Comprendre les ransomwares en 2025 :

Principaux enseignements et stratégies de prévention

Digital Security
Progress. Protected.

Paysage des ransomwares

Les ransomwares restent l'une des menaces les plus pressantes pour la cybersécurité en 2025, et continuent d'évoluer à la fois en termes de sophistication et d'impact. Malgré des années de progrès en matière de cybersécurité, les organisations de toutes tailles et de tous les secteurs restent confrontées à des attaques incessantes qui pénètrent leurs défenses grâce à des techniques de plus en plus affinées. L'un des tous derniers développements dans cette lutte permanente est l'utilisation d'**EDR killers**, des malwares conçus pour désactiver les solutions de détection et de réponse pour endpoints (EDR) avant le déploiement des ransomwares. Cela prouve à quel point les auteurs de menaces s'adaptent aux progrès de la sécurité pour exploiter les faiblesses des défenses des entreprises.

Les attaques de ransomwares restent très motivées, non seulement pour réaliser des gains financiers, mais également pour répondre à des objectifs tactiques et stratégiques. Alors que les groupes de cybercriminels déploient des ransomwares principalement dans un but lucratif, les groupes APT (menaces persistantes avancées) peuvent utiliser les ransomwares pour brouiller les pistes ou comme outil destructeur pour perturber les infrastructures critiques, ce qui a souvent des conséquences géopolitiques. L'évolution de l'utilisation des ransomwares rend le paysage des menaces encore plus complexe. Les groupes de ransomwares motivés par le gain et les groupes APT affinent sans cesse leurs techniques, en exploitant les compromissions de la chaîne d'approvisionnement, en exploitant des vulnérabilités zero-day et en recourant à l'hameçonnage assisté par l'IA pour maximiser leur portée et leur impact.

4,91 millions $

Le coût moyen d'une attaque de ransomware en 2024.

Source : *: Rapport d'IBM sur le coût d'une atteinte à la sécurité des données en 2024.*

Dans ce paysage de menaces en constante évolution, la **prévention** reste la mesure la plus efficace pour renforcer la sécurité des organisations. Si la réponse aux incidents et la reprise après sinistre sont essentielles, stopper les ransomwares avant qu'ils ne s'implantent permet de réduire à la fois les perturbations opérationnelles et les pertes financières.

Une stratégie de sécurité préventive, comprenant une gestion robuste des correctifs, une architecture Zero Trust, une protection conçue autour de l'IA, des politiques de gestion des mots de passe, une authentification multifacteur (MFA), la sensibilisation des collaborateurs et une surveillance continue des menaces, permet de réduire considérablement le risque d'infiltration de ransomwares.

En 2025, il est plus important que jamais d'anticiper, prévenir et neutraliser la menace des ransomwares avant qu'elle ne se concrétise. Cela implique de disposer d'une puissante **technologie de remédiation** prête à vous aider à tout moment.

Dernières observations sur les ransomwares

Plusieurs tendances clés des ransomwares en 2024 devraient façonner le paysage des menaces et les stratégies de défense pour 2025. Il est essentiel de les garder à l'esprit pour rester à l'avant-garde de l'évolution des risques.

L'un des événements les plus marquants de l'année 2024 a été le démantèlement de LockBit qui était le principal groupe de ransomwares sous forme de services (RaaS) diffusant la variante de ransomware la plus déployée dans le monde. La disparition de LockBit a créé un vide important dans le paysage des ransomwares. Ce manque a été rapidement comblé par d'autres acteurs, notamment **RansomHub** apparaissant comme **le plus performant à ce jour**.

À la fin du second semestre 2024, RansomHub avait recensé près de 500 victimes, s'imposant ainsi comme un acteur dominant de l'écosystème des ransomwares. Jusqu'à présent, RansomHub a chiffré et exfiltré des données de victimes issues d'un large éventail de secteurs d'activité : technologies de l'information, installations et services gouvernementaux, santé, services d'urgence, alimentation et agriculture, services financiers, entreprises commerciales, fabrication essentielle, transport ou infrastructures essentielles telles que les communications.

Dans l'environnement cybercriminel hautement compétitif des RaaS, où les gangs innovent et ajustent continuellement leurs programmes d'affiliation pour attirer plus de partenaires et augmenter la rentabilité, ESET s'attend à ce que RansomHub maintienne sa position dominante tout au long de l'année 2025. Cela est dû non seulement à ses **tactiques agressives** et ses méthodes sophistiquées pour contrôler les réseaux compromis et exploiter les vulnérabilités des systèmes, mais également à sa **capacité à attirer des affiliés** anciennement associés à LockBit et BlackCat.

Tandis que le modèle RaaS continue d'évoluer, les auteurs de ransomwares adoptent de plus en plus de techniques spécialisées pour échapper à toute détection et faire plus de dommages. Même si les EDR killers sont utilisés depuis longtemps par les groupes de ransomwares, leur prévalence s'est accrue. Certains gangs développent désormais des outils personnalisés et les proposent via leurs programmes de RaaS. En parallèle, de nombreux acteurs du secteur des ransomwares qui entrent dans l'écosystème des RaaS suivent les tendances des groupes établis, développant souvent leurs outils de chiffrement avec Rust ou Go pour assurer une compatibilité multiplateforme et une plus grande portée.

Les **EDR KILLERS** sont des malwares spécialisés conçus pour désactiver les solutions de sécurité en s'appuyant sur des techniques de BYOVD. Les attaquants commencent par installer des pilotes légitimes mais vulnérables, puis les exploitent pour exécuter des actions privilégiées à partir du noyau du système d'exploitation. Cela leur permet de contourner les contrôles de sécurité, mettre fin aux processus de sécurité, et désactiver les mécanismes de détection et de protection.

Les EDR killers sont devenus un élément courant des attaques de ransomwares. ESET s'attend donc à ce que les acteurs les plus avancés améliorent ce type d'outils en 2025, les rendant de plus en plus sophistiqués, opaques et difficiles à détecter. Cette tendance montre que les outils de sécurité tels que l'**EDR sont une épine dans le pied des cybercriminels**, qui s'efforcent de les désactiver ou au moins de les contourner.

Les techniques avancées et les RaaS ne devraient pas être évoqués sans reconnaître l'implication et le rôle des APT. Ces groupes utilisent les ransomwares non seulement pour réaliser des gains financiers, mais aussi pour atteindre des objectifs stratégiques plus étendus. Les groupes APT suivants se sont récemment impliqués davantage dans les attaques de ransomwares :

Moonstone Sleet (aligné sur la Corée du Nord)

Connu pour avoir développé et déployé son propre ransomware FakePenny, Moonstone Sleet utilise les ransomwares principalement à des fins financières. Anciennement appelé Storm-17, Moonstone Sleet cible les secteurs de la finance et du cyberespionnage. Ses méthodes consistent à utiliser des logiciels, comme PuTTY, intégrant des chevaux de Troie pour l'accès initial, diffuser des jeux malveillants et des paquets Node Package Manager (NPM), déployer des downloaders de malwares personnalisés et créer de fausses sociétés de développement de logiciels telles que StarGlow Ventures et C.C. Waterfall.

Ces fausses entreprises contactent des victimes potentielles via des plateformes telles que LinkedIn, Telegram, des réseaux de freelances et des emails.

ChamelGang (aligné sur la Chine)

Ce groupe utilise des ransomwares pour détourner l'attention de ses opérations secrètes, ce qui rend plus difficile la détection de ses principales activités par les défenseurs.

Ce groupe, parfois appelé CamoFei, utilise la souche de ransomware CatB dans des attaques qui touchent des organisations de premier plan dans le monde entier, y compris des organisations gouvernementales telles que la présidence du Brésil ou des infrastructures critiques telles que l'All India Institute of Medical Sciences (AIIMS), une université et un hôpital publics de recherche médicale.

Pioneer Kitten (aligné sur l'Iran) et Andariel (aligné sur la Corée du Nord)

Ces groupes ont été associés à des attaques de ransomwares, principalement en tant que fournisseurs d'accès initial. Ils vendent probablement cet accès à d'autres cybercriminels pour en tirer un bénéfice financier. Le premier attaque principalement les secteurs de la défense, de l'éducation, de la finance et de la santé, tandis que le second vise les infrastructures critiques et les organismes de soins de santé, en particulier aux États-Unis.

Pioneer Kitten est également connu sous les noms de Fox Kitten, UNC757, Parisite, RUBIDIUM et Lemon Sandstorm, et utilise un large éventail de techniques. Andariel est considéré comme un sous-ensemble du groupe Lazarus et a été attribué au Bureau général de reconnaissance de la Corée du Nord.

Les entreprises et différentes organisations ne sont vraisemblablement pas la seule cible des attaques de ransomwares. Les auteurs de menaces étendent de plus en plus leurs actions et ciblent systématiquement le **grand public**. En août 2024, le ransomware Magniber a lancé une campagne mondiale à grande échelle ciblant les utilisateurs finaux ordinaires et chiffrant leurs appareils dans le monde entier.

Bien que de telles actions aient déjà été observées dans le passé, cette campagne a marqué un changement important dans les stratégies de ciblage des ransomwares, principalement en raison de l'ampleur et de la vaste diffusion de l'attaque, qui se concentre sur les utilisateurs individuels qui ne disposent souvent pas de mesures de cybersécurité efficaces.

Le ransomware Magniber a été diffusé via des téléchargements de malwares, de fausses mises à jour et des générateurs de clés, exigeant des rançons allant de 1 000 à 5 000 $ pour le déchiffrement. Les vulnérabilités zero-day de Windows, les fausses mises à jour de Windows et de navigateurs, ainsi que les logiciels piratés et les générateurs de clés vérolés font partie des méthodes utilisées pour diffuser Magniber.

Le grand public doit donc rester vigilant et proactif dans ses pratiques de cybersécurité. En adoptant des mesures préventives, les particuliers peuvent réduire considérablement le risque d'être victimes d'une attaque de ransomware.

Le montant des demandes de rançon visant des particuliers a augmenté pour atteindre

5 000 $

en 2024.

Source : *BleepingComputer : La recrudescence des attaques du ransomware Magniber touche le grand public dans le monde entier*

Prévenir plus, gérer moins

Les ransomwares sont généralement l'étape finale précédée par d'autres menaces telles que l'hameçonnage, l'exploitation de vulnérabilité, les attaques par brute force, les identifiants compromis, les downloaders ou les malwares personnalisés. De nombreuses attaques de ransomwares sont détectées dès le début du cycle d'une attaque, et ce n'est que lorsque les attaquants parviennent à contourner les défenses de leurs victimes et tentent finalement de déployer un ransomware que l'on peut parler d'attaque de ransomware.

Pour prévenir efficacement les attaques de ransomwares, les entreprises doivent adopter une approche de sécurité multicouche intégrant l'automatisation à chaque étape du cycle d'une attaque. Cela peut être considéré comme une **approche axée sur la prévention** que de nombreuses organisations et entreprises reconnaissent de plus en plus comme une stratégie à fort potentiel. Les raisons ne font aucun doute.

Tout d'abord, la **formation et la sensibilisation des collaborateurs** sont essentielles, car l'hameçonnage reste l'un des principaux vecteurs de ransomwares. Les collaborateurs doivent connaître les signes courants de l'hameçonnage et comprendre l'importance de ne pas cliquer sur des liens inconnus ni de télécharger des pièces jointes non sollicitées.

Former régulièrement le personnel à reconnaître les tentatives d'hameçonnage, utiliser des mots de passe robustes et activer l'authentification multifacteur peut réduire les risques de manière significative. Il est également important de **protéger les postes** au moyen d'un antivirus robuste, de solutions antimalwares et d'outils de détection et de réponse (EDR), car ils sont essentiels pour détecter et bloquer les activités malveillantes.

Aucune solution d'EDR n'est totalement à l'abri des EDR killers, car les attaquants exploitent les vulnérabilités de pilotes légitimement signés pour exécuter du code malveillant dans le noyau du système d'exploitation. Ces pilotes, une fois chargés dans Windows, peuvent être utilisés pour désactiver les outils de sécurité. Les produits ESET bloquent efficacement de nombreux pilotes vulnérables, et les analystes et les administrateurs d'ESET peuvent aider les clients à renforcer leurs défenses. En configurant des paramètres dstricts d' Application Potentiellement Indésirable, seuls les pilotes les plus récents sont autorisés. Cette approche peut être guidée par les conseils d'un expert.

Il est également important de renforcer le système d'exploitation avec des règles WDAC, ce qui ajoute à une stratégie de prévention à long terme qui est nécessaire en soi. Ces conseils d'experts peuvent s'avérer essentiels pour faire face aux EDR killers.

Les **mesures de sécurité réseau** telles que les pare-feu, les systèmes de détection d'intrusion (IDS) et la segmentation du réseau, qui permettent de contrôler et surveiller le trafic, empêcher les accès non autorisés et limiter la propagation des ransomwares, sont d'autres mesures à maîtriser.

Pratiquement aucune de ces mesures ne peut être mise en œuvre sans une **gestion régulière des correctifs** qui veille à ce que tous les systèmes et logiciels soient à jour avec les tous derniers correctifs de sécurité, comblant ainsi les vulnérabilités que les attaquants pourraient exploiter.

67 %

des RSSI ont déclaré avoir augmenté leurs budgets de cybersécurité en 2024 par rapport à 2023.
Source : *IANS, Rapport de référence sur les budgets de sécurité pour 2024*

La mise en œuvre de contrôles d'accès fondés sur le principe du moindre privilège et l'adoption d'un **modèle de sécurité Zero Trust** réduisent encore davantage le risque d'accès non autorisé et constituent aujourd'hui une norme de prévention courante pour la cybersécurité. C'est également le cas pour les **sauvegardes régulières** de données critiques, stockées hors ligne ou dans des environnements sécurisés dans le cloud, qui sont vitales pour la reprise des activités en cas d'attaque. Bien entendu, ces sauvegardes doivent être régulièrement testées pour garantir leur efficacité.

En ce qui concerne les opérations quotidiennes et l'utilité de la prévention, les mesures de **sécurité de la messagerie** telles que le filtrage et la protection antispam permettent de bloquer les pièces jointes et les emails malveillants avant qu'ils n'atteignent les utilisateurs. De nombreux incidents sont encore dus à des erreurs humaines et les emails restent le vecteur d'attaque le plus important.

Étant donné que de nombreuses autres applications sont utilisées pour les activités quotidiennes, l'**établissement d'une liste blanche d'applications** revêt également une grande importance. Cela garantit que seules les applications approuvées peuvent fonctionner sur le réseau, empêchant ainsi l'exécution de logiciels non approuvés.

Le fait de disposer d'un **plan de réponse aux incidents** bien conçu et de procéder à des exercices réguliers veille à ce que les organisations soient prêtes à répondre efficacement aux attaques de ransomwares.

Toutes ces mesures contribuent à la mise en place d'un robuste dispositif de cybersécurité grâce à des stratégies de défense proactives qui partent du principe qu'il vaut toujours mieux prévenir que guérir.

Pourquoi ne pas payer de rançon ?

Mais ne soyons pas naïfs : même avec une bonne approche préventive, une attaque de ransomware peut toujours se produire. Les auteurs de menaces affinent constamment leurs tactiques, exploitant des vulnérabilités Zero Day, des faiblesses dans la chaîne d'approvisionnement ou des erreurs humaines pour contourner même les bonnes défenses. Si une attaque peut être perturbatrice, ce n'est pas une situation insoluble. Les organisations qui agissent rapidement, qui s'appuient sur des plans de réponse aux incidents et sur des sauvegardes sécurisées peuvent se rétablir sans céder à l'extorsion. Cela nous amène à un point essentiel : pourquoi le paiement d'une rançon n'est pas la bonne solution.

63 %

des victimes ayant fait appel aux forces de police
ont évité de payer une rançon en 2024.
Source : *Rapport d'IBM sur le coût d'une atteinte à la sécurité des données en 2024.*

Payer des criminels qui ont chiffré vos données signifie :

- Vous validez le modèle économique du crime
- Vous encouragez la poursuite des activités criminelles en les finançant par inadvertance
- Vous permettez aux cybercriminels de rechercher des vulnérabilités zero-day et de développer de nouvelles exploitations
- Vous risquez de subir de nouvelles attaques et de nouvelles demandes de rançon

Le paiement de la rançon ne garantit pas que les cybercriminels fourniront une clé de déchiffrement fonctionnelle. Après tout, il n'y a aucun moyen de les tenir pour responsables ou d'intenter

une action en justice contre eux. Vous pourriez ne pas pouvoir récupérer vos fichiers pour de nombreuses raisons :

- Certaines données peuvent avoir été corrompues pendant le chiffrement, ce qui les rend irrécupérables
- L'outil de déchiffrement fourni peut contenir d'autres malwares, peut ne pas fonctionner correctement ou être beaucoup plus lent que la restauration à partir de sauvegardes.
- Le processus de livraison de la clé de déchiffrement peut échouer de multiples façons, notamment en raison de bugs dans le code de déchiffrement, d'un chiffrement trop compliqué, de complications dans le traitement des paiements (en particulier avec les cryptomonnaies), ou de tactiques de double extorsion exigeant des paiements supplémentaires
- L'attaquant peut simplement agir de mauvaise foi, sans avoir l'intention de fournir une clé de déchiffrement

En pratique, deux arguments principaux plaident en faveur du paiement de la rançon. La première est l'impossibilité de restaurer les données chiffrées à partir de sauvegardes, soit parce que les sauvegardes n'existent pas, soit parce qu'elles sont incomplètes, soit parce qu'elles ont été endommagées. Il peut cependant y avoir des alternatives au paiement. Avant d'effectuer tout paiement, consultez votre prestataire de sécurité :

(a) vérifiez si un outil de déchiffrement est disponible pour la variante spécifique du ransomware, ce qui pourrait permettre une récupération sans paiement

(b) vérifiez si le paiement de la rançon est réputé inefficace pour cette variante particulière

Le second argument courant est que le paiement revient moins cher que de restaurer à partir des sauvegardes. Bien que cela puisse être techniquement vrai en termes de temps et de travail, cela reste une décision fondamentalement erronée pour plusieurs raisons.

Comme indiqué précédemment, les promesses de déchiffrement ne sont pas fiables. Il est fortement probable d'être à nouveau ciblé après avoir effectué le premier paiement – n'oubliez pas que vous n'avez pas affaire à des individus respectueux de la loi – et en payant, vous financez une opération criminelle, ce qui augmente en fin de compte la probabilité d'attaques ultérieures contre d'autres personnes. Le paiement est parfois même illégal et l'une des raisons est que les attaquants peuvent faire l'objet de sanctions.

Comment ESET vous aide avec les ransomwares et la remédiation

Un outil de **remédiation fiable** dans le cadre d'une stratégie proactive axée sur la prévention peut constituer votre meilleure défense face à des décisions difficiles, qu'il s'agisse d'investir massivement dans la récupération des données ou même d'envisager de payer une rançon. Grâce à une puissante technologie de remédiation des ransomwares, vous gardez une longueur d'avance.

ESET Ransomware Remediation est une couche de sécurité entièrement automatisée de l'ensemble de technologies multicouches de la plateforme ESET PROTECT. Conçue pour améliorer la défense contre les ransomwares, elle fonctionne avec Ransomware Shield qui détecte et bloque les comportements suspects. Elle combine prévention et remédiation, offrant ainsi une approche globale en plusieurs étapes pour lutter contre le chiffrement.

94 %

des organisations interrogées ont signalé des tentatives par des cybercriminels de compromettre leurs sauvegardes pendant une attaque en 2024.
Source : *SC World : Des sauvegardes compromises font grimper en flèche les coûts de récupération*

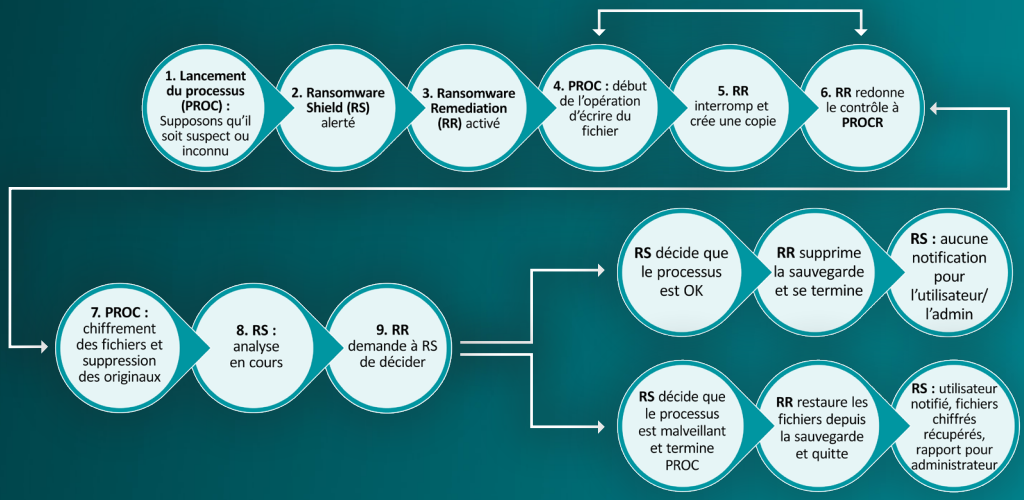
Contrairement aux solutions traditionnelles de remédiation et de retour en arrière qui s'appuient sur le Volume Shadow Copy Service du système d'exploitation et sont souvent une cible de choix pour les attaquants, ESET **utilise une solution propriétaire de mise en cache des fichiers**, qui offre une plus grande flexibilité et une bien meilleure fiabilité. Les opérateurs de ransomwares suppriment ou écrasent fréquemment les copies cachés pour empêcher la récupération, ce qui rend inefficaces les méthodes traditionnelles de retour en arrière.

En revanche, le processus de sauvegarde d'ESET Ransomware Remediation n'est pas un service local ; il fonctionne dans sa **propre section de stockage protégée** sur le disque, dans laquelle les fichiers ne peuvent pas être modifiés, corrompus ou supprimés par les attaquants.

La technologie surveille en permanence tous les processus et intercepte les modifications de fichiers en temps réel. Dès qu'un processus de modification de fichier est détecté, le système de sauvegarde à la volée d'ESET crée des copies des fichiers d'origine, avant même que les systèmes

de réputation des comportements comme Ransomware Shield ne déterminent si l'activité est malveillante. Tout cela en tirant parti des technologies LiveSense d'ESET qui dissèquent et analysent les malwares jusqu'à leurs processus centraux.

En tant qu'approche proactive, ESET Ransomware Remediation veille à ce que les organisations puissent récupérer leurs fichiers instantanément, éliminant ainsi le besoin de payer une rançon. ESET Ransomware Remediation est inclus dans tous les niveaux de la plateforme ESET PROTECT à partir d'ESET PROTECT Advanced. Une version d'évaluation entièrement fonctionnelle de 30 jours est également disponible.



Arbre de processus complexe d'ESET Ransomware Shield et de Ransomware Remediation

QUELS SONT LES AVANTAGES D'ESET RANSOMWARE REMEDIATION ?

- L'outil permet un retour en arrière complet grâce à une restauration transparente et automatisée des fichiers à partir d'un cache sécurisé
- Il ne sécurise que les fichiers affectés par un processus suspect, ce qui réduit considérablement le problème de l'espace disque
- ESET utilise sa propre technologie propriétaire et ne s'appuie pas sur la fonction VSS (Volume Shadow Copy Service) fournie dans les systèmes d'exploitation Microsoft Windows, comme le font d'autres solutions
- La fonctionnalité est activée par défaut dans les niveaux d'abonnement ESET PROTECT éligibles ; aucune interaction avec l'utilisateur n'est nécessaire et les administrateurs peuvent configurer les dossiers et les types de fichiers protégés

Conclusion

Les ransomwares restent une menace redoutable pour la cybersécurité en 2025, avec des tactiques évolutives et de plus en plus sophistiquées. La chute de LockBit et la montée en puissance de RansomHub mettent en évidence la dynamique changeante de l'écosystème des RaaS, où le succès est souvent mesuré par la capacité à attirer et conserver des affiliés.

Après le démantèlement de LockBit par les forces de police, de nombreux affiliés ont perdu confiance et ont migré vers RansomHub, ce qui a considérablement affaibli l'échelle opérationnelle de LockBit. En parallèle, des techniques avancées telles que les EDR killers, ainsi que l'implication de groupes APT, continuent d'ajouter des niveaux de complexité à ces menaces.

Les organisations doivent adopter une approche de sécurité multicouche et préventive pour lutter efficacement contre les ransomwares et les menaces qui les précèdent. Cela comprend la formation des collaborateurs, une robuste protection des endpoints et des données, des sauvegardes régulières et des solutions de sécurité avancées telles que le MDR ou l'XDR.

Grâce à la suite complète de cybersécurité d'ESET, qui intègre la technologie proactive Ransomware Remediation pour se rétablir rapidement et minimiser l'impact des attaques, vous pouvez faire face aux menaces des ransomwares les plus sophistiqués.

EN SAVOIR PLUS

À propos d'ESET

Défense proactive.

Notre activité consiste à minimiser la surface d'attaque.

Prenez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre **approche préventive reposant sur l'IA et l'expertise humaine**.

Bénéficiez d'une protection de haut niveau grâce à notre **Threat Intelligence** interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des **chercheurs reconnus**. ESET protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie.

Prévention multicouche

IA de pointe associée à une expertise humaine

Threat Intelligence de renommée mondiale

Support hyperlocal et personnalisé

eset
Digital Security
Progress. Protected.