Barracuda XDR

Une approche unifiée de la cybersécurité

La cybersécurité est un parcours. Les meilleures pratiques essentielles en matière de cybersécurité d'aujourd'hui nécessitent davantage que des produits de sécurité autonomes. Contrairement à de nombreux concurrents, le système de détection et de réponse étendues (XDR) de Barracuda associe sa plateforme d'analyse avancée à un Centre d'opérations de sécurité (SOC) fonctionnant 24 h/24 et 7 j/7.

Améliorez votre approche de la cybersécurité

Protégez votre entreprise contre les cybermenaces omniprésentes d'aujourd'hui en adoptant les meilleures pratiques de cybersécurité avec Barracuda XDR. Grâce à Barracuda XDR, votre équipe peut désormais protéger, détecter et répondre de manière proactive aux menaces, grâce au soutien d'un centre d'opérations de sécurité (SOC) disponible 24 h/24 et 7 j/7.

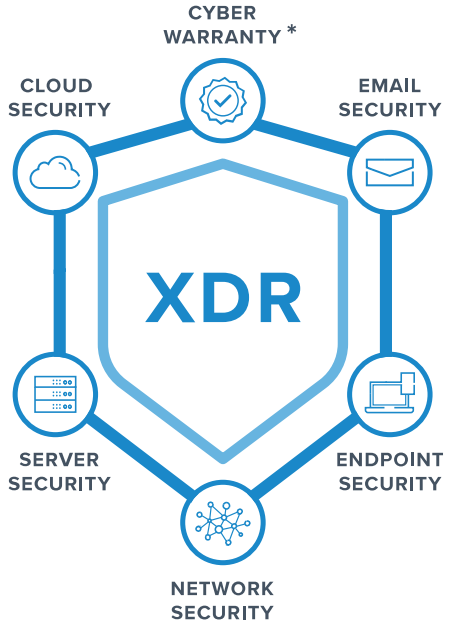
Acquérez une expertise en sécurité et une technologie

Augmentez instantanément vos ressources internes en sécurité grâce à des équipes d'experts chevronnés et à une plateforme SOC innovante. Chaque équipe SOC travaille en arrière-plan pour fournir des services de détection et de réponse proactifs. Les équipes SOC recherchent et développent en permanence de nouvelles avancées et optimisations en matière de sécurité, afin de permettre à Barracuda XDR de garder une longueur d'avance sur le paysage en constante évolution des cybermenaces.

La plateforme Barracuda XDR unifie la gestion des informations et des évènements de sécurité (SIEM), l'orchestration, l'automatisation et la réponse en matière de sécurité (SOAR), et une plateforme de renseignement sur les menaces (TIP) avec plus de 11 milliards d'indicateurs de compromission (IOC). Le résultat combiné garantit que les équipes SOC peuvent détecter et trier les incidents de manière efficace, et vous fournir des alertes enrichies et des recommandations prescriptives pour résoudre rapidement les incidents.

Défense approfondie

Créez des anneaux concentriques de protection autour de vos données, de vos appareils et de vos utilisateurs. Plusieurs niveaux de sécurité sont nécessaires pour fournir la protection dont les entreprises ont besoin. Barracuda XDR ajoute des couches de protection supplémentaires pour les principales surfaces d'attaque telles que la messagerie, les points de terminaison, les serveurs, les firewalls et les dispositifs cloud.



Fonctionnalités principales :

Visibilité étendue : allez au-delà de la triade de visibilité traditionnelle des points de terminaison, du réseau et des journaux. Cette plateforme de cybersécurité cloud native offre une vue unique de la télémétrie supplémentaire dans vos environnements. La plateforme Barracuda XDR analyse également les données des solutions de sécurité existantes pour offrir une visibilité centralisée.

Sécurité en profondeur : créez des niveaux de sécurité autour de vos données, appareils et utilisateurs. Une stratégie de défense en profondeur est nécessaire pour fournir la protection dont les entreprises ont besoin.

Télémétrie indépendante des fournisseurs : la liste croissante des intégrations technologiques permet aux équipes de Barracuda XDR de surveiller les sources de données les plus demandées. Les détections propriétaires sont alimentées par l'apprentissage automatique (ML) et sont cartographiées au cadre MITRE ATT&CK®, ce qui permet à Barracuda XDR de détecter les acteurs malveillants plus rapidement et de prédire leur prochain mouvement.

Renseignements sur les menaces : Barracuda utilise un vaste référentiel mondial d'indicateurs de menaces, alimenté par des flux riches de renseignements de sécurité provenant de sources diverses, y compris l'intelligence propriétaire de Barracuda, pour prendre des mesures efficaces afin de protéger vos précieuses ressources.

SOC 24 h/24 et 7 j/7 : Bénéficiez d'une surveillance des menaces en temps réel ainsi que des conseils d'équipes d'experts en sécurité spécialisés, pour une couverture 24 h/24, 7 j/7 et 365 j/an. L'infrastructure SOC inclut les technologies SOAR (sécurité, orchestration, automatisation et réponse) ainsi que l'apprentissage automatique pour garantir que seules les alertes légitimes sont examinées et remontées sans délai.

Démonstration de valeur : des rapports personnalisables sont disponibles pour illustrer le travail accompli.

Compris dans la suite Barracuda XDR :

XDR : plateforme proactive de cybersécurité en tant que service, soutenue par des équipes d'experts en sécurité chevronnés dans un centre d'opérations de sécurité (SOC) fonctionnant 24 h/24 et 7 j/7.

XDR Endpoint Security : détecte et réponde efficacement aux menaces avancées telles que les attaques zero-day, les ransomwares, et plus encore.

XDR Email Security : surveille de manière proactive votre solution existante de sécurisation des e-mails pour renforcer la protection contre le spear phishing, la compromission de la messagerie d'entreprise (BEC), et plus encore.

XDR Cloud Security : sécurise vos environnements cloud contre les accès non autorisés aux boîtes de réception cloud, les modifications administrateur, les connexions impossibles et les attaques par force brute.

XDR Network Security : détecte les activités potentiellement malveillantes sur vos réseaux, telles que les connexions de commande et contrôle, les attaques par déni de service, l'exfiltration de données et la reconnaissance.

XDR Server Security : protège vos systèmes contre les attaques sophistiquées telles que le bourrage de mots de passe, les attaques par force brute et l'élévation de privilèges.

Pour en savoir plus, rendez-vous sur

fr.barracuda.com/products/managed-xdr

Barracuda®
Your journey, secured.