Symantec™ Email Security.cloud

Descrizione del servizio

Settembre 2018

Questa Descrizione del servizio descrive Symantec Email Security.cloud ("Servizio"). Tutti i termini scritti in lettere maiuscole citati in questa descrizione hanno il significato che gli è stato attribuito nel Contratto (definito di seguito) o nella sezione Definizioni.

La Descrizione del servizio (compreso qualsiasi allegato incluso per riferimento) fa parte ed è incorporata nel Contratto con Symantec che il Cliente ha firmato fisicamente o digitalmente e che disciplina l'utilizzo del Servizio o, nel caso in cui non esista tale Contratto firmato, nei Termini e condizioni di Symantec Online Services (di seguito indicati come il "Contratto").

Indice generale

1: Funzionalità e capacità tecniche/commerciali

Panoramica del servizio

Symantec™ Email Security.cloud è un Servizio in hosting che filtra le E-mail e contribuisce a proteggere le organizzazioni da Malware (inclusi attacchi mirati e phishing), Spam e E-mail di massa indesiderate. Il Servizio offre opzioni di crittografia e protezione dei dati e consente di tenere sotto controllo le informazioni riservate inviate via E-mail. Il Servizio supporta più tipi di cassette postali di fornitori diversi.

Funzionalità del Servizio

- Gli Amministratori del Cliente possono accedere alla console di gestione del Servizio utilizzando una procedura di accesso sicura protetta da password. La console di gestione offre al Cliente la possibilità di configurare e gestire il Servizio, accedere ai report e visualizzare dati e statistiche, laddove disponibili come parte del Servizio.
- Il Servizio viene gestito ventiquattro (24) ore su ventiquattro per sette (7) giorni su sette e ne viene monitorata la disponibilità hardware, la capacità di servizio e l'utilizzo delle risorse di rete. Per ciascun Servizio, viene regolarmente monitorata la conformità con il Livello di servizio, operando adeguamenti ove necessario.
- La console di gestione mette anche a disposizione la funzionalità di report per il Servizio. I report possono includere registri e/o statistiche di attività. Tramite la console di gestione, il Cliente può generare report, configurabili in modo tale da programmarne l'invio via E-mail o il download diretto dalla console stessa.
- Il Servizio ha lo scopo di mettere il Cliente in condizione di implementare criteri di utilizzo del computer che siano validi e applicabili, o loro equivalenti.
- Gli elenchi di parole suggerite e le regole dei modelli o le norme fornite da Symantec possono includere termini potenzialmente offensivi.
- Se il Servizio viene sospeso o interrotto per una qualsiasi ragione, Symantec potrebbe annullare tutte le modifiche della configurazione effettuate alla fornitura del Servizio e sarà responsabilità del Cliente apportare tutte le altre modifiche della configurazione necessarie non appena il Servizio viene reintegrato.

Opzioni e funzionalità del Servizio

Il Servizio viene offerto in due (2) opzioni: Email Protect o Email Safeguard. Il Servizio deve essere acquistato per ciascun Utente della versione o del componente aggiuntivo scelto (soggetto a tutte le limitazioni previste nella presente Descrizione del servizio).

Funzionalità offerte in base alla versione

	Email Protect	Email Safeguard
Email Antimalware: Protezione antimalware, inclusa protezione da phishing e attacchi mirati	✓	✓
Email Antispam: protezione da spam e phishing (con real-time link following), ed e-mail di massa	✓	✓
Email Data Protection: controlli personalizzabili dei criteri di filtro dei contenuti		✓
Email Image Control: rilevamento di immagini offensive		✓
Filtro delle E-mail in uscita	✓	✓

Applicazione crittografia TLS		✓
Crittografia opportunistica TLS	✓	✓
Registrazione indirizzi: gestione dei destinatari non validi	✓	✓
Strumento di sincronizzazione LDAP per utenti e gruppi	✓	✓
Tracciamento messaggi	✓	✓
Dashboard dei report	✓	✓
Report brevi (PDF) e dettagliati (CSV)	✓	✓
Portale e notifiche di Quarantena Spam per utente finale	✓	✓
Gestione esclusione di responsabilità	✓	✓
Policy Based Encryption di base		✓
Email Impersonation Control		✓

Ulteriori informazioni sulle singole funzionalità del Servizio sono disponibili nella guida in linea, consultabile all'indirizzo http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=IT_IT.

Componenti aggiuntivi del Servizio

	Email Protect	Email Safeguard
Advanced Threat Protection: E-mail	Disponibile	Disponibile
Policy Based Encryption avanzata	_	Disponibile
Email Fraud Protection	Disponibile	Disponibile
Email Threat Isolation	Disponibile	Disponibile

Ulteriori informazioni sui singoli componenti aggiuntivi del Servizio sono disponibili nella guida in linea, consultabile all'indirizzo http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=IT_IT. La descrizione del servizio Email Fraud Protection è disponibile in: https://www.symantec.com/about/legal/repository.

Advanced Threat Protection: Email rileva le minacce avanzate inviate via e-mail utilizzando la sandbox Symantec Cynic™, identifica gli attacchi mirati sferrati via e-mail contro l'organizzazione o l'utente di destinazione e individua gli URL che diventano nocivi dopo il recapito delle e-mail tramite Symantec Click-time™ URL Protection. Può ritirare dopo il recapito le e-mail che la sandbox Cynic™ rileva come messaggi nocivi per i clienti di O365.Inoltre offre report dettagliati sui malware che comprendono informazioni sull'URL, categoria del malware, metodo di rilevamento e hash del file. È inclusa una API Data Feed che consente di segnalare i malware attraverso un URL autenticato, senza che sia necessario importare file o inviare dati via e-mail. Advanced Threat Protection: Email fornisce anche accesso al servizio Phishing Readiness, un simulatore di attacchi di phishing utilizzato per determinare la suscettibilità del personale a tali attacchi. L'utilizzo del servizio Phishing Readiness è regolato dai termini e dalle condizioni riportati su https://www.symantec.com/about/legal/repository.

Policy Based Encryption Advanced fornisce: (i) un portale Web di recupero; (ii) supporto per il recapito dei messaggi con protezione PGP e S/MIME; (iii) la possibilità di tentare l'applicazione della crittografia TLS prima di passare a tecnologie di crittografia meno trasparenti; (iv) il recapito push in formato PDF crittografato (l'unico metodo di crittografia fornito come parte della funzionalità Policy Based Encryption Essentials del piano Email Safeguard). Policy Based Encryption Advanced è concesso in licenza per singolo Utente, che può essere un sottogruppo del totale degli Utenti dell'opzione Email Safeguard. Se un Cliente ha bisogno di utilizzare l'opzione Policy Based Encryption avanzata per la consegna di attestati di sicurezza, Symantec può consentirgli di acquistare licenze Utente aggiuntive in base al numero di attestati da consegnare, secondo la formula definita da Symantec.

Symantec™ Email Fraud Protection è un servizio cloud che automatizza l'implementazione della specifica DMARC (Domain-based Message Authentication, Reporting, and Conformance - Autenticazione messaggi, reporting e conformità basate sui domini). Symantec Email Fraud Protection rende ogni passaggio dell'implementazione DMARC più semplice e integrato rispetto al metodo manuale. La funzionalità di imposizione riduce il rischio di attacchi di imitazione in entrata, in quanto tutte le e-mail provenienti da origini non autenticate vengono messe in quarantena o respinte. In modalità imposizione i destinatari delle e-mail o i Mail Transfer Agent sanno che possono considerare attendibile il dominio del cliente, e questo contribuisce a migliorare le statistiche di recapito e-mail.

Symantec™ Email Threat Isolation rafforza la protezione contro lo spear phishing, il furto di credenziali e gli attacchi e-mail avanzati isolando i collegamenti nocivi e rendendo innocue le pagine Web rischiose. Email Threat Isolation permette a Symantec di offrire la protezione più impenetrabile contro minacce e-mail sofisticate che sfruttano collegamenti nocivi, come gli attacchi avanzati di spear phishing o il furto di credenziali.

Email Threat Isolation crea un ambiente di esecuzione sicuro tra gli utenti e i collegamenti nelle loro e-mail, grazie al rendering remoto dei collegamenti sospetti e mostrando agli utenti solo contenuti Web inoculati. Di conseguenza, Symantec impedisce alle minacce contenenti collegamenti dannosi di raggiungere gli utenti, poiché ogni collegamento ricevuto viene considerato nocivo ed eseguito in remoto, lontano dagli utenti e dai loro dispositivi. Email Threat Isolation contrasta inoltre gli attacchi che mirano a carpire le credenziali convertendo i siti Web di phishing in modalità di sola lettura, il che impedisce agli utenti di immettere credenziali aziendali e altre informazioni riservate.

Contratto di servizio

- Symantec fornisce il Contratto di servizio ("SLA") applicabile per il Servizio come specificato nell'Allegato A.

Piattaforme supportate e requisiti tecnici

- Le piattaforme supportate e i requisiti tecnici per il Servizio sono disponibili all'indirizzo http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=IT_IT.

Componenti software del Servizio in hosting

- Il Servizio comprende i Componenti software disponibili nella console di gestione, cui è possibile accedere dietro pagamento della tariffa applicabile, laddove prevista.

2: Responsabilità del Cliente

Symantec garantisce la prestazione del Servizio soltanto se il Cliente fornisce le informazioni necessarie o esegue le operazioni richieste. In caso contrario, la prestazione del Servizio da parte di Symantec potrebbe subire ritardi, risultare compromessa o essere impedita e/o l'idoneità a ricevere i vantaggi previsti dal Contratto di servizio potrebbe venire meno, come descritto di seguito.

- Abilitazione della configurazione: Il Cliente deve fornire le informazioni necessarie a Symantec per avviare l'erogazione del Servizio.
- Personale del Cliente adeguato: il Cliente deve fornire personale adeguato per assistere Symantec nella fornitura del Servizio, dietro richiesta di Symantec.
- Il Cliente è responsabile delle proprie informazioni dell'account, password e altre credenziali di accesso.
- Il Cliente accetta di adottare misure ragionevoli per proteggere le credenziali e avviserà immediatamente Symantec di qualsiasi utilizzo non autorizzato dell'account del Cliente di cui abbia notizia.

- Credenziali di rinnovo: ove applicabile, il Cliente deve utilizzare le credenziali per il rinnovo fornite nel Documento di abbonamento o nella Conferma dell'ordine all'interno dell'amministrazione del proprio account per continuare a ricevere il Servizio o per mantenere le informazioni di account e i dati del Cliente per la Durata del servizio.
- Confronto fra Configurazioni Cliente e Impostazioni predefinite: Il Cliente deve configurare le funzionalità del Servizio tramite la console di gestione, ove applicabile; in caso contrario, si applicheranno le Impostazioni predefinite. In alcuni casi, non sono previste Impostazioni predefinite e non sarà fornito alcun Servizio fino a quando il Cliente non avrà scelto un'impostazione. La configurazione e l'utilizzo del Servizio sono prerogativa esclusiva del Cliente; pertanto, Symantec non è responsabile dell'utilizzo del Servizio da parte del Cliente né è passibile di responsabilità civili o penali addebitabili al Cliente in conseguenza della gestione del Servizio.

Politica di utilizzo accettabile

- Il Cliente è responsabile del rispetto della Politica di utilizzo accettabile di Symantec Online Services.

3: Informazioni sui diritti e sull'abbonamento

Misurazione degli addebiti

Il Servizio è disponibile nella seguente Unità di misura, in base a quanto specificato nella Conferma dell'ordine:

- "**Utente**" fa riferimento a una persona e/o dispositivo autorizzato a utilizzare e/o trarre vantaggio dall'utilizzo del Servizio, o che di fatto utilizza una parte del Servizio.

Modifiche all'abbonamento

Se il Cliente ha ricevuto l'Abbonamento o il Diritto direttamente da Symantec, le comunicazioni relative alle modifiche consentite all'Abbonamento o al Diritto del Cliente devono essere inviate al seguente indirizzo (o all'indirizzo sostitutivo reso noto da Symantec): CLD_cancellations_MLABS@symantec.com, se non diversamente specificato nel contratto del Cliente con Symantec. Le comunicazioni realizzate secondo la procedura descritta saranno considerate valide soltanto all'atto della ricezione. Se il Cliente ha ricevuto un Abbonamento o Abilitazione da un rivenditore Symantec, contattare tale rivenditore.

4: Assistenza e supporto tecnico

Nota: Questa sezione si applica solo se il Cliente ha diritto a ricevere l'Assistenza e il supporto clienti direttamente da Symantec ("Supporto"). Se il Cliente ha diritto a ricevere Assistenza e supporto da un rivenditore Symantec, fare riferimento al contratto stipulato dal Cliente con lo specifico rivenditore per dettagli relativi al Supporto; in questo caso, il Supporto descritto qui non si applica al Cliente.

Assistenza al Cliente

Nel quadro del Servizio, durante l'orario lavorativo locale Symantec fornirà assistenza nei seguenti ambiti:

- Ricezione ed evasione di ordini di implementazione del Servizio;
- Ricezione ed evasione di richieste di modifica autorizzata alle funzionalità del Servizio.
- Risposte a domande relative agli addebiti e alla fatturazione.

Supporto tecnico

Il Supporto di livello base è incluso nel Servizio come specificato di seguito.

- Il Supporto tecnico è disponibile ventiquattro (24) ore su ventiquattro, sette (7) giorni su sette, per assistere il Cliente nella configurazione delle funzionalità e nella risoluzione di eventuali problemi del Servizio. Il Supporto per i Servizi verrà fornito in conformità con i termini e condizioni e le politiche di supporto tecnico pubblicati all'indirizzo https://support.symantec.com/en_US/article.TECH236428.html.
- Una volta assegnato il livello di gravità alla richiesta di Supporto del cliente, Symantec farà ogni ragionevole sforzo per rispondere nei tempi previsti definiti nella tabella seguente. I guasti causati da azioni del Cliente o che richiedono interventi di altri provider di servizi non sono imputabili a Symantec e, come tali, sono esclusi da questo specifico Supporto.

Gravità del problema	Obiettivi di risposta del supporto (24x7)*
Gravità 1: Si è verificato un problema per il quale non è immediatamente disponibile una soluzione alternativa in una delle seguenti situazioni: (i) il server di produzione del Cliente o altri sistemi mission-critical non sono attivi o presentano una considerevole perdita di servizio; oppure (ii) una cospicua porzione dei dati mission-critical del Cliente è esposta a rischio significativo di perdita o corruzione.	Entro 30 minuti
Gravità 2: Una delle funzionalità principali è gravemente compromessa dal problema segnalato. Le attività del Cliente possono proseguire in modo ridotto, ma ci possono essere conseguenze negative sulla produttività a lungo termine.	Entro 2 ore
Gravità 3: Si è verificato un problema con effetto negativo limitato sulle attività aziendali del Cliente.	Entro lo stesso giorno lavorativo**
Gravità 4: Si è verificato un problema in cui le operazioni commerciali del Cliente non sono state influenzate negativamente.	Entro il giorno lavorativo successivo. Symantec suggerisce al Cliente di presentare i propri suggerimenti per nuove funzionalità o migliorie sui forum Symantec.

I suddetti obiettivi di risposta del Supporto sono raggiungibili durante le normali operazioni di servizio e non si applicano durante la manutenzione al Servizio e/o all'infrastruttura di supporto come descritto nella sezione Manutenzione di seguito.

**Gli obiettivi di risposta riguardano il tempo necessario per rispondere alla richiesta e non il tempo richiesto per la risoluzione del problema (il tempo necessario per chiudere la richiesta).*

***Per "giorno lavorativo" si intende l'orario di lavoro locale standard e i giorni della settimana nel fuso orario locale del Cliente, esclusi i fine settimana e le festività locali. Nella maggior parte dei casi, con "orario di lavoro" si intende lo spazio di tempo compreso fra le 9:00 e le 17:00 del fuso orario locale del Cliente.*

Manutenzione del Servizio e/o supporto dell'infrastruttura del Servizio

È obbligo di Symantec effettuare la manutenzione periodica. Symantec si avvarrà di tutti i mezzi commercialmente disponibili per eseguire la Manutenzione ordinaria negli orari di minore attività collettiva del Cliente, in modo da ridurre al minimo i possibili disagi. Il Cliente non riceverà alcuna comunicazione preventiva nel caso di interventi di manutenzione ordinaria. Per tutti gli altri tipi di manutenzione elencati di seguito, Symantec farà il possibile per informare preventivamente le parti interessate pubblicando un avviso nella Pagina di stato di Symantec (https://status.symantec.com/). Per informazioni su stato del Servizio, manutenzione programmata e problemi noti, visitare la Pagina di stato di Symantec e iscriversi alla pagina Symantec Email Security.cloud per ricevere gli aggiornamenti più recenti. **Le funzionalità di servizio di base come la scansione di sicurezza e il recapito e-mail non vengono interrotte da nessuna attività di manutenzione.**

- ***Manutenzione programmata:*** Manutenzione programmata fa riferimento ai periodi di manutenzione pianificata durante i quali il Servizio potrebbe essere interrotto o impedito a causa della non disponibilità dell'Infrastruttura di servizio. Symantec farà il possibile per eseguire la Manutenzione programmata in periodi di bassa attività complessiva del cliente, nel fuso orario in cui è situata l'Infrastruttura e soltanto su una parte della rete. Durante la Manutenzione programmata, il Servizio può essere deviato su sezioni dell'Infrastruttura non soggette a manutenzione, e di conseguenza è possibile che non si registrino disagi.Per ciò che concerne la Manutenzione programmata, Symantec si avvarrà di tutti i mezzi commercialmente disponibili per fornire al Cliente un preavviso di sette (7) giorni di calendario, che sarà pubblicato sulla Pagina di stato di Symantec. I clienti possono anche ricevere notifiche via SMS, e-mail o Twitter iscrivendosi alla Pagina di stato di Symantec.
- ***Manutenzione non programmata:*** Manutenzione non programmata fa riferimento a periodi di manutenzione pianificata che non consentono il preavviso di sette (7) giorni e durante i quali il Servizio potrebbe essere interrotto o impedito a causa della indisponibilità dell'Infrastruttura di servizio. Symantec si avvarrà di tutti i mezzi commercialmente disponibili per fornire al Cliente un preavviso di un (1) giorno di calendario, che sarà pubblicato sulla Pagina di stato di Symantec.Durante la Manutenzione non programmata, il Servizio può

essere deviato su sezioni dell'Infrastruttura non soggette a manutenzione, e pertanto è possibile che non si registrino disagi.In determinati casi, è possibile che Symantec esegua la Manutenzione straordinaria. La Manutenzione straordinaria è una manutenzione che *deve essere implementata prima possibile, per risolvere o evitare un incidente di grave entità*. Symantec farà il possibile per informare preventivamente i soggetti interessati, pubblicando un avviso sulla Pagina di stato di Symantec almeno una (1) ora prima dell'inizio della manutenzione.

- ***Manutenzione della console di gestione:*** Per la Manutenzione della console di gestione, Symantec si avvarrà di tutti i mezzi commercialmente disponibili per fornire al Cliente un preavviso di quattordici (14) giorni di calendario, che sarà pubblicato sulla Pagina di stato di Symantec. Symantec farà il possibile per eseguire la manutenzione della console di gestione negli orari di minore attività collettiva del cliente, in modo da ridurne al minimo la mancata disponibilità. Occasionalmente, Symantec potrebbe eseguire aggiornamenti minori alla console di gestione. I clienti non riceveranno alcuna comunicazione preventiva per questi interventi di manutenzione ordinaria.

5: Termini aggiuntivi

- È possibile accedere al Servizio e utilizzarlo a livello globale, rispettando le limitazioni di conformità delle esportazioni e i limiti tecnici in conformità con gli standard Symantec attuali.
- Symantec si riserva il diritto di modificare e aggiornare le funzionalità del Servizio, con l'obiettivo di fornire un Servizio equivalente o migliore (purché Symantec non riduca sostanzialmente la funzionalità principale del Servizio). Il Cliente riconosce e accetta che Symantec si riserva il diritto di aggiornare questa Descrizione del servizio in qualsiasi momento durante il Periodo di validità dell'abbonamento al fine di rispecchiare accuratamente il Servizio fornito. La Descrizione del servizio aggiornata si applicherà al momento della pubblicazione.
- L'utilizzo di qualsiasi Componente del servizio sotto forma di software sarà disciplinato dal Contratto di licenza relativo al software. Nel caso in cui il Componente del servizio sia privo di EULA, sarà disciplinato dai termini e dalle condizioni disponibili all'indirizzo http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf. Ulteriori diritti ed obblighi aggiuntivi relativi all'uso di tale Componente del servizio faranno riferimento a quanto stabilito nella presente Descrizione del servizio.
- Salvo diversa indicazione fornita nella Descrizione del servizio, il Servizio (e qualsiasi Componente software del Servizio in hosting fornito in abbinamento) può utilizzare componenti open source e di terze parti provvisti di licenza separata.
- Symantec può aggiornare il Servizio in qualsiasi momento al fine di conservarne l'efficacia.

- Tutti i modelli forniti da Symantec sono esclusivamente a titolo di guida e consentono pertanto al Cliente di creare criteri personalizzati e ulteriori modelli.
- Al Servizio saranno applicati i limiti di seguito descritti:
    - Messaggi mensili in entrata e in uscita per Utente: diecimila (10.000). Tale limite non comprende Spam e Malware indirizzati al Cliente.
    - Laddove l'utilizzo superi il limite di messaggi, Symantec si riserva il diritto di fatturare al Cliente eventuali Utenti aggiuntivi, previa notifica, per i mesi residui del Contratto di servizio.
    - Pianificazione dei nuovi tentativi di invio della posta in entrata e in uscita: sette (7) giorni di calendario.
    - Dimensione massima predefinita delle E-mail: cinquanta megabyte (50 MB). Il Cliente può specificare per le E-mail qualsiasi dimensione massima non superiore a mille megabyte (1.000 MB). Le E-mail ricevute dal Servizio che superino il limite specificato saranno bloccate ed eliminate; al mittente, al destinatario previsto e a un Amministratore sarà inviata un'E-mail di notifica.
    - Tracciamento messaggi: i dati rimangono disponibili per 30 giorni per la ricerca di eventuali soluzioni ai problemi. Limiti ulteriori saranno applicati al numero di risultati che una singola ricerca può restituire.
    - Quarantena Malware: le E-mail saranno cancellate automaticamente dopo trenta (30) giorni.
    - Quarantena Spam: le E-mail saranno eliminate automaticamente dopo quattordici (14) giorni, salvo diversa configurazione.
    - Dashboard che segnalano la disponibilità dei dati = quaranta (40) giorni per informazioni dettagliate; dodici (12) mesi per informazioni riepilogative.
    - Disponibilità dati report brevi (PDF): dodici (12) mesi.
    - Disponibilità dati report dettagliati (CSV): quaranta (40) giorni.

- Alla funzionalità Policy Based Encryption saranno applicate le seguenti limitazioni:
    - E-mail Policy Based Encryption (Z) mensili in uscita per Utente: trecento (300).
    - E-mail Policy Based Encryption Essentials/Advanced mensili in uscita per Utente: quattrocentottanta (480).
    - In caso di invio a più destinatari, ciascun indirizzo sarà conteggiato come E-mail sicura. Nel caso in cui il Cliente superi il numero di E-mail sicure consentite in un mese solare, Symantec si riserva il diritto di fatturare al Cliente l'utilizzo effettivo.

- Le E-mail inoltrate tramite il servizio Policy Based Encryption sono limitate a una dimensione massima di cinquanta megabyte (50 MB).
- In caso di utilizzo di crittografia Pull con il servizio Policy Based Encryption (Z), le E-mail saranno archiviate nel portale di recupero protetto per un massimo di novanta (90) giorni.
- In caso di utilizzo di crittografia Pull con il servizio Policy Based Encryption Advanced, le E-mail saranno archiviate nel portale di recupero protetto per un massimo di 30 giorni.
- I Livelli di Disponibilità e di Latenza non si applicano a questo Servizio.

- Per garantire la sicurezza dei messaggi durante tutti i passaggi di trasmissione, Symantec raccomanda ai Clienti di configurare i domini, che verranno utilizzati per la Policy Based Encryption, in modo tale da garantire la crittografia TLS per tutti i messaggi in uscita e in entrata, da e verso l'Infrastruttura di servizio.
- I Clienti devono inoltrare le proprie E-mail in entrata mediante Symantec utilizzando le informazioni di routing fornite, e non a un Tower o a un indirizzo IP specifici.
- Il Servizio è disponibile soltanto per un Cliente che possieda un nome di dominio di e-mail e che per quel nome di dominio possa configurare record MX e/o DNS.
- Il Cliente deve accettare le E-mail in entrata da tutti gli intervalli IP richiesti in modo tale da garantire la continuità del servizio nel caso in cui una parte dell'Infrastruttura non sia disponibile.
- Il Cliente deve comunicare alla propria organizzazione l'indirizzo / gli indirizzi IP o il nome / i nomi host del server di posta per il recapito delle E-mail in entrata.
- Il Cliente deve garantire di effettuare il provisioning di tutti i domini (e i sottodomini) che usufruiscono del Servizio. Il Cliente accetta che le funzionalità del Servizio possano non funzionare correttamente e che il recapito delle E-mail possa non essere disponibile per i domini che non sono stati forniti. Il Cliente accetta di fornire e mantenere un elenco di indirizzi e-mail validi per la ricezione del Servizio ("Elenco di convalida"). È responsabilità del Cliente verificare tale Elenco di convalida prima che il Servizio venga reso disponibile e durante la Durata del servizio. Le E-mail inviate a indirizzi non inclusi nell'Elenco di convalida o inseriti in modo errato verranno rifiutate dal Servizio. Il Cliente accetta che gli SLA non si applichino alle E-mail inviate a indirizzi non validi. A scanso di equivoci, il Cliente che utilizza il sistema di Quarantena Spam deve mantenere un Elenco di convalida e abilitare la funzionalità di Registrazione indirizzi. Ove il Cliente non sia in grado di fornire tale Elenco di convalida e richieda la disabilitazione della funzionalità di Registrazione indirizzi, Symantec valuterà le richieste su base specifica, riservandosi di rifiutarle a proprio esclusivo e insindacabile giudizio.
- Il Cliente può rilasciare E-mail che sono state classificate come contenenti Malware o Spam, oppure richiedere che Symantec rilasci tali E-mail all'interno del dominio del Cliente. IL CLIENTE CONVIENE CHE SYMANTEC NON PUÒ ASSUMERSI ALCUNA RESPONSABILITÀ PER CIÒ CHE CONCERNE IL RILASCIO DI TALI E-MAIL SU RICHIESTA DEL CLIENTE.
- Symantec non potrà essere ritenuta responsabile di alcun danno o perdita derivante direttamente o indirettamente dalla mancata identificazione di Spam o dall'errata identificazione di un'E-mail come Malware o Spam da parte del Servizio. Symantec si riserva il diritto di sottoporre a scansione tutte le E-mail in uscita.
- Nel momento in cui avrà inizio la fornitura del Servizio, alle E-mail da questo scansionate verrà aggiunta una dichiarazione di non responsabilità che il Cliente potrà modificare tramite la console di gestione. Symantec si riserva il diritto di aggiornare in qualsiasi momento la dichiarazione di non responsabilità.
- Il Cliente è tenuto al rispetto di tutte le leggi vigenti per ciò che concerne l'utilizzo del Servizio. In alcuni paesi, potrebbe essere necessario ottenere l'autorizzazione del personale. La configurazione e l'utilizzo dei Servizi sono soggetti al controllo esclusivo da parte del Cliente, pertanto, Symantec non è responsabile dell'utilizzo dei Servizi da parte del Cliente né è passibile di responsabilità civili o penali che possono essere addebitate al Cliente come risultato del funzionamento del Servizio.
- Nel caso in cui la fornitura continuata del Servizio al Cliente comprometta la sicurezza del Servizio stesso, compresi, a titolo esemplificativo, tentativi di pirateria informatica, attacchi di tipo Denial of Service, mail bomb o altre attività nocive indirizzate o provenienti dai domini del Cliente, il Cliente accetta che Symantec possa interrompere temporaneamente il Servizio. Se si verifica tale eventualità, Symantec informerà tempestivamente il Cliente e fornirà la propria collaborazione per risolvere tali problemi. Una volta eliminata la minaccia per la sicurezza, Symantec ripristinerà il Servizio.
- Nel caso in cui venga sospeso per qualsiasi ragione, il Servizio non verrà applicato alle E-mail del Cliente né queste ultime verranno inoltrate tramite l'Infrastruttura Symantec. Il Cliente sarà responsabile del reindirizzamento delle proprie E-mail durante il periodo di sospensione e, in caso di ripristino del Servizio, della conferma di tutte le configurazioni corrette.

- In caso di risoluzione del Servizio per qualsiasi ragione, l'account del Cliente verrà eliminato, e il Cliente non avrà più accesso al Servizio.
- Il Cliente non dovrà consentire che i propri sistemi: (i) funzionino come Open Relay (inoltro aperto) o Open Proxy (proxy aperto); o (ii) inviino Spam. Symantec si riserva il diritto di verificare in qualsiasi momento il rispetto della presente sezione da parte del Cliente. A scanso di equivoci, qualsiasi violazione della presente Clausola costituirà una inadempienza materiale del Contratto, per la quale Symantec si riserva il diritto di sospendere immediatamente il Servizio, interamente o parzialmente, fin tanto che la violazione non venga sanata, oppure di risolvere il Contratto relativo al Servizio in questione.
- Se, in qualsiasi momento, (i) i sistemi di e-mail del Cliente vengono inseriti in una lista nera, o (ii) il Cliente provoca l'inserimento dei sistemi di Symantec in una lista nera a causa dell'invio di Spam, o (iii) il Cliente non adempie agli obblighi stabiliti nella presente Descrizione del servizio, Symantec ne informerà il Cliente, riservandosi il diritto, a proprio insindacabile giudizio, di rifiutare la fornitura, interrompere o cessare interamente o parzialmente il Servizio.
- Il Cliente può utilizzare il Servizio esclusivamente per i propri fini commerciali. Il Cliente accetta di non rivendere, concedere in sublicenza, noleggiare o rendere disponibili il Servizio e la relativa documentazione a terzi in altro modo. Il Cliente accetta di non utilizzare il Servizio allo scopo di realizzare un prodotto o un servizio concorrente, né di copiarne le funzionalità o l'interfaccia utente, effettuare valutazioni del Servizio, test o altre analisi di confronto con l'obiettivo di divulgarli al di fuori della propria organizzazione in assenza di previa autorizzazione scritta da parte di Symantec.

6: Definizioni

"**Registrazione indirizzi**" indica una funzionalità obbligatoria del Servizio che rifiuta le E-mail in entrata inviate a Indirizzi e-mail non inclusi nell'elenco di indirizzi validi del Cliente ("Elenco di convalida").

"**Amministratore**" fa riferimento a un Utente del Cliente provvisto di autorizzazione per la gestione del Servizio per conto del Cliente. In base alle indicazioni del Cliente, gli Amministratori possono gestire un Servizio, interamente o parzialmente.

"**Impostazioni per le best practice antispam**" fa riferimento alle linee guida di configurazione consigliate da Symantec per il Servizio, prescritte al Cliente durante il processo di fornitura o pubblicate nella Guida in linea.

"**Connection Manager**" fa riferimento ai metodi di rilevamento utilizzati nella fase di handshake SMTP.

"**Richiesta di accredito**" indica la comunicazione che il Cliente deve inviare a Symantec via E-mail all'indirizzo support.cloud@symantec.com con oggetto "Richiesta di accredito" (salvo diversa comunicazione da parte di Symantec).

"**Cluster Tower designato**" indica due (2) o più Tower designati per fornire Email Security Services al Cliente.

"**Impostazioni del livello di dominio**" indica le impostazioni di dominio che è possibile personalizzare all'interno della console di gestione di Email Security Services.

"**E-mail**" fa riferimento a tutti i messaggi SMTP in entrata e in uscita che transitano attraverso il Servizio.

"**Email Security Services**" fa riferimento alle opzioni Email Safeguard, Email Protect e qualsiasi altro servizio aggiuntivo disponibile.

"**Malware e-mail falso positivo**" indica un'E-mail legittima identificata erroneamente come contenente un Malware.

"**Contratto di licenza con l'utente finale (EULA)**"" fa riferimento ai termini e alle condizioni che accompagnano il Software (definito di seguito).

"**Impostazioni globali**" indica le azioni che, all'interno della console di gestione, vengono applicate a tutti i livelli di dominio e di gruppo in relazione ai Servizi.

"**Impostazioni a livello di gruppo**" indica le impostazioni di un gruppo specifico che è possibile personalizzare all'interno della console di gestione per le relative funzionalità del Servizio.

"**Infrastruttura**" fa riferimento a qualsiasi tecnologia e proprietà intellettuale di Symantec o di altri licenziatari utilizzate per l'erogazione dei Servizi.

"**Malware conosciuto**" indica Malware per il quale, al momento della ricezione del contenuto da parte di Symantec, è già stata resa disponibile da almeno una (1) ora una firma che può essere utilizzata dalle tecnologie antivirus distribuite da Symantec.

"**Malware**" o "**software nocivo**" indica qualsiasi software utilizzato per interrompere il funzionamento di computer o dispositivi mobili, o per raccogliere informazioni sensibili e/o ottenere accesso a sistemi di computer privati senza l'autorizzazione appropriata.

"**Malware falso positivo**" indica un'E-mail legittima identificata erroneamente come contenente un Malware.

"**Membro**" fa riferimento al Cliente e alle terze parti con le quali il Cliente crea una rete crittografata mediante il Servizio legacy aggiuntivo Email Boundary Encryption.

"**Tariffa mensile**" fa riferimento alla tariffa mensile addebitata per il Servizio o i Servizi forniti, così come definito nel Contratto.

"**Guida in linea**" indica le informazioni aggiuntive disponibili all'indirizzo http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=IT_IT.

"**Proxy aperto**" indica un server proxy configurato per consentire a terze parti sconosciute o non autorizzate di accedere, memorizzare o inoltrare DNS, pagine Web o altri dati per il Servizio.

"**Open Relay**" fa riferimento a un server di e-mail configurato per ricevere E-mail da terzi sconosciuti o non autorizzati e inoltrarle a uno o più destinatari che non siano utenti del sistema di e-mail al quale è connesso lo stesso server di e-mail. Open Relay può anche essere denominato "Spam relay" o "public relay."

"**Conferma dell'ordine**" ha il significato fornito nei Termini e condizioni di Symantec Online Services, laddove applicabile. In assenza di tali termini e condizioni applicabili al Servizio, allora "Conferma dell'ordine" farà riferimento al Documento di abbonamento, così come definito nel presente documento.

"**Servizio**" indica l'opzione Protect o Safeguard di Symantec Email Security.cloud acquistata dal Cliente.

"**Componente del servizio**" fa riferimento a un determinato software di attivazione, le periferiche hardware e la documentazione associata, che possono essere forniti separatamente da Symantec come parte accessoria di un Servizio.

"**Credito di servizio**" fa riferimento all'importo accreditato sulla successiva fattura del Cliente in seguito all'invio di una Richiesta di accredito e alla relativa convalida da parte di Symantec.

"**Software del servizio**" indica il Software (definito di seguito) che deve essere installato sul computer di ciascun Cliente per ricevere il Servizio. Il Software del servizio include il Software e la documentazione associata, che possono essere forniti separatamente da Symantec come parte del Servizio.

"**Software**" fa riferimento a ogni programma software di Symantec o relativo licenziatario, nella forma di codice oggetto, concesso in licenza al Cliente da Symantec e disciplinato dai termini dell'EULA associato, inclusi, a titolo esemplificativo, aggiornamenti o nuove versioni, secondo quanto stabilito qui di seguito.

"**Spam**" fa riferimento alle E-mail promozionali indesiderate.

"**Spam falso negativo**" indica un'E-mail spam che non è stata identificata come Spam dal Servizio.

"**Spam falso positivo**" indica un'E-mail che è stata identificata erroneamente come Spam dal Servizio.

"**Impostazioni consigliate per lo spam**" indica le linee guida di configurazione consigliate da Symantec per il Servizio, prescritte al Cliente durante il processo di fornitura o pubblicate nella Guida in linea.

"**Documento di abbonamento**" indica uno o più dei seguenti documenti applicabili che definiscono ulteriormente i diritti e gli obblighi dell'Utente in relazione al Servizio: un certificato Symantec o un documento di licenza simile rilasciato da Symantec, o un contratto scritto tra il Cliente e Symantec, che accompagna, precede o segue il Servizio.

"**Termini di Symantec Hosted Services**" indica i Termini di Symantec Hosted Services disponibili all'indirizzo https://www.symantec.com/about/legal/service-agreements.jsp.

"**Termini e condizioni di Symantec Online Services**" indica i Termini e le condizioni di Symantec Online Services disponibili all'indirizzo https://www.symantec.com/about/legal/service-agreements.jsp.

"**Symantec Tracker**" fa riferimento a uno strumento Symantec per mezzo del quale vengono misurati i parametri di Disponibilità e Latenza del servizio.

"**Tower**" fa riferimento a un cluster dei server di e-mail con carico bilanciato.

"**Utente**" indica una singola persona che invia e riceve e-mail ed è protetta da una porzione del Servizio.

Allegato A

Contratto di servizio

Disposizioni generali

- Nel caso in cui Symantec non rispetti il livello di servizio definito, il Cliente avrà diritto a un Credito di servizio. Laddove ritenga di avere diritto a un Credito di servizio, il Cliente dovrà inviare una Richiesta di accredito entro dieci (10) giorni lavorativi dalla fine del mese di calendario in cui si è verificata la presunta inadempienza del livello di servizio. Il Cliente riconosce che i registri vengono conservati solamente per un numero limitato di giorni solari, motivo per cui qualsiasi Richiesta di accredito inviata oltre il periodo previsto non sarà ritenuta valida.
- La Richiesta di accredito dovrà essere effettuata mettendosi in contatto con il Supporto tecnico Symantec. Per le istruzioni dettagliate, visitare la pagina di destinazione del supporto prodotti all'indirizzo: https://support.symantec.com/en_US/email-security-cloud..html.
- Tutte le Richieste di accredito saranno soggette a verifica da parte di Symantec in conformità con le relative disposizioni del presente Contratto di servizio. Al fine di convalidare la Richiesta di accredito, Symantec potrebbe richiedere informazioni aggiuntive al Cliente.
- Il presente Contratto di servizio non sarà valido: (i) durante i periodi di Manutenzione programmata o straordinaria, i periodi di mancata disponibilità dovuta a cause di forza maggiore o atti od omissioni da parte del Cliente o di terzi; (ii) durante qualsiasi periodo di sospensione del Servizio da parte di Symantec in conformità con i termini del Contratto o (iii) laddove il Cliente non rispetti i termini del Contratto (incluso, senza limitazione, il caso in cui il Cliente abbia fatture insolute); (iv) laddove il Cliente non abbia configurato il Servizio in accordo con il Contratto; o (v) durante periodi di prova del Servizio.
- I rimedi stabiliti nel presente Contratto di servizio costituiranno per il Cliente l'unico ed esclusivo rimedio contrattuale, per illecito civile (compresa, a titolo esemplificativo, la negligenza) o altro in relazione al presente Contratto di servizio.
- La massima responsabilità complessiva di Symantec in relazione al presente Contratto di servizio in qualsiasi mese di calendario sarà costituita da un credito corrispondente all'importo minore tra il 100% della Tariffa mensile e diecimila dollari/cinquemila sterline/diecimila euro (10.000 $/5.000 £/10.000 €), a seconda della valuta di fatturazione al Cliente.
- Se il Servizio interessato è stato acquistato come parte di un raggruppamento di Servizi, il Credito di servizio viene calcolato in base al Servizio interessato e non all'intero raggruppamento di Servizi.

Eccezioni al Contratto di servizio per Email Security Services

Il presente Contratto di servizio non sarà valido: (i) nel caso di E-mail che non siano transitate attraverso il Servizio (compreso, a titolo esemplificativo, il caso in cui il Cliente non abbia adottato misure adeguate atte a garantire l'accettazione di E-mail in entrata provenienti esclusivamente dall'Infrastruttura Symantec); (ii) nel caso di E-mail in entrata o in uscita che siano state inviate inizialmente a Symantec e che includano più di 500 destinatari per sessione SMTP, (iii) per i Clienti che usufruiscono del Servizio su Tower designati come Bulk Cluster Tower; o (iv) nel caso di E-mail in entrata o in uscita per domini del Cliente non compresi nella fornitura del Servizio.

Disponibilità del servizio

Il Livello di Disponibilità del servizio è definito dalla capacità di stabilire una sessione SMTP sulla porta 25 dal MTA del Cliente all'Infrastruttura Symantec, in conformità con lo standard RFC5321. Il Livello di Disponibilità del servizio non si applica al portale di gestione o al sistema di quarantena spam. Questo livello di servizio non sarà applicato nel caso in cui il Cliente abbia configurato il Servizio in modo non corretto o per effetto di circostanze impreviste o di cause che vanno oltre il ragionevole controllo di Symantec, tra cui a titolo esemplificativo disastro naturale, guerra, terrorismo, tumulto, provvedimento governativo, oppure un guasto a una rete o a un dispositivo che si verifichi all'esterno dei centri dati di Symantec, inclusa la sede del Cliente o l'area compresa tra la sede del cliente e il centro dati di Symantec.

Se la Disponibilità del servizio scende al di sotto del cento percento (100%) nel corso di un qualsiasi mese di calendario, il Cliente può inviare una Richiesta di accredito e può ricevere un Credito di servizio corrispondente a una delle seguenti percentuali di accredito pari all'importo minore tra il 100% della Tariffa mensile e diecimila dollari/cinquemila sterline/diecimila euro (10.000 $/5.000 £/10.000 €), a seconda della valuta di fatturazione al Cliente:

Percentuale di disponibilità per mese solare	Accredito percentuale della Tariffa mensile

Inferiore al 100% e uguale o superiore al 99%	25%
Inferiore al 99% e uguale o superiore al 98%	50%
Inferiore al 98%	100%

Se la Disponibilità del servizio scende al di sotto del novantotto percento (98%) nel corso di un qualsiasi mese di calendario, il Cliente avrà diritto a risolvere il Servizio in questione e ricevere un rimborso proporzionale delle tariffe pagate in anticipo per la porzione del periodo successivo alla risoluzione.

Recapito E-mail

Il Livello di servizio Recapito E-mail è definito dalla capacità di Symantec di recapitare il 100% di tutte le E-mail inviate o ricevute dal Cliente ed è soggetto alle seguenti condizioni:

a) l'E-mail deve essere stata ricevuta da Symantec;

b) L'E-mail non deve contenere Malware, Spam o altro contenuto che ne abbia causato l'intercettazione da parte del Servizio.

In base alle condizioni di cui sopra, nel caso in cui Symantec non riesca a recapitare un messaggio diretto al Cliente, o proveniente dal Cliente, e qualora questi non abbia violato alcun termine del Contratto, il Cliente avrà diritto a risolvere il Servizio entro (trenta) 30 giorni di calendario, previa comunicazione scritta.

Latenza E-mail

Il Livello di servizio Latenza E-mail è definito in funzione del tempo medio di andata/ritorno, misurato da Symantec Tracker, delle E-mail inviate e ricevute ogni cinque (5) minuti da qualsiasi tower del Cluster Tower del Cliente se superiore, nel corso di un mese di calendario, al ritardo definito nella tabella di seguito riportata. Se il Cliente ritiene che il Livello di servizio Latenza non sia stato rispettato, potrà inviare una Richiesta di accredito e ricevere un Credito di servizio in base alla tabella riportata di seguito:

Tempo medio di andata/ritorno (in secondi)	Accredito percentuale della Tariffa mensile
Superiore a 60 s e uguale o inferiore a 90 s	25%
Superiore a 90 s e uguale o inferiore a 120 s	50%
Superiore a 120 s e uguale o inferiore a 180 s	75%
Superiore a 180 s	100%

Il Livello di servizio Latenza non si applicherà nel caso in cui:

a) il Cliente non abbia fornito a Symantec un Elenco di convalida e subisca un attacco di tipo Denial of Service;

b) i periodi di ritardo siano stati causati da un loop di posta da/verso i sistemi del Cliente; o

c) il server di E-mail principale del Cliente non sia in grado di accettare E-mail al primo tentativo di recapito.

Spam falso positivo

Il Livello di servizio Spam falso positivo definisce la Percentuale di intercettazione di spam falso positivo massima. Il Livello di servizio Spam falso positivo si applicherà soltanto nel caso in cui il Cliente adotti le Impostazioni per le best practice antispam specificate nella Guida in linea. Laddove la percentuale di intercettazione di Spam falso positivo superi lo 0,0003% del traffico di E-mail del Cliente in qualsiasi mese di calendario, questi potrà inviare una Richiesta di accredito e ricevere un Credito di servizio in base alla tabella riportata di seguito:

Percentuale di intercettazione di Spam falso positivo	Accredito percentuale della Tariffa mensile
Superiore allo 0,0003% e uguale o inferiore allo 0,003%	25%
Superiore allo 0,003% e uguale o inferiore allo 0,03%	50%
Superiore allo 0,03% e uguale o inferiore allo 0,3%	75%
Superiore allo 0,3%	100%

Ai fini del presente Livello di servizio, non costituiranno Spam falso positivo le seguenti E-mail:
a) E-mail che non siano messaggi aziendali legittimi;
b) E-mail con più di 20 destinatari;
c) E-mail il cui il mittente sia incluso nell'elenco dei mittenti bloccati del Cliente, inclusi, a titolo esemplificativo, quelli definiti dal singolo Utente se il Cliente ha abilitato le impostazioni a livello di Utente;
d) E-mail inviate da un computer compromesso;
e) E-mail inviate da un computer presente nell'elenco di blocco di terzi;
f) E-mail intercettate dalla scansione dello Spam in uscita.

Per avere diritto a un Credito di servizio, il Cliente deve segnalare al Supporto tecnico Symantec le presunte E-mail rilevate come falso positivo entro cinque (5) giorni di calendario dalla loro ricezione. Symantec svolgerà indagini e verificherà se le E-mail sono effettivamente da considerarsi Spam falso positivo, quindi registrerà le conclusioni.

Percentuale di intercettazione dello Spam
Il Livello di servizio Percentuale di intercettazione dello spam definisce la Percentuale di intercettazione dello spam minima. Questo Livello di servizio si applicherà soltanto nel caso in cui il Cliente adotti le Impostazioni per le best practice antispam specificate nella Guida in linea. Il Livello di servizio corrisponde al numero di E-mail Spam falso negativo conteggiate nell'arco di un mese solare. Il Cliente può inviare una Richiesta di accredito e ricevere un Credito di servizio in base alla tabella riportata di seguito:

Percentuale di intercettazione dello Spam	Accredito percentuale della Tariffa mensile
Superiore al 98% e uguale o inferiore al 99%	25%
Superiore al 97% e uguale o inferiore al 98%	50%
Superiore al 96% e uguale o inferiore al 97%	75%
Inferiore al 96%	100%

Il Livello di servizio Percentuale di intercettazione dello spam non si applicherà nel caso in cui l'E-mail sia stata inviata a un indirizzo di e-mail non valido. Alle E-mail contenenti più del cinquanta percento (50%) di set di caratteri a doppio byte verrà applicata una Percentuale di intercettazione dello Spam inferiore al novantacinque percento (95%). Nel caso in cui tale Percentuale di intercettazione dello Spam scenda al di sotto del novantacinque percento (95%), il Cliente avrà diritto a un venticinque percento (25%) di Credito di servizio sulla Tariffa mensile. Nel caso in cui tale Percentuale di intercettazione dello Spam scenda al di sotto del novanta percento (90%), il Cliente avrà diritto a un cento percento (100%) di Credito di servizio sulla Tariffa mensile.

Per avere diritto a un Credito di servizio, il Cliente deve segnalare al Supporto tecnico Symantec le presunte E-mail rilevate come falso negativo entro cinque (5) giorni di calendario dalla loro ricezione. Symantec svolgerà indagini e verificherà se le E-mail sono effettivamente da considerarsi Spam falso negativo, quindi registrerà le conclusioni.

Protezione antimalware

Se i sistemi del Cliente vengono infettati da Malware conosciuto o sconosciuto che si propaga tramite E-mail che sono transitate attraverso il servizio di scansione nel cloud, il Cliente potrebbe avere diritto a un Credito di servizio per l'importo indicato di seguito. Il Cliente deve notificare Symantec entro cinque (5) giorni dal momento in cui viene a conoscenza di tale Malware e tale comunicazione deve essere registrata, investigata e convalidata da Symantec. Il Cliente deve inviare una Richiesta di accredito e, se convalidata, riceverà un Credito di servizio pari all'importo minore tra il 100% della Tariffa mensile o diecimila dollari/cinquemila sterline/diecimila euro ($10.000/£5.000/€10.000), a seconda della valuta di fatturazione al Cliente. Il rimedio stabilito nella presente sezione sarà l'unico ed esclusivo rimedio in caso di ragione, torto (compresa senza limitazione la negligenza) o altro in relazione a qualsiasi infezione da parte di un Malware trasmesso al Cliente o a terzi tramite il Servizio. A scanso di equivoci, il rimedio stabilito nella presente sezione non si applicherà in caso di autoinfezione premeditata.

I sistemi del Cliente sono considerati infetti se è stato ricevuto un Malware allegato a un'E-mail attraverso il Servizio e il Malware è stato attivato all'interno dei sistemi del Cliente in modo automatico o manuale. Nel caso in cui Symantec rilevi ma non blocchi un'E-mail con un Malware allegato, quindi pubblichi un aggiornamento sulla Pagina di stato di Symantec o avvisi altrimenti il Cliente fornendo informazioni sufficienti per consentirgli di identificare ed eliminare l'E-mail infetta, il rimedio sopra stabilito non si applicherà.

Il Servizio sottoporrà a scansione il maggior numero possibile di E-mail e relativi allegati. Potrebbe non essere possibile sottoporre a scansione allegati con contenuti che siano sotto il diretto controllo del mittente (*ad esempio*, allegati protetti da password e/o crittografati e/o la cui password viene inviata separatamente dall'E-mail). Tali E-mail e/o allegati sono esclusi dal livello di servizio e il rimedio stabilito sopra non avrà valore.

Il Livello di servizio Protezione antimalware non si applicherà nel caso di Malware diffusi intenzionalmente dal Cliente o da Symantec su richiesta del Cliente.

Il Livello di servizio Protezione antimalware si applica esclusivamente al Malware specificato nella presente Descrizione del servizio e non si applica a quanto specificato di seguito: spyware, adware, collegamenti URL a siti Web che ospitano contenuti nocivi e Trojan horse sconosciuti.

Malware falso positivo

Il Livello di servizio Malware falso positivo definisce la Percentuale di intercettazione di malware falso positivo massima. Se la percentuale di intercettazione di Malware e-mail falso positivo supera lo 0,0001% del traffico di E-mail del Cliente in qualsiasi mese di calendario, il Cliente può inviare una Richiesta di accredito e ricevere un Accredito del servizio in base alla tabella riportata di seguito:

Percentuale di intercettazione di Malware falso positivo	Accredito percentuale della Tariffa mensile
Superiore allo 0,0001% e uguale o inferiore allo 0,001%	25%
Superiore allo 0,001% e uguale o inferiore allo 0,01%	50%
Superiore allo 0,01% e uguale o inferiore allo 0,1%	75%
Superiore allo 0,1%	100%

Supporto tecnico e risoluzione dei guasti 24x7

Il supporto tecnico è disponibile ventiquattro (24) ore su ventiquattro per sette (7) giorni su sette per:
a) fornire supporto tecnico al Cliente in caso di problemi con il Servizio;
b) assistere il Cliente nella risoluzione di tali problemi.