



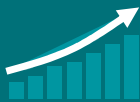
ENJOY SAFER TECHNOLOGY™

# Enjoy Safer Technology™





**13 Laboratoires**  
**400+ chercheurs**  
**1600+ Employés**



**4<sup>ème</sup> éditeur mondial**  
**1er éditeur Européen**



**Société européenne**  
**Siège Bratislava en**  
**Slovaquie**



**Légèreté, Fiabilité,**  
**Facilité**



**30 YEARS OF**  
**CONTINUOUS**  
**IT SECURITY**  
**INNOVATION**

**EMPLOYEES**

**1600**

---

**R&D**

**512**

# 13 centres de recherche à travers le monde

Argentina [1]  
Australia [2]  
Brazil [1]  
Canada [2]  
Czech Republic [3]  
Germany [2]  
Japan [1]  
Mexico [1]  
Poland [1]  
Romania [1]  
Singapore [1]  
Slovakia [3]  
United Kingdom [2]  
United States [1]

**San Diego**  
Regional Center

**Bratislava**  
Headquarters

**Singapore**  
Regional Center

**Buenos Aires**  
Regional Center



Plus de  
**110 000 000**  
d'utilisateurs





Plus de  
**900 000 000**  
d'utilisateurs



chrome









# Technologies





Pro-active detection



#Petya #Wannacry #Ransomware



Bouclier anti-Ransomware



Analyse réseau



Live-Grid | Cloud Protection



# Les 3 piliers de nos solutions



ESET  
LiveGrid



Machine  
Learning



Expertise  
Humaine


## HIPS

  
UEFI Scanner

  
Network Attack Protection


  
Reputation & Cache

  
In-product Sandbox

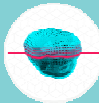
  
Exploit Blocker

  
Ransomware Shield

  
DNA Detections

  
Cloud Malware Protection System

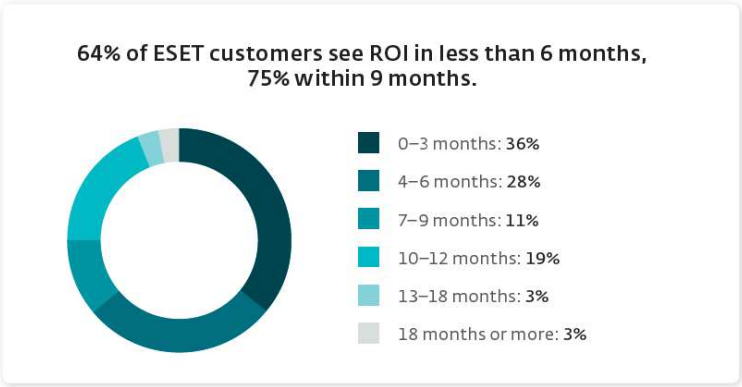
  
Botnet Protection

  
Advanced Memory Scanner

  
Script Scanner (AMSI)

- PRE EXECUTION
- EXECUTION
- POST EXECUTION

# Récompenses



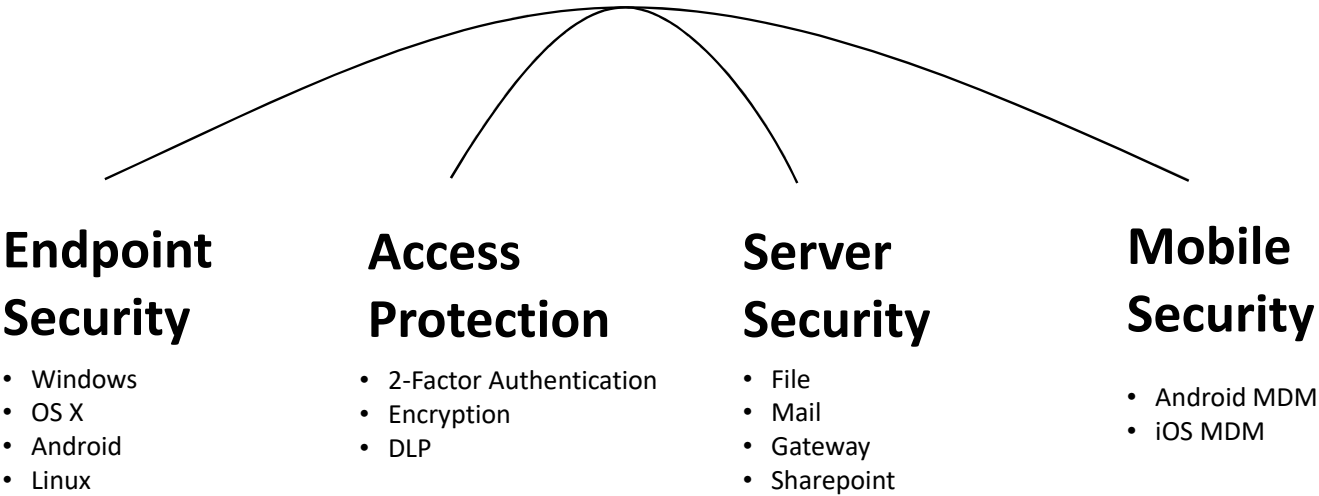
TechValidate survey of 552 users of ESET Security Solutions answering question: "Please estimate how long did it take to realize a return on your investment with ESET security solutions?" Source > <https://www.techvalidate.com/product-research/eset-security-solutions/charts/3DB-C32-728>



# Licences et produits



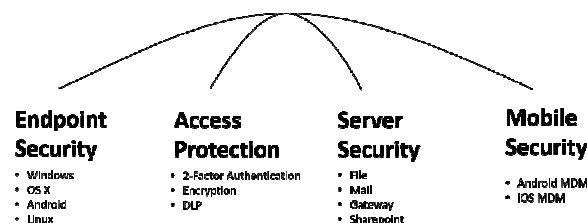
# Produits





# Produits

## Au-delà des protections conventionnelles



### Sandboxing cloud avancé

- **ESET Dynamic Threat Defense**
- Détection basée sur le comportement
- Détection des menaces zero-day
- Catégoriser/Bloquer
- Rapports détaillés

### EDR

- **ESET Enterprise Inspector**
- Collecte des événements en temps réel
- Fournit un filtrage très poussé et permet la recherche d'IOC
- Utilise les systèmes de réputation ESET
- Permet aux clients de créer leurs propres règles de notification
- Mise en place de solutions de blocage et de résolution d'incidents

# Licences bundles

Brique de Sécurité ESET	ESET Endpoint Protection Standard Console sur site (aucune limitation)	ESET Endpoint Protection Advanced Console sur site (aucune limitation)	ESET Secure Business Console sur site (aucune limitation)	ESET Endpoint Protection Advanced Cloud Console hébergée (Max 250 postes)	ESET Secure Business Cloud Console hébergée (Max 250 postes)
Mail Security			✓		✓
Endpoint Security		✓	✓	✓	✓
Virtualisation Security	✓	✓	✓	✗	✗
File Security	✓	✓	✓	✓	✓
Mobile Security	✓	✓	✓	✓	✓
Endpoint Antivirus	✓	✓	✓	✓	✓
Administration centralisée	✓	✓	✓	✓	✓

# Gestion des licences



# Support et Services ESET

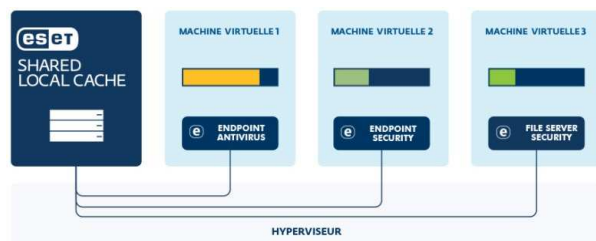
SERVICES	DESCRIPTIFS	COUTS
<b>SUPPORT NIVEAUX 1 &amp; 2</b>	Accès au support technique France de 9h à 19h tous les jours de la semaine   Outil de gestion de tickets	Inclus dans la licence
<b>SUPPORT NIVEAU 3</b>	Lien entre le support technique France et le support international ESET	Inclus dans la licence
<b>SUPPORT INTERNATIONAL 24/7</b>	Accès au support international ESET 24h/24 et 7j/7 en anglais	Sur devis

# Protection des environnements virtuels

## SHARED LOCAL CACHE

### Solution avec agent optimisé

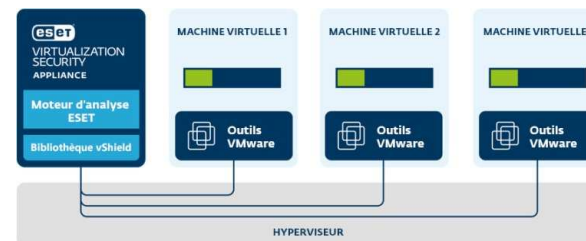
- Compatibilité avec tous les hyperviseurs
- Windows, Linux, Mac et Windows Server
- Solution pour les environnements virtuels à forte densité
- Appliance virtuelle
- Gestion centralisée via ERA
- Protection multicouches



## VIRTUALIZATION SECURITY FOR VMWARE VSHIELD

### Solution sans agent

- Compatibilité VMware vSphere
- Windows et Windows Server
- Solution pour les environnements virtuels à forte densité
- Appliance virtuelle
- Gestion centralisée via ERA
- Protection antivirus



# Protection des postes de travail

Antivirus – Antispyware - Antimalwares

Faible impact système

Exclusions basées sur le Hash

Horodatage

Mises à jour automatiques

Exploit blocker

Bouclier système (HIPS)

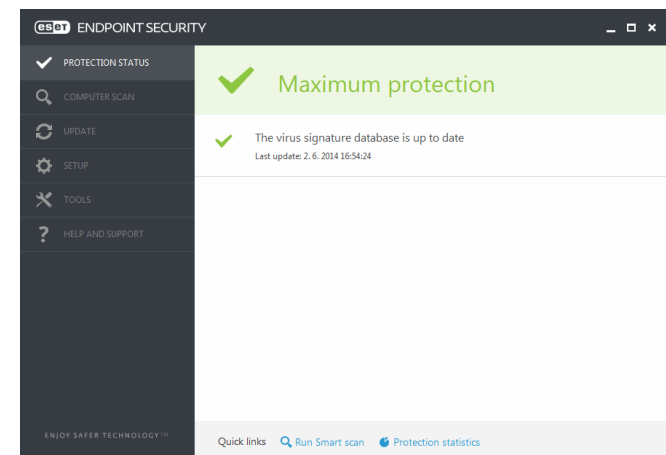
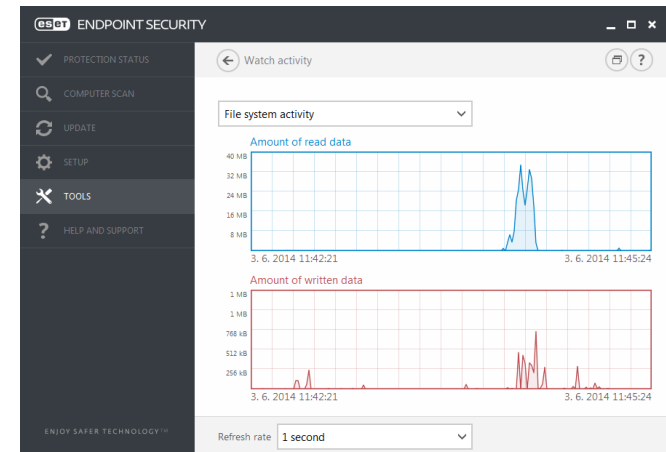
Support Microsoft NAP

SysInspector

DLP

Version Security :

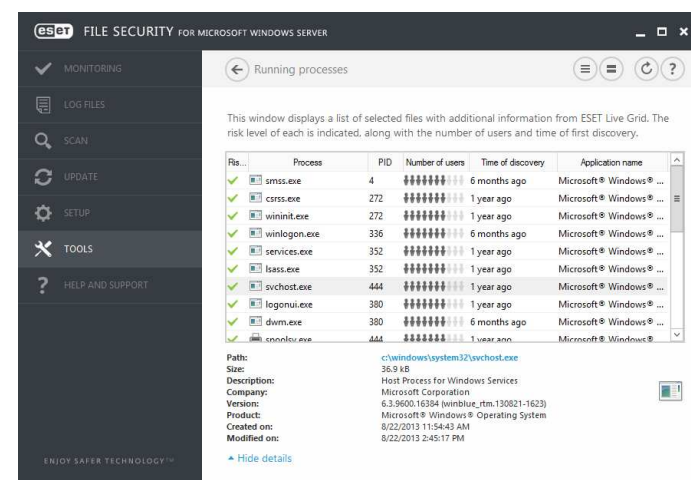
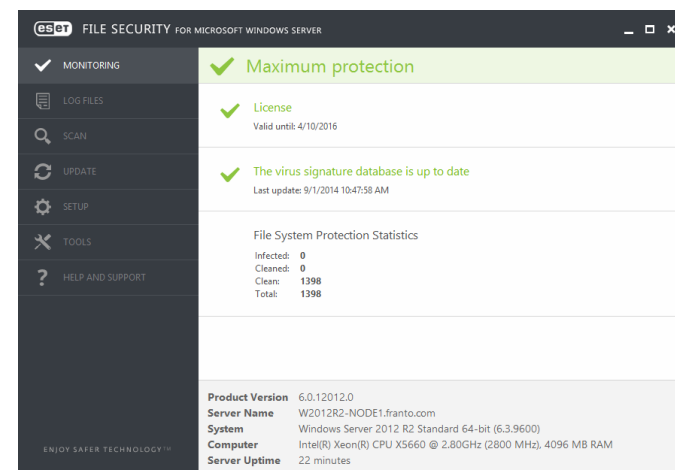
- Pare-feu
- Antispam
- Filtrage web





# Protection des serveurs

Windows et Linux  
 Antivirus & Antispyware  
 Exploit blocker  
 Analyse mémoire avancée  
 Optimisation pour les environnements virtuels  
 Exclusions automatiques  
 Compatibilité Cluster  
 Analyse stockage  
 Compatibilité WMI  
 Installation par composants  
 Faible impact système





# Contacts



# Vos contacts privilégiés

## Nicolas CHAUBARD

Resp. Commercial clients finaux

Tel. +33(0)1.55.89.09.62

Mob. +33(0)6.72.42.76.86

[Nicolas.c@eset-nod32.fr](mailto:Nicolas.c@eset-nod32.fr)

## Benjamin MALIZIA

Responsable Avant-Vente

Tel. +33 (0)1.72.59.42.04

Mob. +33 (0)6.87.45.68.10

[benjamin.m@eset-nod32.fr](mailto:benjamin.m@eset-nod32.fr)







Démo



# ESET est leader

## Dans le Forrester Wave™

## Endpoint Security Suites 2018

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.



# ESET est l'unique challenger Dans le Gartner Magic Quadrant 2018

Gartner, "Magic Quadrant for Endpoint Protection Platforms," Ian McShane, Avivah Litan, Eric Ouellet, Prateek Bhajanka, 24 January 2018.

Gartner does not endorse any vendor, product or service depicted in its research publications. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



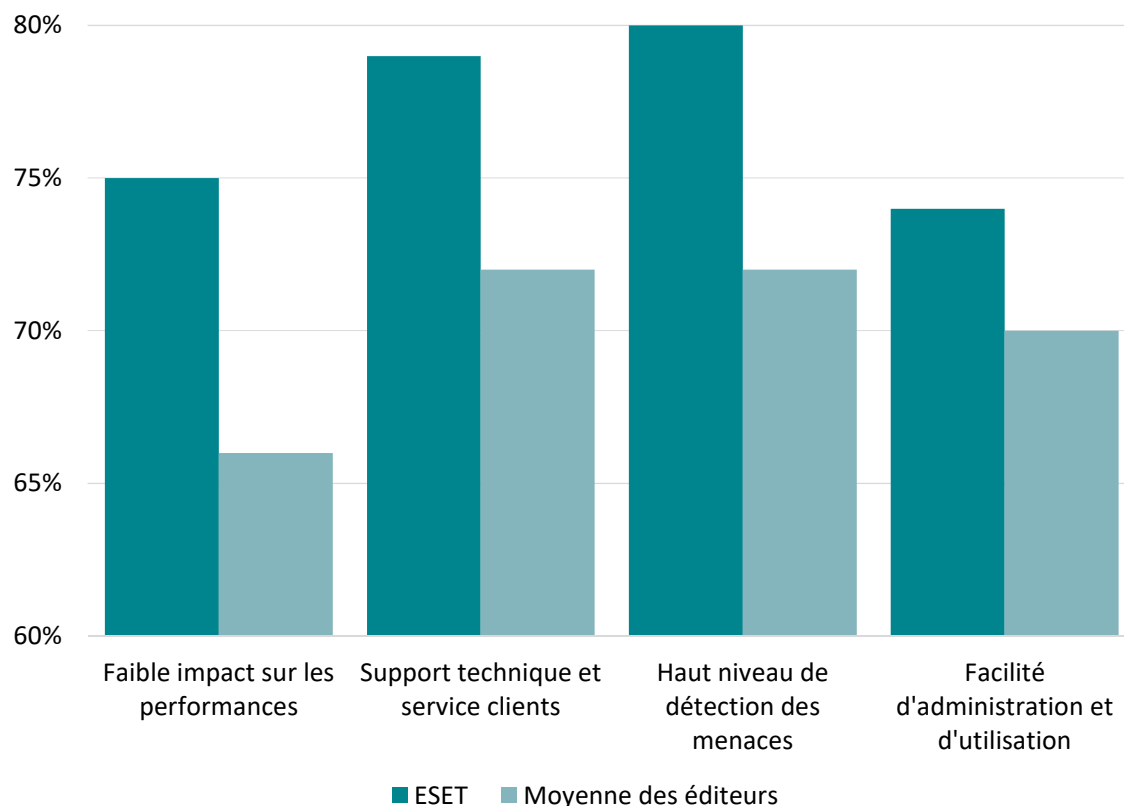


## Top 5 Mondial - Editeurs de solutions de sécurité pour entreprises



Source: Gartner Market Share: All Software Markets, Worldwide, revenue in USD, Business (EPP) Endpoint Security

# Pourquoi nos clients nous choisissent ?



- Faible impact sur performances
- Haut niveau de détection des menaces
- Facilité d'utilisation des solutions
- Qualité du service client et du support technique
- Compétitivité des offres

Source: TNS survey – US, UK, DE, JP, NL – 2952 participants

# Blog d'informations

welive  
security™

BY **eset**

ÉDUCATION À LA  
CYBERSÉCURITÉ



15 cours en ligne gratuits sur la sécurité



## MEMBRE DU DISPOSITIF

**RMALVEILLANCE.GOUV.FR**  
du risque numérique

Cinq conseils pour se remettre d'un piratage



BRÈCHE DE DONNÉES

2,6 milliards de données ont été compromises

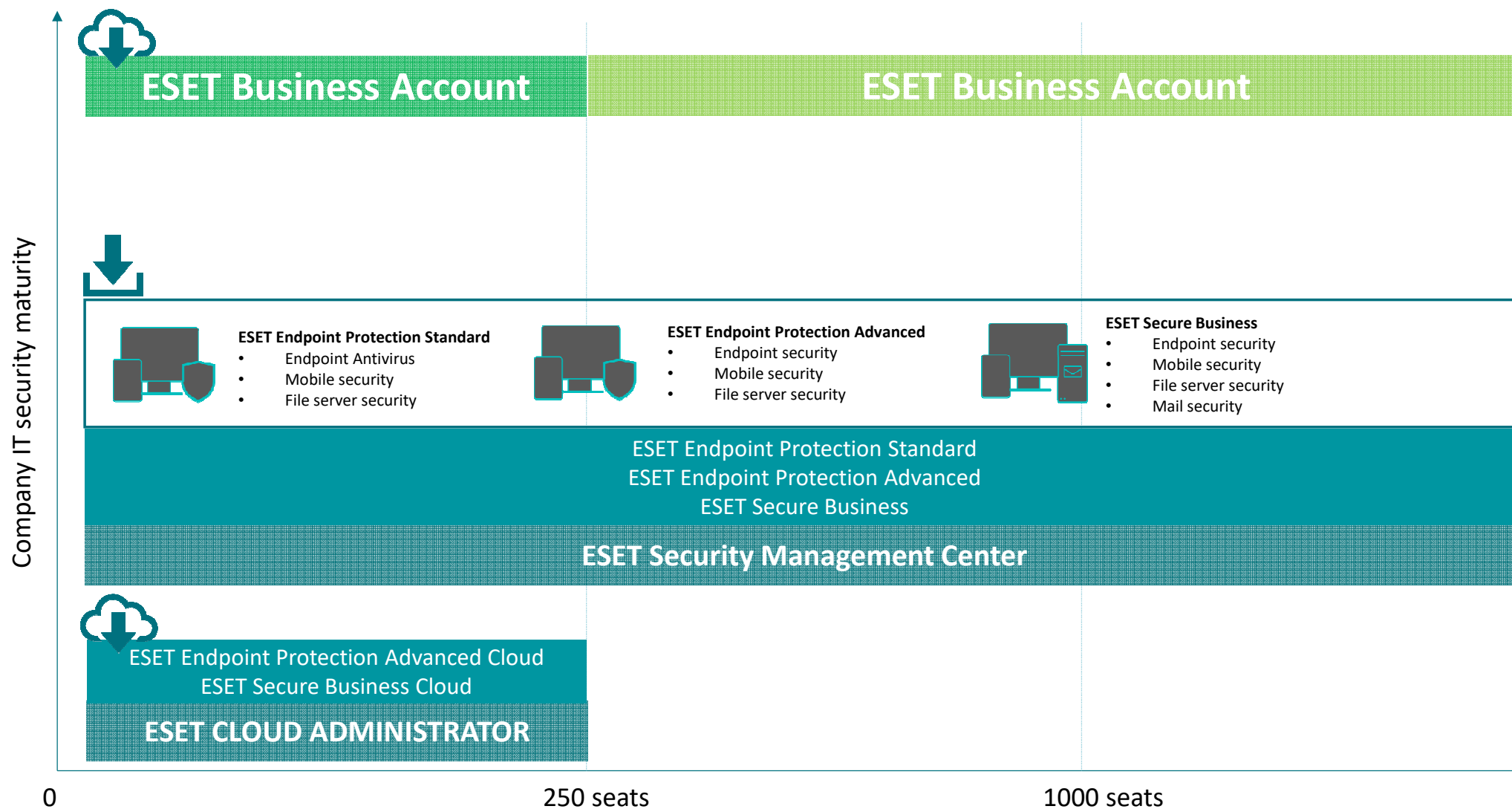


HAMEÇONNAGE

**Mordre à l'hameçon : Comment éviter d'être confondu avec un appât**

Les meilleurs conseils pour vous aider à éviter de recevoir ou d'envoyer des courriels ressemblant à des tentatives d'hameçonnage.

## Bundles Entreprises ESET V7 administrables par ESMC



# ECA / ESMC quelles différences ?

Différence	ECA	ESMC
Hébergement	Dans le Cloud ESET - AWS	Sur site du client protégé
Limitations de parc	Limitation à 250 users	<b>Aucune limitation</b>
OS supportés	Windows et Mac OS	Windows – Mac OS – <b>Linux Android - IOS</b>
Composants possibles	Agent – Rd Sensor Outils de déploiement	Agent – Rd Sensor Outils de déploiement - <b>MDM</b>
Virtualisation	Installation classique	Optimisation possible
Active Directory	Pas de synchro	<b>Synchro possible</b>
Groupes dynamiques	Préconfigurés	<b>Personnalisables</b>
Notifications	Préconfigurées	<b>Personnalisables</b>
Certificats	Managés par ESET	<b>Possibilité de création, personnalisation, export/import</b>
Droits d'accès	Accès simplifiés par <b>EBA</b> (Lecture/écriture sur ECA) Interface non multi-tenants	Accès configurables via <b>ESMC</b> Droits paramétrables <b>Interface multi-tenants</b>
Déploiements	Live Installer – GPO - Script	<b>AD Sync</b> – GPO – Script – RD Sensor Report - Agents



Au delà des protections conventionnelles







DYNAMIC THREAT DEFENSE



# DYNAMIC THREAT DEFENSE

Technologie de sandboxing cloud avancée  
pour détecter les menaces inconnues

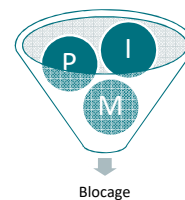
---



Détection basée sur  
le comportement



Détection des  
menaces zero-day



Catégoriser  
Bloquer



Rapports  
détaillés



# DYNAMIC THREAT DEFENSE

## Prérequis au fonctionnement



ESET Business  
Account



ESET Security  
Management  
Center



Solutions de  
sécurité V7



Licence EDTD  
active

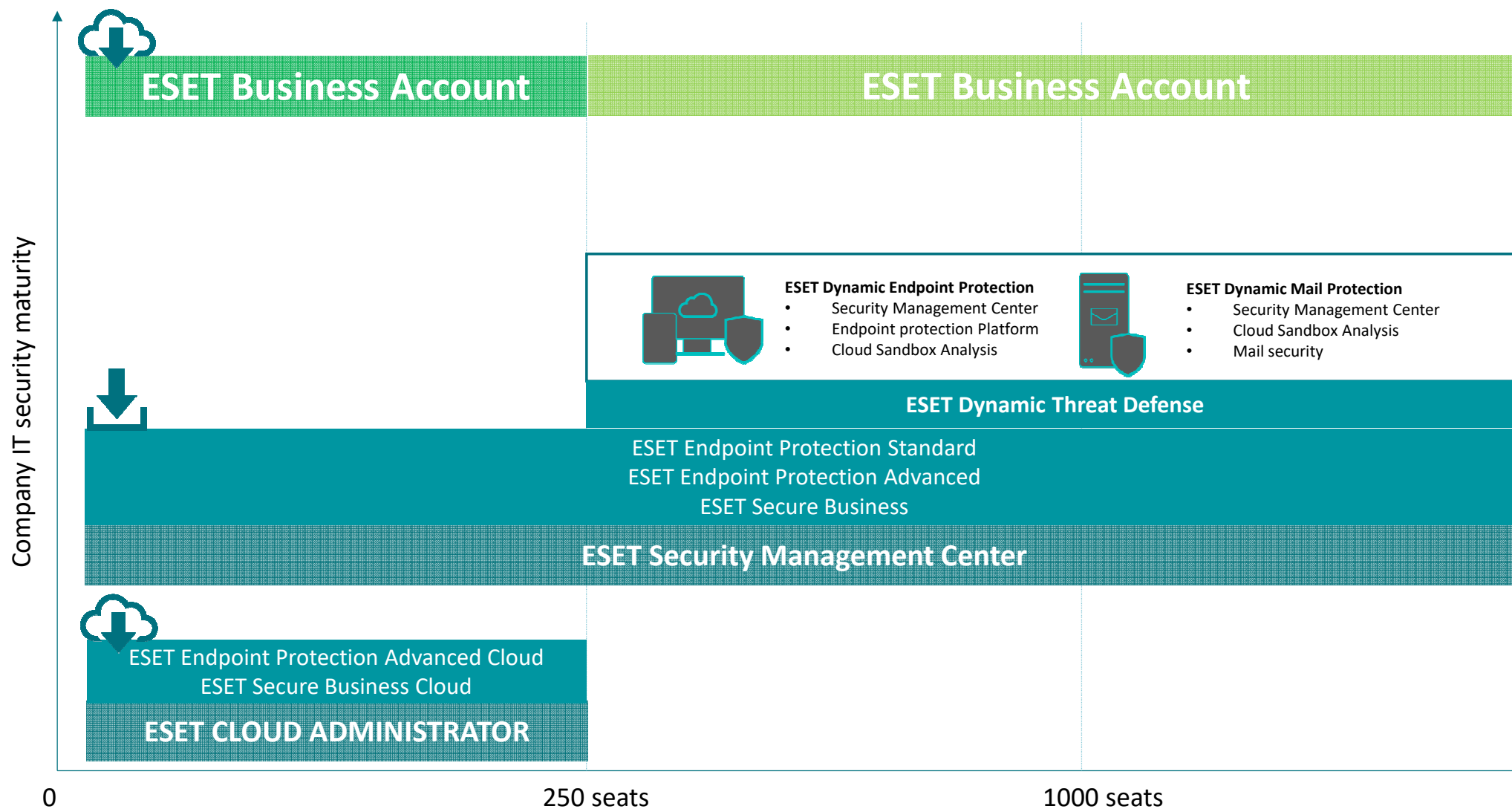


# DYNAMIC THREAT DEFENSE

## Licensing



## Bundles Entreprises ESET V7 administrables par ESMC





ENTERPRISE INSPECTOR



# ENTERPRISE INSPECTOR

- Les menaces sont modifiées pour échapper à la détection
- Délai de détection trop long
- Les attaquants n'utilisent pas seulement des fichiers exécutables



# ENTERPRISE INSPECTOR

## Comment ça fonctionne ?

- Collecte des événements en temps réel
- Fournit un filtrage très poussé et permet la recherche d'IOC
- Utilise les systèmes de réputation ESET
- Permet aux clients de créer leurs propres règles de notification
- Mise en place de solutions de blocage et de résolution d'incidents





# ENTERPRISE INSPECTOR

Solution EDR Next-Gen pour lutter  
contre les APTs, menaces ciblées, Zero-day...

---



## Detection

Identifier une anomalie  
malveillante  
automatiquement



## Visibilité

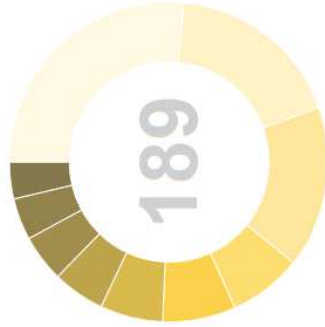
Qu'est-ce qui est affecté?  
Quand est-ce arrivé?  
Comment est-ce arrivé?



## Réponse

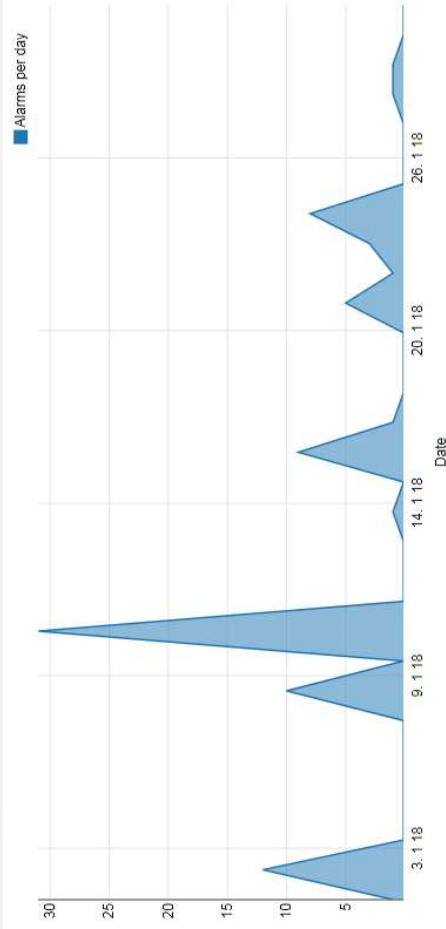
Bloquez le !  
Retirez-le !

Top 10 Unresolved Threat and Warning Alarms



- Detected by ESET Endpoint Security product (50)
- Unpopular process has started from %Temp% [Z0402] (34)
- EXE patching or dropping [B0304] (31)
- Common AutoStart registry modified by unpopular process [A0103]...
- Processes killing from commandline [B0401] (14)
- Process with a suspicious extension has started [Z0406] (12)
- Unpopular process with a suspicious extension has started [D0423]...
- Windows Firewall rules manipulation [B0202] (9)
- File modified in %startup% folder [A0127] (8)
- Unpopular process has been added to startup folder [D0115] (7)

Threat and Warning Alarms

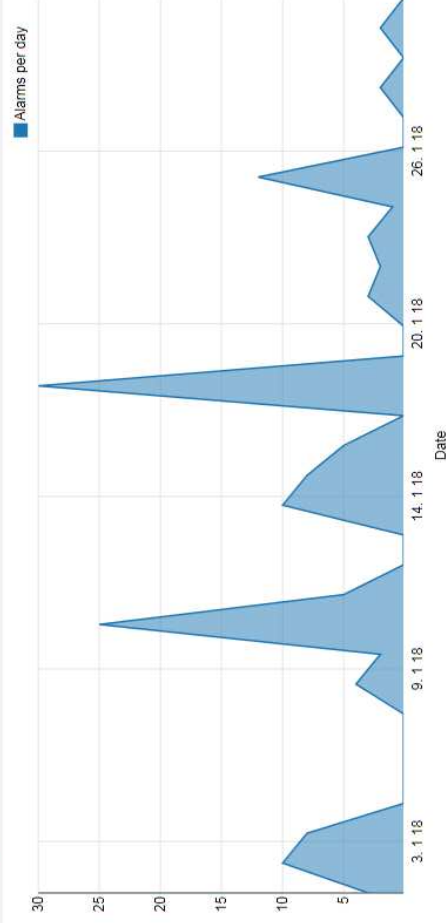


Top 10 Unresolved Informational Alarms

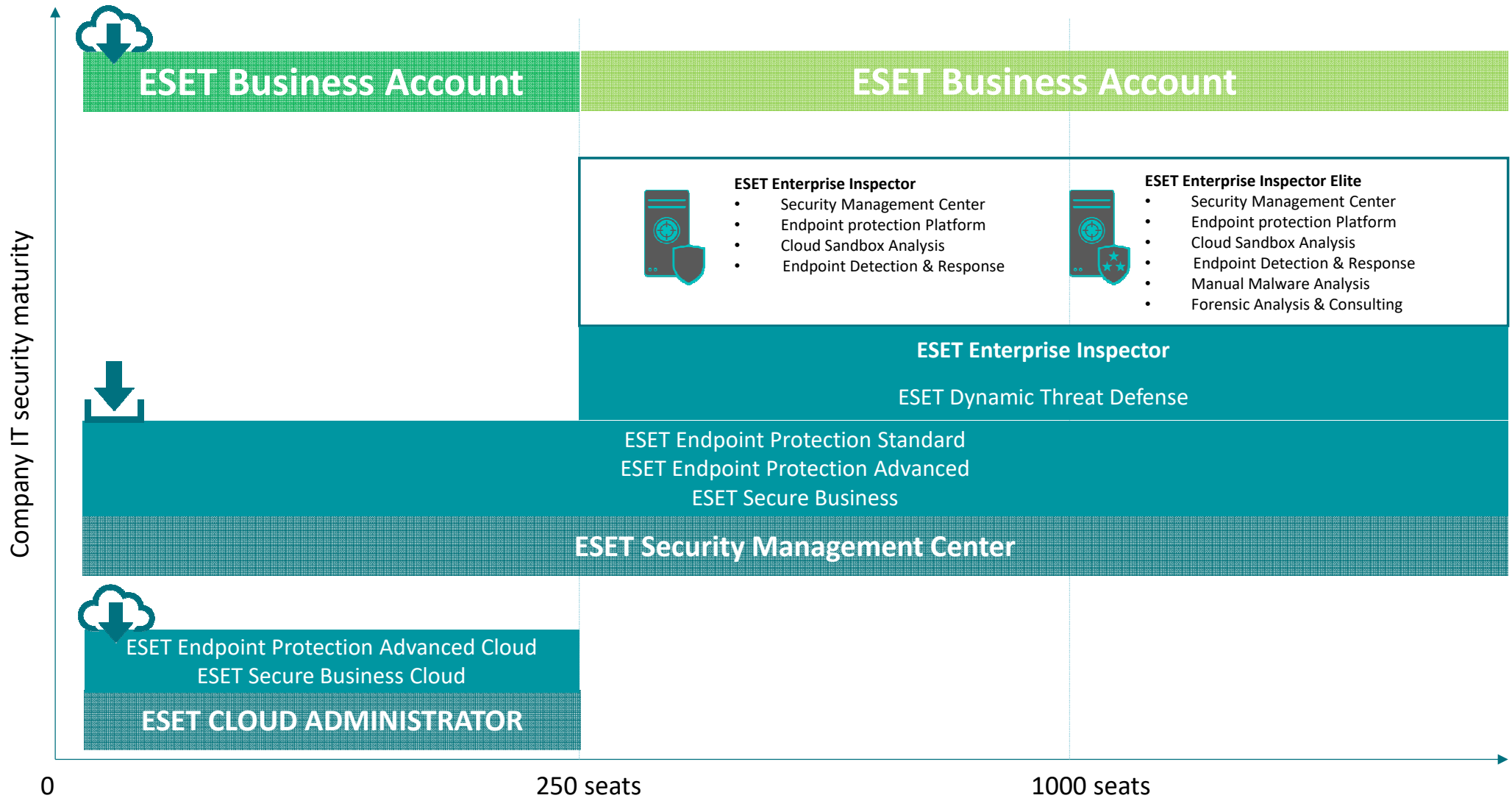


- System utility was executed test [A0403] (99)
- Unpopular process has started from %AppData%\%ProgramData% [Z04...
- Process started from desktop [Z0405] (30)
- Management of the services from commandline [B0403] (28)
- Cmd.exe executed with '/c' by unpopular process [A0400] (16)
- Autorun.inf file was created/modified [A0301] (12)
- Service installation or modification [B0402] (8)
- Saving script file [Z0301] (8)
- Autorun.inf file was deleted [A0301] (5)
- Powershell suspicious activity executed [D0414] (4)

Informational Alarms



## Bundles Entreprises ESET V7 administrables par ESMC





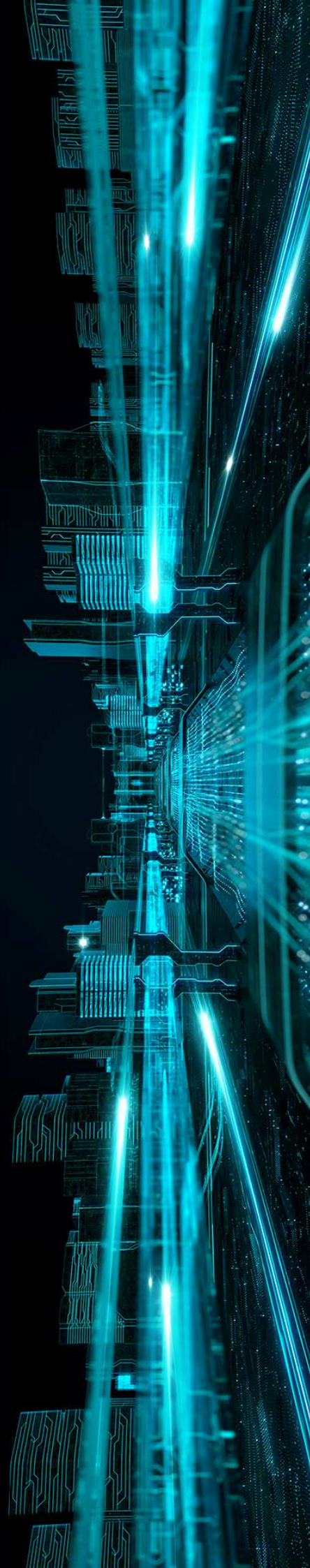


TESTEZ NOUS !



# 30

30 YEARS OF  
CONTINUOUS  
IT SECURITY  
INNOVATION







Solutions de chiffrement



# Ce que précise le RGPD

## Article 32 EU RGPD "Sécurité du traitement"

=> Raison: 83, 74, 75, 76, 77

=> administrative fine Art. 83 (4) lit a

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité approprié, y compris entre autres, selon les besoins:

a) la pseudonymisation et le **chiffrement** des données à caractère personnel;

=> Article 4

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services;

c) des moyens permettant de restaurer la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer le niveau de sécurité approprié.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la transmission, de la conservation ou du traitement non autorisé de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données.

=> Raison: 75

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 est considérée comme une mesure technique et organisationnelle appropriée, à moins qu'elle ne soit incompatible avec les mesures prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ne traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit, des données à caractère personnel qu'elle ne doit pas traiter.

La pseudonymisation et le **chiffrement** des données à caractère personnel

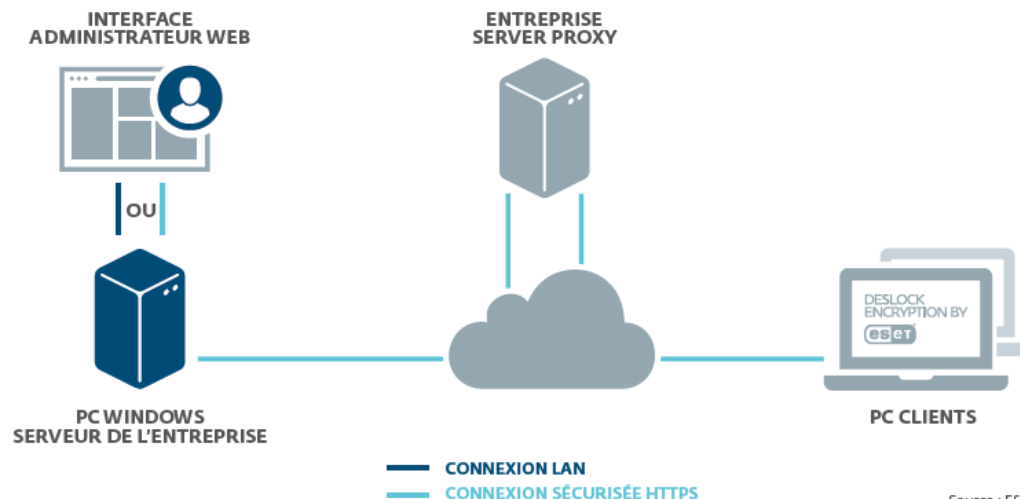
# ESET Endpoint Encryption



## Chiffrer les données pour les rendre illisibles

- Chiffrement des informations stockées sur les postes de travail, serveurs, médias amovibles
- Plusieurs options dans le chiffrement
- Collaboration en toute sécurité
- Chiffrement puissant norme FIPS 140-2 et algorithme AES 256 bits

La solution a été reconnue par le laboratoire indépendant AV Comparatives comme **“la référence à suivre en matière de chiffrement** considérant le produit comme performant et simple à configurer”.



Source : ESET



# ESET Endpoint Encryption

## Article 32 EU RGPD "Sécurité du traitement"

=> Raison: 83, 74, 75, 76, 77.  
=> administrative fine: Art. 83 (4) lit a

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature des droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant, y compris entre autres, selon les besoins:

a) la pseudonymisation et le **chiffrement** des données à caractère personnel;

=> Article 4

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures de sécurité.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier du caractère des données à caractère personnel transmises, conservées ou traitées d'une manière susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

## Article 34 EU RGPD

### "Communication à la personne concernée d'une violation de données à caractère personnel"

4  
75, 86, 87, 88  
administrative fine: Art. 83 (4) lit a

1. Lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le **chiffrement**;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser et qu'il n'exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace;

c) si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

... en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès telles que le **chiffrement**



# Solution d'authentification à double facteurs





# ESET Secure Authentication



## Sécuriser les accès aux données

- Protection contre les risques liés aux mots de passe standards
- Authentification à double-facteurs
- Renforcement des accès aux systèmes d'exploitation, VPN, machines distantes...
- Utilisation des tokens via SMS ou l'application mobile

