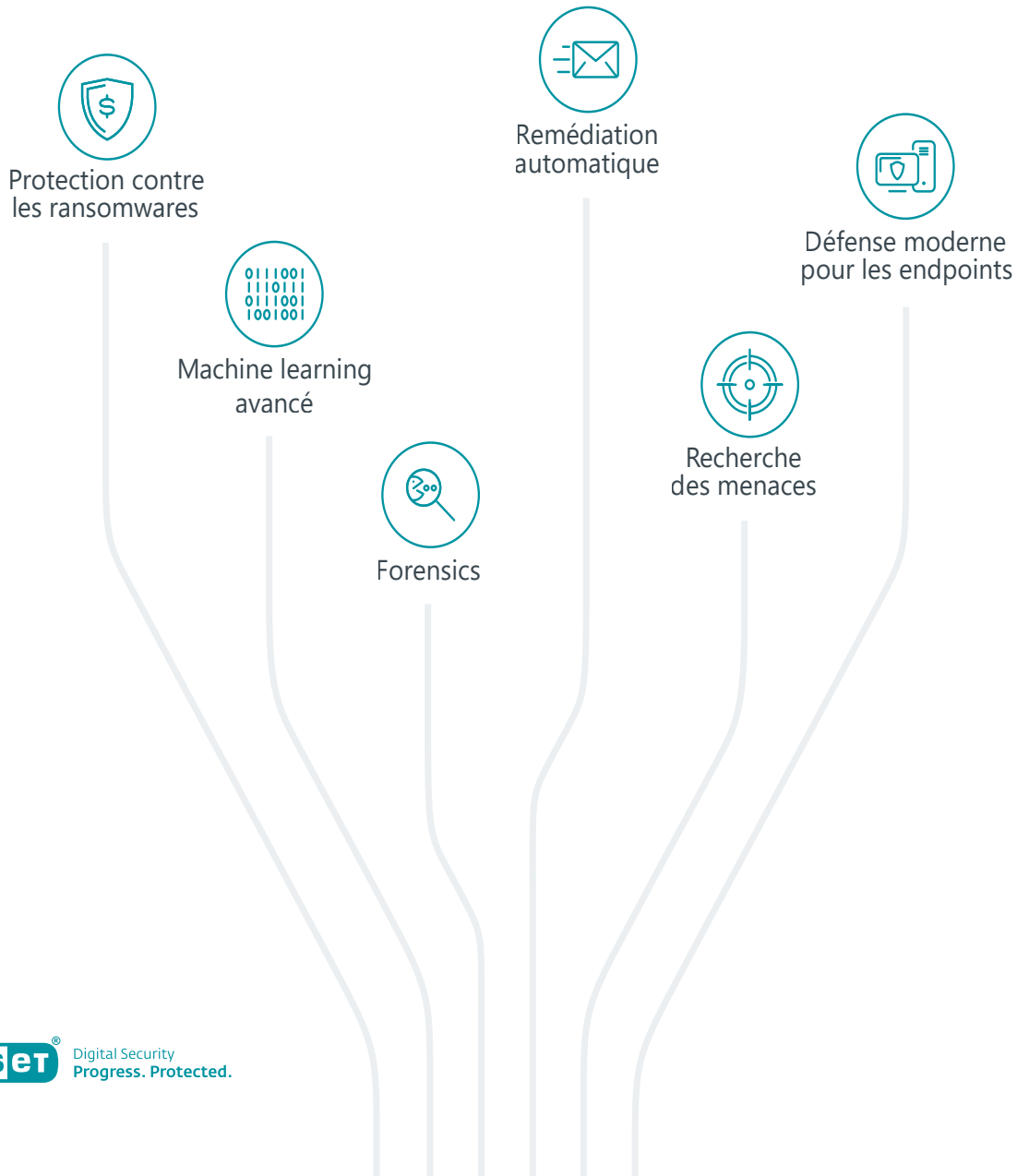
L'interface de notre plateforme d'administration unifiée de la sécurité qui fournit une visibilité approfondie sur votre système d'information

Progress. Protected.

Qu'est-ce qu'une **console d'administration de la sécurité des endpoints ?**

ESET PROTECT est une console d'administration polyvalente et unifiée des endpoints qui fournit un accès à la puissante plateforme ESET PROTECT. Elle peut être déployée sur site ou dans le Cloud, pour assurer une visibilité en temps réel sur les endpoints sur site et dans le Cloud, générer des rapports complets et assurer l'administration de la sécurité pour tous les systèmes d'exploitation.

Il s'agit d'une console unique qui prend en charge toutes les solutions de sécurité ESET déployées dans le réseau. Elle contrôle les couches de prévention, de détection et de réponse sur les endpoints de toutes les plateformes, qu'il s'agisse de postes de travail, de serveurs, de machines virtuelles ou d'appareils mobiles managés.



eset Digital Security
Progress. Protected.

Les avantages ESET

DE LA PRÉVENTION À L'INTERVENTION

ESET PROTECT combine l'administration de plusieurs solutions de sécurité ESET grâce à une console unique. Elle se charge de la prévention et de la détection des menaces, ainsi que des réponses, pour apporter le meilleur niveau de protection à l'ensemble de votre entreprise.

REMÉDIATION EN UN SEUL CLIC

À partir du tableau de bord principal, un administrateur peut rapidement évaluer la situation et répondre aux problèmes. Des actions telles que la création d'une exclusion, l'envoi de fichiers pour une analyse plus approfondie dans le Cloud ou une analyse des disques, peuvent être déclenchées d'un seul clic. Les exclusions peuvent être configurées par nom, URL ou hachage des menaces, ou une combinaison de ces éléments.

RBAC AVANCÉ

En plus de l'accès protégé par MFA, la console est équipée d'un système avancé de contrôle des accès en fonction des rôles (RBAC). Affectez les administrateurs et les utilisateurs de la console à des segments spécifiques du réseau ou à des groupes d'objets, et spécifiez des ensembles de permissions avec un degré élevé de granularité.

ACCESSIBLE POUR LES MSP

Si vous êtes un prestataire de services managés (MSP) chargé du parc informatique de vos clients, vous apprécierez les fonctionnalités multi-tenant complètes d'ESET PROTECT. Les licences MSP sont automatiquement détectées et synchronisées avec le serveur de licences, et la console vous permet d'effectuer des actions avancées telles que l'installation/le retrait de toute application tierce, l'exécution de scripts et de commandes à distance, l'énumération des configurations matérielles et des processus en cours d'exécution, etc.

ÉPROUVÉ ET FIABLE

ESET est présent dans le secteur de la sécurité depuis plus de 30 ans, et nous continuons de faire évoluer notre technologie pour conserver une longueur d'avance sur les menaces les plus récentes. Cela nous a valu la confiance de plus de 110 millions d'utilisateurs dans le monde entier. Notre technologie est constamment inspectée et validée par des organismes de tests impartiaux qui montrent l'efficacité de notre approche pour stopper les toutes dernières menaces.

RAPPORTS DYNAMIQUES PERSONNALISÉS

ESET PROTECT fournit plus de 170 rapports intégrés et vous permet de créer des rapports personnalisés à partir de plus de 1 000 points de données. Les entreprises peuvent ainsi créer des rapports dont l'aspect et le contenu correspondent exactement à ce qu'elles souhaitent. Une fois créés, les rapports peuvent être générés et envoyés par email à intervalles réguliers.

FRAMEWORK D'AUTOMATISATION

Les groupes dynamiques peuvent classer les ordinateurs en fonction de leur état actuel ou de critères d'inclusion définis. Des tâches peuvent ensuite être configurées pour déclencher des actions telles que des analyses, des changements de politique, ou des installations/désinstallations de logiciels en fonction des changements dynamiques d'appartenance à un groupe.

PRISE EN CHARGE DE VDI ENTIÈREMENT AUTOMATISÉE

Un algorithme complet de détection du matériel est utilisé pour déterminer l'identité de la machine en fonction de ses éléments. Cela permet le clonage et la réinstallation automatisés d'environnements matériels non persistants. La prise en charge de VDI par ESET ne nécessite aucune interaction manuelle et est entièrement automatisée.

SYSTÈME DE NOTIFICATION ENTIÈREMENT PERSONNALISABLE

Le système de notification comporte un éditeur WYSIWYG complet, dans lequel vous pouvez configurer entièrement les notifications pour être précisément alerté sur les informations que vous souhaitez.

Fonctionnalités

CONSOLE UNIQUE

Tous les produits ESET pour endpoints peuvent être administrés à partir d'une seule console ESET PROTECT, notamment sur les postes de travail, les mobiles, les serveurs et les machines virtuelles, ainsi que les systèmes d'exploitation suivants : Windows, macOS, Linux et Android.

PRISE EN CHARGE DE L'XDR

Pour améliorer davantage la connaissance de la situation et fournir une visibilité sur l'ensemble de votre réseau, ESET PROTECT fonctionne en collaboration avec ESET Inspect, le composant XDR de la plateforme ESET PROTECT. ESET Inspect est multi-plateforme (Windows, macOS et Linux), avec des fonctionnalités d'analyse des menaces et des mesures correctives avancées, et une intégration de manière transparente à votre centre des opérations de sécurité (SOC).

MDM CLOUD

Le MDM Cloud est inclus et ne nécessite pas d'outils spécialisés pour fonctionner. Microsoft Intune, Apple Business Manager et VMware Workspace ONE sont pris en charge.

CHIFFREMENT COMPLET DES DISQUES

Cette fonctionnalité native d'ESET PROTECT prend en charge le chiffrement des données sur les endpoints Windows et Mac (FileVault) pour améliorer la sécurité des données et la conformité des entreprises aux réglementations sur les données.

DÉFENSE CONTRE LES MENACES AVANCÉES

La défense contre les menaces avancées améliore considérablement la détection des menaces zero-day telles que les ransomwares, en analysant rapidement les fichiers suspects dans la sandbox d'ESET dans le Cloud. Elle effectue une batterie d'analyses complètes pour rechercher les malwares, avec la possibilité de révéler les menaces les plus discrètes dans le Cloud. Vous pouvez en faire plus via une seule interface qui regroupe dynamiquement les ordinateurs selon leur marque, modèle, système d'exploitation, processeur, mémoire, espace disque et bien d'autres éléments.

INVENTAIRE MATÉRIEL ET LOGICIEL

ESET PROTECT collecte non seulement des informations sur toutes les applications logicielles installées dans l'entreprise, mais également sur le matériel déployé. Cela permet d'optimiser complètement les responsabilités au sein des équipes des grandes entreprises.

ENTIÈREMENT MULTI-TENANT

Plusieurs utilisateurs et groupes de permission peuvent être créés pour permettre l'accès à certains groupes de la console ESET PROTECT uniquement, afin d'optimiser complètement les responsabilités au sein des équipes des grandes entreprises.

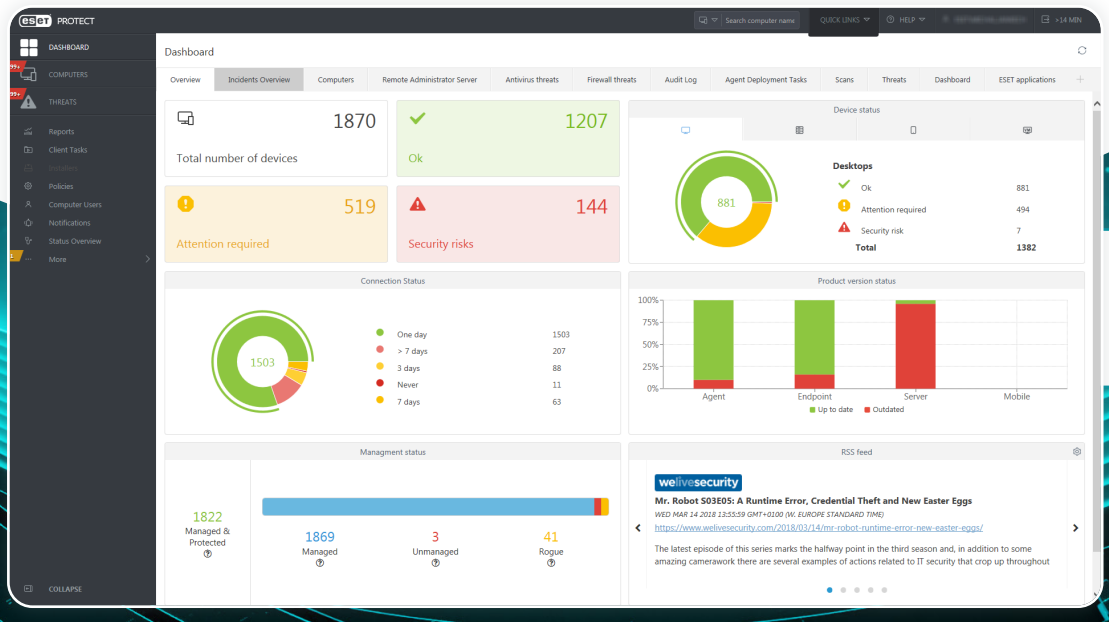


Tableau de bord ESET PROTECT

eset Digital Security
Progress. Protected.

CONTRÔLE GRANULAIRE DE LA POLITIQUE DE SÉCURITÉ

Les entreprises peuvent mettre en place plusieurs politiques pour le même ordinateur ou le même groupe, et peuvent imbriquer des politiques pour des autorisations en cascade. Les entreprises peuvent également configurer les paramètres des politiques comme étant modifiables ou non par l'utilisateur, afin de verrouiller certains des paramètres et empêcher les utilisateurs finaux de les modifier.

INTÉGRATIONS COMPLÈTES

L'intégration avec des outils tels que SIEM et SOAR est possible grâce à nos API complètes et faciles à utiliser, documentées via Swagger. ESET PROTECT prend également en charge les formats JSON et LEEF pour toutes les informations de journalisation.

ESET VULNERABILITY & PATCH MANAGEMENT

Traque activement les vulnérabilités des systèmes d'exploitation et des applications courantes, et permet l'application automatisée de correctifs sur tous les endpoints gérés par ESET PROTECT.

Cas d'utilisation

Déploiements de VDI

PROBLÈME

Les environnements matériels non persistants nécessitent généralement une interaction manuelle de la part du service informatique, et entraînent des difficultés quant à la visibilité et au reporting.

SOLUTION

- ✓ Après le déploiement d'une image maîtresse sur les ordinateurs déjà présents dans ESET PROTECT, les ordinateurs continueront d'être associés à l'instance précédente malgré une réinstallation complète du système.
- ✓ Les machines qui reviennent à leur état initial après leur utilisation ne provoqueront pas de doublons et seront associées à un seul enregistrement.
- ✓ Lors du déploiement d'images non persistantes, vous pouvez créer une image qui inclut l'agent. Ainsi, chaque fois qu'une nouvelle machine est créée avec une autre empreinte matérielle, elle crée automatiquement de nouveaux enregistrements dans ESET PROTECT.

Remédiation des logiciels

PROBLÈME

Les entreprises doivent savoir quand un logiciel non approuvé a été installé, et y remédier.

SOLUTION

- ✓ Créez un groupe dynamique dans ESET PROTECT pour rechercher un logiciel spécifique non approuvé.
- ✓ Créez une notification pour alerter le service informatique lorsqu'un ordinateur répond à ce critère.
- ✓ Configurez une tâche de désinstallation de logiciel dans la console ESET PROTECT pour qu'elle s'exécute automatiquement lorsqu'un ordinateur répond aux critères du groupe dynamique.
- ✓ Mettez en place une notification qui s'affiche automatiquement sur l'écran de l'utilisateur, indiquant qu'il a commis une infraction en installant le logiciel en question.

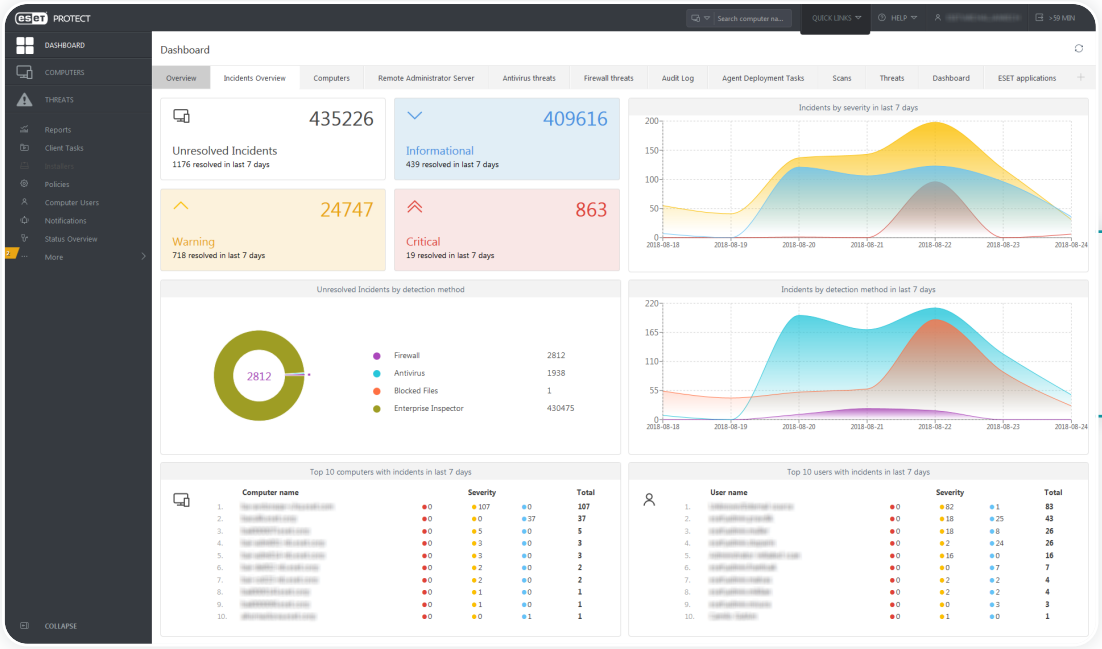


Tableau de bord ESET PROTECT — Aperçu des incidents

Ransomwares

PROBLÈME

Un utilisateur ouvre un email malveillant contenant une nouvelle forme de ransomware.

SOLUTION

- ✓ Le service informatique reçoit une notification de la part de son SIEM via email qu'une nouvelle menace a été détectée sur un certain ordinateur.
- ✓ Une analyse est lancée d'un simple clic sur l'ordinateur infecté.
- ✓ Un autre clic envoie le fichier à notre sandbox Cloud ESET LiveGuard Advanced.
- ✓ Après confirmation que la menace a été contenue, les avertissements de la console ESET PROTECT sont automatiquement désactivés.

Développeurs

PROBLÈME

Les programmeurs qui travaillent avec du code sur leurs ordinateurs ont tendance à générer de faux positifs durant le processus de compilation.

SOLUTION

- ✓ Le département informatique reçoit une notification de la part de son SIEM via email qu'une nouvelle menace a été détectée.
- ✓ La notification montre que la menace provient de l'ordinateur d'un développeur.
- ✓ En un clic, le fichier est envoyé à ESET LiveGuard Advanced pour confirmer qu'il n'est pas malveillant.
- ✓ Le service informatique configure une exclusion pour empêcher de futurs faux positifs sur ce dossier, d'un simple clic.

Inventaire matériel et logiciel

PROBLÈME

Les entreprises doivent savoir quels logiciels sont installés sur chaque ordinateur, ainsi que l'âge de chaque ordinateur.

SOLUTION

- ✓ La fiche de l'ordinateur comporte chaque logiciel installé, y compris son numéro de version.
- ✓ Consultez les détails du matériel de chaque ordinateur, tels que l'appareil, le fabricant, le modèle, le numéro de série, le processeur, la mémoire, l'espace disque dur et bien plus encore.
- ✓ Produisez des rapports pour obtenir une visibilité plus globale sur l'entreprise et prendre des décisions budgétaires quant aux actualisations du matériel dans les années à venir, en se basant sur les marques et les modèles actuels.

COMMENT ACHETER :

Il suffit d'acheter l'une des solutions pour entreprises directement sur notre site web dédié.

COMMENCEZ VOTRE ÉVALUATION GRATUITE DE 30 JOURS DÈS MAINTENANT

Testez toutes les fonctionnalités de la solution, y compris la protection des endpoints.

À propos d'ESET

Cybersécurité de nouvelle génération pour les entreprises

NOUS NE NOUS CONTENTONS PAS DE STOPPER LES MENACES, NOUS LES ANTICIPONS

Contrairement aux solutions conventionnelles qui se concentrent sur la réaction aux menaces une fois qu'elles se sont déclenchées, ESET offre une approche inégalée axée sur la prévention via l'IA et soutenue par l'expertise humaine, la renommée mondiale de sa Threat Intelligence, et un vaste réseau de R&D dirigé par des chercheurs reconnus dans le secteur, tout cela au service de l'innovation continue de notre technologie de sécurité multicouche.

Bénéficiez d'une protection sans pareil contre les ransomwares, l'hameçonnage, les menaces zero-day et les attaques ciblées grâce à notre plateforme de cybersécurité XDR primée, qui combine des fonctionnalités nouvelle génération pour la prévention, la détection et la recherche proactive de menaces. Nos solutions hautement personnalisables incluent un support hyperlocal. Elles ont un impact minimal sur les performances des endpoints, et sont en mesure d'identifier et de neutraliser les menaces émergentes avant qu'elles ne se déclenchent, garantissent la continuité des activités et réduisent les coûts de mise en œuvre et d'administration.

Dans un monde où la technologie permet le progrès, protégez votre entreprise avec ESET.

ESET EN QUELQUES CHIFFRES

+ 1 Md
internautes protégés

+ 400 k
entreprises clientes

200
pays et territoires

13
centres de recherche

QUELQUES-UNS DE NOS CLIENTS

MITSUBISHI MOTORS
Drive your Ambition

Protégés par ESET depuis 2017 : 9 000 endpoints

Allianz Suisse

Protégé par ESET depuis 2016 : +4 000 boîtes mail

Canon
Canon Marketing Japan Group

Protégés par ESET depuis 2016 : 32 000 endpoints

Partenaire de sécurité FAI depuis 2008 : 2 millions d'utilisateurs

RECONNAISSANCES

AV comparatives APPROVED Business Security JUL 2023

ESET a reçu le prix Business Security APPROVED de AV - Comparatives dans le cadre du test de sécurité des entreprises de juillet 2023.

G2 Leader SUMMER 2023

ESET obtient régulièrement les meilleures notes sur la plateforme mondiale d'évaluation des utilisateurs G2, et ses solutions sont appréciées par les clients du monde entier.

The Radicati Group, Inc.
A Technology Market Research Firm

ESET a été reconnu parmi les « Top Player » pour la quatrième année consécutive dans le rapport Market Quadrant Advanced Persistent Threat de Radicati en 2023.