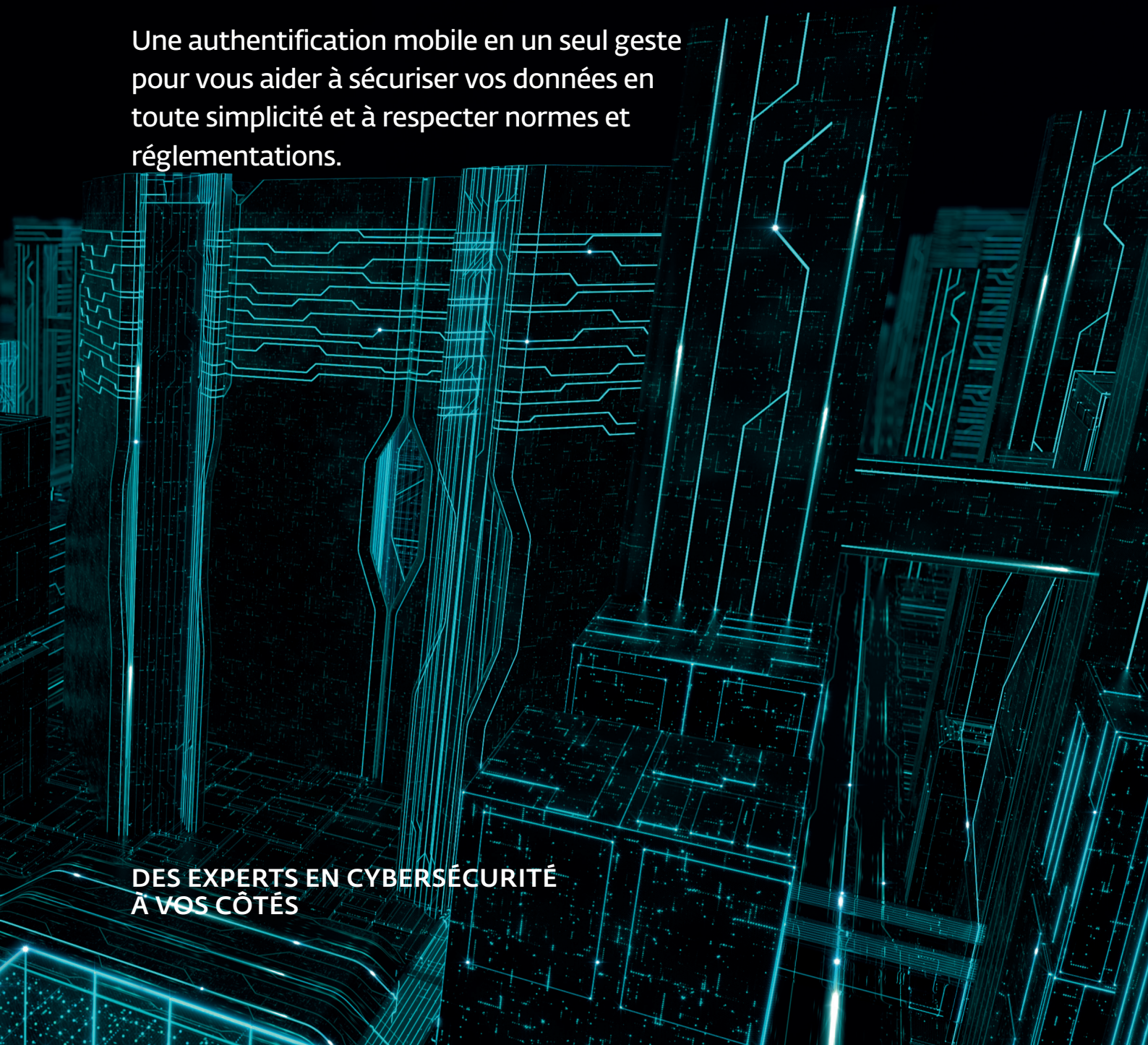
FICHE PRODUIT

SECURE AUTHENTICATION

Une authentification mobile en un seul geste pour vous aider à sécuriser vos données en toute simplicité et à respecter normes et réglementations.



DES EXPERTS EN CYBERSÉCURITÉ
À VOS CÔTÉS

Qu'est-ce que l'**authentification multi-facteurs ?**

L'authentification multi-facteurs (MFA), également nommée authentification à deux facteurs (2FA), est une méthode d'authentification qui, pour vérifier l'identité d'un utilisateur, se base sur deux informations distinctes. La 2FA est beaucoup plus puissante qu'une authentification traditionnelle avec mot de passe ou code PIN statique. En complétant l'authentification traditionnelle grâce à un deuxième facteur dynamique, la 2FA réduit efficacement les risques de violations de données dues à des mots de passe trop faibles ou divulgués.

Grâce à ESET Secure Authentication, les entreprises de toute taille peuvent facilement intégrer la MFA à tous les systèmes couramment utilisés, tels que les VPN, Remote Desktop, Office 365, Outlook Web Access, la connexion à un système d'exploitation, et plus encore.

Pourquoi une **authentification multi-facteurs ?**

Non seulement les employés utilisent le même mot de passe pour différents sites Internet et différentes applications, mais ils les communiquent parfois ouvertement à leurs amis, leur famille et leurs collègues.

UNE MAUVAISE HYGIÈNE DES MOTS DE PASSE

C'est bien connu, « les employés sont le maillon faible de la sécurité de votre entreprise ». En effet, ils la mettent en péril de nombreuses manières. L'un des principaux risques réside dans la mauvaise hygiène des mots de passe. Non seulement les employés utilisent le même mot de passe pour différents sites Internet et différentes applications, mais ils les communiquent parfois ouvertement à leurs amis, leur famille et leurs collègues. Et, comme si cela ne suffisait pas, lorsque les entreprises mettent en œuvre des politiques de mots de passe, leurs employés réagissent bien souvent en utilisant des variantes de leur mot de passe précédent ou en écrivant leurs mots de passe sur des post-its.

Une solution d'authentification multi-facteurs permet de protéger l'entreprise contre la mauvaise hygiène des mots de passe en générant, en plus du mot de passe habituel, un mot de passe supplémentaire – par exemple, en le délivrant sur le téléphone de l'employé. Grâce à cette solution, les pirates informatiques ne peuvent plus avoir accès à vos systèmes simplement en devinant un mot de passe trop faible.

VIOLATIONS DE DONNÉES

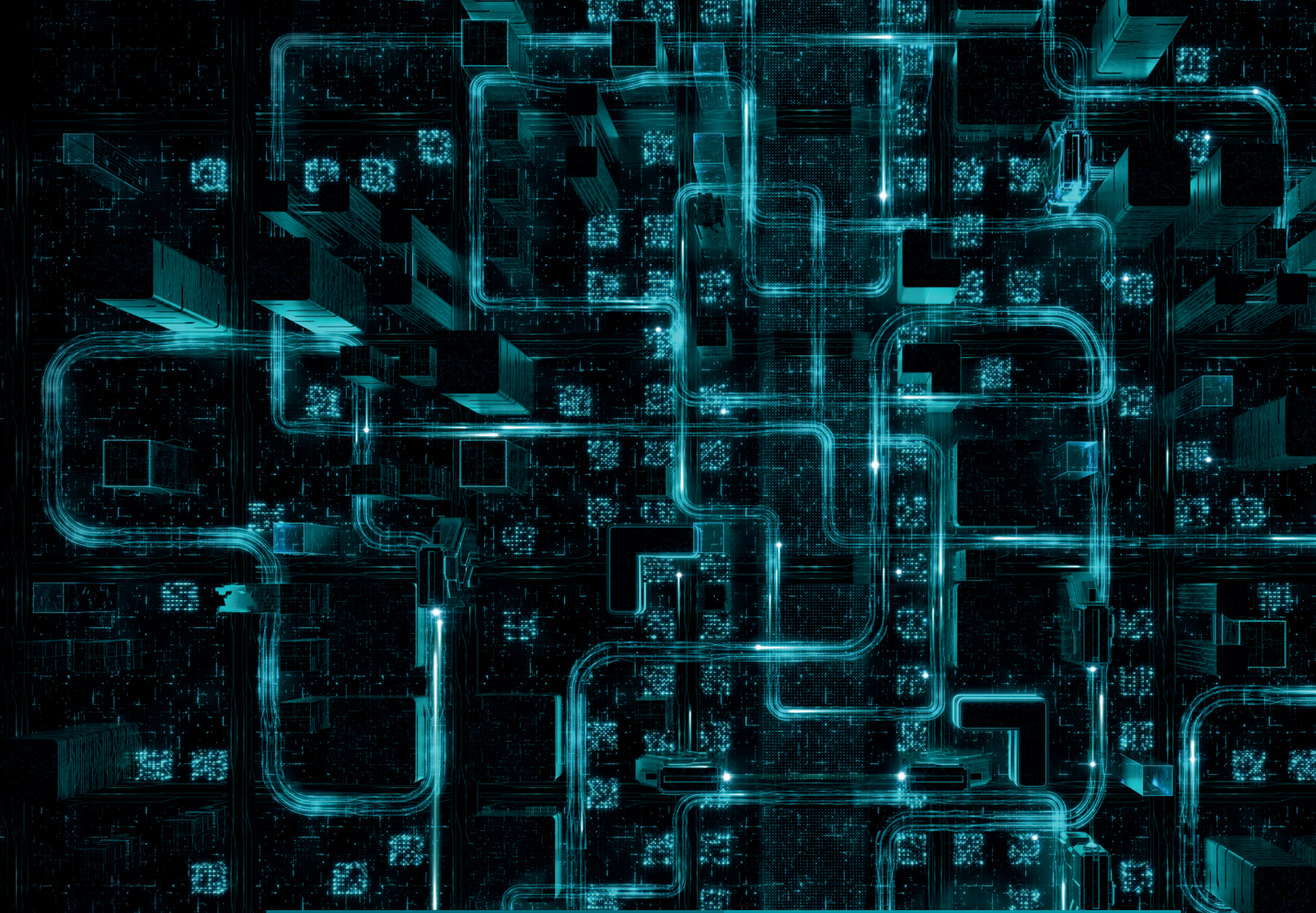
Le contexte actuel de la cybersécurité est marqué par un nombre croissant de violations de données au quotidien. Les pirates parviennent le plus souvent à accéder aux données de votre entreprise par le biais de mots de passe faibles ou volés. En plus de protéger uniquement les connexions normales des utilisateurs aux services critiques, les entreprises peuvent également mettre en place une authentification multi-facteurs sur toute l'escalade des privilèges afin d'éviter tout accès administratif non autorisé.

En ajoutant une solution multi-facteurs, il sera beaucoup plus difficile pour les pirates d'accéder à vos systèmes et donc de les mettre en péril. Les secteurs les plus vulnérables aux violations de données sont généralement ceux qui – comme le secteur financier, le secteur du commerce de détail, le secteur de la santé ou le secteur public – gèrent des données précieuses. Cependant, cela ne veut pas dire que les autres secteurs soient à l'abri, mais simplement que les pirates calculent généralement le rapport entre efforts requis et bénéfices escomptés.

CONFORMITÉ

En matière de conformité, la plupart des entreprises doivent dans un premier temps déterminer si elles sont ou non concernées par une éventuelle norme ou réglementation. Ensuite, elles doivent examiner à quelles exigences, recommandées ou obligatoires, elles doivent répondre. L'authentification multi-facteurs est désormais exigée par certaines normes, telles que la PCI-DSS, et lois, telles que la GLBA ; en outre, la plupart des réglementations, dont le RGPD et l'HIPAA, insistent sur la nécessité de renforcer l'authentification.

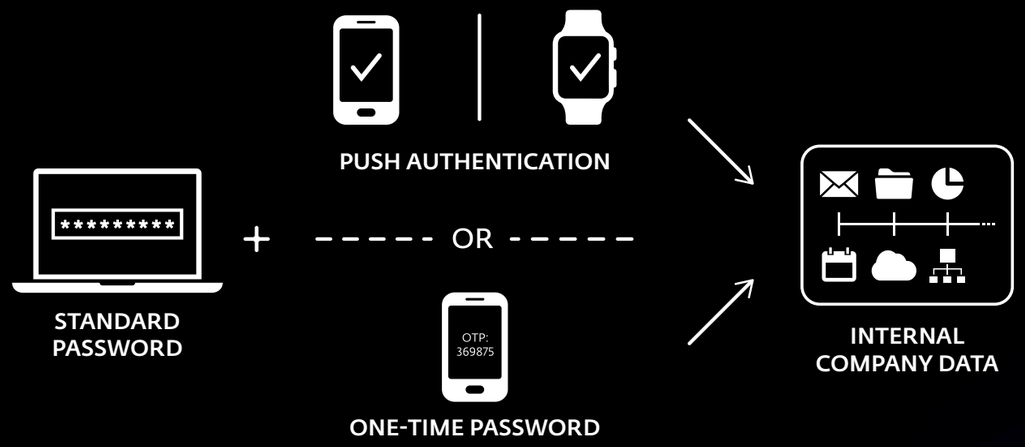
Ainsi, l'authentification multi-facteurs n'est plus une option pour la plupart des entreprises qui gèrent des cartes de crédit ou bien des transactions financières : elle est devenue obligatoire. Toutes les entreprises devraient se renseigner afin de déterminer si elles doivent se conformer ou non à certains règlements.



Les pirates accèdent le plus souvent aux données de votre entreprise par le biais de mots de passe faibles ou volés.

Grâce à cette solution, les pirates ne peuvent plus avoir accès à vos systèmes simplement en devinant un mot de passe trop faible.

Une authentification en un seul geste, sans avoir besoin de retaper le mot de passe à usage unique.



Les avantages ESET

CHOISISSEZ TOUT SIMPLEMENT VOTRE MÉTHODE D'INTÉGRATION

ESET Secure Authentication a été conçue pour fonctionner en tant que solution autonome, gérée grâce à une console Web. Dans un environnement de domaine Windows, vous pouvez choisir une intégration avec Active Directory. Vous bénéficiez ainsi d'une installation et configuration simples et rapides, et vous n'avez pas besoin d'une formation supplémentaire pour déployer la 2FA au sein de votre organisation.

AUCUN MATÉRIEL SPÉCIFIQUE REQUIS

ESET Secure Authentication ne nécessite pas de matériel spécifique, donc aucun coût supplémentaire n'est à prévoir. Installez simplement l'application de 10 MB sur n'importe quel serveur et commencez à la configurer.

FONCTIONNE AVEC LES SMARTPHONES EXISTANTS

Les employés n'ont pas besoin d'utiliser des tokens ou appareils spécifiques. ESET Secure Authentication fonctionne avec un large éventail de smartphones.

INSTALLATION EN 10 MINUTES

Lors de la création d'ESET Secure Authentication, de nombreuses heures de développement ont été consacrées à faire en sorte que son installation soit aussi simple que possible. Nous avons entrepris de créer une application qu'une petite entreprise dénuée de personnel informatique sera en mesure d'installer et de configurer. Qu'une entreprise ait cinq ou 100 000 utilisateurs, ESET Secure Authentication s'installe très rapidement, grâce à sa capacité de configurer plusieurs utilisateurs en même temps.

SDK ET API COMPLETS INCLUS

Pour les entreprises qui souhaitent aller encore plus loin avec ESET Secure Authentication, nous fournissons un SDK et une API complets qu'elles pourront utiliser pour étendre les fonctionnalités de la solution afin de répondre à leurs besoins.

AUTHENTIFICATION PUSH

Elle permet une authentification en un seul geste, sans avoir besoin de retaper le mot de passe à usage unique. Elle fonctionne avec des téléphones sous iOS, Android et Windows 10 Mobile.

" L'installation sur un serveur unique, en toute simplicité, l'intégration avec Active Directory et, l'un de ses atouts majeurs : une application que nous pouvions offrir à notre personnel, ce qui évite de recourir constamment aux SMS. De surcroît, le fait que la solution fonctionne avec OpenVPN nous a ravis car nous n'avons pas eu à modifier notre configuration VPN pour nous adapter au logiciel. "

Tom Wright, Responsable Informatique chez Gardners Books

Cas d'utilisation

Éviter les violations de données

Chaque jour, des entreprises informant leurs clients qu'une violation de données s'est produite font la une des journaux.

SOLUTION

- ✓ Protéger les canaux de communication vulnérables, tels que Remote Desktop, grâce à l'ajout d'une authentification multi-facteurs.
- ✓ Ajouter une authentification multi-facteurs à tous les VPN utilisés.
- ✓ Exiger une authentification multi-facteurs pour toute connexion à des appareils contenant des données sensibles.
- ✓ Protéger les données sensibles grâce à ESET Endpoint Encryption.

PRODUITS ESET

- ✓ ESET Secure Authentication
- ✓ ESET Endpoint Encryption

Vérifier le processus de connexion des utilisateurs

Les entreprises utilisent des ordinateurs partagés dans des espaces de travail dédiés et souhaitent obtenir une vérification de toutes les parties qui se connectent, tout au long de la journée de travail.

SOLUTION

- ✓ Mettre en place l'authentification forte pour les connexions de bureau sur tous les appareils dans les espaces de travail partagés.

PRODUITS ESET

- ✓ ESET Secure Authentication

Renforcer la protection par mot de passe

Les utilisateurs se servent de mots de passe identiques pour différentes applications et différents services Internet, ce qui représente un risque pour l'entreprise.

SOLUTION

- ✓ Limiter l'accès aux ressources de l'entreprise en tirant parti d'une authentification multi-facteurs.
- ✓ Exiger une authentification multi-facteurs réduit les tracas associés aux mots de passe partagés ou volés, car un mot de passe à usage unique supplémentaire est requis.

PRODUITS ESET

- ✓ ESET Secure Authentication

Fonctionnalités et plateformes protégées

AUTHENTIFICATION PUSH

Une authentification en un seul geste avec tous les smartphones sous iOS, Android et Windows 10 Mobile.

AUTRES MÉTHODES D'AUTHENTIFICATION

Pour la génération du mot de passe à usage unique, ESET Secure Authentication est compatible avec les applications mobiles, les notifications push, les tokens, les SMS ou autres méthodes sur mesure.

ADMINISTRATION À DISTANCE

Par le biais de la console Web ESET Secure Authentication ou de Microsoft Management Console (MMC). S'intègre avec Active Directory pour une administration facile ou bien fonctionne de manière autonome pour les organisations sans domaine Windows.

COMPATIBILITÉ EN MATIÈRE DE PROTECTION

ESET Secure Authentication est compatible nativement avec Virtual Private Networks (VPN), Remote Desktop Protocol (RDP), Outlook Web Access (OWA), VMware Horizon View et les services basés sur Radius.

PROTECTION SUPPLÉMENTAIRE DES SYSTÈMES D'EXPLOITATION

L'authentification multi-facteurs permet également de protéger l'authentification supplémentaire lors des ouvertures de sessions et l'escalade des privilèges.

Elle est compatible avec Windows ainsi qu'avec macOS et Linux.

COMPATIBILITÉ CLOUD

ESET Secure Authentication est non seulement compatible avec les applications sur site mais également avec les services Web/Cloud tels que Google Apps et Microsoft ADFS 3.0 (y compris Office 365).

COMPATIBILITÉ HARD TOKEN

la solution ne requiert pas l'utilisation de hard tokens mais elle est compatible avec tous les tokens event-based HOTP qui sont conformes avec OATH et les clés hardwares FIDO 2 et FIDO U2F.

VPN COMPATIBLES

Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall.

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

Gartner peerinsights customers' choice 2019

canalys Cybersecurity Champion 2020

LES AVIS DES ANALYSTES

Gartner

ESET reconnu unique Challenger dans le Magic Quadrant Gartner 2019 « Endpoint Protection Platforms », pour la 2ème année consécutive.

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.

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 mentionné 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'entreprises. 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 alliés.

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