Août 2025

Étude de marché

Rapport 2025 sur les ransomwares

Les ransomwares dans les entreprises : expériences et impacts

Barracuda®
Your business, secured.

Sommaire

Introduction 3

Résultats clés 5

Les ransomwares affectent plus de la moitié des organisations 6

Les ransomwares atteignent des victimes d'un profil particulier en matière de sécurité, eu égard à leurs outils et priorités 6

Les ransomwares proviennent de gangs qui, dans le tiers des cas, reçoivent des paiements 8

Les données sont chiffrées mais, désormais, cet élément ne constitue qu'une partie des attaques ransomware 8

Les ransomwares affectent leurs victimes en leur faisant perdre des clients et de nouveaux marchés potentiels 10

Conclusion 11

Introduction

Les ransomwares constituent une menace très répandue et en constante évolution. Cette menace est alimentée par des kits de ransomware-as-a-service, qui permettent à de plus en plus de pirates de lancer des attaques. Toute attaque par ransomware est susceptible de nuire à la réputation d'une marque et de paralyser les opérations quotidiennes de l'entreprise visée, provoquant des perturbations, des pertes de données, une perte de confiance de la clientèle et bien plus encore. Toutes les organisations sont des cibles potentielles.

Ce rapport traite des attaques par ransomware qui ont visé des organisations dans le monde entier au cours des 12 derniers mois. Il aborde le vécu des victimes et l'impact des attaques. Il s'appuie sur les résultats d'une enquête internationale menée par Barracuda et Vanson Bourne auprès de 2 000 décideurs en informatique et en sécurité.

Ses conclusions s'articulent autour de trois thèmes principaux, à savoir :

- **Les victimes d'un ransomware sont plus susceptibles de disposer d'un système de sécurité fragmenté**, avec une quantité excessive d'outils de sécurité sans connexions entre eux et une couverture insuffisante dans des domaines de sécurité clés.
- **Les attaques par ransomware sont multidimensionnelles.** Il ne s'agit plus simplement de chiffrer des données, mais également d'en obtenir frauduleusement pour les divulguer, d'installer des charges utiles malveillantes multiples, etc.

Méthodologie

Barracuda a chargé l'agence d'études de marché indépendante Vanson Bourne de mener une enquête mondiale auprès de 2 000 preneurs de décision de haut niveau en matière de sécurité, occupant des postes informatiques et commerciaux dans des organisations comptant entre 50 et 2 000 employés et issues d'un large éventail de secteurs aux États-Unis, au Royaume-Uni, en France, dans la région DACH (Allemagne, Autriche, Suisse), au Benelux (Belgique, Pays-Bas, Luxembourg), dans les pays nordiques (Danemark, Finlande, Norvège, Suède), en Australie, en Inde et au Japon. Le travail de terrain a été mené en avril et mai 2025.

Introduction

- **Lorsque les attaques par ransomware réussissent,** l'étendue de leurs effets néfastes s'étend de plus en plus. Par exemple, de nouvelles opportunités commerciales sont perdues et des pressions sont exercées sur les employés, les partenaires et les clients de la cible, ainsi que sur les services officiels, afin d'obtenir des paiements.

Nous espérons que ce rapport aidera les organisations de toutes les tailles et de tous les secteurs à comprendre la menace constituée par les ransomwares en 2025, ainsi que l'impact des attaques. Nous espérons également qu'il aidera les organisations à déceler ce qui les expose à des risques potentiels et à prendre les mesures appropriées.

Résultats clés

57 %

des organisations ont été, au cours des 12 derniers mois, victimes d'une attaque par ransomware qui a réussi

71 %

des organisations dont la messagerie e-mail avait été piratée ont également été touchées par un ransomware

32 %

ont payé une rançon pour récupérer leurs données — 41 % d'entre eux n'ont pas récupéré toutes leurs données

65 %

des victimes d'un ransomware ont pu restaurer leurs données à partir d'un dispositif de sauvegarde

24 %

des victimes d'un ransomware ont vu leurs données chiffrées, tandis que ces données ont été volées dans 27 % des cas et 29 % des victimes ont déclaré que les pirates avaient installé des charges utiles multiples.

25 %

des victimes d'un ransomware ont perdu des clients existants, et la même proportion de victimes ont perdu de nouvelles opportunités commerciales.

Les ransomwares touchent plus de la moitié des organisations

Au total, 57 % des organisations interrogées ont été, au cours des 12 derniers mois, victimes d'une attaque par ransomware qui a réussi.

Une victime sur trois (31 %) a été touchée deux fois ou plus.

Les cas où plusieurs attaques réussissent sont donc fréquents. Ce fait semble indiquer que les lacunes en matière de sécurité ne font pas systématiquement l'objet d'une enquête et de mesures rectificatives après chaque incident. Tout au long de ce rapport, nous examinons ce qui différencie les organisations touchées une fois de celles touchées plusieurs fois, afin de tirer les enseignements des données recueillies et de comprendre comment les organisations peuvent les utiliser pour renforcer leur posture de sécurité.

Selon notre enquête, les secteurs d'activité les plus affectés ont été ceux de la santé (avec 67 % des organisations touchées), des administrations locales (65 %) et du commerce de détail (61 %). Nos données indiquent que le secteur manufacturier a été le moins touché, un peu moins de la moitié des participants à notre enquête (46 %) ayant signalé une attaque réussie.

La taille ne semble pas constituer un facteur pour les attaques par ransomware, les chiffres de notre enquête étant restés semblables pour les entreprises de toutes les tranches de tailles, de 50 à 2 000 employés.

71 % des organisations qui ont été victimes d'un piratage d'e-mails ont également été la cible d'un ransomware. Ce chiffre met en évidence le lien entre les deux types d'attaques.

Les victimes de ransomware ont un profil de sécurité distinctif eu égard à leurs outils et priorités

La prolifération des outils de sécurité et l'exposition aux ransomwares

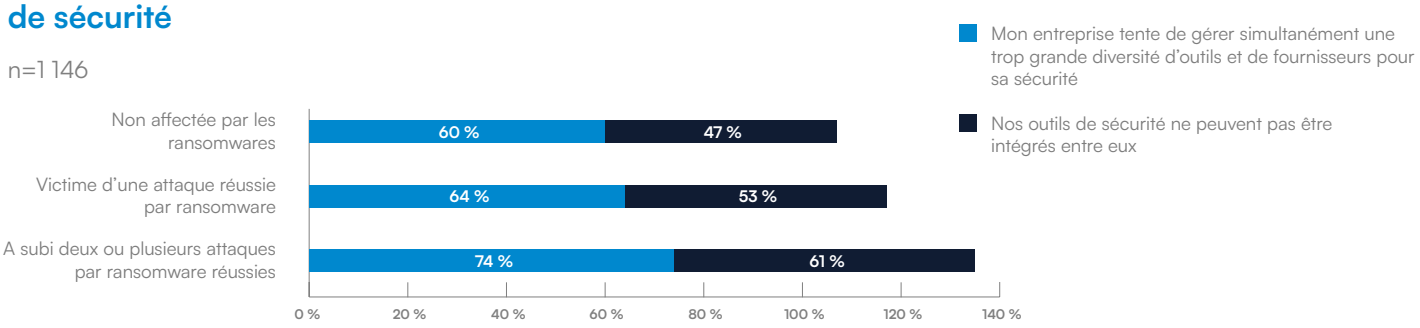
Notre enquête montre que l'excès d'outils de sécurité — connu sous le nom de prolifération d'outils — accompagné d'un manque d'intégration peut créer un risque accru. Avec ce type de dispositif, des lacunes apparaissent dans la protection, ce qui rend plus difficile de détecter et de contrecarrer les menaces actives, dont les ransomwares.

Selon nos données, la proportion d'organisations affectées par la prolifération d'outils peu intégrés entre eux est corrélée à l'ampleur de leur expérience des ransomwares.

FIGURE 1

Incidents de ransomware et prolifération des outils de sécurité

n=1 146



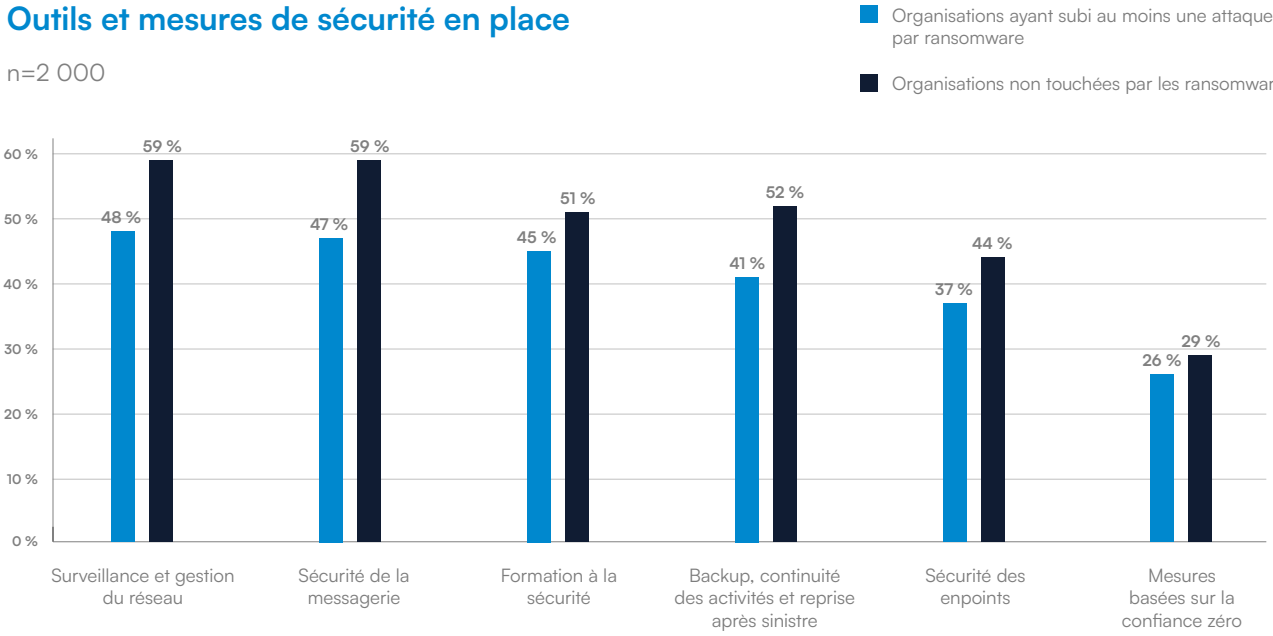
Les différents types d'outils et de mesures de sécurité

Selon les participants à notre enquête, les mesures de sécurité les plus mises en œuvre étaient la protection des e-mails (utilisée dans 52 % des cas), celle des réseaux (52 %) et les formations de sensibilisation à la sécurité (48 %). Ces mesures étaient moins susceptibles d'être mises en œuvre parmi les organisations ayant signalé une attaque réussie par ransomware.

FIGURE 2

Outils et mesures de sécurité en place

n=2 000



En voici quelques exemples :

- 47 % des victimes d'un ransomware avaient mis en place un dispositif de sécurisation de leurs e-mails, contre 59 % des non-victimes
- 48 % des victimes d'un ransomware avaient mis en place un système de gestion et de surveillance de leurs réseaux, contre 59 % des non-victimes
- 45 % des victimes d'un ransomware avaient organisé des formations de sensibilisation à la sécurité, contre 51 % des non-victimes
- 37 % avaient sécurisé leurs endpoints, contre 44 % des non-victimes

Ces résultats semblent indiquer que les victimes d'un ransomware n'investissent peut-être pas suffisamment dans les domaines de sécurité qui pourraient contribuer à réduire leur exposition aux risques.

Par exemple, considérons la sécurisation des e-mails, des réseaux et des endpoints, ainsi que les formations de sensibilisation à la sécurité. Ces mesures offrent une protection robuste contre les attaques de phishing et de social engineering , agissements par lesquels les pirates cherchent à se procurer frauduleusement des identifiants — pour pénétrer dans les réseaux, compromettre des appareils et se déplacer latéralement, autant de techniques qui caractérisent les attaques par ransomware.

Les gangs de pirates rançonneurs ont une chance sur trois d'être payés

32 % des victimes d'un ransomware ont payé une rançon pour récupérer ou restaurer des données.

Nos résultats montrent qu'une corrélation existe entre la propension d'une organisation à payer une rançon et le nombre d'attaques par ransomware qu'elle subit.

Selon notre enquête, les organisations qui n'ont subi qu'une attaque réussie par ransomware ont été légèrement moins susceptibles de payer la rançon, 29 % d'entre elles l'ayant fait. Par contre, 37 % de celles qui ont été affectées deux fois ou plus ont payé une rançon pour récupérer leurs données.

Ces chiffres ont peu évolué depuis notre dernière enquête réalisée il y a deux ans. En 2023, nos résultats montraient que 31 % des victimes touchées une fois avaient payé une rançon pour récupérer leurs données, contre 38 % de celles touchées deux fois ou plus.

Une explication peut être avancée pour comprendre le lien entre la multiplicité des attaques et les paiements des rançons : une fois qu'il est démontré qu'une organisation est prête à payer, de nouveaux pirates commencent à cibler la même victime, ou un même criminel peut attaquer plusieurs fois.

La bonne nouvelle est que dans la majorité des cas (65 %), les victimes d'un ransomware ont pu restaurer leurs données à partir de sauvegardes.

Malheureusement, les paiements de rançon restent peu efficaces : 41 % de ceux qui ont payé un rançon (13 % du total) n'ont pas récupéré la totalité de leurs données. Il est même arrivé qu'ils ne récupèrent rien.

Le chiffrement des données ne constitue désormais qu'une partie des attaques par ransomware

Outre le coût financier occasionné par le paiement de la rançon, notre étude a démontré que lorsqu'une attaque par ransomware réussit, son impact commercial, opérationnel et même émotionnel est considérable.

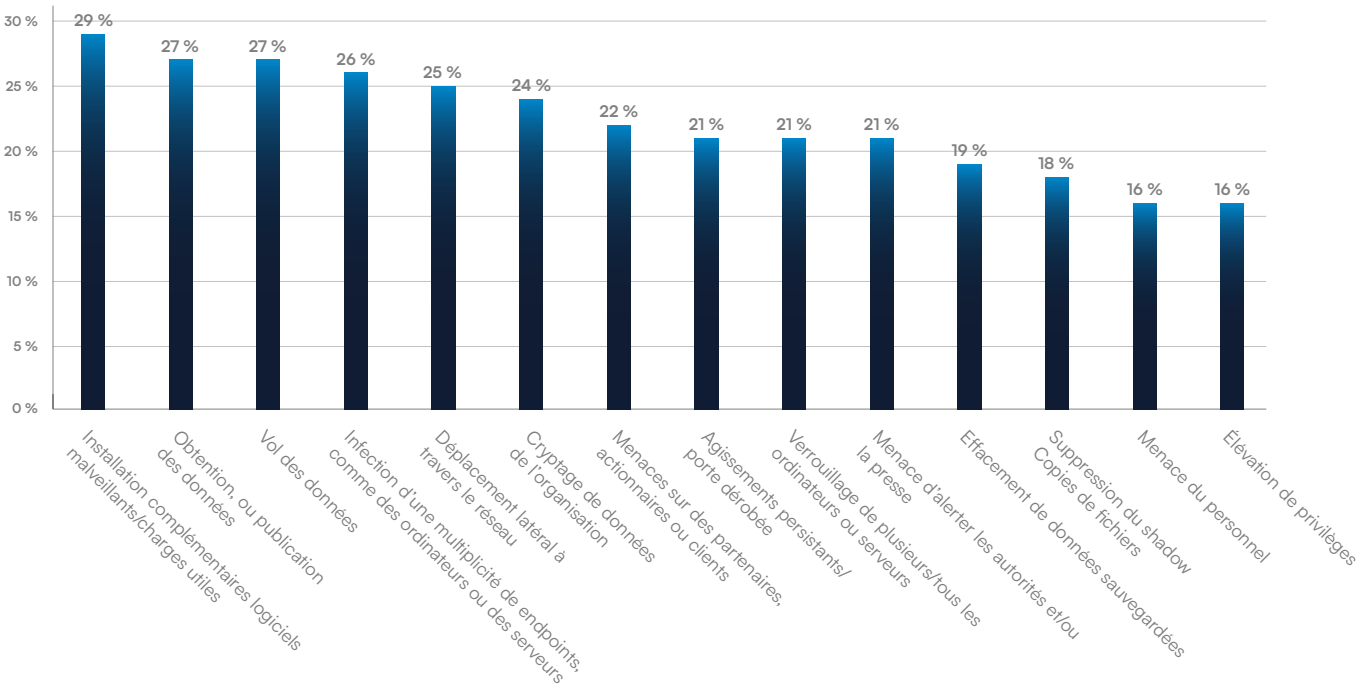
Pour la plupart des attaques par ransomware le chiffrement des données et le verrouillage des systèmes et des ordinateurs constituent les étapes finales. Ce sont les parties les plus visibles d'une attaque et, par conséquent, ce sont les plus susceptibles de révéler la présence d'intrus aux équipes de sécurité et de déclencher l'endiguement et l'élimination d'une menace.

Les résultats de notre recherche mettent en évidence l'ampleur de l'activité qui passe inaperçue avant l'exécution d'un ransomware, activité visant soit à permettre l'attaque, soit à ouvrir la voie à d'autres agissements potentiels.

FIGURE 3

Activités menées par les gangs de pirates rançonneurs lors des incidents les plus notables

n=1 146



Dans environ le quart des cas couverts par notre enquête, les attaques par ransomware incorporaient un chiffrement de données (24 %), un verrouillage de endpoints(21 %) ou une obtention frauduleuse de données (27 %).

Ces attaques ont également incorporé des mouvements latéraux à travers les réseaux (25 %), l'infection d'une multiplicité de endpoints dont des ordinateurs et des serveurs (26 %), l'installation de charges utiles malveillantes multiples (29 %), des élévations de privilèges (16 %) et l'installation de portes dérobées ou d'autres mécanismes de persistance (21 %).

De plus, certains pirates ont cherché à entraver au maximum la possibilité pour leurs cibles de restaurer leurs données sans payer. Environ un attaquant sur cinq a accédé aux fichiers de sauvegarde de ses cibles pour les effacer et a supprimé les clichés instantanés (chacun de ces cas ayant été rencontrés par 19 % des victimes).

Nos résultats montrent aussi qu'après l'exécution d'un ransomware et l'envoi d'une demande de paiement, les pirates commencent à exercer des pressions sur leur victime à l'aide de tactiques psychologiques. Ces méthodes comprennent notamment l'émission de menaces à l'encontre de partenaires, d'actionnaires ou de clients (22 %), des menaces d'alerter la presse ou les autorités (21 %) et même des menaces à l'encontre de membres du personnel (16 %).

Dans 27 % des cas où une attaque par ransomware a réussi, les pirates ont ensuite divulgué, exposé ou publié les données qu'ils s'étaient procurées frauduleusement.

Les victimes de ransomware perdent des clients et de nouvelles opportunités commerciales

Quand les activités reprennent leur cours après une attaque, les victimes d'un ransomware doivent faire face à des répercussions opérationnelles et commerciales.

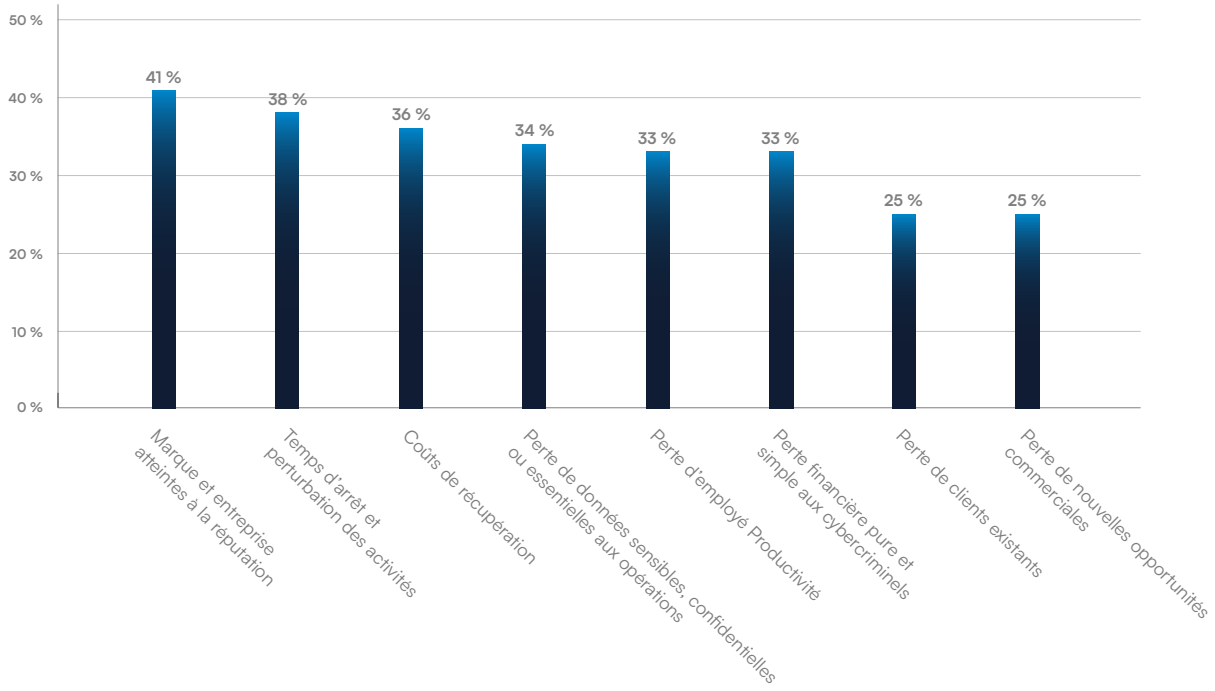
L'impact le plus souvent cité par ces victimes est l'atteinte à leur réputation et à leur marque commerciale (41 % sont affectées). Viennent ensuite les temps d'arrêt (38 %) et les coûts des mesures de récupération (36 %). Le tiers des victimes (34 %) ont admis avoir perdu des données sensibles.

Dans le quart des cas, les victimes d'un ransomware sont confrontées aux impacts commerciaux à long terme constitués par la perte de clients existants et par celle de nouvelles opportunités commerciales (25 % pour chaque cas de figure).

FIGURE 4

Les répercussions de l'attaque par ransomware la plus notable des 12 derniers mois

n=1 146



Conclusion

Pour pouvoir résister aux attaques par ransomware les organisations ont besoin d'un système de sécurité intégrée et multicouche contre les menaces en ligne. Ce système doit être apte à protéger une surface d'attaque en constante expansion.

Les mesures pratiques énoncées ci-dessous pourraient vous être utiles :

- **Assurez-vous que vos données sont sauvegardées régulièrement et en toute sécurité** et qu'elles sont conservées hors ligne. Procédez à des tests pour vous assurer que vous pouvez restaurer efficacement vos données.
- **Mettez en œuvre une procédure d'authentification multifacteur et appliquez le principe du moindre privilège,** afin de limiter les accès aux ressources et aux applications de votre entreprise. Ces mesures rendent vos données et systèmes de grande valeur inaccessibles aux pirates, même s'ils se servent d'identifiants obtenus frauduleusement.
- **Maintenez vos logiciels à jour** en y appliquant les derniers correctifs, afin de combler les lacunes dans leur sécurité.
- **Organisez régulièrement des formations de sensibilisation à la cybersécurité** pour vos employés, en mettant l'accent sur les tactiques les plus récentes utilisées pour l'hameçonnage et les attaques par ransomware.
- **Morcelez votre réseau,** en y isolant les systèmes critiques pour empêcher les pirates de se livrer à des mouvements latéraux.
- **Vérifiez toutes vos configurations,** y compris dans le cloud. Les configurations inadéquates constituent l'une des principales causes des incidents de sécurité.
- **Installez un dispositif robuste pour la sécurisation de vos e-mails.** Les e-mails sont souvent un point d'entrée capital pour les ransomwares et, si vous utilisez un système de protection de pointe alimenté par l'IA, vous pouvez détecter les charges utiles malveillantes. Ces systèmes peuvent aussi reconnaître les tactiques de manipulation sociale sophistiquées conçues pour contourner vos mesures de sécurité.
- **Sécurisez vos applications en ligne,** comme les services de partage de fichiers, les formulaires sur Internet et les sites de commerce électronique. Ces applications sont souvent ciblées par le biais de leur interface utilisateur ou d'une interface d'API.
- **Préparez un plan de réponse aux incidents et mettez-le régulièrement à l'épreuve en procédant à des exercices.**

Conclusion

- **Envisagez de collaborer avec des experts externes**, comme des prestataires de services d'infogérance et des fournisseurs d'outils de sécurité, afin de bénéficier d'une meilleure assistance. Ces partenaires peuvent vous aider à adopter des plateformes et des solutions intégrées de pointe pour votre sécurité. Ils peuvent également intervenir à toute heure du jour ou de la nuit pour détecter les menaces actives, ce qui leur permet d'y réagir et de les bloquer, jugulant et neutralisant ainsi les incidents avant qu'ils ne causent de graves dommages.

Barracuda en quelques mots

Barracuda est une entreprise mondiale de cybersécurité de premier plan qui fournit une protection complète contre les menaces complexes aux entreprises de toutes tailles. Notre plateforme basée sur l'IA sécurise les e-mails, les données, les applications et les réseaux grâce à des solutions innovantes, à un service XDR géré et à un tableau de bord centralisé afin d'optimiser la protection et de renforcer la cyber-résilience. Forte de la confiance de centaines de milliers de professionnels de l'informatique et de fournisseurs de services gérés dans le monde entier, Barracuda propose des défenses puissantes, faciles à acheter, à déployer et à utiliser.

Barracuda Networks, Barracuda, BarracudaONE et le logo Barracuda Networks sont des marques déposées de Barracuda Networks, Inc. aux États-Unis et dans d'autres pays

À propos de Vanson Bourne

Vanson Bourne est un cabinet indépendant spécialiste des études de marché pour le secteur des technologies. Sa réputation de produire des analyses solides, fiables et basées sur des études est elle-même fondée sur des principes rigoureux ainsi que sur sa capacité à interroger des décisionnaires majeurs qui occupent des fonctions techniques et métier dans tous les secteurs et sur les marchés principaux. Pour plus d'informations, accédez à vansonbourne.com.