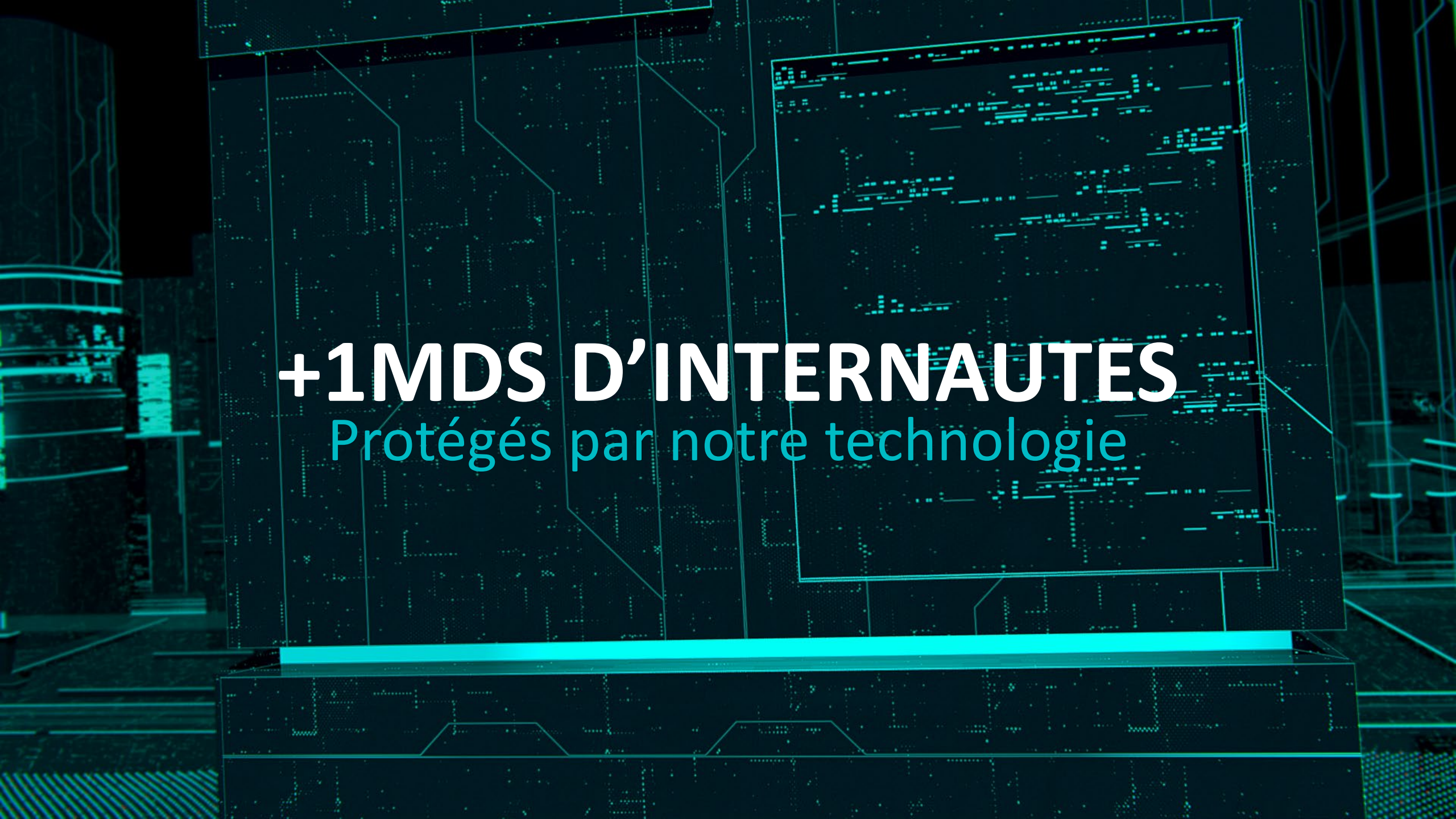
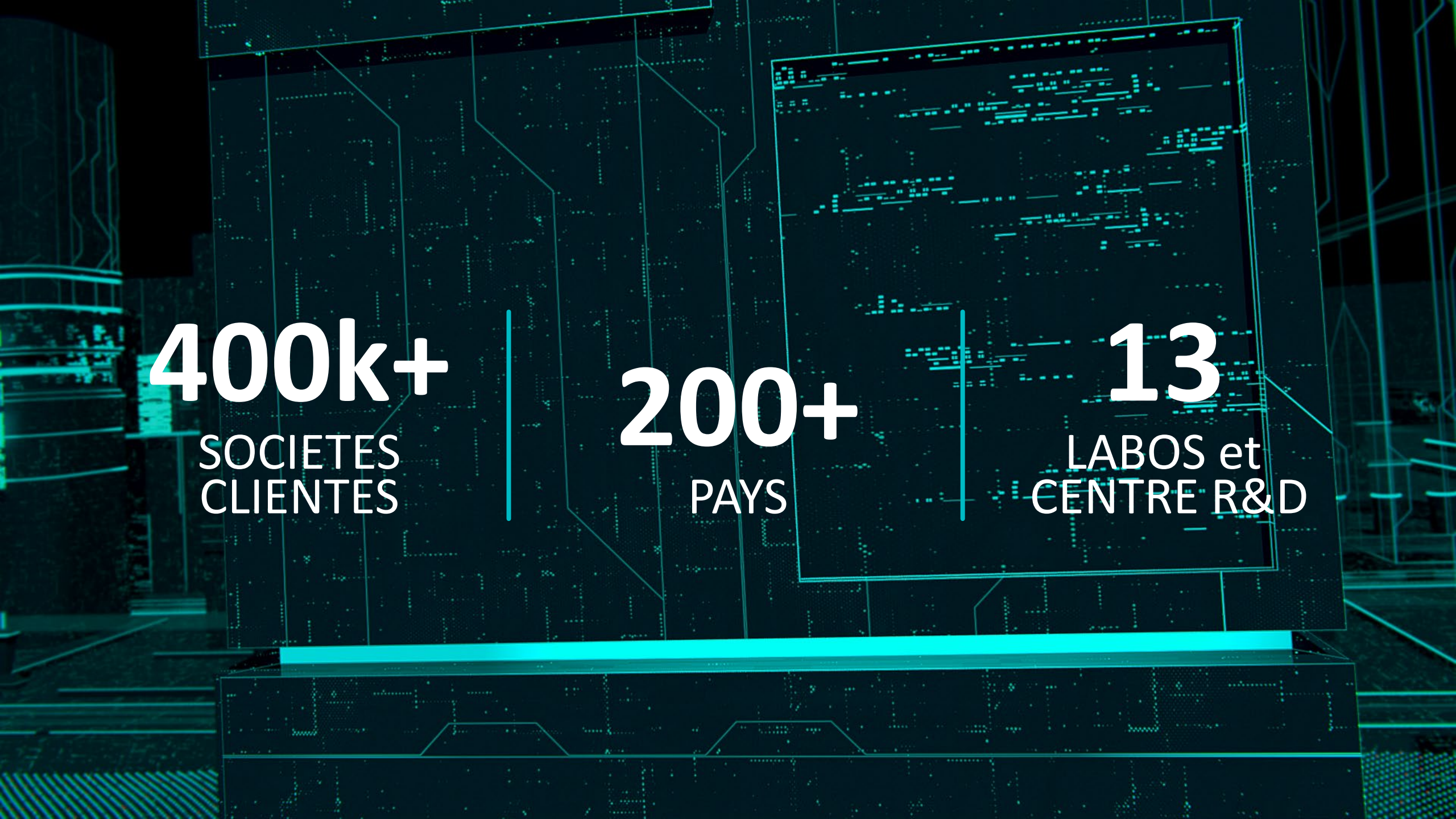

eset
LAFI


1er éditeur de cybersecurité en Europe


+ 30 ANS D’INDEPENDANCE ET D’INNOVATION
Eset est une société non cotée en bourse et en fonds propres


+1MDS D’INTERNAUTES
Protégés par notre technologie


400k+
SOCIETES CLIENTES
200+
PAYS
13
LABOS et CENTRE R&D


Les grandes entreprises
confient leur sécurité à ESET
Gendarmerie
nationale
FNAC DARTY
DECATHLON
RENAULT

Le Contexte de la Cybersécurité

3 millions d'adresses e-mail et
1 millions de mots de passe révélées suite à
ne diffusion massive de données

Tomáš Foltýn

La société mère de Ray Ba
importante attaqu

welivesecurity BY eset

e données de Marriott Starwood
que les voyageurs devraient
er maintenant

welivesecurity BY eset

Mozilla corrige une faille permet
détourner Firefox pour Android

Amer Owaida 22 Sep 2020 - 05:30PM

welivesecu

La PDG d
annuelle
l'affaire d

Editor 4 Mar 2017 - 08:53PM

welivesecurity BY eset

Emotet frappe le Ministère de la justice du Québec

Gabrielle Ladouceur Despins 16 Sep 2020 - 10:53PM

80%

des entreprises victimes d’une cyberattaque selon L’ANSSI

43%

des attaques viseraient des petites entreprises

80%

des entreprises victimes d'une cyberattaque selon L'ANSSI

L'ANSSI a traité 104 ransomwares depuis le début de l'année et alerte sur leur virulence croissante

Alexandre Boero
04 septembre 2020 à 10h53

5

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le ministère de la Justice publient un guide visant à sensibiliser les collectivités et entreprises sur les ransomwares, incluant les témoignages d'institutions ou de marques fortes ayant été récemment piégées.

CYBER MOIS

COMMUNIQUÉ DE PRESSE

Paris, le 01/10/2020

Cybermoi/s 2020 : un mois pour se protéger du chantage numérique

La crise sanitaire et le confinement ont engendré une hausse fulgurante de l'utilisation des technologies dans nos vies personnelles et professionnelles. Les pirates du net en ont profité pour intensifier le chantage numérique à coups de rançongiciels et de chantage à la webcam. Pour y faire face, la campagne de sensibilisation du Cybermoi/s donne aux professionnels et aux particuliers les clés pour mieux comprendre et prévenir les menaces liées au chantage numérique.

Rançongiciels : une menace qui explose

Les rançongiciels sont des programmes malveillants permettant aux attaquants de prendre le contrôle à distance d'un ordinateur ou d'un système d'information. Ils rendent la consultation ou l'utilisation des données impossibles, sans le paiement d'une rançon.

[1] Étude *Menaces informatiques et pratiques de sécurité en France*, CLUSIF, 2020 : https://clusif.fr/publications/mips-2020-menaces-informatiques-et-pratiques-de-securite-en-france-edition-2020-rapport-global/?visible=public

Avec le soutien du

GOUVERNEMENT

« Entre janvier et septembre 2020, l'industrie, les collectivités territoriales et la santé ont été les secteurs d'activité les plus affectés par les attaques par rançongiciels traitées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). » indique François Deruty, sous-directeur Opérations de l'ANSSI.

43%

des attaques viseraient des petites entreprises

ITRNews

FOURNISSEURS DISTRIBUTION ET SERVICES MARKETING PRODUITS PLUS

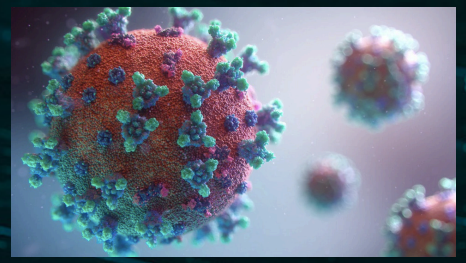
L'INFO DU JOUR

75 % des petites entreprises françaises accélèrent leur transformation numérique en raison de la pandémie

lundi 14 septembre 2020

Les 2/3 des petites entreprises seulement ont aujourd'hui entrepris des projets liés au numérique et ceux-ci restent fragiles et limités. Dans les 18 prochains mois, les petites entreprises françaises indiquent qu'elles vont investir dans le travail à distance (32 %) ou encore le développement de solutions numériques (27 %). Elles pourraient accroître le PIB du pays de 208 milliards de dollars d'ici 2024 grâce à leur transformation numérique. Tel est le constat dressé par Cisco qui tente, au travers de l'étude menée par IDC en juin 2020, de mieux comprendre les opportunités et les défis auxquels les petites entreprises sont actuellement confrontées, ainsi que la corrélation entre la maturité numérique et une reprise économique plus rapide.

Pour comprendre le niveau de maturité de la numérisation des petites entreprises, IDC a mis au point un cadre qui les aide à évaluer clairement leurs capacités actuelles et à comprendre où elles se situent sur un indice numérique à quatre niveaux – allant du stade le plus précoce de Digital Indifferent au plus avancé de Digital Natives.



70 % des DSI rapportent que le télétravail au moins un jour par semaine était pratiqué dans leur organisation, 49 % n'avait pas prévu, dans leur plan de continuité d'activité, de devoir ainsi basculer vers un télétravail généralisé. 46 % ont jugé la transition difficile, **74 % des responsables IT se jugeant en situation de stress. »**

Parmi les solutions déployées dans l'urgence, **la généralisation du VPN (Virtual Private Network ou « réseau privé virtuel »)** a évidemment été plébiscitée. L'accès VPN, qui permet d'accéder au réseau de l'entreprise depuis l'extérieur, n'était auparavant pas accessible à tous les collaborateurs mais souvent réservé à certaines populations nomades et/ou VIP

Télétravailleurs sont davantage vulnérables aux cybermenaces et risques de détournement d'identités et d'accès
Certains accès distants ouverts à la hâte ont parfois généré des accès exceptionnels, attribués manuellement en dehors de tout processus habituel conforme à la PSSI (Politique de Sécurité du Système d'Information). Utilisation de Pcs personnels sur les réseaux professionnels

C'est une véritable démarche qualitative de sécurisation des accès distants que les organisations doivent désormais entreprendre.

La sensibilisation des utilisateurs aux risques de cybersécurité dans un environnement de Flex-office est devenue une nécessité absolue.

Coronavirus (COVID-19)

LES PRINCIPAUX RISQUES ET CYBERMENACES LIÉS AU TÉLÉTRAVAIL

L'hameçonnage (*phishing*)

Les rançongiciels (*ransomware*)

Le vol de données

Les faux ordres de virement (FOVI/BEC)

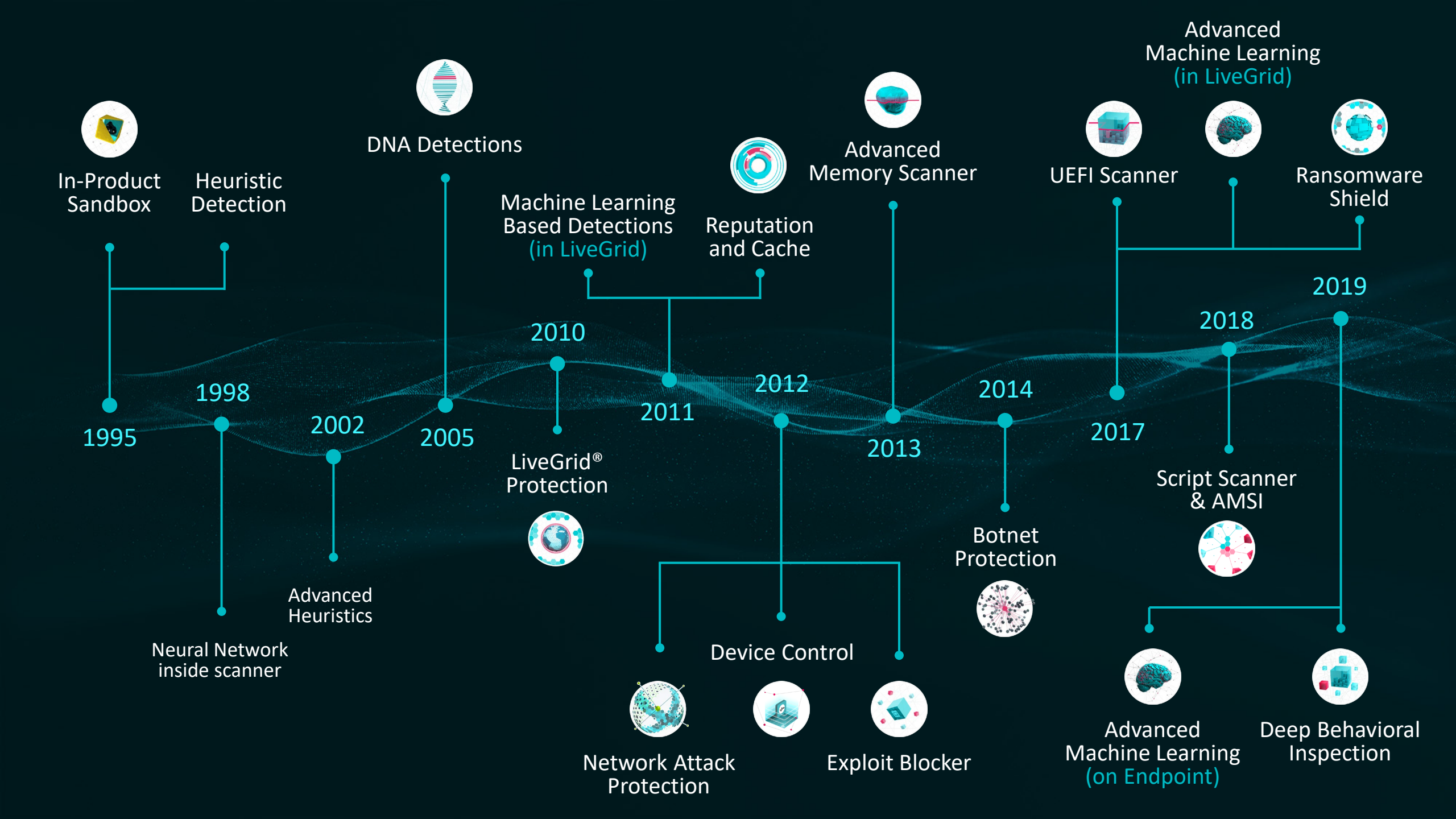
Tous ces conseils en détail sur
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

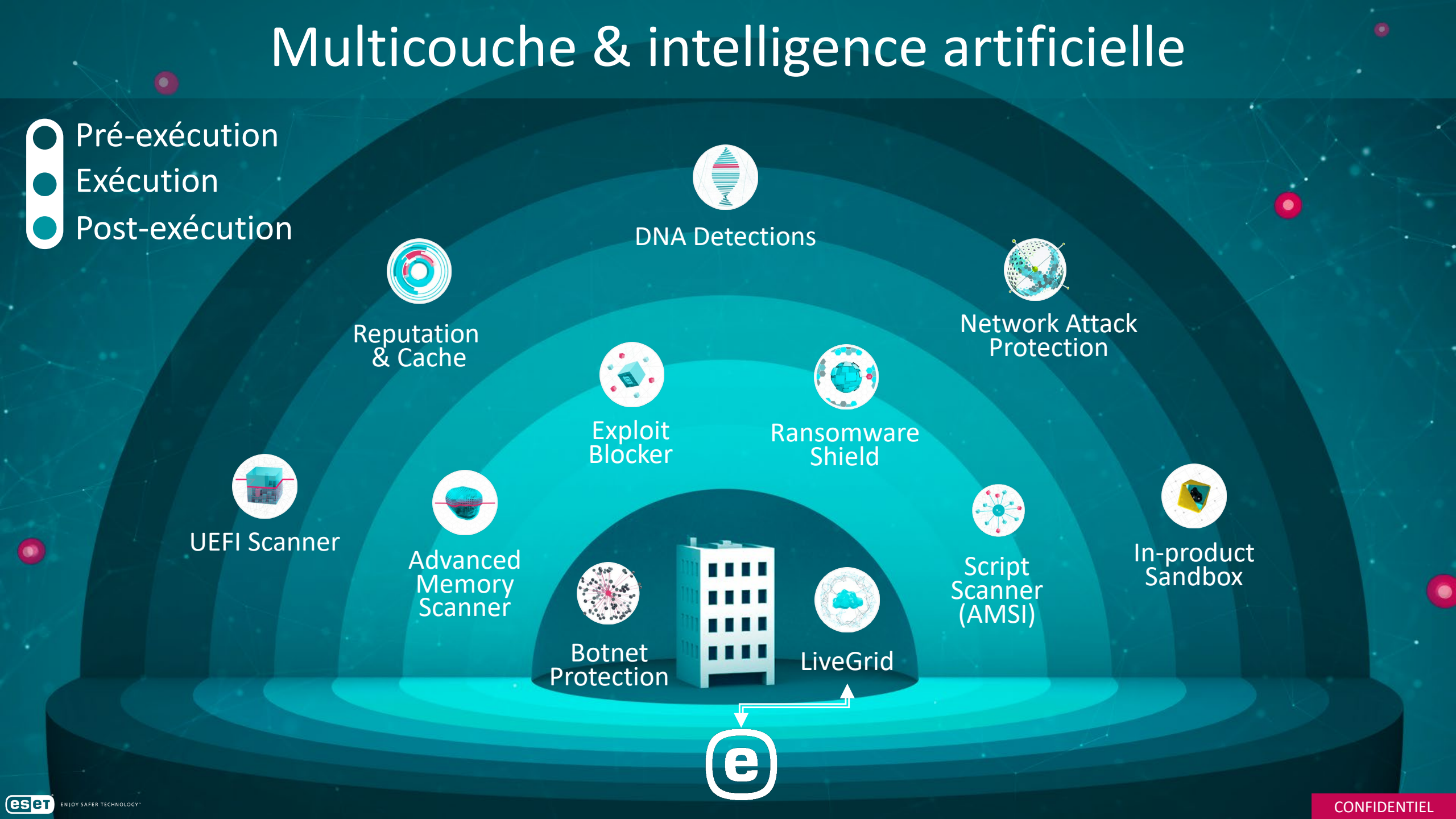
de sécurisation des accès distants
que les organisations doivent désormais
entreprendre.

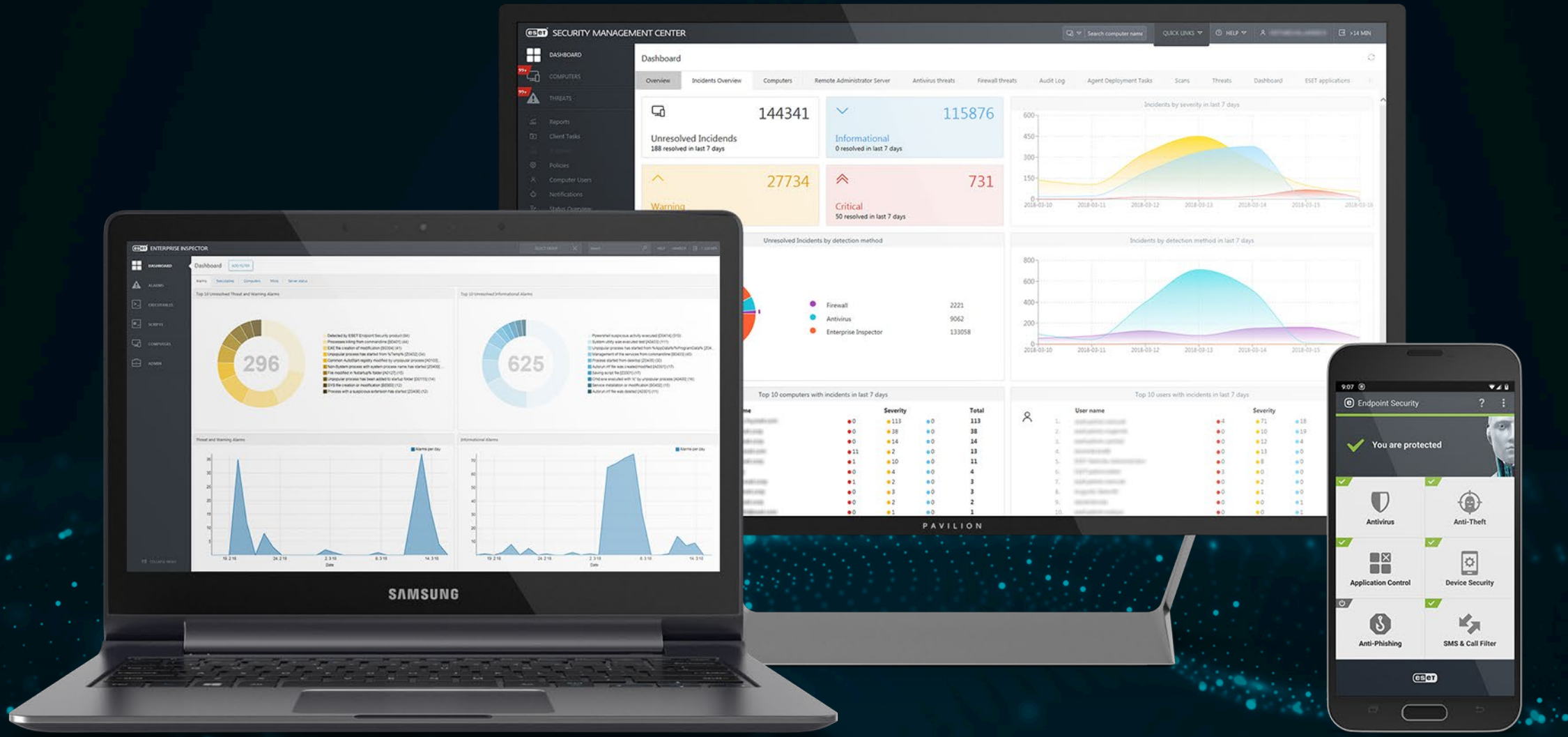
de cybersécurité dans un environnement
de Flex-office est devenue une nécessité
absolue.

La technologie ESET

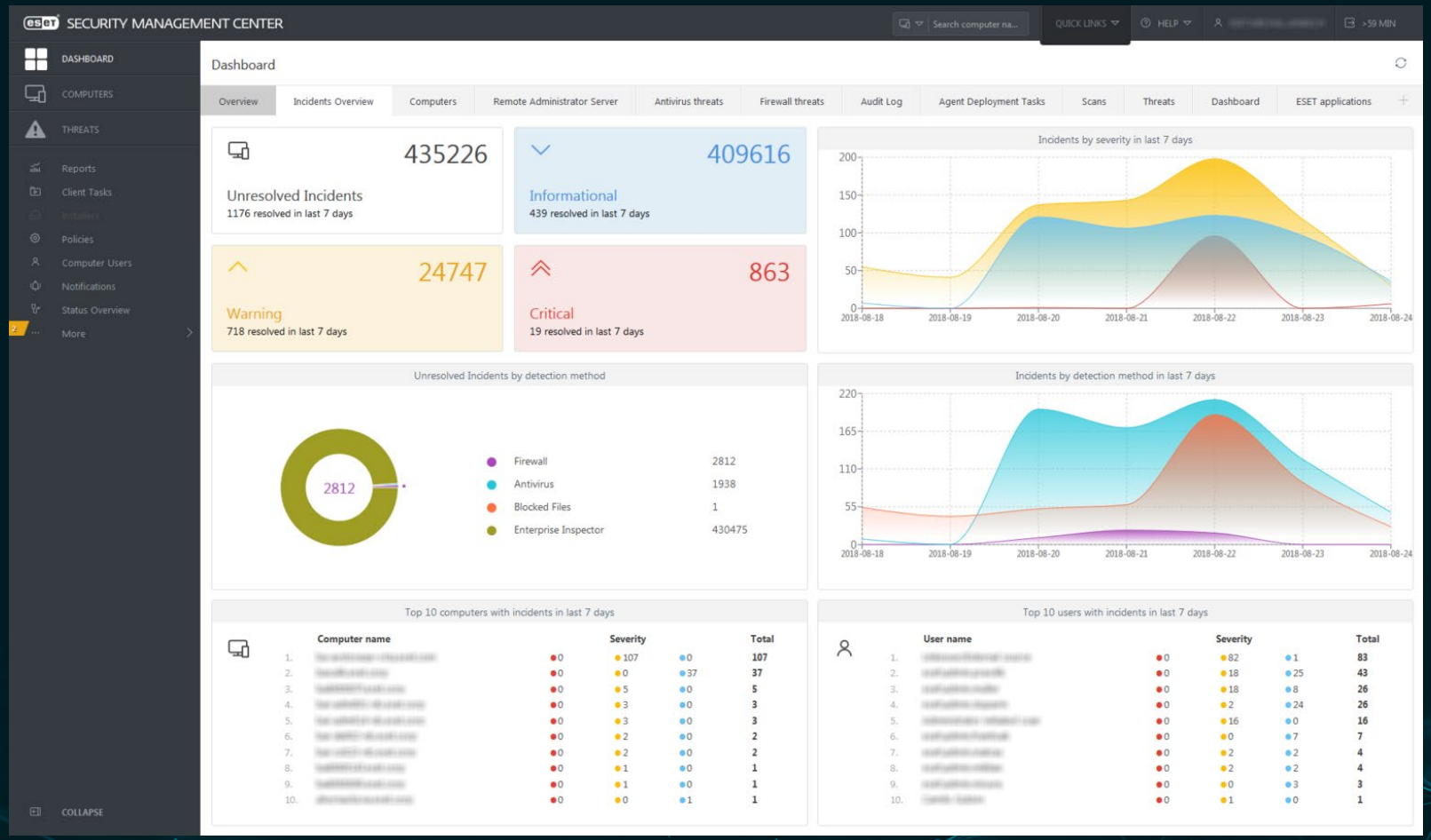

In-Product Sandbox
Heuristic Detection
DNA Detections
Machine Learning Based Detections (in LiveGrid)
Reputation and Cache
Advanced Memory Scanner
Advanced Machine Learning (in LiveGrid)
UEFI Scanner
Ransomware Shield
1995
1998
2002
2005
2010
2011
2012
2013
2014
2017
2018
2019
Neural Network inside scanner
Advanced Heuristics
LiveGrid® Protection
Botnet Protection
Script Scanner & AMSI
Device Control
Network Attack Protection
Exploit Blocker
Advanced Machine Learning (on Endpoint)
Deep Behavioral Inspection

Multicouche & intelligence artificielle




SECURITY MANAGEMENT CENTER
Dashboard
144341
Unresolved Incidents
188 resolved in last 7 days
115876
Informational
0 resolved in last 7 days
27734
Warning
731
Critical
50 resolved in last 7 days
Unresolved Incidents by detection method
Firewall 2221
Antivirus 9062
Enterprise Inspector 133058
Incidents by detection method in last 7 days
Top 10 computers with incidents in last 7 days
Top 10 users with incidents in last 7 days
ENTERPRISE INSPECTOR
296
625
SAMSUNG
PAVILION
Endpoint Security
You are protected
Antivirus
Anti-Theft
Application Control
Device Security
Anti-Phishing
SMS & Call Filter

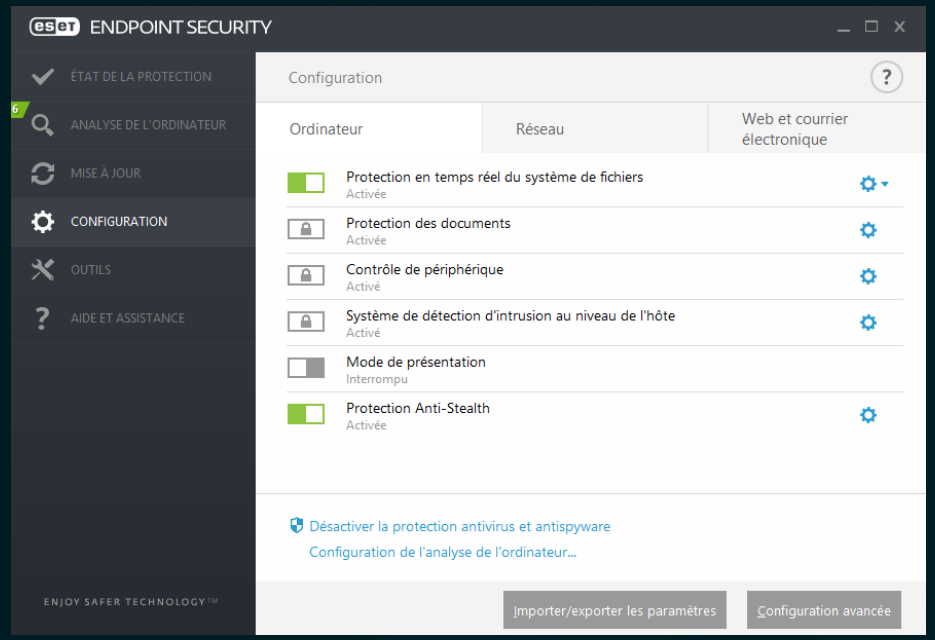
Consoles d’administration



- Console centralisée
- Installation flexible
- Groupes dynamiques
- Désinstallation de softwares tierces
- Réponse aux incidents en un simple clic
- Reporting dynamique et personnalisé

Protection des Endpoints & Serveurs

Une approche multicouche qui allie différentes technologies dynamiques, pour offrir
un juste équilibre entre performance, détection et faux positifs



Antimalware

Bouclier Anti-Ransomware

Analyse Mémoire Avancée

Anti-Botnet

Antispyware

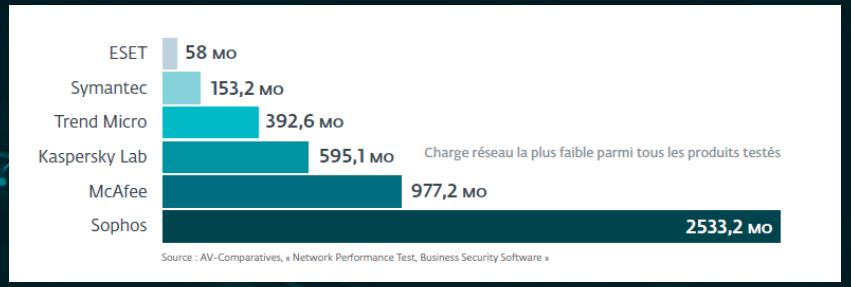
Sandbox locale

Pare-feu local

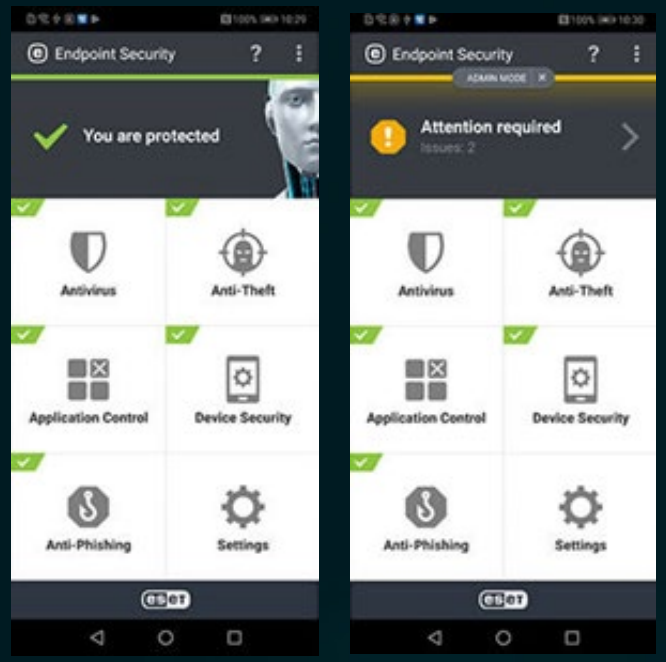
Anti-Phishing

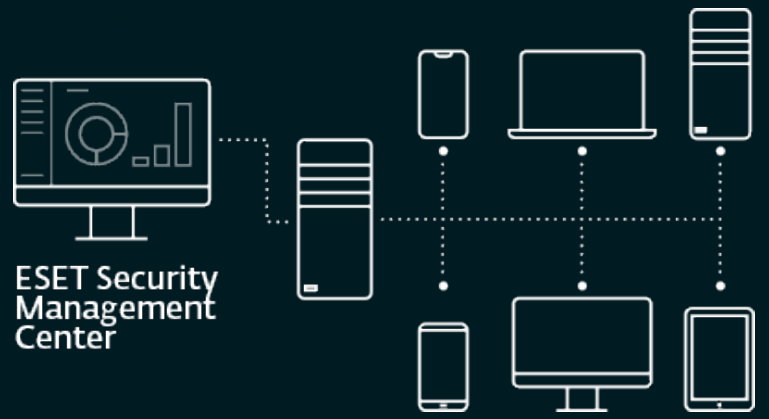
Filtrage URL

Détection comportementale



Protection des mobiles





- Contrôle des applications
- Mobile Device Management
- Blocage de l'appareil en cas de perte ou vol
- Protection contre les ransomwares

iOS

Les menaces évoluent
Les solutions aussi !

Les failles “Zéros days”

Des attaques impossible à détecter par les outils anti-malware…

Définition

Vulnérabilité inconnue n’ayant pas fait l’objet d’une publication ou d’un correctif connu

Problématiques

- Menaces inconnues
- Comportements polymorphes
- Faux positifs

Solutions

- Analyse comportementale
- Machine learning
- Cloud sandboxing

Une seule couche de défense n’est plus suffisante

Le Cloud Sandboxing

Une technologie de sandboxing basée sur le cloud pour détecter de nouveaux types de menaces jamais vus auparavant.

Détection basée sur le comportement

Détection des menaces Zero-day

Cloud sandbox

Le Cloud Sandboxing

Déploiement simple et sans coût d'infra

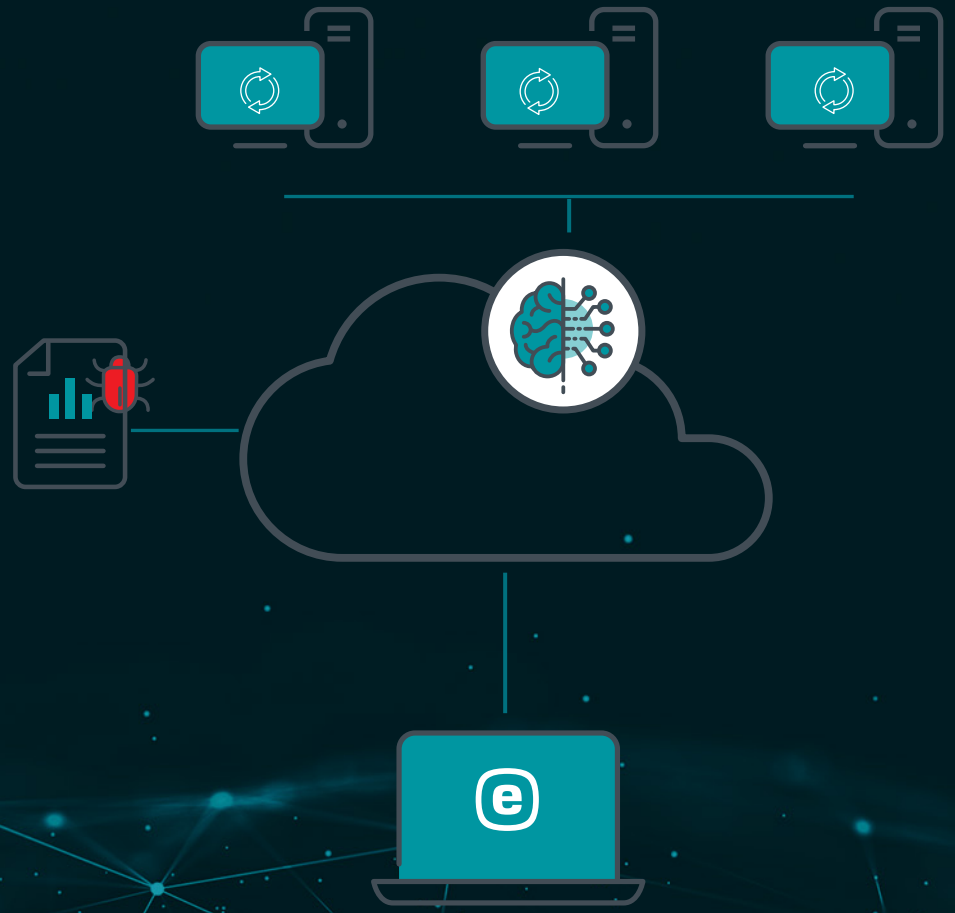
Pas d'infrastructure = pas d'impact sur les performances

Analyse en moins de 5 minutes

Protection des utilisateurs pendant l'analyse

Simulation dans le temps

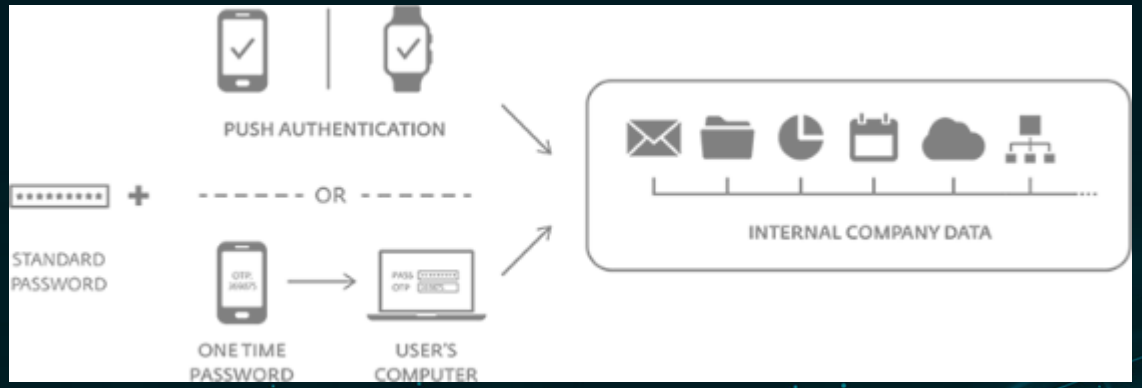
Ressources infinies dans le Cloud ESET



Double Authentification

Une **authentification à double facteurs** qui vous aide à
sécuriser vos accès en toute simplicité et à **respecter les réglementations**

- Installation possible sans AD
- Remplace le token physique
- Conforme aux exigences légales
- Simple d'utilisation



- Pas de matériel supplémentaire requis
- Gestion à distance
- Compatible avec plusieurs OS de mobiles
- Authentification push
- Installation simple
- Renforcement des accès aux systèmes d'exploitation, VPN, machines distantes…
- Utilisation des tokens via SMS ou l'application mobile
- Protection contre les risques liés aux mots de passe standards


eset
LAFI

12 années de partenariat

ESET
Partenaire
Silver

+ de 150 clients équipés

+ de 30 000 machines protégées

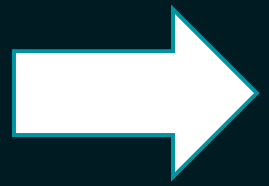
P.O.C

Continuité de service

Évaluation sur mesure

Support avant-vente

Multi-plateforme



Aucune surprise suite à l'évaluation

MERCI !

30 YEARS OF
CONTINUOUS
IT SECURITY
INNOVATION