

Barracuda Email Protection

Sécurité totale pour Microsoft Office 365

Pour les entreprises qui veulent protéger leurs activités, leurs marques et leur personnel contre les menaces les plus avancées véhiculées par e-mail, Barracuda Email Protection est une solution complète et simple à utiliser : protection des passerelles, protection des boîtes de réception par API, réponse aux incidents, protection des données et capacités de mise en conformité.

Bloquez le spam, les malwares et les menaces zero-day

Barracuda utilise des techniques avancées pour détecter le spam et les malwares connus. La protection comprend la continuité du service de messagerie, le filtrage sortant et le chiffrement pour lutter contre les fuites de données. La protection contre les menaces avancée intégrée utilise l'analyse de la charge utile et le sandboxing pour découvrir les programmes malwares zero-day. Enfin, Link Protection redirige les URL suspectes et typosquattées et la sécurité web bloque l'accès aux domaines malicieux pour empêcher les destinataires de télécharger des malwares par inadvertance.

Protégez-vous en temps réel contre le Spear Phishing

L'architecture API unique de Barracuda permet à son moteur IA d'étudier l'historique des e-mails et d'en déduire les modèles de communication propres aux différents utilisateurs. La solution peut ensuite identifier les anomalies dans les métadonnées et le contenu des messages afin de trouver et de bloquer en temps réel les attaques d'ingénierie sociale.

Protégez votre entreprise contre le piratage de comptes

Bloquez les attaques par phishing

utilisées pour collecter les identifiants et pirater les comptes. La solution détecte les comportements anormaux et alerte le service informatique, puis identifie et supprime tous les e-mails frauduleux envoyés à partir des comptes piratés.

Réagissez aux menaces e-mail après leur réception

Identifiez les menaces potentielles après leur distribution en vous appuyant sur les informations recueillies lors de l'analyse des e-mails précédemment distribués et sur les renseignements fournis par la communauté. Protégez vos ressources informatiques grâce à la suppression automatique des messages malicieux et aux manuels de réponse automatisés. Gardez une longueur d'avance sur les cybercriminels et bloquez les futures attaques grâce à une restauration continue.

Formez les utilisateurs aux dernières menaces

Ainsi, vos utilisateurs sauront reconnaître les dernières techniques de phishing et empêcheront les attaques de se propager dans votre entreprise. Nous vous proposons des supports de formation stimulants et des simulations de phishing basées sur des menaces réelles.

Protégez vos données et votre conformité

Bénéficiez d'une sauvegarde cloud de toutes vos données Office 365, notamment les boîtes de messagerie Exchange Online, SharePoint Online, OneDrive Entreprise et Teams. Récupérez rapidement vos données à un moment précis en cas de suppression accidentelle ou malicieuse. L'archivage cloud vous permet de répondre aux exigences de conformité grâce à l'e-Discovery, les règles de rétentions granulaires et le stockage illimité.

Protégez-vous contre les attaques latérales

La transformation digitale vers le cloud - tout particulièrement vers Microsoft 365 - s'est accélérée au cours des dernières années. Ce phénomène s'est accompagné d'une augmentation du nombre d'employés et d'entrepreneurs à distance, ainsi que des politiques de BYOD. Résultat : une nouvelle surface d'attaque, où un compte compromis expose l'ensemble de la suite collaborative à des attaques latérales. Barracuda superpose la sécurité de la messagerie avec Zero Trust Access afin que pour que vous puissiez vérifier en permanence l'identité et la conformité de votre personnel et de vos appareils.

Principales caractéristiques

Protection contre le phishing et l'usurpation d'identité

- Connectivité directe à Office 365
- Configuration simple et rapide (moins de 5 minutes)
- Bloquez les attaques de spear phishing, la compromission de la messagerie professionnelle, l'extorsion et les autres attaques d'ingénierie sociale
- Intelligence artificielle pour détecter et stopper les attaques par e-mail en temps réel
- Détection et signalement des activités de piratage de comptes
- Notification des utilisateurs externes et suppression des e-mails piratés
- Blocage de l'accès aux comptes piratés pour les attaquants
- Visibilité des modifications des règles des boîtes de réception et des ouvertures de session suspectes
- Rapports et analyse de l'environnement de menaces

La réponse aux incidents

- Module Outlook complémentaire et signalement des menaces en un clic
- Les alertes relatives aux incidents de sécurité
- Données géographiques
- Données sur les menaces provenant de la communauté
- Données sur les destinataires et les comportements
- Suppression des e-mails de la boîte de réception des utilisateurs
- Définition de règles pour les e-mails entrants
- Blocage de l'accès au contenu malicieux
- Restauration automatique en cas d'identification de contenu malicieux
- Correction continue
- Conception automatisée de workflows
- Intégration API pour les plateformes SOAR/SIEM/XDR

Cloud-to-Cloud Backup

- Sauvegarde et restauration pour Office 365 (Exchange Online, SharePoint Online, OneDrive et Teams Entreprise)
- Programmation et restauration détaillées
- Sauvegardes automatisées ou manuelles
- Nombreuses options de restauration
- Restauration granulaire des éléments SharePoint
- Restauration sur Exchange Online ou OneDrive Entreprise ou téléchargement des fichiers localement

Email Gateway Defense

- Solution de protection cloud contre le spam, les malwares, les virus, le phishing et les autres menaces véhiculées par e-mail
- Advanced Threat Protection (protection avancée contre les menaces) utilisant le sandboxing avec émulation complète du système.
- Chiffrement des e-mails et protection contre la perte de données sans agent
- Protection contre les liens suspects et le typosquattage
- Continuité des e-mails avec basculement du service de messagerie sur le cloud
- Boîte de réception d'urgence pour envoyer, recevoir, lire et répondre aux e-mails

Archivage sur le cloud

- Archiver directement depuis Office 365 vers le cloud
- Gestion PST de la messagerie électronique existante
- Politiques de conservation précises
- Recherche dans l'intégralité du texte avec plusieurs opérateurs

Formation à la sécurité

- Simulation des menaces pour les e-mails, les SMS, la voix et les supports physiques
- Modèles de menaces réelles
- Formation à la sécurité et vidéos de micro-apprentissage
- Quiz et formulaires d'évaluation des risques
- Collecte de plus de 16 000 points de données
- Analyse détaillée des tendances
- Rapports et tableaux de bord personnalisables

Protection contre l'usurpation du nom de domaine

- Authentification, rapports et analyses DMARC
- Blocage du spoofing de domaine et du détournement de la marque

Sécurité web

- Protection contre les menaces Web
- Filtrage du contenu Web
- Journaux de filtrage Web
- Rapports d'administration
- Alertes automatiques

Data Inspector

- Analyse les données OneDrive et SharePoint à la recherche d'informations sensibles et de fichiers malveillants
- Identification des fichiers malicieux
- Paramètres de classification des données
- Envoi de notifications automatiques par e-mail aux administrateurs, responsables de la conformité et utilisateurs
- Contrôle d'accès basé sur les rôles
- Capacités de chiffrement avancées

Accès Zero Trust

- Protection contre le phishing et blocage des menaces au niveau de l'appareil
- Moteur de politique de contrôle d'accès basé sur des rôles et des attributs
- Approvisionnement simplifié
- Mise en œuvre de politiques globales - Conformité

La protection des e-mails Barracuda est disponible dans trois forfaits. Trouvez celui le plus adapté à vos besoins.

CAPACITÉS	ADVANCED	PREMIUM	PREMIUM PLUS
Protection contre les spams et les malwares	✓	✓	✓
Protection des pièces jointes	✓	✓	✓
Protection des liens	✓	✓	✓
Continuité du service de messagerie	✓	✓	✓
Chiffrement des e-mails	✓	✓	✓
Prévention contre la fuite de données	✓	✓	✓
Protection contre le phishing et l'usurpation d'identité	✓	✓	✓
Protection contre le piratage de comptes	✓	✓	✓
Restauration automatique	✓	✓	✓
Protection contre l'usurpation du nom de domaine		✓	✓
Sécurité web		✓	✓
Chasse et réponse aux menaces		✓	✓
Workflows automatisés		✓	✓
Intégration SIEM/SOAR/XDR		✓	✓
Archivage dans le cloud			✓
Cloud-to-Cloud Backup			✓
Data Inspector			✓
Simulation d'attaques			✓
Formation à la sécurité			✓
Accès Zero Trust			✓

