NUOVI SERVIZI

BARRACUDA EMAIL PROTECTION

Barracuda

Scopri il piano di sicurezza che fa per te: ADVANCED, PREMIUM o PREMIUM PLUS

ADVANCED

Barracuda Email Protection ADVANCED

Combina email gateway e intelligenza artificiale per bloccare le minacce.
Garantisce la protezione contro 13 tipi di minacce e-mail.
Ripara automaticamente le minacce successivamente alla consegna.

PREMIUM

Barracuda Email Protection PREMIUM

Include tutto Advanced.
Protegge il tuo marchio dalle frodi sui domini.
Rende la navigazione web sicura per i tuoi utenti. Automatizza la ricerca e la risposta alle minacce dopo la consegna.

PREMIUM PLUS

Barracuda Email Protection PREMIUM PLUS

Include tutto Premium.
Migliora la consapevolezza della sicurezza degli utenti. Protegge e ripristina i tuoi dati di Office365. Scopre i dati sensibili e il malware archiviato non rilevato. Risponde alla conformità normativa.

	ADVANCED	PREMIUM	PREMIUM PLUS
• Spam and Malware Protection Identifica e blocca spam, virus e malware inviati tramite email. Utilizzando l'antivirus, il punteggio spam, l'analisi dell'intento in tempo reale, la protezione dei collegamenti URL, i controlli della reputazione e altre tecniche, Barracuda esegue la scansione di messaggi e file di posta elettronica.	✓	✓	✓
• Attachment Protection Barracuda combina tecnologie comportamentali, euristiche e sandboxing per proteggere da attacchi zero-hour e mirati. Un ambiente sandbox viene utilizzato per far esplodere e osservare il comportamento degli allegati sospetti.	✓	✓	✓
• Link Protection Link Protection riscrive automaticamente gli URL in modo che la sandbox di Barracuda blocchi i collegamenti dannosi.	✓	✓	✓
• Email Continuity In caso di interruzione del server di posta o perdita di connettività, una cassetta postale di emergenza consente agli utenti di continuare a inviare e ricevere e-mail, rimanendo produttivi fino a quando i server primari non tornano online.	✓	✓	✓

BARRACUDA EMAIL PROTECTION

	ADVANCED	PREMIUM	PREMIUM PLUS
• Email Encryption Protegge la tua posta crittografandola durante il trasporto al Barracuda Message Center, crittografandola a riposo per l'archiviazione nel cloud e fornendo un recupero sicuro da parte dei tuoi destinatari tramite l'accesso web HTTPS. Crea un criterio per crittografare automaticamente le e-mail in base al mittente, al contenuto e ad altri criteri.	✓	✓	✓
• Data Loss Prevention Crea e applica criteri di contenuto per impedire che dati sensibili, inclusi numeri di carte di credito, di previdenza sociale, dati HIPAA, elenchi di clienti e altre informazioni private, vengano inviati tramite e-mail. I criteri possono crittografare, mettere in quarantena o bloccare automaticamente determinate e-mail in uscita in base al contenuto, al mittente o al destinatario.	✓	✓	✓
• Phishing and Impersonation Protection Rileva e previene automaticamente la rappresentazione, la compromissione della posta elettronica aziendale e altri attacchi mirati. Il motore di intelligenza artificiale di Barracuda apprende i modelli di comunicazione unici di ogni azienda e sfrutta questi modelli per identificare le anomalie e prevenire attacchi di ingegneria sociale in tempo reale.	✓	✓	✓
• Account Takeover Protection Arresta gli attacchi di phishing utilizzati per raccogliere le credenziali per l'acquisizione dell'account. L'intelligenza artificiale rileva il comportamento anomalo delle e-mail e avvisa l'IT, quindi trova e rimuove tutte le e-mail fraudolente inviate dagli account compromessi.	✓	✓	✓
• Automatic Remediation Tutti i messaggi segnalati dall'utente vengono scansionati alla ricerca di URL o allegati dannosi. Quando viene rilevata una minaccia, tutte le e-mail corrispondenti vengono spostate dalle cassette postali degli utenti nelle cartelle della posta indesiderata.	✓	✓	✓
• Threat Hunting and Response Identifica rapidamente e risolve in modo efficiente le minacce successive alla consegna automatizzando i flussi di lavoro investigativi e consentendo la rimozione diretta delle e-mail dannose.		✓	✓
• Automated Workfows [NEW] Crea playbook personalizzati per automatizzare completamente il processo di risposta agli incidenti. Gli amministratori a qualsiasi livello tecnico possono creare un flusso di lavoro definendo un trigger, determinando le condizioni e assegnando le azioni desiderate tramite una semplice interfaccia utente.		✓	✓
• SIEM/SOAR/XDR Integration [NEW] Orchestra la risposta agli incidenti tra prodotti con API RESTful (beta) e integrazioni syslog. Amministra e configura in remoto le funzionalità di risposta agli incidenti e archivia i dati degli eventi per il monitoraggio, l'analisi e la risoluzione dei problemi.		✓	✓

BARRACUDA EMAIL PROTECTION

	ADVANCED	PREMIUM	PREMIUM PLUS
• Domain Fraud Protection Previene le frodi del dominio e-mail con i rapporti e l'analisi DMARC. Barracuda fornisce visibilità e analisi granulari dei report DMARC e aiuta a ridurre al minimo i falsi positivi, a proteggere le e-mail legittime e a prevenire lo spoofing.		✓	✓
• DNS Filtering [NEW] Protegge gli utenti dall'accesso a contenuti Web dannosi con DNS e filtri URL avanzati.		✓	✓
• Cloud Archiving Un archivio indicizzato e basato su cloud consente criteri di conservazione granulari, ricerche approfondite, controllo/permessi basati sui ruoli, blocco per motivi legali ed esportazione. Rispetta facilmente le richieste di e-discovery e i requisiti normativi o di conservazione delle policy.			✓
• Cloud-to-Cloud Backup Ottieni la protezione dei dati e il backup nel cloud per i dati di Office 365, incluse le cassette postali di Exchange Online, SharePoint Online, OneDrive for Business e Teams. Recupero rapido point-in-time in caso di cancellazione accidentale o dolosa.			✓
• Data Inspector [NEW] Scansiona automaticamente i tuoi dati di OneDrive for Business e SharePoint alla ricerca di informazioni riservate e file dannosi contenenti malware. Usalo per sviluppare politiche conformi a GDPR, CCPA e altre normative sulla privacy dei dati.			✓
• Attack Simulation Gli attacchi di phishing simulati vengono costantemente aggiornati per riflettere le minacce più recenti e più comuni. Le simulazioni non si limitano all'e-mail, ma includono anche attacchi vocali, SMS e supporti portatili (chiavetta USB).			✓
• Awareness Training Ottieni l'accesso a una tecnologia didattica avanzata e automatizzata che include formazione basata sulla simulazione, test continui, potenti rapporti per gli amministratori e consapevolezza attiva della risposta agli incidenti.			✓