

Barracuda Email Protection

Completa per Microsoft Office 365

Per le organizzazioni che desiderano proteggere il proprio business, i marchi e le persone dalle minacce più avanzate, veicolate tramite e-mail, Barracuda Email Protection è una soluzione completa e semplice da utilizzare, in grado di fornire funzionalità di difesa del gateway, difesa della posta in arrivo basata su API, risposta agli incidenti, protezione dei dati e conformità.

Blocco di spam, malware e minacce zero-day

Barracuda si avvale di tecniche avanzate per rilevare spam e malware noti, apporta inoltre continuità al servizio e-mail e utilizza filtri e crittografia in uscita per evitare la perdita di dati. Advanced Threat Protection è integrato e utilizza l'analisi del payload e il sandboxing per individuare malware zero-day. La protezione dei link reindirizza gli URL sospetti e dirottati (typosquatting), e i filtri per i DNS bloccano l'accesso a domini Web dannosi per evitare che i destinatari scarichino malware inavvertitamente.

Difesa in tempo reale dallo spear phishing

L'esclusiva architettura basata su API di Barracuda consente al motore AI di analizzare le e-mail cronologiche e acquisire gli schemi di comunicazione tipici degli utenti. È in grado di identificare anomalie nei metadati e nel contenuto dei messaggi per individuare e bloccare in tempo reale gli attacchi di social engineering.

Difesa dell'organizzazione dal furto di account

Barracuda blocca gli attacchi di phishing utilizzati dagli hacker per acquisire le credenziali e portare a termine il furto di account. Rileva i comportamenti anomali nell'e-mail e avverte l'IT, quindi individua e rimuove le e-mail fraudolente inviate dagli account compromessi.

Risposta alle minacce e-mail dopo la consegna

Le possibili minacce vengono identificate dopo la consegna, in base a informazioni raccolte dall'analisi di altre e-mail recapitate in precedenza e dall'intelligence basata su community. Per preservare le risorse IT sono disponibili funzionalità di rimozione automatica dei messaggi dannosi e schemi di risposta automatizzati, per rimanere sempre un passo avanti rispetto ai criminali informatici e bloccare gli attacchi futuri con correzioni continue.

Formazione degli utenti sulle minacce più recenti

Insegnando agli utenti a riconoscere le tecniche di phishing più recenti si può evitare che gli attacchi si diffondano all'interno dell'organizzazione. Barracuda mette a disposizione materiale di formazione e simulazioni di phishing altamente coinvolgenti, basati su minacce in circolazione.

Protezione dei dati e garanzia di conformità

Backup in cloud per i dati di Office 365, compresi quelli delle caselle di posta di Exchange Online, di SharePoint Online, di OneDrive for Business e di Teams. Ripristino temporizzato rapido in caso di eliminazione accidentale o dolosa. L'archiviazione in cloud consente di far fronte ai requisiti di conformità, grazie a e-discovery, criteri di conservazione granulari e storage illimitato.

Funzioni chiave

Protezione dal phishing e dall'impersonificazione

- Connettività diretta a Office 365
- Configurazione rapida e semplice (meno di 5 minuti)
- Blocco degli attacchi di spear phishing, business email compromise (BEC), estorsione e di altri attacchi basati sul social engineering
- Intelligenza artificiale (AI) per rilevare e bloccare in tempo reale gli attacchi e-mail
- Rilevamento e avvisi in caso di attività di furto di account
- Invio di notifiche agli utenti esterni ed eliminazione delle e-mail compromesse
- Blocco dell'accesso da parte degli autori dell'attacco agli account compromessi
- Visibilità delle modifiche apportate alle regole della posta in arrivo e accessi sospetti
- Analisi e report relativi all'ambiente delle minacce

Risposta agli incidenti

- Componente aggiuntivo per Outlook e segnalazione delle minacce con un solo clic.
- Avvisi per gli incidenti di sicurezza
- Informazioni geografiche
- Dati delle minacce basati su community
- Dati su destinatari e comportamenti
- Rimozione delle e-mail dalle caselle di posta degli utenti
- Impostazione di criteri per le e-mail in arrivo
- Blocco dell'accesso a contenuti Web dannosi
- Risoluzione automatica dei contenuti dannosi
- Correzione continua
- Creazione di flussi di lavoro automatizzati
- Integrazione API per piattaforme SOAR/SIEM/XDR

Cloud-to-Cloud Backup

- Backup and recovery for Office 365: Exchange Online, SharePoint Online, OneDrive, and Teams for Business.
- Granular scheduling and restores
- Automated or manual backups
- Multi-selection restores
- Granular recovery of SharePoint items
- Restore back to Exchange Online or OneDrive for Business, or download files locally

Email Gateway Defense

- Protezione basata sul cloud contro spam, malware, virus, phishing e altre minacce veicolate tramite e-mail
- Advanced Threat Protection con sandbox di emulazione dell'intero sistema
- Crittografia dell'e-mail senza agente e prevenzione della perdita di dati
- Protezione dei link e contro il dirottamento (typosquatting)
- Continuità dell'e-mail con failover su un servizio basato sul cloud
- Caselle di posta di emergenza per di inviare, ricevere, leggere e rispondere alle e-mail

Archiviazione in cloud

- Inoltro diretto da Office 365 all'archivio basato sul cloud
- Gestione file PST per le e-mail legacy
- Criteri di conservazione granulari
- Ricerca di testo completo con più operatori

Security Awareness Training

- Simulazione di minacce per e-mail, SMS, caselle vocali e supporti fisici
- Modelli basati su minacce in circolazione
- Informazione sulla sicurezza e video di microlearning
- Quiz e questionari per la valutazione dei rischi
- Raccolta di oltre 16.000 punti dati
- Analisi dettagliata delle tendenze
- Report e dashboard personalizzabili

Protezione dalla frode sui domini

- Autenticazione DMARC, report e analisi
- Prevenzione dello spoofing di dominio e brand hijacking

Filtri per i DNS

- Protezione dalle minacce basate sul Web
- Filtri per i contenuti Web
- Registri dei filtri Web
- Report amministrativi
- Avvisi automatici

Data Inspector

- Esegue la scansione di OneDrive e SharePoint alla ricerca di informazioni sensibili e file dannosi
- Identificazione dei file dannosi
- Impostazioni di classificazione dei dati
- Notifiche automatizzate via e-mail per amministratori, responsabili della conformità e utenti
- Controllo degli accessi basato su ruoli
- Funzionalità di crittografia avanzata

Barracuda Email Protection è disponibile con tre piani diversi. Ogni piano consente di soddisfare esigenze specifiche.

FUNZIONALITÀ	ADVANCED	PREMIUM	PREMIUM PLUS
Protezione da spam e malware	✓	✓	✓
Protezione allegati	✓	✓	✓
Protezione link	✓	✓	✓
Continuità servizio e-mail	✓	✓	✓
Crittografia e-mail	✓	✓	✓
Prevenzione perdita di dati	✓	✓	✓
Protezione da phishing e impersonificazione	✓	✓	✓
Protezione dal furto di account	✓	✓	✓
Correzione automatica	✓	✓	✓
Protezione dalla frode sui domini		✓	✓
Filtri per i DNS		✓	✓
Ricerca di minacce e risposta		✓	✓
Flussi di lavoro automatizzati		✓	✓
Integrazione con SIEM/SOAR/XDR		✓	✓
Archiviazione in cloud			✓
Cloud-to-Cloud Backup			✓
Data Inspector			✓
Simulazione attacchi			✓
Security Awareness Training			✓

