Février 2026

Rapport sur les menaces

Le rapport Managed XDR sur les menaces mondiales

Comment les pirates ciblent les organisations et exploitent les failles de sécurité

Barracuda®
Your business, secured.

Sommaire

Introduction

Les outils avancés et les experts de Barracuda Managed XDR surveillent et protègent les réseaux des clients 24 heures sur 24, 365 jours par an. Chaque minute, la solution détecte et traite une alerte de sécurité. Toutes les 15 minutes, elle envoie une alerte à un client, et toutes les 60 minutes, elle bloque automatiquement une menace de gravité élevée, comme un appareil compromis ou une attaque par ransomware en cours.

Si elle n'est pas traitée, une seule alerte critique peut rapidement dégénérer en incident généralisé, perturbant les opérations, réduisant la productivité, compromettant des données sensibles et nuisant à la stabilité financière ainsi qu'à la réputation de la marque. Aucune organisation n'est à l'abri : les pirates ciblent des entreprises de toutes tailles, dans tous les secteurs et toutes les zones géographiques.

Les facteurs de vulnérabilité peuvent être multiples : failles de sécurité, appareils non autorisés, systèmes non corrigés, négligences, mauvaises configurations, ainsi qu'un manque de temps et de ressources pour détecter l'intrusion, expulser les pirates et verrouiller solidement l'accès derrière eux.

L'objectif de ce rapport est d'aider les professionnels de l'informatique et de la sécurité des organisations disposant de ressources limitées à mieux comprendre comment les pirates ciblent leurs victimes potentielles et quelles faiblesses ils chercheront à exploiter. Nous présentons des exemples d'incidents réels ainsi que des recommandations pour vous aider à rester protégé et à renforcer la résilience cyber.

Dans un monde où les cybermenaces deviennent de plus en plus complexes et furtives, les organisations ne sont pas seules face à ce défi. Votre fournisseur de sécurité dispose des outils et de l'expertise nécessaires pour vous aider à traiter les problématiques identifiées dans ce rapport, et nous sommes là pour vous accompagner à chaque étape.

Les données sous-jacentes

Les conclusions détaillées dans ce rapport reposent sur Barracuda Managed XDR et son ensemble de données unique comprenant plus de 2 000 milliards d'événements informatiques collectés en 2025, près de 600 000 alertes de sécurité et plus de 300 000 endpoints, firewalls, serveurs, ressources cloud protégés, et plus encore. Environ 53 000 menaces de gravité élevée ont été traitées par la plateforme d'orchestration et de réponse automatisée à la sécurité (SOAR) de Barracuda Managed XDR.

Résultats clés

100 %

des incidents de sécurité impliquaient au moins un terminal non protégé ou non autorisé

96 %

des incidents impliquant des mouvements latéraux se sont soldés par le déploiement d'un ransomware

66 %

des incidents impliquaient la chaîne d'approvisionnement ou un tiers (contre 45 % en 2024)

3 heures

attaque par ransomware la plus rapide, de l'intrusion au chiffrement

90 %

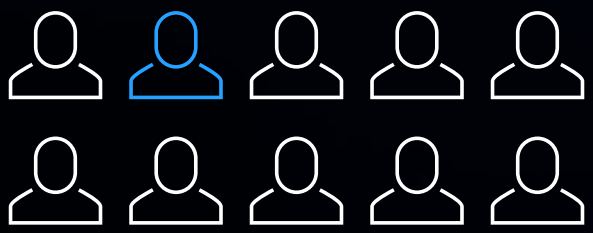
des incidents de ransomware ont exploité des firewalls

13 ans

la vulnérabilité la plus détectée est un bug de 2013 dans un protocole de chiffrement obsolète

1 sur 10

des vulnérabilités détectées disposent d'un exploit connu



Comment les pirates ciblent les organisations

Les solutions efficaces de détection et de réponse étendues (XDR) sont conçues pour intercepter les menaces entrantes dès les premières étapes de la chaîne d'attaque, au moment de la compromission initiale et de l'accès. Barracuda Managed XDR ne fait pas exception. La solution offre également une visibilité accrue sur les phases ultérieures de l'attaque, notamment les mouvements latéraux et l'impact final. Cette capacité étendue se reflète dans le contenu de ce rapport.

En tête de liste des menaces les plus détectées contre les organisations au cours des 12 derniers mois figurent les attaques visant les identités et la sécurité des identités.

Cela inclut des connexions inhabituelles ou inattendues à un compte utilisateur. Il s'agit de connexions qui ne correspondent pas au comportement habituel de l'utilisateur en termes d'appareil, de localisation ou d'heure. Ces détections constituent un indicateur fort de vol d'identifiants et de compromission de compte. Parmi les autres signaux d'alerte figurent des tentatives de connexion depuis une zone géographique bloquée et la règle dite du « voyage impossible », lorsqu'un utilisateur se connecte depuis un second emplacement qu'il n'aurait pas pu atteindre dans le laps de temps écoulé entre deux connexions.

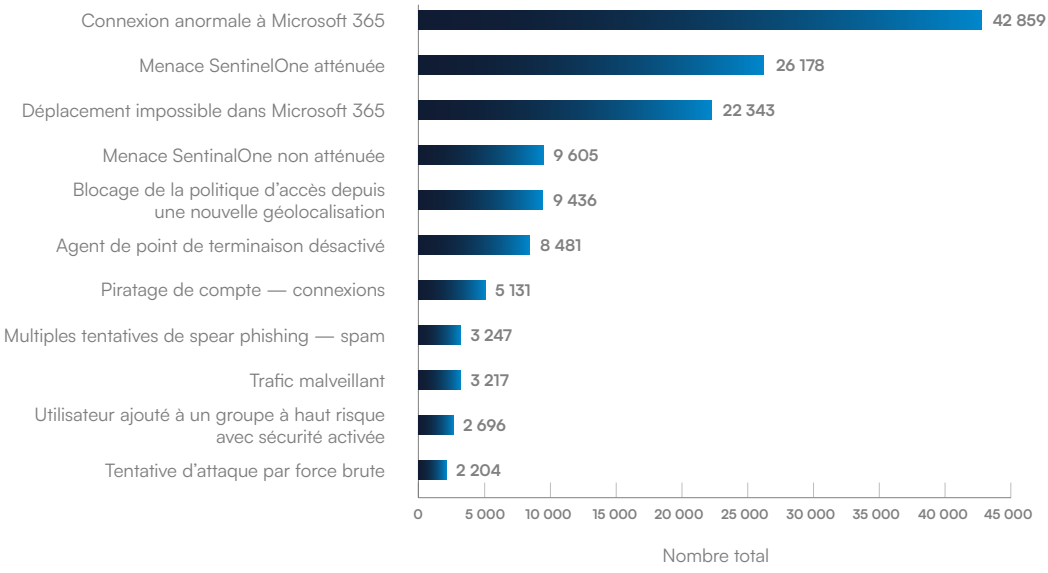


FIGURE 1

Principales détections d'attaques contre des organisations

La liste des principales détections inclut également des activités pouvant indiquer qu'un compte a été compromis et que les pirates sont déjà présents dans le réseau. Les équipes de sécurité doivent enquêter immédiatement sur ce type d'alerte. Cela comprend des signes indiquant qu'une tentative de contournement ou de désactivation de la protection des endpoints a eu lieu, ainsi que des notifications signalant l'ajout d'un utilisateur à un groupe sensible en matière de sécurité, ce qui peut révéler une tentative d'élévation de privilèges.

Comment les pirates manipulent les droits d'accès privilégiés une fois dans le système

L'élévation de privilèges est essentielle pour les pirates, car elle transforme un accès limité en contrôle administratif complet, leur permettant de désactiver les défenses, de se déplacer latéralement entre les systèmes et d'accéder à des données sensibles. Le résultat peut être une compromission à grande échelle et le déploiement d'un ransomware.

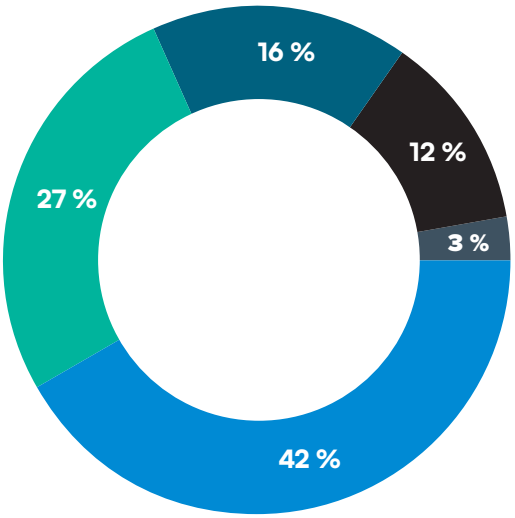


FIGURE 2

Comment les pirates manipulent les droits d'accès privilégiés

- Windows — Ajout d'un utilisateur à un groupe disposant de droits de sécurité à haut risque
- Windows — Suppression d'un utilisateur d'un groupe disposant de droits de sécurité à haut risque
- Microsoft 365 — Ajout d'un utilisateur en tant qu'administrateur global
- Microsoft 365 — Suppression d'un utilisateur en tant qu'administrateur général
- FortiGate Firewall — Ajout d'un utilisateur en tant qu'administrateur

Les outils de sécurité de firewall, Windows et Microsoft 365 de Barracuda Managed XDR ont détecté les comportements suivants indiquant une tentative d'élévation de privilèges :

Windows — Ajout d'un utilisateur à un groupe disposant de droits de sécurité à haut risque (42 % des élévations de privilèges suspectes)

- **Ce que cela signifie :** Un utilisateur a été ajouté à un groupe disposant d'autorisations puissantes (par exemple, administrateurs de domaine).
- **Ce que les pirates peuvent en faire :** Mouvement latéral, déploiement de logiciel malveillant ou exfiltration de données.
- **Comment se protéger :** Surveiller les modifications apportées aux groupes et gérer l'attribution de tous les droits d'accès privilégiés.

Windows — suppression d'un utilisateur d'un groupe disposant de droits de sécurité à haut risque (27 %)

- **Ce que cela signifie :** Un utilisateur a été retiré d'un groupe à haut niveau de privilèges.
- **Ce que les attaquants peuvent en faire :** Effacer leurs traces après une élévation de privilèges.
- **Comment se protéger :** Examiner les raisons de la suppression et vérifier toute utilisation abusive antérieure.

Microsoft 365 — Ajout d'un utilisateur en tant qu'administrateur global (16%)

- **Ce que cela signifie :** Une personne s'est vu attribuer le plus haut niveau d'accès dans Microsoft 365.
- **Ce que les attaquants peuvent en faire :** Créer de nouveaux comptes, voler des données ou désactiver des dispositifs de sécurité.
- **Comment se protéger :** Examiner les modifications de rôles administrateur, appliquer l'authentification multifacteur (MFA) et mettre en place des processus formels de validation et d'approbation.

Microsoft 365 — Suppression d'un utilisateur en tant qu'administrateur général (12 %)

- **Ce que cela signifie :** Une personne a perdu ses droits d'administrateur global.
- **Ce que les attaquants peuvent en faire :** Éviter la détection en supprimant les comptes qu'ils ont ajoutés.
- **Comment se protéger :** Vérifier si la modification était autorisée et analyser les journaux d'audit pour détecter toute activité suspecte.

FortiGate Firewall — Ajout d'un utilisateur en tant qu'administrateur du firewall (3 %)

- **Ce que cela signifie :** Un nouveau compte administrateur a été créé sur le firewall.
- **Ce que les attaquants peuvent en faire :** Désactiver les protections et ouvrir des portes dérobées.
- **Comment se protéger :** Confirmer la légitimité du compte et appliquer des contrôles stricts sur les comptes administrateur.

Rapport d'incident — La pièce jointe malveillante ayant conduit à l'installation d'un RAT

Un cheval de Troie d'accès distant (RAT) a été découvert sur les systèmes d'un client après qu'un employé a involontairement téléchargé un fichier exécutable malveillant. Le fichier a immédiatement tenté d'assurer sa persistance : il a cherché à s'enregistrer comme service Windows, ce qui lui aurait permis de démarrer automatiquement, de s'exécuter en arrière-plan et d'opérer avec des privilèges système afin de contrôler l'ordinateur à distance sans intervention. Il a également tenté d'installer l'outil de gestion à distance légitime ScreenConnect via PowerShell.

Se cacher à la vue de tous

L'ajout et la suppression d'utilisateurs dans les groupes à accès privilégiés est une activité informatique légitime. La capacité des pirates à dissimuler des comportements malveillants parmi les tâches et outils quotidiens normaux constitue aujourd'hui l'un des plus grands défis pour les équipes de sécurité.

Cette approche dite du living off the land (LOTL) est en forte progression : les acteurs malveillants exploitent des outils logiciels et techniques légitimes pour échapper à la détection. Heureusement, l'IA aide les systèmes de sécurité avancés à repérer des anomalies subtiles dans des activités apparemment bénignes, afin qu'elles puissent être examinées et neutralisées.

Un mot sur les outils d'accès et de gestion à distance (RMM)

Les outils d'accès à distance sont une cible croissante pour les pirates. La compromission réussie d'un outil RMM donne aux pirates un pouvoir considérable tout en réduisant le risque de détection, car ces outils sont largement utilisés par les organisations.

Au cours des 12 derniers mois, Barracuda Managed XDR a neutralisé des incidents impliquant l'abus, entre autres, de SonicWall SSL-VPN (un réseau privé virtuel populaire), ScreenConnect, RDP (Remote Desktop Protocol), PsExec (outil en ligne de commande permettant d'exécuter des programmes et des commandes sur des ordinateurs distants), AnyDesk, ainsi que d'autres VPN de firewall.

Pour réduire les risques, les équipes de sécurité doivent déployer des systèmes de détection spécifiquement conçus pour identifier les abus d'outils RMM. Par exemple, Barracuda Managed XDR a développé une règle de détection utilisant la télémétrie des endpoints pour identifier les requêtes envoyées par ScreenConnect vers des domaines de premier niveau (TLD) suspects.

Rapport d'incident — Le ransomware Akira retourne l'outil de gestion à distance de la victime contre elle

Les pirates ont obtenu l'accès au contrôleur de domaine (DC) et installé Datto RMM. Leur activité imitait étroitement celle d'un agent de sauvegarde effectuant des tâches planifiées, ce qui donnait l'apparence d'une activité informatique normale.

Combinaisons de signaux d'alerte

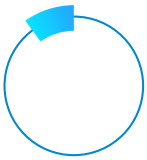
Les activités suspectes peuvent également être détectées en examinant la situation dans son ensemble. L'analyse d'incidents réels impliquant Barracuda Managed XDR au cours des 12 derniers mois a mis en évidence les combinaisons récurrentes suivantes d'outils, techniques et comportements :

66 %

des cas de malwares sans fichier utilisaient PowerShell comme méthode principale d'exécution. PowerShell est un outil multiplateforme permettant d'automatiser des tâches et de gérer des configurations.

44 %

des incidents liés aux firewalls impliquaient des attaques par password spraying, technique consistant à tester de nombreux mots de passe courants avec des identifiants volés.



10 %

des violations de la sécurité des serveurs incluaient l'effacement des journaux d'activité afin de couvrir les traces des pirates.

96 %

des cas de mouvements latéraux ont abouti au déploiement d'un ransomware.

90 %

des incidents de ransomware exploitaient des firewalls via un CVE (vulnérabilité logicielle référencée) ou un compte vulnérable.

34 %

des incidents impliquaient de l'ingénierie sociale incitant des utilisateurs à télécharger des fichiers potentiellement malveillants.

Pour que les attaques réussissent, les pirates doivent trouver des failles dans la sécurité de leurs victimes et en tirer parti. Les données de détection et les analyses d'incidents de Barracuda Managed XDR mettent en lumière certains points faibles potentiels qui ont rendu des organisations vulnérables aux cybermenaces au cours de l'année écoulée.

Comment les organisations s'exposent elles-mêmes

Principales vulnérabilités de sécurité réseau

Des méthodes de chiffrement inadéquates ou obsolètes, qui ne protègent pas correctement le trafic sensible, ainsi que l'absence de validation ou de certification appropriée des activités réseau, peuvent être exploitées par les pirates pour progresser dans leurs attaques.

Au cours de l'année passée, Barracuda Managed XDR a identifié les risques de sécurité réseau suivants :

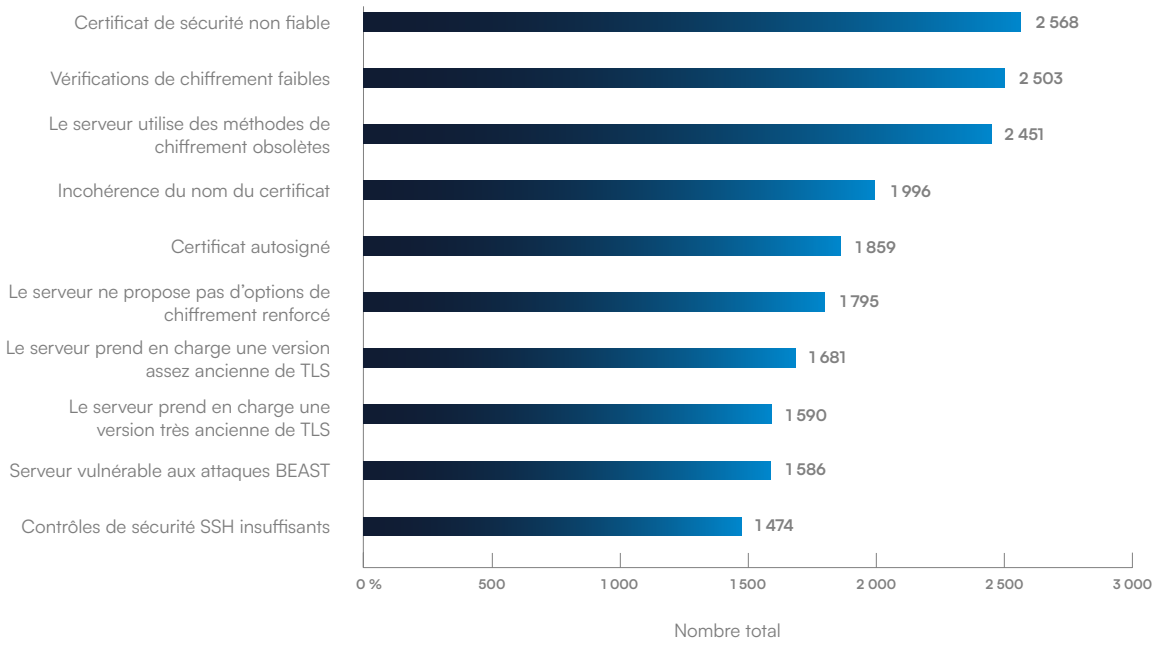


FIGURE 3

Principales vulnérabilités de sécurité réseau

Certificat de sécurité non fiable

Ce que cela signifie :

Le certificat présenté par le serveur n'est pas émis par une autorité de certification (CA) de confiance.

Ce que les pirates peuvent en faire :

Usurper un site légitime à l'aide d'un faux certificat, leur permettant de s'insérer dans des communications légitimes afin de voler des données, contourner des mécanismes de sécurité, injecter du contenu malveillant, etc.

Comment se protéger :

Utiliser des certificats émis par des autorités de certification reconnues.

Pour les équipes techniques : Mettre en œuvre une validation stricte des certificats et activer le certificate pinning (l'application ne fait confiance qu'à un certificat spécifique lors de la connexion à un serveur). Vérifier également si le certificat de l'application a été révoqué (via CRL ou OCSP) afin d'éviter de faire confiance à des certificats compromis. Voir : OWASP - Validation des certificats.

Faiblesse des contrôles de chiffrement

Ce que cela signifie :

Le serveur utilise des algorithmes faibles ou des longueurs de clés insuffisantes pour le chiffrement.

Ce que les pirates peuvent en faire :

Exploiter les faiblesses ou mener des attaques par force brute pour déchiffrer des données sensibles telles que des mots de passe ou des informations financières. La force brute consiste à tester de nombreuses combinaisons identifiant/mot de passe jusqu'à en trouver une qui fonctionne.

Comment se protéger :

Appliquer des standards de chiffrement robustes tels que AES-256 ou RSA-2048 et plus.

Pour les équipes techniques : Désactiver les suites cryptographiques faibles et auditer régulièrement les configurations. Envisager l'utilisation de la cryptographie à courbe elliptique (ECC), comme ECDSA ou ECDHE, pour améliorer la sécurité et les performances. (Voir : Recommandations ECC du NIST). Mettre en œuvre des suites compatibles avec la Perfect Forward Secrecy (PFS) afin de protéger les sessions passées en cas de compromission des clés.

Le serveur utilise des méthodes de chiffrement obsolètes

Ce que cela signifie :

Le serveur repose sur des algorithmes obsolètes tels que MD5, SHA-1 ou RC4.

Ce que les pirates peuvent en faire :

Exploiter des vulnérabilités connues pour casser le chiffrement ou falsifier des signatures, entraînant des violations de données.

Comment se protéger :

Migrer vers des algorithmes modernes tels que SHA-256 ou AES et suivre les recommandations des standards du secteur (par exemple les recommandations du NIST ci-dessus).

Pour les équipes techniques : Supprimer la prise en charge des algorithmes dépréciés (MD5, SHA-1, RC4) dans toutes les configurations. Tester avec des outils comme SSL Labs afin de vérifier qu'aucun algorithme obsolète n'est activé. Voir : Test SSL Labs.

Incohérence du nom du certificat

Ce que cela signifie :

Le nom de domaine ne correspond pas au nom commun (CN) ni au nom alternatif du sujet (SAN) du certificat.

Ce que les pirates peuvent en faire :

Lancer des attaques d'interception en redirigeant le trafic vers un serveur malveillant.

Comment se protéger :

S'assurer que les certificats couvrent tous les domaines et sous-domaines utilisés.

Pour les équipes techniques : Utiliser les champs SAN pour les certificats multi-domaines. Automatiser la gestion des certificats pour éviter les erreurs lors des renouvellements.

Certificat autosigné

Ce que cela signifie :

Le certificat est signé par la même entité qui le possède, et non par une autorité de confiance.

Ce que les pirates peuvent en faire :

Faciliter l'usurpation de serveurs, puisque n'importe qui peut créer un certificat autosigné.

Comment se protéger :

Utiliser des certificats émis par une CA pour les services exposés publiquement et limiter les certificats autosignés aux systèmes internes.

Pour les équipes techniques : Maintenir une autorité de certification privée pour l'usage interne et distribuer son certificat racine de manière sécurisée. Surveiller l'apparition de certificats autosignés non autorisés sur le réseau.

Le serveur manque d'options de chiffrement robustes

Ce que cela signifie :

Le serveur ne propose pas de suites cryptographiques modernes et sécurisées.

Ce que les pirates peuvent en faire :

Forcer une rétrogradation vers un chiffrement plus faible.

Comment se protéger :

Configurer les serveurs pour prendre en charge des suites robustes, telles que Transport Layer Security (TLS) 1.2/1.3 avec AES-GCM.

Pour les équipes techniques : Désactiver les options de chiffrement TLS faibles ou non sécurisées (comme NULL ou EXPORT) afin d'autoriser uniquement des connexions chiffrées et authentifiées fortes. Mettre régulièrement à jour les logiciels serveur pour qu'ils prennent en charge les protocoles et suites cryptographiques les plus récents.

Le serveur prend en charge des versions plus anciennes de TLS

Ce que cela signifie :

La version de TLS utilisée est dépassée et vulnérable aux attaques.

Ce que les pirates peuvent en faire :

Exploiter des faiblesses du protocole pour mener des attaques d'interception ou de rétrogradation, forçant le système à utiliser un protocole de sécurité plus ancien et moins sûr.

Comment se protéger :

Mettre à jour la version de TLS utilisée.

Pour les équipes techniques : Désactiver TLS 1.0 et 1.1. Ne prendre en charge que TLS 1.2 et 1.3. Voir : Mozilla - Recommandations TLS.

Le serveur prend en charge une version très ancienne de TLS

Ce que cela signifie :

La version de TLS utilisée est obsolète et non sécurisée.

Ce que les pirates peuvent en faire :

Exploiter des vulnérabilités connues.

Comment se protéger :

Mettre à jour la version de TLS utilisée.

Pour les équipes techniques : Supprimer totalement SSLv2, SSLv3 et les premières versions de TLS. Utiliser des outils automatisés pour analyser la prise en charge éventuelle de protocoles hérités.

Serveur vulnérable aux attaques BEAST

Ce que cela signifie :

Les attaques BEAST (Browser Exploit Against SSL/TLS) ciblent les anciennes versions de TLS présentant des faiblesses dans leur chiffrement par blocs.

Ce que les pirates peuvent en faire :

Déchiffrer HTTPS (Hypertext Transfer Protocol Secure) — une version sécurisée du protocole de communication web de base, et exposer des données confidentielles.

Comment se protéger :

Mettre à jour vers la version la plus récente de TLS et utiliser des suites cryptographiques sécurisées.

Pour les équipes techniques : Privilégier TLS 1.2 ou supérieur avec des suites AES-GCM ou ChaCha20-Poly1305. Désactiver les chiffrements en mode CBC sur les anciennes versions de TLS.

Contrôles de sécurité SSH insuffisants

Ce que cela signifie :

La configuration SSH utilise des algorithmes faibles ou des protocoles obsolètes. SSH (Secure Shell) est un protocole réseau sécurisé permettant d'accéder et de contrôler des ordinateurs à distance via un réseau non sécurisé, comme Internet.

Ce que les pirates peuvent en faire :

Mener des attaques par force brute sur les identifiants ou exploiter des clés faibles pour obtenir un accès non autorisé.

Comment se protéger :

Imposer des algorithmes d'échange de clés robustes, désactiver les protocoles SSH faibles, utiliser l'authentification par clé et déployer des outils spécialisés de prévention des intrusions protégeant contre les attaques par force brute (par exemple Fail2Ban ou équivalent).

Pour les équipes techniques : Utiliser uniquement le protocole SSH version 2. Imposer des longueurs de clé minimales (par exemple RSA 4096 ou Ed25519). Désactiver l'authentification par mot de passe quand c'est possible et privilégier l'authentification par clé. Restreindre l'accès SSH par adresse IP et via des règles de firewall. Mettre régulièrement à jour le serveur SSH. Voir : Best practices en matière de sécurité SSH.

Les principales vulnérabilités logicielles CVE détectées

Les logiciels obsolètes et non patchés constituent un aimant à cybermenaces. Selon Barracuda Managed Vulnerability Security, voici les principales vulnérabilités identifiées dans les réseaux clients au cours de l'année écoulée :

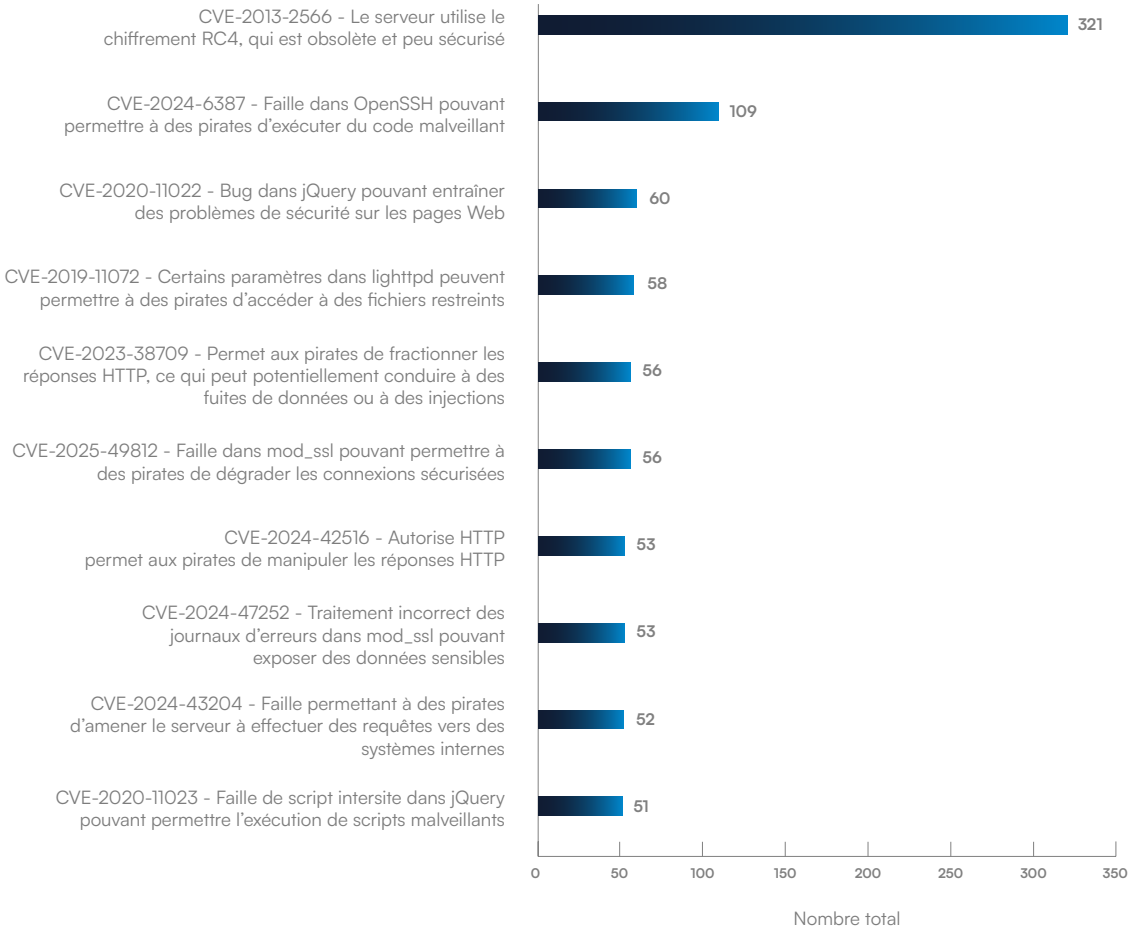


FIGURE 4

Principales vulnérabilités identifiées par un CVE dans les organisations

La vulnérabilité la plus largement détectée est aussi la plus ancienne. CVE-2013-2566 existe depuis près de 13 ans et demeure présente dans des systèmes hérités tels que d'anciens serveurs, des équipements embarqués ou des applications.

Ces systèmes peuvent être encore utilisés activement, mais ils sont souvent inactifs et oubliés. La prévalence de cette vulnérabilité constitue un avertissement sévère quant au risque d'exposition dormante. Plus une vulnérabilité est corrigée rapidement, moins elle risque d'être négligée.

Une seule CVE de la liste est classée critique, mais cinq sont classées à gravité élevée. Le score de gravité moyen des vulnérabilités détectées au cours des 12 derniers mois est de 5,9.

CVE-2013-2566 — Le serveur repose sur un chiffrement RC4 vulnérable et obsolète

Gravité : **MOYENNE**

Ce que les pirates peuvent en faire :

Exploiter la faiblesse du chiffrement pour convertir des données sensibles en texte clair. RC4 est un type d'algorithme de chiffrement.

Comment se protéger :

Désactiver RC4 dans les configurations TLS (voir ci-dessus) et utiliser des chiffrements modernes tels qu'AES avec TLS 1.2 ou supérieur.

CVE-2024-6387 — Faille dans OpenSSH pouvant permettre à des pirates d'exécuter du code malveillant

Gravité : **CRITIQUE**

Ce que les pirates peuvent en faire :

Prendre le contrôle total des systèmes affectés à distance. SSH (Secure Shell) est un protocole utilisé pour se connecter de manière sécurisée à des systèmes distants via un réseau non sécurisé comme Internet, et OpenSSH est son implémentation gratuite open source.

Comment se protéger :

Appliquer immédiatement les derniers correctifs OpenSSH et restreindre l'accès SSH.

CVE-2020-11022 — Bug dans jQuery pouvant entraîner des problèmes de sécurité sur les pages web

Gravité : **MOYENNE**

Ce que les pirates peuvent en faire :

Injecter des scripts malveillants dans les pages web et voler des sessions et des données. jQuery est une bibliothèque JavaScript qui simplifie le codage pour les développeurs.

Comment se protéger :

Mettre à jour jQuery vers la dernière version et nettoyer les données avant traitement par le système.

CVE-2019-11072 - Certains paramètres du serveur web lighttpd peuvent permettre à des pirates d'accéder à des fichiers restreints

Gravité : **ÉLEVÉE**

Ce que les pirates peuvent en faire :

Accéder à des fichiers restreints sur le serveur, y compris des configurations ou des données sensibles. Un serveur lighttpd est un serveur web open source conçu pour les environnements où la rapidité d'exécution est critique.

Comment se protéger :

Mettre à jour le serveur web lighttpd vers la version la plus récente et vérifier/nettoyer tout emplacement de fichier fourni par l'utilisateur afin d'éviter les utilisations abusives.

CVE-2023-38709 — Permet aux pirates de fractionner les réponses HTTP dans les serveurs web Apache vulnérables, ce qui peut potentiellement conduire à des fuites de données ou à des injections

Gravité : **ÉLEVÉE**

Ce que les pirates peuvent en faire :

Insérer de fausses instructions dans les réponses web, forcer les systèmes à stocker des données malveillantes ou à injecter du code nuisible dans les pages web, compromettant l'intégrité des données et la sécurité des utilisateurs.

Comment se protéger :

Mettre à jour le serveur web Apache et vérifier/nettoyer correctement les données d'en-têtes et instructions navigateur-serveur.

CVE-2025-49812 — Faille dans mod_ssl pouvant permettre à des pirates de dégrader les connexions sécurisées

Gravité : **ÉLEVÉE**

Ce que les pirates peuvent en faire :

Rétrograder le niveau de chiffrement ou intercepter le trafic afin d'exposer des données sensibles. mod_ssl est un module Apache ajoutant la prise en charge du chiffrement.

Comment se protéger :

Appliquer les derniers correctifs Apache et imposer des configurations de chiffrement TLS robustes.

CVE-2024-42516 — Une faille de sécurité qui permet aux pirates de manipuler les réponses web HTTP envoyées aux utilisateurs

Gravité : **ÉLEVÉE**

Ce que les pirates peuvent en faire :

Exploiter des faiblesses dans la manière dont un système reçoit et traite les données afin d'injecter du contenu nuisible, ou d'effectuer des redirections pouvant entraîner du phishing, la diffusion de malwares ou le vol de sessions utilisateur.

Comment se protéger :

Appliquer rapidement les correctifs éditeur et imposer des en-têtes de sécurité stricts.

CVE-2024-47252 — Traitement incorrect des journaux d'erreurs dans mod_ssl pouvant exposer des données sensibles

Gravité : **MOYENNE**

Ce que les pirates peuvent en faire :

Injecter du contenu malveillant dans les journaux afin de les corrompre (log poisoning) et potentiellement élever leurs privilèges.

Comment se protéger :

Mettre à jour Apache et restreindre l'accès aux journaux.

CVE-2024-43204 — Faille permettant à des pirates d'amener le serveur à effectuer des requêtes vers des systèmes internes

Gravité : **ÉLEVÉE**

Ce que les pirates peuvent en faire :

Forcer le serveur à effectuer des requêtes vers des systèmes internes et exposer le réseau interne.

Comment se protéger :

Mettre à jour Apache et vérifier les configurations d'en-têtes.

CVE-2020-11023 — Faille de script intersite dans jQuery pouvant permettre l'exécution de scripts malveillants

Gravité : **MOYENNE**

Ce que les pirates peuvent en faire :

Injecter des scripts malveillants.

Comment se protéger :

Mettre à niveau jQuery, nettoyer les entrées utilisateur et utiliser des outils de blocage du code malveillant.

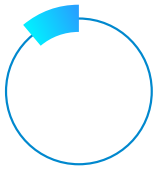
Conclusions supplémentaires de Barracuda Managed Vulnerability Security

4 146

Nombre total de vulnérabilités critiques détectées.

2 525

Nombre total de vulnérabilités uniques identifiées.



11 %

Proportion de vulnérabilités disposant d'un exploit connu.

Rapport d'incident — Firewall non corrigé utilisé dans une tentative RansomHub

Les pirates ont exploité des vulnérabilités non corrigées dans un firewall Fortinet. Ils ont lancé une attaque par force brute contre le réseau d'un client, mais ont été bloqués. Un mois plus tard, ils ont tenté une connexion à distance (SSL VPN), à nouveau bloquée. Deux jours après, ils ont effectué une troisième tentative. Barracuda Managed XDR a détecté une activité PsExec (commande distante) et identifié un logiciel malveillant sur le contrôleur de domaine principal ainsi que sur le serveur de sauvegarde.

Mauvaise configuration : incidents impliquant des outils de sécurité désactivés, accidentellement ou volontairement

Des outils de sécurité mal configurés représentent un risque majeur. Le danger est amplifié par le faux sentiment de sécurité lié au simple fait que l'outil est installé. Au cours des 12 derniers mois, Barracuda Managed XDR a identifié des fonctionnalités désactivées, notamment : agents de protection des endpoints (94 % des détections d'outils de sécurité désactivés), MFA (3,62 %), règle « liens sécurisés » (1,4 %), règle « pièce jointe sécurisée » (0,6 %).

Les études montrent que la plupart des organisations tentent de gérer un trop grand nombre d'outils de sécurité. Lorsque les ressources sont limitées, les erreurs de configuration apparaissent facilement. La meilleure protection repose sur une plateforme de sécurité intégrée offrant une visibilité complète sur les paramètres et configurations, capable d'identifier rapidement et automatiquement les failles à corriger.

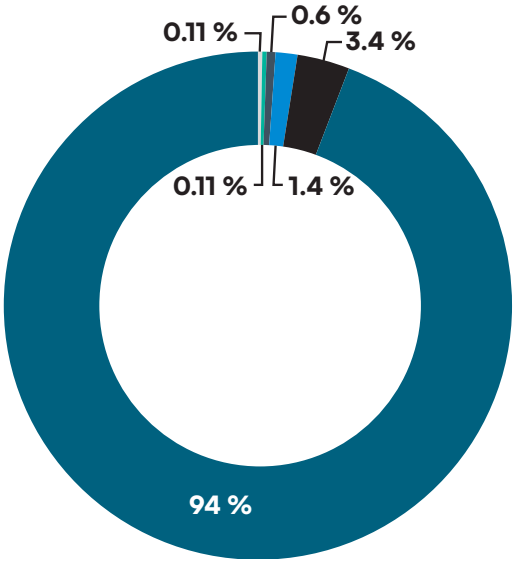


FIGURE 5

Fonctions de sécurité les plus couramment désactivées

- Agent SentinelOne Endpoint désactivé
- MFA Microsoft 365 désactivée
- La règle « Liens sécurisés » de Microsoft 365 ATP est désactivée
- Règle « pièce jointe sécurisée » de Microsoft Office ATP désactivée
- MFA Microsoft Azure désactivée
- Google Workspace MFA désactivé

100 %

Proportion d'incidents traités par Barracuda Managed XDR impliquant au moins un endpoint non protégé ou non autorisé

66 %

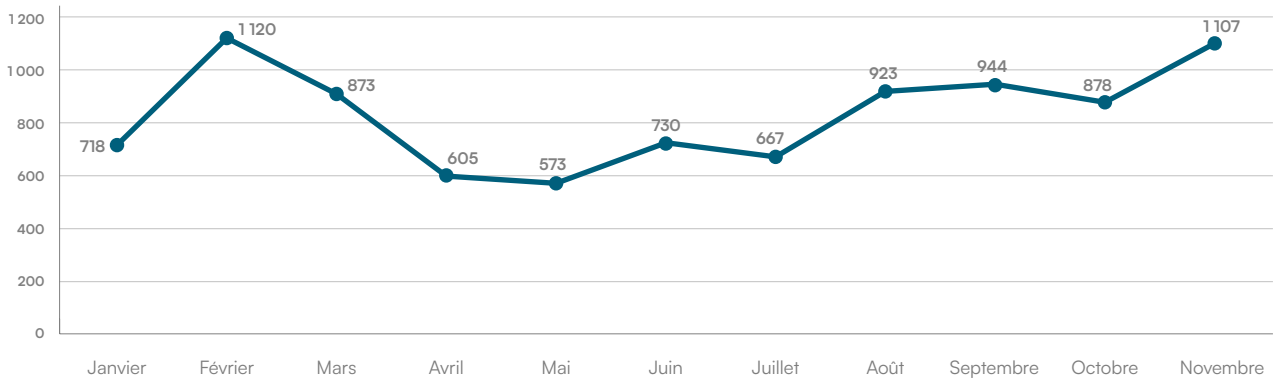
Proportion d'incidents auxquels Barracuda Managed XDR a répondu et qui impliquaient la chaîne d'approvisionnement ou un tiers (en hausse par rapport à 45 % en 2024)

La menace persistante du ransomware

Au cours des 12 derniers mois, Barracuda Managed XDR a identifié 13 514 indicateurs pointant vers des attaques par ransomware en cours, incluant outils, techniques et comportements. Contrairement aux années précédentes, il n'y a plus de pics marqués ou de creux importants, mais un niveau élevé et constant d'incidents tout au long de l'année.

FIGURE 6

2 025 incidents liés à des ransomwares



1,5 % à 5,6 %

Proportion de toutes les organisations touchées par un ransomware chaque mois en 2024

5,1 % à 10,9 %

Proportion de toutes les organisations touchées par un ransomware chaque mois en 2025

Principales familles de ransomware rencontrées en 2025

Akira

- Akira est un groupe de ransomware relativement récent, connu pour cibler des organisations via des attaques sophistiquées. Il utilise fréquemment la double extorsion : chiffrement des données et menace de divulgation d'informations sensibles en cas de non-paiement de la rançon.
- **Tactiques** : Utilisation de malwares avancés, attaques ciblées et vol de données.

Qilin

- Qilin est un groupe de ransomware qui a attiré l'attention avec ses attaques ciblées contre les infrastructures critiques et les grandes entreprises.
- **Tactiques** : Double extorsion, exploitation de vulnérabilités, chiffrement des données via malware.

RansomHub

- RansomHub est un groupe de ransomware qui fonctionne comme un ransomware-as-a-service (RaaS), permettant à ses affiliés de déployer des ransomwares sous leur propre marque.
- **Tactiques** : Modèle « Ransomware-as-a-Service » (RaaS), vol de données et extorsion.

Cactus

- Cactus est un groupe de ransomware impliqué dans des attaques ciblées, exigeant souvent des rançons élevées.
- **Tactiques** : Chiffrement des données, double extorsion et exploitation des vulnérabilités.

Rapport d'incident — De multiples failles de sécurité exposent la cible à Cactus

Les cibles ont été piégées via des appels Teams les incitant à télécharger des fichiers malveillants. Les pirates ont mis en place des canaux leur permettant d'envoyer des commandes à distance, de se déplacer latéralement et d'assurer leur persistance. Des tâches planifiées malveillantes, des modifications du registre et du DLL sideloading (technique consistant à tromper un programme pour qu'il charge une fausse bibliothèque partagée afin d'exécuter le code malveillant à la place du code légitime) ont permis aux pirates d'élever les privilèges et d'échapper à la détection. L'équipe Barracuda Managed XDR a découvert des appareils non autorisés et plus de 1 600 dispositifs non protégés sur le réseau, des autorisations Microsoft Teams trop permissives, des déploiements vulnérables de RDP et SSH, des fichiers non signés ainsi qu'un manque de sensibilisation des employés.

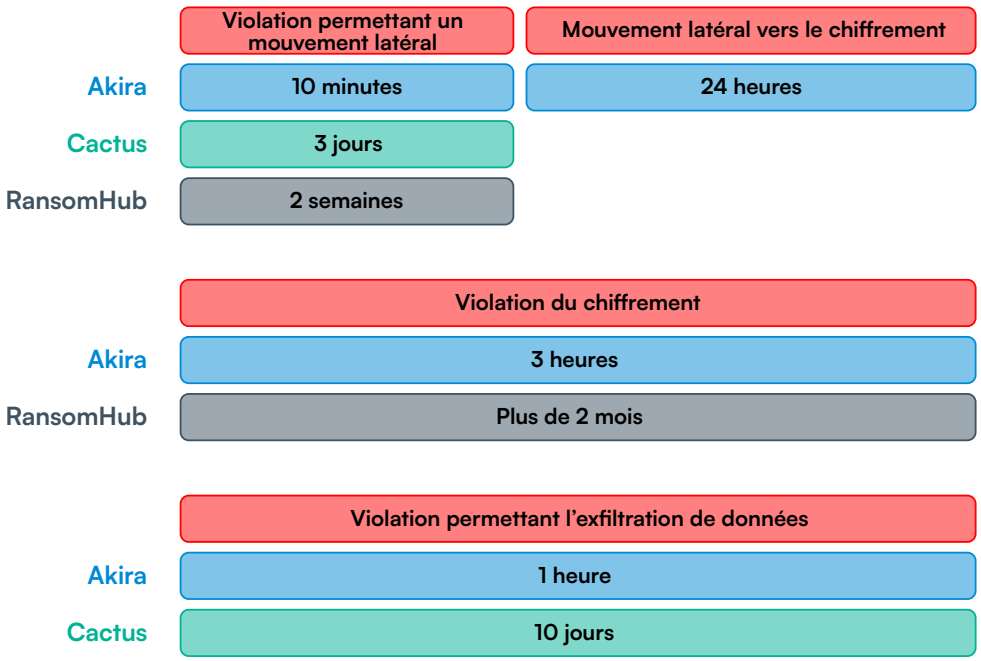
Le ransomware avance à des vitesses variables

Selon les données de détection et d'incidents de Barracuda Managed XDR, les attaques par ransomware les plus rapides en 2025 ont pris seulement quelques heures de bout en bout, tandis que les plus longues ont duré plusieurs mois.

Les intrusions prolongées permettent un maximum de dégâts : reconnaissance approfondie, exfiltration de données, sabotage, etc. Les attaques ultra-rapides, elles, sont plus difficiles à détecter et à contenir avant qu'elles ne soient exécutées et que des dommages ne soient causés.

Les organisations doivent être prêtes pour ces deux scénarios, et disposer d'outils de sécurité en veille permanente.

La rapidité des ransomwares — 3 acteurs



Temps estimés à partir d'incidents réels

Rapport d'incident — XDR intercepte le ransomware Akira exploitant un « compte fantôme » et un serveur non protégé

Les pirates ont pénétré le réseau via un compte créé pour un fournisseur tiers et non désactivé après son départ. Ils ont tenté un mouvement latéral et la désactivation de la sécurité des endpoints, mais ont été bloqués. Ils se sont alors tournés vers un serveur non protégé, ont élevé leurs privilèges et lancé le ransomware. Tous les appareils affectés ont été neutralisés. Parmi les autres risques identifiés : dispositifs non protégés, canal VPN ouvert dans le firewall et MFA appliquée de manière incohérente.

Conclusion : Comment rester protégé dans un monde de menaces complexes

Les équipes de sécurité font face à des défis croissants. Avec des ressources limitées, elles doivent protéger un environnement en constante expansion : appareils, applications, vulnérabilités critiques et outils fragmentés, souvent sans la visibilité unifiée nécessaire pour anticiper les menaces.

La situation va se compliquer davantage avec l'essor de l'IA agentique.

Les systèmes d'IA agentique automatiseront les premières phases répétitives d'une attaque, scanneront les environnements en continu, identifieront des configurations faibles et lanceront des exploits ciblés en quelques minutes. Les acteurs malveillants utilisant des agents IA pourront prendre des décisions, ajuster leurs stratégies et corriger ou réécrire du code malveillant en cas d'échec ou d'obstacle. Ce changement augmentera considérablement la vitesse, l'ampleur et la cohérence des attaques.

Les organisations ont besoin d'une stratégie de sécurité unifiée intégrant des technologies avancées de détection alimentées par l'IA, un SOC entièrement autonome, une formation des utilisateurs, une réponse automatisée aux menaces et une culture de sécurité résiliente.

Des gains rapides sont possibles, comme décrit dans ce rapport : Authentification multifacteur systématique et contrôles d'accès stricts, gestion rigoureuse des correctifs, protection robuste des données, sensibilisation régulière des employés à la cybersécurité.

Ces mesures doivent être soutenues par une plateforme de sécurité complète et gérée, ainsi qu'une solution XDR 24/7 intégrant sécurité réseau, endpoints, serveurs, cloud et messagerie, offrant une visibilité et un contrôle de gestion de bout en bout, appuyés par un SOC entièrement autonome.

La sécurité à long terme repose sur la cyber-résilience. La détection et la prévention sont les fondements de toute stratégie de sécurité. Mais face à des menaces de plus en plus complexes et furtives, la capacité à répondre rapidement et à se remettre d'une attaque avec un impact minimal est déterminante.

Les conclusions de ce rapport sont basées sur les données de détection provenant de Barracuda Managed XDR, plateforme étendue de visibilité, de détection et de réponse (XDR) appuyée par un centre d'opérations de sécurité (SOC) ouvert 24 heures sur 24 et 7 jours sur 7. Cette plateforme permet à nos clients de bénéficier en permanence de services couvrant la détection, l'analyse et la neutralisation des menaces ainsi que la réponse aux incidents. Les prestations fournies font appel à des interventions humaines aussi bien qu'à l'intelligence artificielle.

Barracuda Managed XDR fait partie de BarracudaONE, une plateforme alimentée par l'IA qui sécurise les e-mails, les données, les applications et les réseaux grâce à des solutions innovantes et un tableau de bord centralisé visant à maximiser la protection et à renforcer la cyber-résilience.

Barracuda en quelques mots

Barracuda est une entreprise mondiale de cybersécurité de premier plan qui offre une protection complète contre les menaces complexes aux entreprises de toutes tailles. Notre plateforme BarracudaONE alimentée par l'IA protège les e-mails, les données, les applications et les réseaux grâce à des solutions innovantes, à une plateforme XDR gérée et à un tableau de bord centralisé afin de maximiser 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.