PRÉSENTATION DE SOLUTION

# PROTECT

**Console sur site ou dans le Cloud**
Visibilité et administration de la sécurité
sur tous les systèmes d'exploitation

Digital Security
**Progress. Protected.**

# Qu'est-ce qu'une **console d'administration ?**

**ESET PROTECT est une console d'administration qui assure une visibilité en temps réel sur les terminaux, permet de gérer la sécurité de tous les systèmes d'exploitation et propose des reportings complets.**

Pilotez toutes vos solutions ESET déployées sur le réseau depuis une interface unique. Celle-ci contrôle les différentes couches de protection - la prévention, la détection et la réponse - sur toutes les plateformes, y compris les postes de travail, les serveurs, les machines virtuelles et les appareils mobiles.

# Pourquoi utiliser **une console ?**

## VISIBILITÉ

Les menaces zero-day, les menaces persistantes avancées, les attaques ciblées et les botnets sont autant de préoccupations pour les entreprises du monde entier. Il est extrêmement important de disposer d'une visibilité en temps réel sur ces menaces pour permettre au personnel informatique de répondre rapidement et d'atténuer tout risque. Comme les entreprises continuent de recourir fortement au télétravail, la visibilité n'est pas seulement nécessaire sur site, mais également hors site.

ESET PROTECT fournit des informations actualisées sur tous les terminaux, qu'ils soient connectés au réseau privé ou à Internet, et offre une visibilité complète sur tous les systèmes d'exploitation sans exception. La console permet de suivre les terminaux au niveau des inventaires matériels et logiciels.

## ADMINISTRATION

Le monde de la cybersécurité évolue au rythme soutenu des nouvelles méthodes d'attaques et de menaces inédites. En cas d'attaque ou de violation de données, les organisations sont généralement surprises par la compromission de leur système de protection ou ignorent qu'un incident a eu lieu. Lorsqu'elles s'en aperçoivent, elles exécutent généralement des tâches spécifiques telles que des analyses sur tous les appareils et changent leurs configurations pour mieux se protéger d'une future attaque.

ESET PROTECT vient avec des politiques prédéfinies intelligentes et puissantes. La console permet cependant aux administrateurs, à tout moment, de modifier ces dernières ou encore d'affiner les configurations des logiciels de sécurité installés sur les terminaux. En outre, les tâches peuvent être automatisées pour éviter une exécution manuelle sur chaque ordinateur.

## REPORTING

La plupart des organisations sont aujourd'hui tenues de respecter les réglementations sur la protection des données en plus de répondre à des spécificités internes en matière de reporting. Toute entreprise doit régulièrement générer des rapports à fournir à différentes parties ou à conserver en vue d'un usage futur.

ESET PROTECT permet de configurer des intervalles de création des rapports, de les sauvegarder dans des dossiers spécifiques ou de les envoyer automatiquement par e-mail. Il existe des dizaines de modèles de rapports personnalisables en fonction des besoins, un gain de temps essentiel pour les administrateurs.

La visibilité en temps réel sur les incidents de sécurité est fondamentale pour les administrateurs afin de réagir rapidement et atténuer tout risque.

Quelle que soit l'entreprise, des rapports doivent être régulièrement générés, distribués ou conservés pour un usage futur.

*« Le principal avantage avec ESET est que la sécurité de tous les utilisateurs peut être gérée et supervisée depuis une seule console. »*

— Jos Savelkoul, Team Leader ICT-Department,
Hôpital Zuyderland, Pays-Bas, + 10 000 postes

# Les avantages ESET

## DE LA PRÉVENTION À LA RÉPONSE

ESET centralise la gestion des produits Endpoint avec sa solution EDR (Endpoint Detection and Response), ESET Enterprise Inspector, et avec sa Sandbox Cloud sophistiquée, ESET Dynamic Threat Defense sous une seule et même console d'administration simple d'utilisation.

## RÉPONSE AUX INCIDENTS EN UN SIMPLE CLIC

Depuis l'onglet des menaces, les administrateurs peuvent créer une exclusion, envoyer des fichiers pour une analyse approfondie ou lancer un scan en un clic. Les exclusions peuvent être configurées par nom de menace, URL, hachage 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.

## SYSTÈME DE NOTIFICATIONS PERSONNALISABLES

Le système de notifications comporte un éditeur, qui vous permet de configurer les notifications de façon à recevoir les informations que vous souhaitez.

## REPORTINGS DYNAMIQUES ET PERSONNALISÉS

ESET PROTECT propose plus de 170 rapports prédéfinis et personnalisables avec plus de 1 000 types de données. Adaptez les rapports à vos besoins. Une fois créés, ils peuvent être paramétrés pour être générés et envoyés par e-mail à intervalles définis.

## AUTOMATISATION DES TÂCHES

Les ordinateurs peuvent être classés dans des groupes dynamiques en fonction de leur état ou des critères d'inclusion définis. Vous pouvez ainsi configurer le déclenchement de tâches telles que des analyses, des modifications à apporter aux politiques ou des installations/désinstallations de logiciels sur la base des changements d'appartenance aux groupes dynamiques.

## PRISE EN CHARGE DES VDI AUTOMATISÉE

Un algorithme de détection matérielle avancé est utilisé pour identifier la machine en fonction de son matériel, ce qui permet la réinitialisation et le clonage automatiques des environnements matériels non persistants. Par conséquent, la prise en charge des VDI est entièrement automatisée et ne nécessite aucune intervention manuelle.

## UNE TECHNOLOGIE ÉPROUVÉE ET FIABLE

Avec plus de 30 ans d'expérience dans le secteur de la sécurité informatique, ESET s'efforce d'innover en permanence afin de garder une longueur d'avance sur les menaces émergentes. Plus de 110 millions d'utilisateurs nous font confiance partout dans le monde. Nos solutions sont systématiquement évaluées et validées par des testeurs tiers, qui vérifient l'efficacité de notre approche contre les menaces les plus récentes.

## ADAPTÉ POUR LES MSP

Si vous êtes infogérant (MSP) chargé des réseaux 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.

*« Une entreprise exceptionnelle, un support technique remarquable, une protection efficace contre les menaces et une administration centralisée. »*

— Dave, Manager of IT,
District scolaire unifié de Deer Valley, USA, + 15 500 postes

# Pourquoi choisir **une console dans le Cloud ?**

## ÉCONOMIES SUR LE COÛT TOTAL DE POSSESSION

À première vue, passer d'une console hébergée sur site à une console dans le Cloud peut sembler coûteux. Détrompez-vous ! Vous n'aurez plus besoin de serveur, d'effectuer des mises à jour, d'installer des correctifs ou encore de régulièrement redémarrer le serveur, sans parler des licences et des sauvegardes. La console dans le Cloud s'avère être, très rapidement, moins coûteuse.

## SOYEZ OPÉRATIONNEL EN QUELQUES MINUTES

Avec une console Cloud, la protection est activée plus rapidement. Ne gaspillez plus de ressources à attendre l'installation de composants, ou encore à planifier l'installation d'un serveur. Il vous suffit d'ouvrir un compte ESET et d'ajouter tous les terminaux à protéger.

## UTILISEZ LES VERSIONS LES PLUS RÉCENTES

Nous mettons la console à jour en arrière-plan. Vous utiliserez toujours la version la plus récente avec les tous derniers composants. Ainsi, votre entreprise profitera des dernières évolutions, et les administrateurs d'une expérience utilisateur améliorée et des plus innovantes.

## CONNECTEZ-VOUS N'IMPORTE OÙ, N'IMPORTE QUAND

Vous avez seulement besoin de votre navigateur préféré. Si la plupart des consoles déployées sur site sont aussi accessibles de cette manière, dans le Cloud, il n'est plus nécessaire d'ajouter des exclusions sur le pare-feu ou de configurer des VPN compliqués. Vous pouvez également compter sur une disponibilité optimisée grâce à une infrastructure robuste.

## RÉSOLVEZ LES PROBLÈMES RAPIDEMENT

Avec une console Cloud, les experts ESET pourront vous assister ou vous dépanner de manière plus efficace, sans perdre de temps à rechercher la version que vous utilisez, car vous serez toujours sur la dernière.

# Cas d'usage

## Ransomwares

Un utilisateur ouvre un e-mail malveillant contenant une nouvelle forme de ransomware.

### SOLUTION

- ✓ Le service IT reçoit une notification de son SIEM, via e-mail, indiquant qu'une nouvelle menace a été détectée sur un ordinateur.
- ✓ Une analyse est lancée d'un simple clic sur l'ordinateur infecté.
- ✓ Un autre clic envoie le fichier à la sanbox Cloud ESET Dynamic Threat Defense.
- ✓ Une fois la menace neutralisée, les alertes affichées dans la console ESET PROTECT sont automatiquement sont supprimées.

## Développeurs

Les programmeurs qui codent sur leurs ordinateurs génèrent parfois des faux positifs dus processus de compilation.

### SOLUTION

- ✓ Le service IT est notifié par e-mail et via son système SIEM qu'une nouvelle menace a été détectée.
- ✓ La notification indique que la menace provient de l'ordinateur d'un développeur.
- ✓ En un clic, le fichier est envoyé à la sandbox Cloud ESET Dynamic Threat Defense pour vérifier qu'il n'est pas malveillant.
- ✓ Le service IT, d'un simple clic, configure une exclusion pour empêcher de futurs faux positifs sur ce dossier.

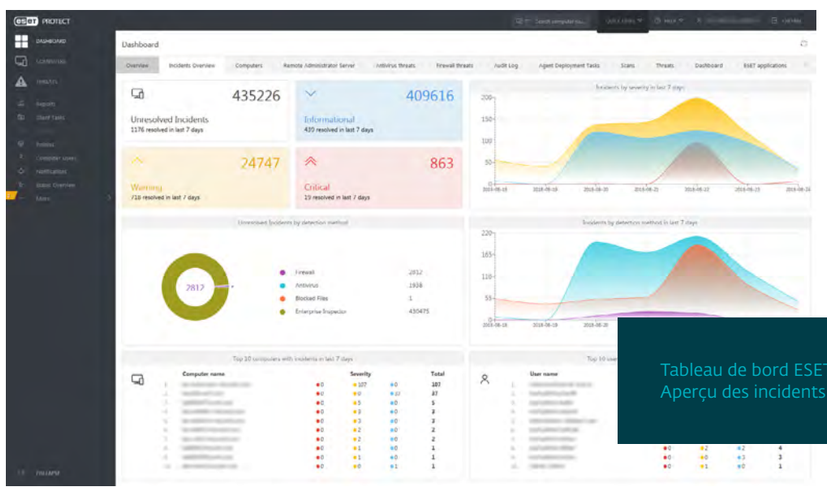


Tableau de bord ESET PROTECT — Aperçu des incidents

## Déploiements VDI

Typiquement, les environnements matériels non-persistants nécessitent une intervention manuelle du service informatique, et entraînent des difficultés quant à la visibilité et au reporting.

### SOLUTION

- ✓ Après le déploiement d'un master sur des ordinateurs virtuels non-persistants déjà présents dans ESET PROTECT, ces derniers continuent d'envoyer leur nouvel état à l'ancienne instance et ce malgré la nouvelle copie intégrale du système.
- ✓ Les machines qui reviennent à leur état initial à la fin d'une session ne créeront pas de versions dupliquées et seront fusionnées en un seul enregistrement.
- ✓ Lors du déploiement d'images non-persistantes, vous pouvez créer une image qui inclut l'agent. Ainsi, à chaque fois qu'une nouvelle machine est ajoutée avec une autre empreinte matérielle, elle crée automatiquement de nouveaux enregistrements dans ESET PROTECT.

## Inventaire matériel et logiciel

Les entreprises doivent être au fait des logiciels installés sur chaque ordinateur, ainsi que l'âge de chacun de ces derniers.

### SOLUTION

- ✓ Visualisez tous les logiciels installés, ainsi que le numéro de la version, dans les informations de l'ordinateur.
- ✓ Consultez les informations matérielles sur chaque ordinateur, telles que le nom, le fabricant, le modèle, le numéro de série, le processeur, la mémoire vive, l'espace disque, etc.
- ✓ Générez des rapports pour obtenir vue d'ensemble sur l'entreprise et par conséquent planifier les décisions budgétaires sur l'actualisation du parc informatique en s'appuyant sur les marques et les modèles actuels.

## Gestion des logiciels non autorisés

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

### SOLUTION

- ✓ Créez un groupe dynamique dans ESET PROTECT pour spécifiquement retrouver un logiciel non autorisé.
- ✓ 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 pour qu'elle s'exécute automatiquement lorsqu'un ordinateur répond aux critères du groupe dynamique.
- ✓ Paramétrez 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.

ESET PROTECT peut être installé sur Windows et Linux, ou déployé sous forme d'Appliance Virtuelle.

L'architecture multi-tenant et les connexions sécurisées par authentification forte permettent de rationaliser les responsabilités dans les grandes entreprises.

*« L'administration centralisée de la sécurité sur tous les endpoints, serveurs et appareils mobiles est un avantage clé. »*

— IT Manager, Diamantis Masoutis S.A., Grèce,
+ 6 000 postes

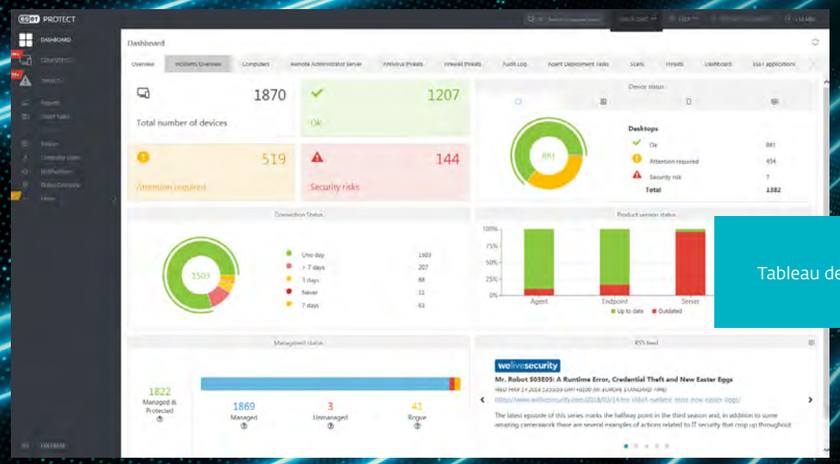


Tableau de bord ESET PROTECT

# Fonctionnalités techniques

## CONSOLE UNIQUE

Toutes les solutions de protection des endpoints ESET peuvent être administrées à partir de la seule console ESET PROTECT. Ceci comprend les postes de travail, les appareils mobiles, les serveurs, les machines virtuelles, ainsi que les systèmes d'exploitation suivants : Windows, macOS, Linux et Android.

## CHIFFREMENT COMPLET DU DISQUE (FDE)

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 de la sécurité des données.

## SANDBOX CLOUD

Celle-ci améliore considérablement la détection des menaces zero-day telles que les ransomwares, en analysant rapidement les fichiers suspects dans la puissante Sandbox Cloud d'ESET.

## INVENTAIRE MATÉRIEL & LOGICIEL

ESET PROTECT collecte non seulement des informations sur tous les logiciels installés dans l'entreprise, mais également sur le matériel physique.

## ENTIÈREMENT MULTI-TENANT

Définissez différents types ou groupes d'utilisateurs, avec des accès limités à ESET PROTECT pour rationaliser plus facilement les responsabilités dans les grandes structures.

Ceci vous permet d'en faire plus depuis une seule et même interface en créant des groupes dynamiques d'ordinateurs selon leur marque, modèle, système d'exploitation, processeur, mémoire, espace disque, etc.

## CONTRÔLE GRANULAIRE DES POLITIQUES

Configurez des politiques pour chaque ordinateur ou groupe, et définissez-en les permissions. Vous pouvez également créer des politiques paramétrées en fonction des utilisateurs ou des groupes, et ainsi choisir de fermer un certain nombre d'accès.

## PRISE EN CHARGE DES SIEM ET DES SOC

ESET PROTECT prend entièrement en charge les outils de SIEM et exporte des journaux d'événements aux formats JSON et LEEF, pour une intégration avec les SOC (Security Operations Centers).

## VOUS SOUHAITEZ HÉBERGER LA CONSOLE EN LOCAL ?

Pour certaines entreprises, l'hébergement de logiciels en local est une nécessité pour diverses raisons, internes ou juridiques. Outre la console dans le Cloud, ESET PROTECT peut être déployée, avec toutes ses fonctionnalités, sur site pour satisfaire ces besoins spécifiques.

## INSTALLATION FLEXIBLE

ESET PROTECT peut être installé sur Windows et Linux, ou sous forme d'Appliance virtuelle. Après l'installation, l'administration se fait via une console web, pour faciliter l'accès depuis n'importe quel appareil ou système d'exploitation.

## PRISE EN CHARGE DE L'EDR*

Pour accroître accroître la conscience situationnelle et obtenir une visibilité sur le réseau, ESET PROTECT prend en charge notre solution d'EDR, ESET Enterprise Inspector. EEI est multi-plateforme (Windows et macOS), avec des fonctionnalités d'analyse des menaces, des mesures correctives avancées et une intégration à votre SOC.

**La prise en charge de la solution EDR n'est disponible que pour les déploiements ESET PROTECT sur site*

# Prochaines étapes

**Comment profiter d'ESET PROTECT ?**
Il suffit d'acheter l'une des solutions pour entreprises directement sur *notre site web dédié*.

**Obtenir une version d'essai 30 jours :**
Testez gratuitement toutes les fonctionnalités de la console et de nos solutions de sécurité pour endpoints.

JE TESTE MAINTENANT

**Je souhaite migrer depuis la console sur site :**
Vous utilisez actuellement la console ESET sur site ? Contactez un partenaire ESET dans votre région.
*https://www.eset.com/fr/business/partner/*

# À propos d'ESET

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatiques à la pointe de la technologie. Ces solutions protègent et accompagnent les entreprises et les particuliers du monde entier contre des menaces en constante évolution.

En tant que société entièrement détenue par des fonds privés, nous sommes libres d'œuvrer dans l'intérêt de nos clients pour fournir les meilleures technologies.

## ESET EN QUELQUES CHIFFRES

**+110 millions**
d'utilisateurs partout dans le monde

**+ 400 000**
Entreprises Clients

**+ 200**
pays et territoires

**13**
centres R&D

## QUELQUES-UNS DE NOS CLIENTS

MITSUBISHI MOTORS
Drive your Ambition

Protégé par ESET depuis 2017
+14 000 endpoints

Canon
Canon Marketing Japan Group

Protégé par ESET depuis 2016
+9 000 endpoints

Allianz Suisse

Protégé par ESET depuis 2016
+4 000 boîtes mails

T

Partenaire de sécurité FAI depuis 2008
2 millions d'utilisateurs

# Pourquoi choisir ESET ?

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

## NOS RÉCOMPENSES

AV comparatives Approved Business Product 2017

SE Labs AAA ENTERPRISE ENDPOINT PROTECTION JAN-MAR 2020

AV-TEST av-test.org 2019 AWARD Best Usability ESET Endpoint Security

G2 Leader SUMMER 2020

canalys CYBERSECURITY CHAMPION 2020

## LES AVIS DES ANALYSTES

FORRESTER®

ESET nommé « Strong Performer » dans le rapport Forrester Wave(TM) « Endpoint Security Suites » Q3 2019.

The Radicati Group, Inc.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET est classé Top Player dans le rapport Radicati 2019, catégorie « Endpoint Security » sur la base des fonctionnalités de ses solutions et de sa vision stratégique.

Digital Security
Progress. Protected.