FICHE PRODUIT

ENDPOINT ENCRYPTION

POWERED BY DESLOCK

Solution de chiffrement simple et puissante
pour les entreprises de toutes tailles

ENJOY SAFER TECHNOLOGY™

30 ANNÉES D'INNOVATION POUR PROTÉGER VOTRE VIE NUMÉRIQUE

Qu'est-ce qu'une **solution de chiffrement des terminaux ?**

Outils essentiels pour la sécurité des données, les solutions de chiffrement des terminaux permettent de chiffrer les fichiers et les disques au niveau des endpoints de l'entreprise. Les données sont ainsi protégées de toute lecture ou utilisation abusive par des personnes non autorisées.

ESET Endpoint Encryption est une solution de chiffrement conviviale destinée aux entreprises de toutes tailles, qui permet de chiffrer des disques complets (FDE, full disk encryption), des fichiers/dossiers, des e-mails et des clés USB.

Pourquoi utiliser une solution **de chiffrement des terminaux**

VIOLATIONS DE DONNÉES

Le monde de la cybersécurité actuel est frappé par un nombre croissant de violations de données chaque jour. Lorsque ces incidents surviennent, les données non chiffrées risquent d'être rendues publiques ou utilisées à des fins malveillantes. Si certaines entreprises sous-estiment une telle divulgation, toute organisation possède en réalité des informations sensibles, telles que les listes de clients, la propriété intellectuelle et les données commerciales.

La mise en œuvre d'une solution de chiffrement empêche les pirates informatiques de consulter les données dérobées. 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. Cependant, les autres industries ne sont pas à l'abri pour autant, les hackers mettent simplement en balance les efforts nécessaires et les récompenses potentielles.

TÉLÉTRAVAIL

Les employés en télétravail ou itinérants sont devenus la norme dans la plupart des entreprises. Les employés travaillent désormais depuis des cafés ou des aéroports durant leurs déplacements. Or, plus vos effectifs en télétravail sont importants, plus le risque de perte ou de vol d'appareils augmente. Les entreprises doivent également se préoccuper du personnel itinérant qui quitte définitivement l'entreprise.

Avec une solution de chiffrement des endpoints, il est beaucoup plus difficile pour les personnes qui volent ou trouvent vos appareils d'accéder à vos données. De plus, la plupart de ces produits vous permettent de désactiver les terminaux à distance en cas de vol/perte ou lors du départ d'un collaborateur.

CONFORMITÉ

En matière de conformité, les entreprises doivent identifier la réglementation qui leur est applicable, afin de déterminer les recommandations à suivre et les exigences à satisfaire. De nombreux règlements et lois – tels que le RGPD, la norme PCI-DSS, ainsi que les lois américaines HIPAA, SOX et GLBA – exigent le chiffrement des données.

Le chiffrement des terminaux est désormais indispensable pour la plupart des établissements qui gèrent des cartes de paiement ou des dossiers médicaux. Toutes les entreprises doivent se renseigner sur les éventuelles exigences de conformité qu'elles doivent respecter.

Plus vos effectifs en télétravail sont importants, plus le risque de perte ou de vol d'appareils augmente.

Le chiffrement des terminaux est désormais indispensable pour la plupart des établissements qui gèrent des cartes de paiement ou des dossiers médicaux.

Les avantages ESET

GESTION DES APPAREILS EN TOUT LIEU

Avec ESET Endpoint Encryption, les appareils peuvent être gérés partout dans le monde, sans nécessiter de VPN ni d'exceptions du pare-feu, par simple connexion HTTPS via un serveur proxy. Cela permet d'éviter les connexions entrantes à risque, ce qui sécurise et simplifie la gestion du chiffrement pour les entreprises de toutes tailles. Toutes les connexions client et serveur sont chiffrées en SSL ; les commandes et les données en RSA et AES.

AUCUN IMPACT SUR LA PRODUCTIVITÉ

La mise en œuvre du chiffrement est entièrement transparente pour les utilisateurs et ne nécessite aucune action de leur part, tout en améliorant leur mise en conformité. Aucune surcharge n'est engendrée ni pour le service informatique ni pour les usagers, et aucune formation utilisateur n'est nécessaire.

SYSTÈME UNIQUE DE CLÉS DE CHIFFREMENT

L'utilisation de clés de chiffrement partagées et centralisées permet d'éviter les problèmes liés aux solutions reposant sur des mots de passe collectifs ou des clés publiques. Le système employé par ESET Endpoint Encryption présente une analogie avec les clés physiques utilisées pour verrouiller les portes de nos domiciles, véhicules, etc. Le personnel est déjà familier avec ce concept, donc une simple explication suffit. Associées à un système performant de gestion à distance, les clés de chiffrement partagées sont hautement sécurisées et pratiques.

SÉCURISATION DES SUPPORTS AMOVIBLES

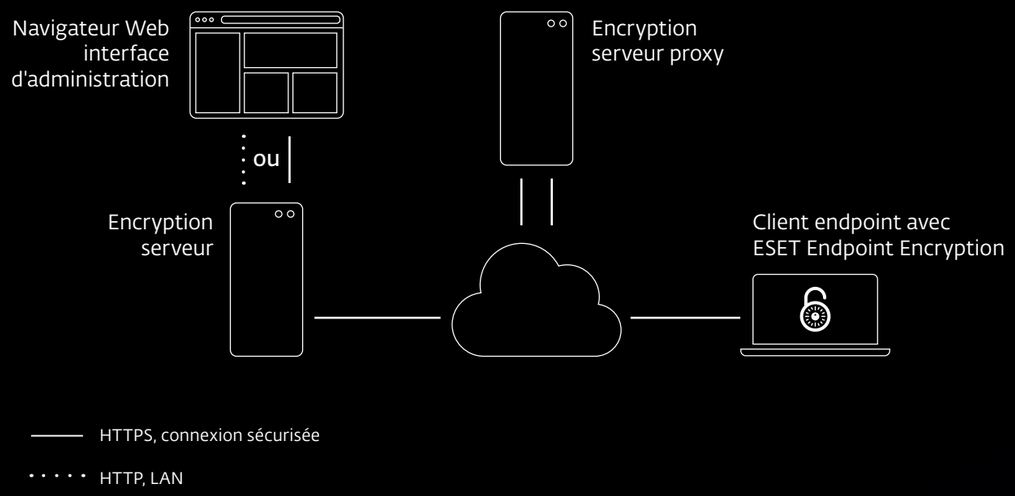
Il n'est pas toujours évident de gérer des médias amovibles dans un environnement sécurisé. ESET Endpoint Encryption crée automatiquement des partitions sur les supports amovibles, l'une réservée à l'environnement sécurisé et l'autre accessible partout ailleurs. Ce fonctionnement est extrêmement simple pour les utilisateurs finaux. Sans action particulière de la part des employés, les fichiers personnels et professionnels sont confinés dans leurs environnements respectifs.

DÉSACTIVATION DES APPAREILS À DISTANCE

De plus en plus d'entreprises se tournent vers une main-d'œuvre mobile où les employés travaillent non seulement dans les aéroports ou à la maison, mais aussi dans les cafés. Pour cette raison, les entreprises ont besoin de tranquillité d'esprit et la possibilité de désactiver ou de verrouiller à distance les appareils en cas de perte ou de vol.

ESET Endpoint Encryption fournit un moyen simple de le faire et, une fois de plus, n'exige aucun VPN ou d'exception du pare-feu.

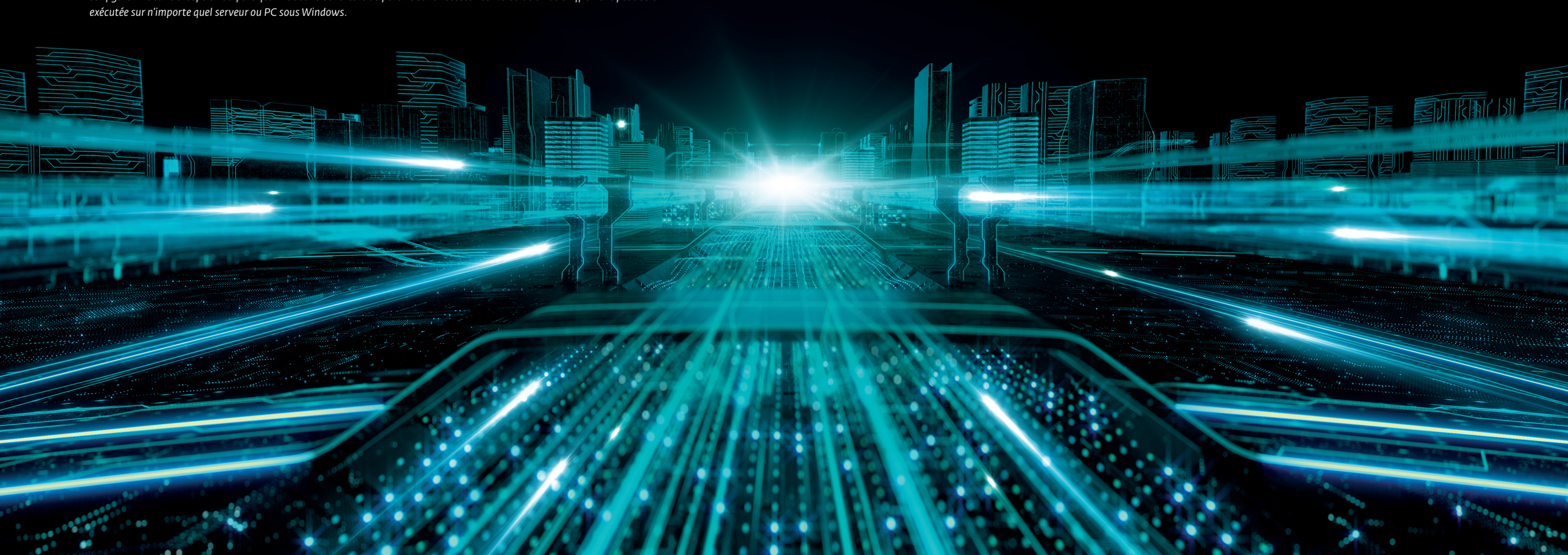
Le système de clés de chiffrement partagées ESET Endpoint Encryption présente une analogie avec les clés physiques utilisées pour verrouiller les portes de nos domiciles, véhicules, etc. Le personnel est déjà familier avec ce concept, donc une simple explication suffit.



La gestion des terminaux via un serveur proxy, qui ne requiert aucune connexion entrante, est extrêmement sécurisée et facile à configurer. Aucune exception du pare-feu ni aucune ouverture de port ne sont nécessaires. La solution de chiffrement peut être exécutée sur n'importe quel serveur ou PC sous Windows.

L'installation de la solution ESET Endpoint Encryption prend généralement moins de 10 minutes.

La configuration complète de la solution dure normalement moins d'une heure, ce qui accélère considérablement son adoption à l'échelle de l'entreprise.



Cas d'utilisation

Prévention des violations de données

CAS D'UTILISATION

Des violations de données clients sont régulièrement relayées par les médias.

SOLUTION

- ✓ Protégez vos données sensibles grâce à la fonctionnalité de chiffrement complet de disques (FDE, full disk encryption) ESET Endpoint Encryption.
- ✓ Sécurisez les communications vulnérables telles que le Bureau à distance à l'aide d'une authentification multifacteur.
- ✓ Exiger une authentification multifacteur lors de la connexion aux périphériques contenant des données sensibles.

SOLUTIONS ESET RECOMMANDÉES

- ✓ **ESET Endpoint Encryption**
- ✓ **ESET Secure Authentication**

Gestion des employés en télétravail

CAS D'UTILISATION

Les entreprises doivent pouvoir protéger leurs données sensibles en cas de départ d'un employé ou de vol/perte d'un appareil.

SOLUTION

- ✓ Limitez l'accès aux ressources de l'entreprise grâce à une authentification multifacteur.
- ✓ Utilisez la fonctionnalité de verrouillage à distance pour protéger les appareils perdus ou volés.
- ✓ Supprimez la possibilité aux utilisateurs qui quittent l'entreprise de s'authentifier sur les terminaux chiffrés.

SOLUTIONS ESET RECOMMANDÉES

- ✓ **ESET Endpoint Encryption**
- ✓ **ESET Secure Authentication**

" En tant que prestataire de services et travaillant sur des accords de niveau de service, il est rassurant de pouvoir recommander, acquérir, installer et maintenir une solution de chiffrement qui aide à assurer la continuité dans les établissements d'enseignement du Staffordshire, réduisant ainsi les coûts globaux. "

Andy Arnold, CS Team Leader pour les solutions système, Staffordshire Learning Technologies (SLT), Royaume-Uni

Prévention des fuites de données

CAS D'UTILISATION

Toutes les entreprises utilisent des supports amovibles pour transférer des fichiers d'un ordinateur à un autre, mais la plupart d'entre elles n'ont aucun moyen de s'assurer que les données restent au sein de l'organisation.

SOLUTION

- ✓ Chiffrez les supports amovibles pour empêcher les transferts de données en dehors de l'entreprise.
- ✓ Limitez l'accès aux médias amovibles à certains utilisateurs.

SOLUTIONS ESET RECOMMANDÉES

- ✓ **ESET Endpoint Encryption**

" La version pilote a été installée dans un environnement en temps réel et nous avons trouvé la solution extrêmement conviviale, avec son interface en ligne. Très performant, le serveur permet même de contrôler les appareils via Internet, quelle que soit la structure du réseau ou des répertoires. "

Simon Goulding, analyste services réseau, Aster, Royaume-Uni

Fonctionnalités ESET Endpoint Encryption

TYPES DE CHIFFREMENT PRIS EN CHARGE

ESET Endpoint Encryption permet de chiffrer des disques complets (FDE), des fichiers/dossiers, des e-mails et des clés USB.

SOLUTION ENTIÈREMENT VALIDÉE

ESET Endpoint Encryption est certifié FIPS 140-2 pour le chiffrement AES 256 bits.

ALGORITHMES ET NORMES

AES 256 bits, AES 128 bits, SHA 256 bits, SHA1 160 bits, RSA 1024 bits, Triple DES 112 bits, Blowfish 128 bits.

SYSTÈMES D'EXPLOITATION PRIS EN CHARGE

Microsoft® Windows® 10, 8, 8.1 y compris UEFI et GPT, 7, Vista, XP SP 3 ; Microsoft Windows Server 2003-2012 ; Apple iOS.

AUCUN MATÉRIEL SPÉCIFIQUE REQUIS

Les puces TPM sont facultatives pour le chiffrement complet de disques.

AUCUN SERVEUR REQUIS

ESET Endpoint Encryption ne nécessite aucun serveur et permet de chiffrer des appareils distants en toute simplicité.

CHIFFREMENT D'E-MAILS ET DE PIÈCES JOINTES

Envoyez et recevez facilement des e-mails et des pièces jointes chiffrés via Outlook.

CHIFFREMENT DE TEXTE ET DU PRESSE-PAPIERS

Chiffrez tout ou partie d'une fenêtre de texte (navigateurs Internet, champs mémo de bases de données ou webmail).

GESTION CENTRALISÉE

Disposez d'un contrôle total sur les licences, les fonctionnalités logicielles, les stratégies de sécurité et les clés de chiffrement.

ARCHIVES CHIFFRÉES ET DISQUES VIRTUELS

Créez un volume chiffré sécurisé sur votre PC ou dans un autre emplacement, ou une copie chiffrée d'une arborescence complète et de ses fichiers.

Toutes les entreprises possèdent des données sensibles telles que des listes de clients, des informations personnelles et des données commerciales.

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

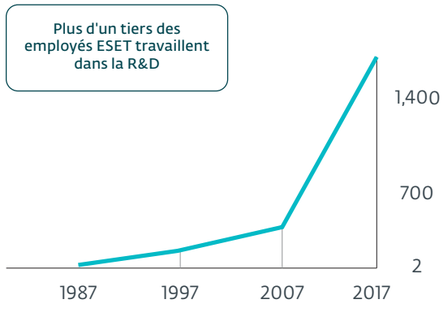
+110 millions
d'utilisateurs partout dans le monde

+ 400 000
Clients Entreprises

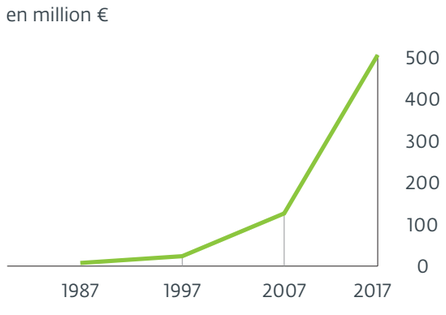
+ 200
pays et territoires couverts

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™