Specifiche delle prestazioni
365 Extended Email Protection

365 Extended Email Protection offre un ulteriore livello di sicurezza per proteggere il traffico e-mail dei clienti Microsoft 365 attraverso il suo approccio Integrated Cloud Email Security. I filtri anti-spam e malware di Hornetsecurity, basati sull'AI, analizzano il traffico e-mail in arrivo in tempo reale per individuare le minacce informatiche avanzate e rimuovere in modo affidabile lo spam e le e-mail dannose dalle caselle di posta degli utenti in pochi secondi. L'integrazione completamente automatizzata e senza soluzione di continuità del servizio con la piattaforma Microsoft 365 consente il monitoraggio continuo di tutte le caselle di posta elettronica e si affida all'intelligence sulle minacce di Hornetsecurity 24 ore su 24, 7 giorni su 7, per garantire la protezione più aggiornata.

Il prerequisito per l'utilizzo del servizio è l'uso di licenze Microsoft Cloud con funzionalità Exchange abilitate da Microsoft.

I seguenti servizi sono inclusi nel prodotto 365 Extended Email Protection:

1. Facilità di inserimento
    a. La configurazione di 365 Extended Email Protection è automatizzata. Tutti i domini, le caselle di posta e i gruppi del cliente vengono trasferiti direttamente da Microsoft 365 al pannello di controllo di Hornetsecurity.
    b. Il prerequisito per l'utilizzo dei servizi Hornetsecurity per Microsoft 365 è l'abilitazione dell'App ID Hornetsecurity per il tenant Microsoft 365 da parte di un utente amministrativo del cliente. Questa operazione viene eseguita una volta durante il processo di onboarding.
    c. Non è necessario modificare i record MX per utilizzare il servizio, poiché 365 Extended Email Protection si integra perfettamente con la piattaforma 365 tramite l'interfaccia API. Tutte le e-mail in arrivo dal client vengono copiate tramite il journaling delle e-mail e filtrate dai filtri avanzati di Hornetsecurity.
    d. L'onboarding può essere eseguito direttamente nel Pannello di controllo o tramite un link di onboarding esterno.

2. Accesso singolo
    a. Tutti gli utenti con accesso amministrativo possono autenticarsi a Hornetsecurity utilizzando le proprie credenziali amministrative di Microsoft 365.
    b. Se gli utenti hanno già effettuato l'accesso a Microsoft 365, non hanno bisogno di autenticarsi nuovamente a Hornetsecurity.

3. Minacce rilevate

a. Le e-mail rilevate come minacce vengono mostrate agli utenti e rimosse dalle caselle di posta elettronica in una panoramica configurabile e filtrabile individualmente. Inoltre, vengono visualizzate informazioni dettagliate su ciascuna e-mail.

b. Le e-mail del cliente ricevute attraverso l'email journaling vengono analizzate da Hornetsecurity alla ricerca di contenuti dannosi (ad esempio, virus) e pubblicità indesiderate (ad esempio, spam). Le e-mail dannose e le pubblicità indesiderate vengono automaticamente rimosse dalle caselle di posta del cliente finale.

c. Gli utenti possono recuperare le e-mail dalla panoramica e consegnarle al destinatario.

d. Le e-mail rimosse vengono conservate in quarantena per tre mesi per essere visualizzate e recuperate dagli utenti.

e. Il tasso di rilevamento dello spam e delle minacce è almeno del 99,9% su una media mensile, basata sul numero di tutte le e-mail che raggiungono i sistemi di Hornetsecurity per i domini del cliente nel periodo di tempo misurato.

f. Il tasso di falsi positivi è inferiore a 0,00015 su una media mensile, basata sul numero di tutte le e-mail pulite che raggiungono i sistemi di Hornetsecurity per i domini del cliente nel periodo di tempo misurato.

4. Cruscotto

La dashboard fornisce all'utente una panoramica dei servizi Hornetsecurity prenotati.

5. Rapporti e conformità

a. Il cliente riceve ampie informazioni e statistiche sul suo attuale stato di sicurezza.

b. Questo include le statistiche sulle e-mail e le statistiche sulle minacce avanzate:

- Somma totale delle e-mail scansionate
- Somma totale delle minacce rilevate
- Email classificate per minaccia nel tempo
- Le 100 principali caselle di posta elettronica attaccate
- Attacchi nel tempo
- Minacce per tipo e vettore di attacco
- Vettori di attacco nel tempo

c. Le attività svolte dagli utenti del Pannello di controllo vengono registrate in un Registro attività, ad esempio il recupero di un'e-mail o l'impostazione di un altro servizio.

6. Policy sull'uso avveduto

a. La larghezza di banda, la memoria, l'infrastruttura e le risorse che sono richieste per l'utilizzo della soluzione e che rendiamo disponibili a tal fine sono condivise con tutti i nostri clienti. Abbiamo il diritto, di conseguenza, di assumere misure per assicurare che tutti i clienti utilizzino la soluzione in modo ragionevole e corretto in modo tale che tale uso non interferisca o impedisca la normale esecuzione del servizio per altri clienti.

b. Abbiamo deciso di non impostare valori di riferimento pre-definiti che determinino un uso eccessivo o irragionevole poiché, a nostra discrezione, potremmo scegliere di preservare i nostri normali livelli di servizio ricollocando risorse riservate ad altri utenti che, in quel particolare momento, non sono utilizzate, ovvero bilanciare le risorse. Se decidiamo di non applicare attivamente la nostra policy sull'uso avveduto non significa che abbiamo rinunciato al diritto di operare in quel modo, né che vi abbiamo permesso di continuare ad utilizzare i nostri servizi allo stesso livello in ogni momento.

c. Per beneficiare dei nostri servizi vi richiediamo di acquistare unità fatturabili. Il numero di unità fatturabili che richiedete dipende da alcuni criteri, come le dimensioni dell'organizzazione, il numero di utenti, le dimensioni di archiviazione dei dati delle fonti specifiche, ecc.

d. Indipendentemente dal numero delle unità fatturabili che avete acquistato dovrete usare i nostri servizi in modo avveduto, specificatamente in un modo che non richieda una nostra allocazione sproporzionata delle risorse. Per determinare quanto sopra confronteremo il vostro uso delle nostre risorse (ad esempio, requisiti di memoria, numero di connessioni parallele) con quello del cliente medio. Determiniamo il cliente medio non tenendo in considerazione il 5% dei clienti che utilizzano di più una particolare risorsa e il 5% dei clienti che la utilizzano di meno e facendo la media di tutti i nostri clienti attivi.

e. Qualsiasi caratteristica relativa al settore in cui operate non sarà tenuta in considerazione nello stabilire se l'utilizzo debba essere considerato ragionevole.

f. Se noi, agendo in modo responsabile e in buona fede, riterremo che il vostro uso della nostra soluzione non tenga conto o sia contrario rispetto a questa policy, assumeremo uno dei seguenti provvedimenti a nostra sola discrezione:

   i. Vi consentiremo di continuare a utilizzare le nostre soluzioni previo pagamento di oneri addizionali e il rispetto di qualsiasi condizione che considereremo ragionevole in tali circostanze.
   ii. Vi notificheremo la chiusura del vostro account entro un determinato periodo di tempo ragionevolmente impostato a nostra discrezione. Durante questo periodo, tutti i servizi e/o le operazioni saranno sospesi.

g. Se esercitiamo il diritto di chiudere il vostro account come sopra indicato si verificherà quanto segue:

   i. Tutti i dati (metadati, dati di backup o altro) saranno cancellati al termine del periodo di tempo indicato nella notifica che vi invieremo, nonostante qualsiasi cosa in contrario indicata nei Termini e condizioni.
   ii. Vi saranno rimborsati i costi da voi sostenuti in anticipo per i giorni rimanenti del periodo di sottoscrizione.