



MOBILE PROTECTION

**Une protection maximale et légère
pour vos terminaux mobiles.**



ENJOY SAFER
TECHNOLOGY™

®Profitez de la vie numérique en toute sécurité.



30 YEARS OF
CONTINUOUS
IT SECURITY
INNOVATION



Qu'est-ce qu'une **solution de sécurité mobile ?**

Les solutions de sécurité mobiles peuvent être classées dans deux catégories distinctes : la sécurité et la gestion.

La sécurité inclut notamment la protection contre les malwares et l'hameçonnage, les restrictions d'accès aux connexions non sécurisées, et bien plus encore.

La gestion comprend le formatage à distance des appareils, la restriction des installations d'applications non reconnues, la préconfiguration des appareils destinés aux utilisateurs et d'autres éléments liés à la gestion IT.

Il convient de noter que les smartphones et tablettes Apple ne peuvent pas bénéficier de certaines fonctionnalités comme l'anti-malware, en raison des restrictions imposées aux applications non-Apple. Pour les appareils Apple, seules les fonctionnalités de gestion des produits de protection mobile peuvent être utilisées.

Pourquoi protéger les terminaux mobiles

RANSOMWARE

Le ransomware a longtemps sévi sur les ordinateurs et les serveurs, mais depuis 2014, il touche également les appareils Android. Le premier ransomware Android, Simplocker, a en effet vu le jour en 2014. Tout comme leurs équivalents sur ordinateur, les ransomwares mobiles ont évolué pour adopter de nouvelles pratiques et de nouvelles méthodes de contenus pour prendre en otage les mobiles. Lors de tels cyber-attaques, les sociétés se rendent souvent compte que leurs sauvegardes ne sont pas récentes et se sentent obligées de payer la rançon.

ESET Endpoint Security pour Android offre plusieurs couches de protection, en bloquant les ransomware et en les détectant si jamais ils réussissent à s'infiltrer dans l'environnement mobile de l'entreprise. La prévention et la détection des ransomwares sont importantes, car à chaque fois qu'une victime cède au chantage, cela encourage les cybercriminels à poursuivre ce type d'attaque.

APPAREILS VOLÉS OU PERDUS

Les entreprises permettent aujourd'hui à leurs salariés de travailler à distance, par exemple chez eux ou dans un lieu public. Mais ces nouvelles habitudes de travail génèrent malheureusement des risques, car les appareils mobiles sont susceptibles d'être volés ou perdus. Ces derniers contiennent non seulement des documents, fichiers et courriels sensibles et confidentiels, mais aussi des informations qui peuvent compromettre la réputation de l'entreprise en cas de divulgation.


Les solutions de sécurité et de gestion des appareils mobiles (MDM) d'ESET permettent aux organisations de verrouiller ou de formater ces appareils à distance. Ainsi, elles s'assurent que leurs informations confidentielles ne tombent pas entre les mains d'utilisateurs mal intentionnés en cas de perte, de vol ou de licenciement d'un salarié.

GESTION DES APPAREILS

Pour des raisons de responsabilité et de temps, les organisations tiennent à ce que leurs salariés travaillent uniquement sur des appareils à usage exclusivement professionnel. De plus, la sécurité des mobiles est compromise lorsque les utilisateurs sont autorisés à s'authentifier sur des réseaux peu fiables ou à utiliser certaines fonctionnalités.

Les solutions d'ESET pour les plateformes mobiles permettent aux entreprises de bloquer l'accès à certaines applications. Il est possible d'activer les applications à des moments précis, pour restreindre l'accès uniquement pendant les heures de travail.

Le premier ransomware Android, Simplocker, a en effet vu le jour en 2014.



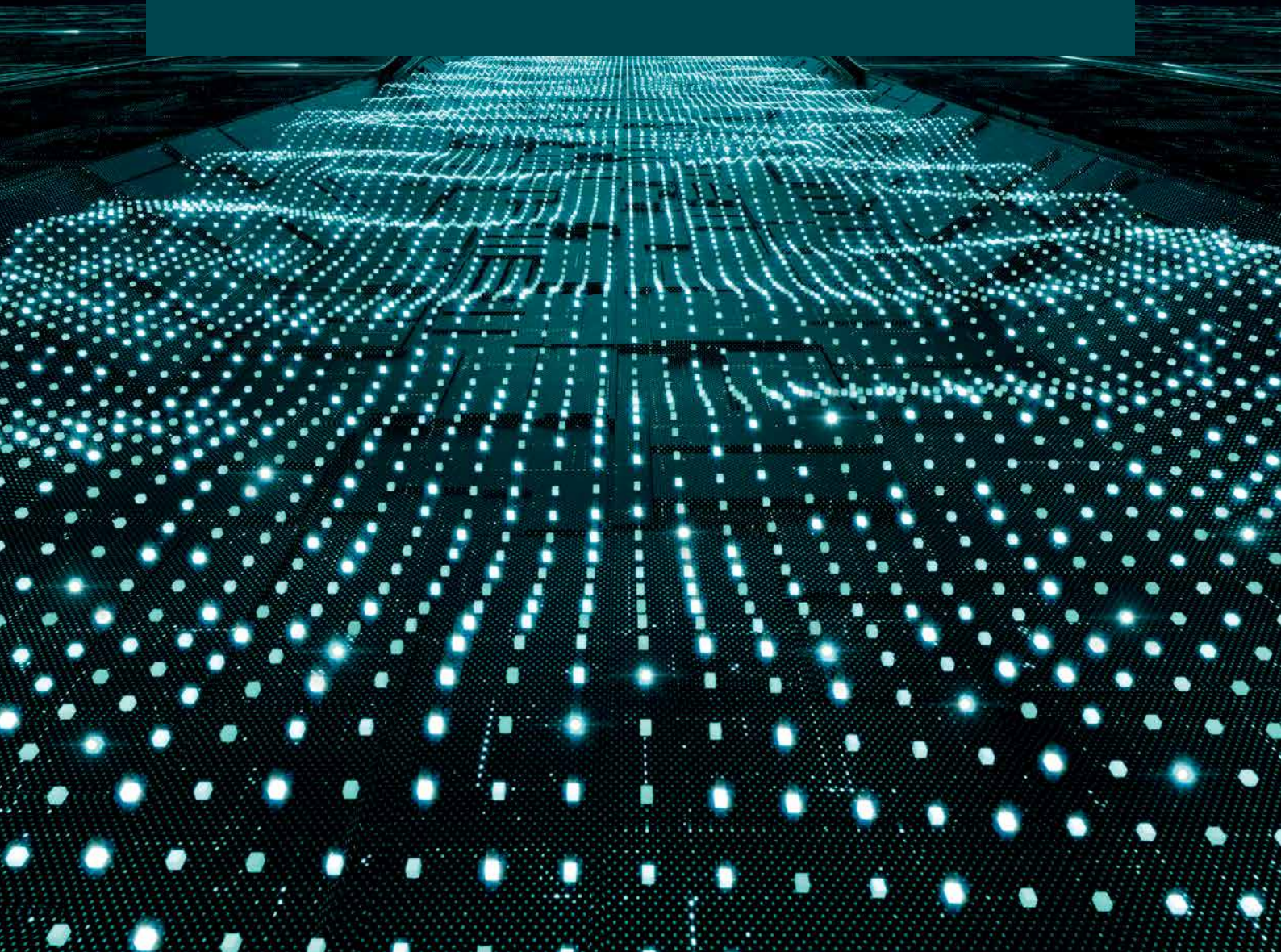
Les entreprises permettent aujourd'hui à leurs salariés de travailler à distance, par exemple chez eux ou dans un lieu public. Mais ces nouvelles habitudes de travail génèrent malheureusement des risques, car les appareils mobiles sont susceptibles d'être volés ou perdus. Ces derniers contiennent non seulement des documents, fichiers et e-mails professionnels, mais aussi des informations qui peuvent compromettre la réputation de l'entreprise en cas de divulgation.

La prévention et la détection des ransomware sont importantes, car à chaque fois qu'une victime cède au chantage, cela encourage les cybercriminels à poursuivre ce type d'attaque.

Plus besoin de solutions exclusivement dédiées à la gestion des appareils mobiles. Gerez et surveillez tous vos appareils iOS, Android et autres depuis une console unique ESET Security Management Center.

“ Le principal avantage des solutions ESET, c’est que la sécurité de tous les endpoints peut être gérée et vérifiée depuis une console unique.”

Jos Savelkoul, responsable d’équipe du service des technologies de l’information et de la communication, Hôpital Zuyderland, Pays-Bas ; 10 000 postes



La différence ESET

RENTABLE

Plus besoin de solutions exclusivement dédiées à la gestion des appareils mobiles. Gerez et surveillez tous vos appareils iOS, Android et autres depuis une console unique ESET Security Management Center.

PROTECTION MULTICOUCHE

ESET allie technologie multicouche, machine learning et expertise humaine afin d'offrir à ses clients un niveau de protection optimal. Nous adaptons nos solutions en permanence pour parvenir à un juste équilibre entre performance, détection et faux positifs.

SYSTÈME CLOUD DE PROTECTION ANTI-MALWARE

Lorsqu'une menace zero-day, telle qu'un ransomware, est détectée, le fichier est envoyé à notre sandbox Cloud. Il est ainsi exécuté et son comportement est analysé. Les résultats sont transmis à tous les endpoints de par le monde en quelques minutes, sans nécessiter de mise à jour.

TECHNOLOGIE ÉPROUVÉE ET FIABLE

Depuis 30 ans, 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.

PERFORMANCES INÉGALÉES

L'impact des solutions sur les performances des ordinateurs est une source de préoccupation majeure pour de nombreuses entreprises. Les solutions ESET sont excellentes dans ce domaine et passent haut la main des tests tiers qui montrent leur faible impact sur les systèmes.

PRÉSENCE INTERNATIONALE

ESET est implanté dans 22 pays partout dans le monde, avec 13 centres de R&D et une présence dans plus de 200 pays et territoires. Cela nous permet d'offrir à nos clients une perspective mondiale sur les dernières tendances et menaces.

“ Les solutions de sécurité d'ESET protègent nos endpoints et envoient des alertes au service IT de Primoris en cas de menaces et infections sérieuses comme les ransomwares.”

Joshua Collins, Responsable des opérations des centres de données ;
Primoris Services Corporation, États-Unis ; 4 000 postes

Cas d'utilisation

Ransomware

Les ransomwares menacent non seulement les PC et les serveurs, mais également les appareils mobiles. Les entreprises veulent s'assurer que toutes leurs données soient protégées contre ces attaques.

SOLUTION

- ✓ Déployez ESET Mobile Security sur tous vos appareils mobiles pour une protection fiable.
- ✓ Bloquez l'installation d'applications issues de sources inconnues sur les appareils Android pour limiter les risques.

Perte de données

Les entreprises se soucient non seulement de la perte et du vol des appareils, mais aussi des vols de données lors du licenciement des salariés.

SOLUTION

- ✓ Appliquez une politique de sécurité pour chiffrer les appareils mobiles.
- ✓ Mettez en place des politiques nécessitant l'utilisation de mots de passe ou codes PIN sur tous les appareils.
- ✓ Verrouillez ou formatez les appareils à distance si nécessaire.



ENDPOINT
SECURITY
FOR ANDROID

Conformité des appareils


Les entreprises appliquent différentes politiques d'utilisation des appareils mobiles, et les administrateurs doivent s'assurer que tous les appareils et utilisateurs soient conformes.

SOLUTION

- ✓ Implémentez des restrictions pour limiter les appels téléphoniques et messages pendant les heures de travail.
- ✓ Limitez les installations d'applications sur les appareils.
- ✓ Limitez l'accès aux réseaux Wi-Fi non sécurisés.
- ✓ Assurez-vous que les fonctionnalités de sécurité des téléphones soient installées et activées.



MOBILE DEVICE
MANAGEMENT
FOR APPLE iOS



“ La gestion centralisée de la sécurité de tous nos postes de travail, serveurs et appareils mobiles est pour nous l’un des principaux avantages de cette solution.”

Responsable informatique, Diamantis Masoutis S.A., Grèce ; 6 000 postes

Les entreprises se soucient non seulement de la perte et du vol des appareils, mais aussi des vols de données lors du licenciement des salariés.

Fonctionnalités techniques

Android/iOS

ANTIVOL

Verrouillez, formatez ou déclenchez un signal sonore à distance pour tout appareil perdu ou volé. Envoyez des notifications personnalisées aux appareils ou verrouillez leur écran pour vous assurer qu'ils soient rendus à leur propriétaire.

CONTRÔLE DES APPLICATIONS

Permettez aux administrateurs de surveiller les applications installées, de bloquer l'accès à certaines applications, permissions ou catégories et de demander aux utilisateurs de désinstaller des applications précises.

SÉCURITÉ DES APPAREILS

Sans supervision, les utilisateurs ne prennent pas toujours les mesures nécessaires pour garantir la sécurité des appareils. ESET permet aux administrateurs de définir des mots de passe complexes, de demander aux utilisateurs de chiffrer leur appareil, de bloquer l'appareil photo, et plus encore.

GESTION CENTRALISÉE

Les solutions mobiles sont gérées dans une interface unique installable sous Windows et Linux. Outre l'installation, ESET propose également une appliance virtuelle que vous pouvez importer pour une installation rapide.

Android uniquement

PROTECTION MULTICOUCHE

Une seule couche de défense est insuffisante dans un contexte de menaces en constante évolution. Toutes les solutions de la gamme Endpoint détectent les malwares avant, pendant et après leur exécution et sont optimisées pour mobile.

MACHINE LEARNING

ESET s'intéresse aux algorithmes de Machine Learning dans le but de détecter et bloquer les menaces depuis les années 1990, intégrant les réseaux neuronaux dans ses produits dès 1998. Nous combinons la puissance de réseaux neuronaux et d'un groupe de six algorithmes de classification performants pour atteindre ces objectifs. Nous intégrons cette technologie à l'ensemble de nos solutions multicouches.

ANTI-HAMEÇONNAGE (ANTI-PHISHING)

Protège les utilisateurs des faux sites qui tentent de dérober leurs mots de passe, leurs coordonnées bancaires et d'autres informations sensibles.

AUDIT D'APPLICATIONS

Surveille les applications et leurs accès aux données personnelles/de l'entreprise par catégories, permettant ainsi aux administrateurs de surveiller et contrôler les accès aux applications.

Android uniquement

APPLE iOS MANAGEMENT FRAMEWORK

Plus besoin de solutions dédiées : appuyez-vous sur Apple iOS Management Framework pour surveiller la sécurité de tous vos appareils iOS, le tout depuis une interface unique dans ESET Security Management Center.

RÉGLAGE DES PARAMÈTRES DE COMPTE À DISTANCE

Réglez les paramètres de compte à distance, notamment pour le Wi-Fi, les VPN et Exchange.

GESTION DES APPAREILS MOBILES

Les utilisateurs et administrateurs sont automatiquement informés si les paramètres de l'appareil ne sont pas conformes aux politiques de sécurité de l'entreprise et reçoivent des recommandations sur les changements nécessaires.

ESET SECURITY MANAGEMENT CENTER PARAMÈTRES POUR LA GESTION MOBILE

The screenshot displays the 'New Policy' configuration window in the ESET Security Management Center. The policy is titled 'ESET Mobile Device Management for iOS'. The left sidebar shows navigation options: Dashboard, Computers, Threats, Reports, Client Tasks, Installers, Policies, Computer Users, Notifications, Status Overview, and More. The main content area is divided into sections: Basic, Settings (selected), Assign, and Summary. The 'Settings' section is further divided into sub-sections: PASSCODE, RESTRICTIONS, and OTHERS. The 'RESTRICTIONS' sub-section is expanded, showing various settings for device functionality, airprint, iCloud, security and privacy, and device security. Each setting has a toggle switch and a dropdown menu for configuration. At the bottom, there are buttons for 'BACK', 'CONTINUE', 'FINISH', and 'CANCEL'.

ESET SECURITY MANAGEMENT CENTER PARAMÈTRES POUR ANDROID

The screenshot displays the 'New Policy' configuration window in the ESET Security Management Center. The policy is titled 'ESET Endpoint for Android Q+1'. The left sidebar shows navigation options: Dashboard, Computers, Threats, Reports, Client Tasks, Installers, Policies, Computer Users, Notifications, Status Overview, and More. The main content area is divided into sections: Basic, Settings (selected), Assign, and Summary. The 'Settings' section is further divided into sub-sections: ANTIVIRUS, ANTI-THEFT, APPLICATION CONTROL, SMS & CALL FILTER, ANTI-PHISHING PROTECTION, DEVICE SECURITY, and SETTINGS. The 'DEVICE SECURITY' sub-section is expanded, showing various settings for device security, screen lock policy, device settings policy, user restrictions, data protection, extra device protection, and extra cost protection. Each setting has a toggle switch and a dropdown menu for configuration. At the bottom, there are buttons for 'BACK', 'CONTINUE', 'FINISH', and 'CANCEL'.

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

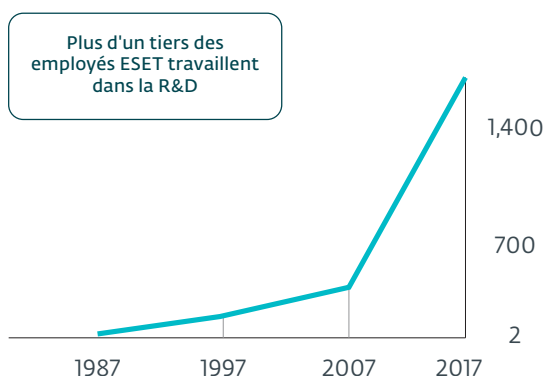
+110 millions
d'utilisateurs
partout dans le
monde

+ 400 000
Clients
Entreprises

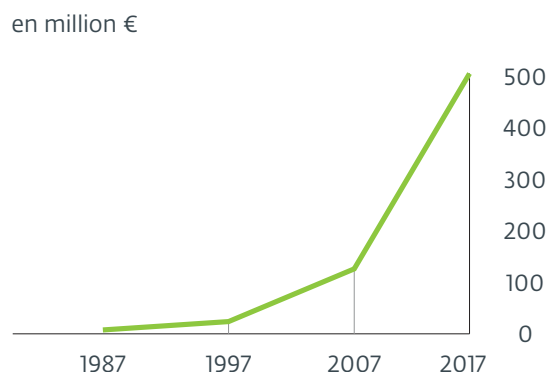
+ 200
pays et
territoires
couverts

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

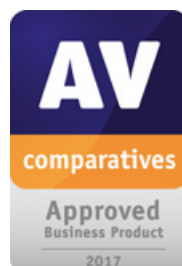
Plus de 14 000 endpoints



Partenaire de sécurité FAI depuis 2008

2 millions d'utilisateurs

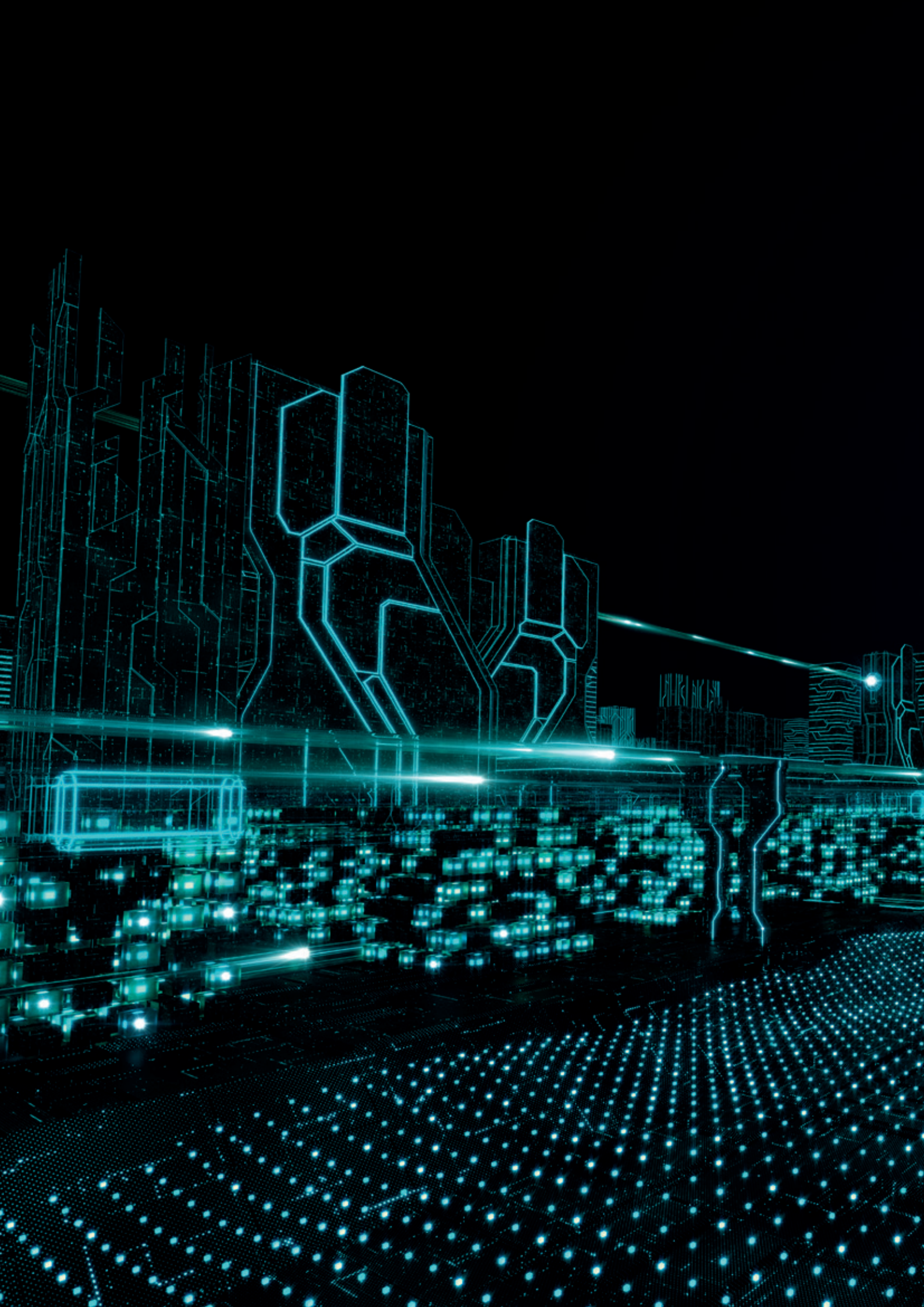
NOS RÉCOMPENSES LES PLUS PRESTIGIEUSES



“ 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







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