Allegato 1
Descrizione generale del Servizio

LE DESCRIZIONI DI SERVIZI E/O SLA ELENCATE NEGLI ALLEGATI 2 E 3 DI SEGUITO, NON ORDINATE PER CLIENTE NELLA SEZIONE B DEL CONTRATTO, NON SARANNO APPLICABILI AL CLIENTE.

1. Definizioni

I termini sotto indicati che iniziano con lettera maiuscola avranno i seguenti significati per gli scopi del Contratto:

"E-mail di Grosso Volume"	indica un insieme di più di cinquemila (5000) messaggi E-mail, con un contenuto sostanzialmente uguale, inviati o ricevuti in una singola operazione o serie di operazioni correlate;
"E-mail"	indica qualunque messaggio SMTP inviato o ricevuto attraverso il Servizio;
"Bundle di Servizi non divisibile"	indica un insieme (bundle) di Servizi come indicato nella Sezione B "Servizi e Costi" del Contratto e nella Clausola 7 riportata di seguito, che sono soggetti alle disposizioni della Clausola 3.6 del Contratto;
"Membro"	indica il Cliente e le organizzazioni con le quali il Cliente crea una rete crittografata utilizzando il Servizio di Crittografia di Delimitazione;
"Normale orario di lavoro"	indica fra le 8.30 e le 17.30 ora di Londra, dal lunedì al venerdì, ad eccezione delle festività pubbliche riconosciute nel Regno Unito;
"Proxy Aperto"	indica un server proxy configurato per consentire a terzi sconosciuti o non autorizzati di accedere, archiviare o inoltrare DNS, pagine web o altri dati;
"Relay Aperto"	indica un server E-mail configurato per la ricezione di E-mail da una terza parte sconosciuta o non autorizzata e l'inoltro dell'E-mail a uno o più destinatari che non siano utenti del sistema E-mail al quale tale server E-mail è collegato. Relay Aperto può anche essere indicato con le espressioni "Spam relay" o "public relay";
"Spam"	indica E-mail commerciali non richieste;
"Tower"	indica un gruppo (cluster) di server E-mail a carico bilanciato (load balanced server);
"Utente"	indica una persona fisica, casella di posta o macchinario che utilizza il Servizio; e
"Virus"	indica una parte di codice programma, compreso un elemento auto-replicante, solitamente nascosto dietro a qualcosa di diverso, programmato in modo tale da infettare altri sistemi informatici.

2. Introduzione

2.1 Symantec è un fornitore di servizi gestiti specializzato in sicurezza a livello di Internet per E-mail, Messaggistica Istantanea e Web.

2.2 Il Servizio è gestito ventiquattro (24) ore al giorno, sette (7) giorni su sette dal Centro Operativo Globale di Symantec. Il Servizio è monitorato per verificare la disponibilità dell'hardware, la capacità di servizio e l'utilizzo delle risorse di rete.

2.3. Qualora Symantec non sia in grado di consegnare l'E-mail al server di posta del Cliente, Symantec archivierà l'E-mail in entrata del Cliente fino a sette (7) giorni in attesa della consegna.

2.4. Il Servizio è disponibile ai Clienti che sono collegati in modo permanente a Internet con un indirizzo IP fisso. Il servizio non può essere fornito ai Clienti i cui sistemi siano collegati a Internet attraverso linee di accesso remoto (dial up)o ISDN o i cui indirizzi IP siano allocati in modo dinamico.

2.5. La reputazione IP del mittente viene controllata per tutte le E-mail in entrata. Le E-mail che hanno origine da una fonte di dubbia reputazione (come uno spammer) saranno rallentate per minimizzare l'impatto sulla capacità della rete.

2.6 Il Cliente deve configurare i propri server di e-mail in modo da limitare a meno di 500 il numero di destinatari per connessione SMTP in uscita. Un destinatario è un singolo indirizzo di e-mail. Un gruppo di e-mail può contenere uno o più destinatari. Se un'E-mail in entrata o in uscita contiene più di 500 destinatari in una connessione SMTP, Symantec elaborerà i primi 500 destinatari e invierà un codice di risposta SMTP al server di e-mail di invio per reinviare l'E-mail ai destinatari rimanenti.

3. Manutenzione programmata

3.1. Per gli scopi della presente Clausola 3, "Manutenzione Programmata" indica i periodi di manutenzione per i quali al Cliente sia stata data una notifica anticipata di sette (7) giorni da parte di Symantec e che potrebbe causare un'interruzione del Servizio a causa della non disponibilità di una o più Tower. La Manutenzione Programmata non supererà le otto (8) ore per mese di calendario, e in ogni caso non avrà luogo fra le ore 8.00 e le ore 18.00 (dell'ora locale in cui si trova il server Tower).

3.2. Ovunque sia possibile, la Manutenzione Programmata sarà eseguita senza influire sul Servizio. Ciò sarà generalmente realizzato eseguendo la Manutenzione Programmata nel corso di periodi di basso traffico previsto ed eseguendo la Manutenzione Programmata su parte della rete, e non su tutta la rete in un'unica volta. Nel corso dei periodi di Manutenzione Programmata, il traffico può essere trasferito su sezioni della rete che non siano sottoposte alla manutenzione, al fine di minimizzare l'interruzione del Servizio.

3.3. Laddove fosse necessaria una manutenzione di emergenza che potrebbe influenzare il Servizio, Symantec tenterà di informare le parti coinvolte e pubblicherà messaggi di avviso su ClientNet non appena possibile, e in ogni caso entro un'ora (1) dall'inizio della manutenzione di emergenza.

4. ClientNet

4.1. Una parte integrante del Servizio è lo strumento di configurazione, gestione e reporting basato su Internet di Symantec, chiamato ClientNet. ClientNet è a disposizione del Cliente attraverso un login sicuro protetto da password, che non deve essere divulgata a terzi. ClientNet fornisce i mezzi che consentono al Cliente di visualizzare i dati e le statistiche relativi all'utilizzo del Servizio e offre diverse strutture di gestione e configurazione.

5. Supporto tecnico

5.1. Symantec si impegna, ventiquattro (24) ore su ventiquattro, sette (7) giorni su sette a:

a) fornire supporto tecnico al Cliente in caso di problemi con il Servizio; e
b) interagire con il Cliente al fine di risolvere tali problemi.

6. Servizio clienti

6.1. Symantec fornirà un servizio clienti nel corso del Normale Orario di Lavoro per:

a) ricevere ed elaborare gli ordini per la fornitura del Servizio;
b) ricevere ed elaborare le richieste di modifiche agli aspetti operativi del Servizio; e
c) rispondere alle richieste relative alla fatturazione.

6.2. A meno che non sia diversamente indicato nella Descrizione del Servizio rilevante, alla ricezione di un ordine completo e compiutamente eseguibile , o di una Richiesta di Cambiamento di Servizio, la Squadra di Fornitura Globale di Symantec dovrà fornire il Servizio entro ventisette (27) ore del Normale Orario Lavorativo, a condizione che tutte le dovute fasi di verifica tecnica siano state completate.

7. Bundle di Servizi non divisibili

7.1 I bundle di Servizi non divisibili (se selezionati nella Sezione B "Servizio e Costi" del Contratto) comprendono i seguenti Servizi costitutivi:

Nome attuale del bundle di servizi non separabili	Servizi costitutivi (Servizio costitutivo precedente)	Nome precedente del bundle di servizi non separabili
Symantec MessageLabs Email Protect.cloud	Email AV, Email AS	MessageLabs Email Protect
Symantec MessageLabs Email Control.cloud	Email IC, Email CC	MessageLabs Email Control
Symantec MessageLabs Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC	MessageLabs Email Safeguard (or MessageLabs Email Protect & Control)
Symantec MessageLabs Web v2 Protect & Control.cloud	Web v2 Protect, Web v2 URL	MessageLabs Web Protect & Control
Not Offered	(Email AV, Email AS, Web AVASv2)	MessageLabs Email Protect & Web Protect
Not Offered	(Email AV, Email IC, Email AS, Email CC, Web AVASv2)	MessageLabs Email Protect & Control & Web Protect
Not Offered	(Email AV, Email AS, Web AVASv2, Web URLv2)	MessageLabs Email Protect & Web Protect & Control
Symantec MessageLabs Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web v2 Protect, Web v2 URL (Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2)	MessageLabs Email & Web Safeguard (or MessageLabs Email & Web Protect & Control)
Symantec MessageLabs 2 Email Services Bundle	2 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 2 Email Services Bundle
Symantec MessageLabs 3 Email Services Bundle	3 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 3 Email Services Bundle
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving (P))	MessageLabs Email Protect & Control & Archiving (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Lite (P))	MessageLabs Email Protect & Control & Archiving Lite (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Premium(P))	MessageLabs Email Protect & Control & Archiving Premium(P)
Symantec MessageLabs Security Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2, IMSS	MessageLabs Security Safeguard
Symantec MessageLabs Complete Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud	MessageLabs Complete Email Safeguard
Symantec MessageLabs Complete Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL	MessageLabs Complete Email & Web Safeguard
Symantec MessageLabs Ultimate Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL , IMSS	MessageLabs Ultimate Safeguard
Symantec Enterprise Vault.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud	MessageLabs Email Archiving L or Email Archiving.cloud (L)
Symantec Enterprise Vault Enhanced.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec EnterpriseVault Mailbox Continuity.cloud	Messagelabs Email Enhanced Archive L or Email Enhanced Archiving.cloud (L)

8. Nomi precedenti dei servizi

8.1 Per i clienti che hanno acquistato Servizi prima dell'1 giugno 2011, i Nomi dei servizi in questo documento sono citati utilizzando una nomenclatura diversa dai nomi originali dei Servizi precedenti. Il diagramma di seguito indica i corrispondenti termini precedenti della nomenclatura riveduta in modo che i Clienti possano determinare quali sezioni del documento sono applicabili ai Servizi acquistati in base alla nomenclatura precedente.

Nomi precedente del servizio	Nome attuale del servizio
MessageLabs Email Anti-Virus	Symantec MessageLabs Email Anti-Virus.cloud
MessageLabs Email Image Control	Symantec MessageLabs Email Image Control.cloud
MessageLabs Email Anti-Spam	Symantec MessageLabs Email Anti-Spam.cloud
MessageLabs Email Content Control	Symantec MessageLabs Email Content Control.cloud
MessageLabs Boundary Encryption	Symantec MessageLabs Email Boundary Encryption.cloud
MessageLabs Web Anti-Spyware and Anti-Virus Service v2	Symantec MessageLabs Web v2 Protect.cloud
MessageLabs Web URL Service v2	Symantec MessageLabs Web v2 URL.cloud
MessageLabs Email Archiving P	Symantec MessageLabs Email Archiving.cloud (P)
MessageLabs Enterprise Instant Messenger (EIM)	Symantec MessageLabs EIM.cloud
MessageLabs EIM Connect	Symantec MessageLabs EIM Connect.cloud
MessageLabs EIM Communicate	Symantec MessageLabs EIM Communicate.cloud
MessageLabs Policy Based Encryption	Symantec MessageLabs Policy Based Encryption.cloud
MessageLabs Email Continuity (EC), or Symantec MessageLabs Email Continuity.cloud (D)	Symantec Email Continuity.cloud (EC)
Schemus Tool	Schemus Tool
MessageLabs Instant Messaging Security Service (IMSS)	Symantec MessageLabs Instant Messaging Security.cloud
MessageLabs Email Archiving D, or Symantec MessageLabs Email Archiving.cloud (D)	Symantec Email Continuity Archive.cloud
MessageLabs Email Archiving Lite D, or Symantec MessageLabs Email Archiving.cloud Lite (D)	Symantec Email Continuity Archive Lite.cloud
MessageLabs Volume Mail	Symantec MessageLabs Volume Mail
Hosted Endpoint Protection	Symantec Endpoint Protection.cloud
MessageLabs Personal Archive L or Symantec MessageLabs Email Personal Archiving.cloud (L)	Symantec Enterprise Vault Personal.cloud
MessageLabs Email Discovery Archive L, or Symantec MessageLabs Email Discovery Archiving.cloud (L)	Symantec Enterprise Vault Discovery.cloud
MessageLabs Personal Archive L for BlackBerry®, or Symantec MessageLabs Personal Archive for BlackBerry®.cloud (L)	Symantec Enterprise Vault.cloud Blackberry Option
MessageLabs Email Archiving Premiium L , or Symantec MessageLabs Email Premium Archiving.cloud (L)	AdvisorMail on Symantec.cloud™

MessageLabs Email Archiving IM Premium L, or Symantec MessageLabs Email Premium Archiving.cloud for IM (L)	AdvisorMail IM Option on Symantec.cloud™
MessageLabs Email Archiving Bloomberg Message Premium L, or Symantec MessageLabs Premium Archiving.cloud for Bloomberg	AdvisorMail Bloomberg Option on Symantec.cloud™
MessageLabs Email Archive Import Service L, or Symantec MessageLabs Email Archiving.cloud (L) Import	Symantec Enterprise Vault.cloud Data Import Option
MessageLabs Email Continuity L, or Symantec MessageLabs Email Continuity.cloud (L)	Symantec Enterprise Vault Mailbox Continuity.cloud
MessageLabs User Roaming Agent Service (“Smart Connect”)	Symantec MessageLabs Web v2 Smart Connect.cloud

Allegato 2
Descrizioni del Servizio

Appendice 1 - Servizio Symantec MessageLabs Email Anti-Virus.cloud

1. Panoramica

1.1. Il Servizio Symantec MessageLabs Email Anti-Virus.cloud ("E-mail AV") è il Servizio di scansione a livello di Internet alla ricerca di Virus nelle E-mail di Symantec. Le E-mail in entrata e in uscita del Cliente, compresi tutti gli allegati, le macro o i file eseguibili, sono indirizzate attraverso E-mail AV utilizzando le impostazioni di registrazione DNS e MX.

1.2. Le E-mail e gli allegati vengono scansionati da prodotti anti-virus multipli leader nel settore, compreso lo scanner euristico di Symantec, Skeptic™.

2. Messaggi di avviso

2.1 Qualora un'E-mail o gli allegati in entrata contengano un Virus, un avviso automatico potrà essere inviato al mittente e al destinatario, se selezionato dal Cliente, come notifica. Con un'E-mail in uscita del Cliente, il Servizio può inviare la notifica esclusivamente al mittente e non al destinatario. Le notifiche utente possono essere inviate anche all'amministratore dell'E-mail in entrambi i casi. L'E-mail infetta viene inoltrata ad un server sicuro per la distruzione automatica dopo sette (7) giorni, a condizione che non sia trasportata come virus di mass mail, nel cui caso sarà cancellata immediatamente.

2.1. In caso di infezione di grosse dimensioni causata da un nuovo Virus, un messaggio di avviso sarà pubblicato su ClientNet.

3. Configurazione

3.1. ClientNet può essere usata per la personalizzazione dei testi dei banner, per rilasciare E-mail infette da Virus e per impostare le dimensioni massime delle E-mail.

4. Rilascio di un'E-mail infetta da Virus

4.1. Qualora un'E-mail infetta da Virus appare rilasciabile, il rilascio può avvenire tramite server sicuro usando ClientNet. L'E-mail sarà rilasciata al primo indirizzo della lista originale di destinatari, oppure a un indirizzo specificato precedentemente e notificato a Symantec e archiviato da Symantec su ClientNet (Nota: questi indirizzi possono essere nomi di gruppi di E-mail o alias, nel cui caso l'E-mail sarà rilasciata a tutti gli indirizzi del gruppo o alias). Come opzione, l'E-mail infetta da Virus può essere rilasciata ad un indirizzo alternativo da Symantec, alla ricezione del Modulo di Autorizzazione al Rilascio appropriato. Symantec agirà esclusivamente su richiesta autorizzata dai Clienti di inoltrare le E-mail infette da Virus. Symantec non restituirà le E-mail infette da Virus al mittente. Symantec non inoltrerà le E-mail infette da Virus a terzi. Alcune E-mail infette da Virus inviate al cliente non sono rilasciabili in quanto contengono un Virus particolarmente infetto o dannoso. Queste e-mail vengono specificate su ClientNet come non rilasciabili.

5. Termini e Condizioni di E-mail AV

5.1. Se viene richiesto di rilasciare un'E-mail infetta da Virus, Symantec la rilascerà entro otto (8) ore del Normale Orario Lavorativo dalla ricezione della richiesta di rilascio debitamente autorizzata.

Appendice 2 - Servizio Symantec MessageLabs Email Image Control.cloud

1. Panoramica

1.1. Il servizio Symantec MessageLabs Email Image Control.cloud ("E-mail IC") è il servizio di controllo delle immagini E-mail a livello di Internet di Symantec ed è progettato per rilevare immagini pornografiche contenute nei file di immagini.

2. Descrizione del Servizio

2.1. Le E-mail in entrata e in uscita del Cliente possono essere scansionate usando l'Image Composition Analysis (ICA), alla ricerca di immagini pornografiche contenute nei file di immagini allegati alle E-mail.

2.2. Nel caso in cui l'E-mail in entrata o in uscita di un Cliente sia sospetta e si ritenga possa contenere un'immagine pornografica, sarà eseguita una tra le varie possibili azioni, a seconda delle opzioni di configurazione selezionate dal Cliente.

3. Configurazione

3.1. Alla ricezione di un ordine completo e accettato, Symantec renderà E-mail IC disponibile al Cliente. Inizialmente E-mail IC sarà abilitato per ciascuno dei domini del Cliente. Il Cliente ha la responsabilità di impostare le opzioni di configurazione per E-mail IC per ciascun dominio, secondo le necessità del Cliente. Il Cliente configura E-mail IC usando ClientNet.

3.2. Sono disponibili opzioni per specificare il livello di sensibilità di rilevamento in base al quale funzionerà il filtro ICA. La sensibilità può essere impostata come Elevata, Media o Bassa. Queste impostazioni sono particolarmente soggettive; tuttavia, come guida generale, più immagini saranno sospettate di essere pornografiche quando si imposta una sensibilità Elevata, e meno immagini saranno sospettate di essere pornografiche quando si imposta una sensibilità Bassa.

3.3. Sono disponibili opzioni per definire le azioni da intraprendere nel momento in cui si rileva un'immagine pornografica sospetta. Tali opzioni possono essere impostate indipendentemente per le E-mail in entrata e in uscita, e devono essere impostate in conformità con gli adeguati termini d'uso per i computer del Cliente (o suo equivalente) previgenti . Tali opzioni sono:

3.3.1. registrare le E-mail sospette (fornisce dati statistici visualizzabili via ClientNet);

3.3.2. taggare le E-mail sospette all'interno dell'intestazione (solo per le E-mail in entrata);

3.3.3. copiare le E-mail sospette in un indirizzo E-mail predefinito;

3.3.4. ridirigere le E-mail sospette ad un indirizzo E-mail predefinito;

3.3.5. cancellare l'E-mail sospetta;

3.3.6. taggare l'E-mail sospetta nella riga dell'oggetto.

3.4. Laddove il Cliente abbia preventivamente identificato mittenti o destinatari fidati di E-mail per l'amministrazione di E-mail IC, le E-mail provenienti da tali mittenti e destinatari non saranno scansionate da E-mail IC.

4. Reporting

4.1. Se le opzioni scelte nella Clausola 3.3 della presente Appendice sono quelle di reindirizzare o cancellare l'E-mail contenente una sospetta immagine pornografica, un avviso automatico può essere inviato al mittente. Se l'E-mail del Cliente è in entrata, può essere mandato un avviso automatico anche al destinatario. Tali allarmi automatici possono essere attivati o disattivati dal Cliente attraverso ClientNet.

4.2. Il reporting dell'efficacia di E-mail IC viene fornito attraverso ClientNet, in cui sono disponibili dati statistici sul numero di E-mail in entrata e in uscita sospette di contenere immagini pornografiche. ClientNet può essere configurato per generare rapporti inviati via E-mail al Cliente settimanalmente o mensilmente.

5. Termini e Condizioni di E-mail IC

5.1. NESSUN SOFTWARE DI RILEVAMENTO DI IMMAGINI PORNOGRAFICHE PUÒ GARANTIRE UN TASSO DI RILEVAMENTO DEL 100% E, DI CONSEGUENZA, SYMANTEC NON PUÒ ESSERE CONSIDERATA RESPONSABILE IN ALCUN MODO PER DANNI O PERDITE DERIVANTI, DIRETTAMENTE O INDIRETTAMENTE, DA QUALUNQUE MANCATO RILEVAMENTO DA PARTE DEL SERVIZIO DI UN'IMMAGINE PORNOGRAFICA, O PER UNA IDENTIFICAZIONE ERRONEA DI UN'IMMAGINE COME PORNOGRAFICA CHE SUCCESSIVAMENTE SI DIMOSTRI NON ESSERE TALE.

5.2. Potrebbe non essere possibile scansionare gli allegati con contenuti sotto il diretto controllo del mittente (ad es., allegati protetti da password e/o crittografati).

5.3. E-mail IC è in grado di scansionare alla ricerca di immagini pornografiche nascoste in alcune versioni di documenti in Word, Excel, PowerPoint e pdf, ma non in altri documenti.

5.4. Symantec sottolinea che la configurazione di E-mail IC è completamente sotto il controllo del Cliente. E-mail IC deve essere usato esclusivamente per consentire al Cliente di implementare i previgenti adeguati termini d'uso per i computer del Cliente (o suo equivalente) . In alcuni paesi, potrebbe essere necessario ottenere il consenso di ciascun singolo dipendente. Symantec consiglia al Cliente di controllare sempre le normative locali prima di attivare E-mail IC. Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento di E-mail IC. Il Cliente riconosce che la definizione di ciò che costituisce e ciò che non costituisce un'immagine pornografica è soggettiva. Il Cliente deve tenere presente questo quando esegue la configurazione del Servizio.

5.5. Nel caso in cui il Cliente rilasci o richieda il rilascio di E-mail infette da Virus, l'E-mail rilasciata non sarà sottoposta a scansione tramite E-mail IC prima del rilascio.

Appendice 3 - Servizio Symantec MessageLabs Email Anti-Spam.cloud

1. Panoramica

1.1. Il servizio Symantec MessageLabs Email Anti-Spam.cloud ("E-mail AS") è il servizio Anti-Spam E-mail a livello di Internet di Symantec, progettato per proteggere il Cliente da E-mail non richieste o non desiderate.

2. Descrizione del Servizio

2.1. L'E-mail in entrata del Cliente può essere scansionata utilizzando diversi metodi di rilevamento, per stabilire se si tratti o meno di Spam. Nel caso in cui un'E-mail in entrata sia sospettata di essere Spam, è possibile intraprendere un'azione tra varie, a seconda delle opzioni di configurazione selezionate dal Cliente nella Clausola 3.2 riportata di seguito.

2.2. Il Cliente, e anche l'Utente individuale, se il Cliente ha abilitato le impostazioni a livello di Utente, può compilare una lista privata di mittenti approvati. Se viene selezionato questo metodo di rilevamento, e viene ricevuta un'E-mail in entrata da un dominio elencato in una lista di mittenti approvati, questa supererà automaticamente qualunque altro metodo di rilevamento di Spam selezionato.

2.3. Il Cliente, e anche un Utente individuale, se il Cliente ha abilitato le impostazioni a livello di Utente, può compilare una lista privata di mittenti bloccati. Se viene selezionato questo metodo di rilevamento e viene ricevuta un'E-mail da un dominio elencato nella lista di mittenti bloccati, verrà eseguita l'azione definita dalle opzioni di configurazione nella Clausola 3.2 riportata di seguito.

2.4. Possono essere usate diverse liste di mittenti bloccati pubblici. Se sono selezionati uno o più di questi metodi di rilevamento, e viene ricevuta un'E-mail da un dominio elencato in una delle liste di blocco pubbliche selezionate, verrà intrapresa l'azione definita nell'opzione di configurazione nella Clausola 3.2 riportata di seguito.

2.5. Se un'E-mail non è stata cancellata dopo essere stata bloccata come descritto precedentemente, e viene selezionato il sistema di firma e l'azione che dovrebbe essere intrapresa nel momento in cui viene rilevata l'E-mail come Spam che sia più grave di quella già selezionata a causa del rilevamento della lista di mittenti bloccati, l'E-mail in entrata del Cliente viene scansionata usando un sistema di firma. Se viene rilevata un'E-mail come Spam con questo metodo, sarà intrapresa l'azione definita dalle opzioni di configurazione nella Clausola 3.2 riportata di seguito. Tale azione sostituirà qualunque azione meno rigida precedentemente allocata da qualunque metodo della lista di mittenti bloccati.

2.6. Se, a seguito ai processi precedenti, l'E-mail non è stata cancellata, e viene selezionato un rilevamento euristico, e l'azione che dovrebbe essere intrapresa quale risultato del rilevamento dell'E-mail come Spam configurata dal Cliente è più rigida di quella già selezionata, come risultato del rilevamento da parte dei processi precedenti, l'E-mail in entrata del Cliente viene scansionata utilizzando la scansione euristica. Se un'E-mail in entrata viene rilevata con il sistema euristico come Spam, saranno intraprese le azioni descritte nelle opzioni di configurazione della Clausola 3.2 riportata di seguito. Questa azione sostituirà qualunque azione meno rigida precedentemente allocata da uno qualunque dei metodi precedenti.

2.7. Le liste di mittenti bloccati/mittenti approvati fornite da Symantec sono fornite esclusivamente a titolo esemplificativo.

3. Configurazione

3.1. Alla ricezione di un ordine completo e accettato, Symantec abiliterà E-mail AS per il Cliente. Inizialmente, E-mail AS sarà abilitato per ciascuno dei domini del Cliente. IL CLIENTE ACCETTA CHE E-MAIL AS SARÀ FORNITA CON LE IMPOSTAZIONI PREDEFINITE DI SYMANTEC APPLICATE DALL'INIZIO, E CHE È RESPONSABILITÀ DEL CLIENTE CONFIGURARE E-MAIL AS ATTRAVERSO CLIENTNET SECONDO LE PROPRIE ESIGENZE. Le impostazioni predefinite applicate per E-mail AS comprendono le seguenti azioni:

3.1.1. Bloccare e cancellare l'E-mail; oppure
3.1.2. Mettere l'E-mail in quarantena; e
3.1.3. Usare una lista di mittenti approvati per indirizzi IP, domini e indirizzi e-mail; e
3.1.4. Usare un sistema di rilevamento Spam (Skeptic).

3.2. Sono disponibili opzioni per specificare le azioni da intraprendere nel caso di E-mail sospettata di essere Spam. Tali opzioni, elencate di seguito, sono selezionabili per ciascun metodo di rilevamento disponibile:

3.2.1. taggare l'E-mail sospetta nell'intestazione;

3.2.2. taggare l'E-mail sospetta nella riga dell'oggetto;

3.2.3. ridirigere l'E-mail sospetta a un indirizzo E-mail pre-definito (che deve essere in un dominio scansionato dal Servizio);

3.2.4. cancellare l'E-mail sospetta;

3.2.5. Mettere lo Spam in quarantena.

4. Descrizione del Servizio di Quarantena dello Spam

4.1. Se il Cliente configura la Quarantena dello Spam per un dominio, viene creato automaticamente un account di Quarantena dello Spam per ciascun Utente la prima volta che uno Spam sospetto viene identificato daE-mail AS e l'Utente riceverà automaticamente una notifica via E-mail.

4.2. L'Utente può accedere alla Quarantena dello Spam attraverso l'interfaccia Spam Manager.

4.3. Lo Spam sospetto può essere memorizzato fino a un massimo di quattordici (14) giorni, dopo i quali sarà cancellato automaticamente. Il Cliente può acquistare un periodo di memorizzazione superiore, oltre tale periodo di quattordici (14) giorni, su pagamento di un costo aggiuntivo calcolato per Utente al giorno ("Symantec MessageLabs Extended Spam Quarantine").

4.4. Se la Quarantena dello Spam non è in grado di accettare E-mail, lo Spam sospetto sarà taggato e inviato al destinatario.

5. Configurazione della Quarantena dello Spam

5.1. Il Cliente configura la Quarantena dello Spam attraverso ClientNet.

5.2. Le notifiche Utente predefinite sono impostate in conformità con la clausola 5.2.1di seguito. L'Utente può selezionare in qualunque momento una delle seguenti opzioni di notifica:

5.2.1. Notifiche da ricevere quotidianamente;

5.2.2. Notifiche da ricevere a frequenze varie;

5.2.3. Notifiche da non ricevere.

5.3. Le seguenti opzioni di rilascio sono disponibili tramite lo Spam Manager: (i) Cancellare l'E-mail; (ii) Rilasciare l'E-mail all'indirizzo del destinatario originale; (iii) Revisionare il testo dell'E-mail.

5.4. Per utilizzare la Quarantena dello Spam, il Cliente deve aver registrato una Lista di Convalida con Symantec. La Lista di Convalida comprende tutti gli indirizzi E-mail validi utilizzati dal Cliente. Qualunque indirizzo di un destinatario che non si trovi nella Lista di Convalida viene considerato invalido e l'E-mail non sarà consegnata a tale indirizzo.

5.5. Attraverso ClientNet, un Cliente può controllare altri aspetti dello Spam Manager: (a) politica di notifica automatizzata o manuale; (b) impostazione delle notifiche riassuntive; (c) impostazioni della lingua predefinita; (d) impostazioni a livello di Utente; (e) E-mail con alias preimpostati e (f) Utenti specializzati (ad es., Amministratori di Quarantena).

5.6. Il Cliente può stabilire gruppi di indirizzi e-mail per la Quarantena dello Spam, per collegare diversi indirizzi e-mail individuali ad un indirizzo e-mail 'proprietario' a fini di alias delle e-mail e accesso delegato. Il numero massimo di indirizzi e-mail che possono essere collegati a un singolo indirizzo e-mail è cinquanta (50). Symantec si riserva il diritto di eliminare il gruppo di account del Cliente o link di alias nel caso in cui venga superato il numero massimo.

6. Reporting

6.1. Il reporting sull'efficacia di E-mail AS viene fornito attraverso ClientNet. ClientNet può essere configurato per generare rapporti inviati via E-mail al Cliente settimanalmente o mensilmente.

7. Termini e Condizioni di E-mail AS

NESSUN SOFTWARE ANTI-SPAM È IN GRADO DI GARANTIRE UN TASSO DI RILEVAMENTO DEL 100%, E, DI CONSEGUENZA, SYMANTEC NON PUO' ESSERE CONSIDERATA RESPONSABILE IN ALCUN MODO PER ALCUN DANNO O PERDITA DERIVANTI DIRETTAMENTE O INDIRETTAMENTE DA QUALUNQUE MANCATO RILEVAMENTO DA PARTE DEL SERVIZIO DELLO SPAM O PER AVER IDENTIFICATO ERRONEAMENTE UN'E-MAIL SOSPETTA DI ESSERE SPAM CHE SUCCESSIVAMENTE SI DIMOSTRI NON ESSERE TALE. 7.2 Symantec sottolinea che la configurazione di E-mail AS è sotto il pieno controllo del Cliente. Symantec raccomanda al Cliente di disporre adeguati termini d'uso per i computer del Cliente (o suo equivalente). In alcuni paesi, potrebbe essere necessario ottenere il consenso di ciascun singolo dipendente. Symantec consiglia al Cliente di controllare sempre le normative locali prima di utilizzareE-mail AS. Symantec non accetta alcuna responsabilità civile o penale attribuita al Cliente a causa del funzionamento di E-mail AS.

Appendice 4 - Servizio Symantec MessageLabs Email Content Control.cloud

1. Panoramica

1.1. Il Symantec MessageLabs Email Content Control.cloud ("E-mail CC") di Symantec è il servizio di controllo del contenuto di Symantec progettato per consentire al Cliente di configurare la sua strategia di filtro basata su regole in linea con gli adeguati termini d'uso per i computer del Cliente (o suo equivalente) in relazione alle E-mail.

2. Descrizione del Servizio

2.1. E-mail CC consente a un Cliente di creare un insieme di regole sulla base delle quali le E-mail in entrata e in uscita vengono filtrate, secondo la presente Appendice 4. Una regola è un'istruzione impostata dal Cliente che viene utilizzata per identificare un formato di messaggio/allegato particolare o un contenuto particolare che sia collegato ad una particolare azione intrapresa in merito alle E-mail.

3. Configurazione

3.1. Alla ricezione di un ordine completo e accettato, Symantec abiliterà E-mail CC per ciascun dominio applicabile del Cliente. Il Cliente è responsabile di implementare le opzioni di configurazione per E-mail CC per ciascun dominio, secondo le proprie esigenze. Il Cliente configura E-mail CC attraverso ClientNet.

3.2. Il Cliente può configurare le regole su base 'dominio', 'gruppo' o 'individuale'.

3.3. I cambiamenti effettuati dal Cliente alle regole entreranno in vigore entro 24 ore dall'esecuzione di tali cambiamenti.

3.4. Sono disponibili opzioni per la definizione delle azioni da intraprendere al momento del rilevamento di un'E-mail sospetta. Tali opzioni possono essere impostate indipendentemente per le E-mail in entrata e in uscita, e devono essere impostate in linea con la politica d'uso già esistente accettabile per i computer del Cliente (o suo equivalente). Tali opzioni sono:

3.4.1. Bloccare e cancellare l'E-mail sospetta;

3.4.2. Taggare (se in entrata) e ridirigere l'E-mail a un amministratore specifico;

3.4.3. Taggare (se in entrata) e inviare in copia l'E-mail sospetta a un amministratore specifico;

3.4.4. Taggare (se in entrata) l'intestazione dell'E-mail sospetta;

3.4.5. Comprimere gli allegati all'E-mail;

3.4.6. Inserirla soltanto fra i dati statistici di ClientNet;

3.4.7. Taggare nella riga dell'oggetto.

4. Reporting

4.1. Attraverso ClientNet, un Cliente sarà in grado di revisionare i risultati delle proprie regole sotto forma di riassunti quotidiani, settimanali, mensili e annuali, organizzati sia per regola che per Utente.

4.2. I rapporti che contengono documentazione di attività di servizio possono essere generati settimanalmente o mensilmente ed inviati via e-mail al Cliente su richiesta.

4.3. Attraverso ClientNet, il Cliente è in grado di attivare e disattivare le notifiche configurate dal Cliente a seconda della regola.

5. Supporto al Controllo del Contenuto

5.1. Il Supporto comprende descrizione dettagliata dell'interfaccia di E-mail CC, compresa una descrizione del Servizio e una sessione di Domande e Risposte.

6. Wildcarding

6.1. E-mail CC funziona sulla base delle regole configurate dal Cliente. Quale eccezione specifica, tuttavia, wildcarding consente al Cliente di configurare E-mail CC attraverso ClientNet, per identificare alcune formule alfanumeriche che seguono un pattern specifico (ad es., numeri della Previdenza Sociale, numeri di Assicurazione Nazionale, e dati delle carte di credito).

7. Termini e Condizioni di Controllo dei Contenuti

7.1. Le liste dei termini suggeriti e i modelli di regole forniti da Symantec contengono termini che possono essere considerati offensivi.

7.2. Il Cliente accetta e riconosce che Symantec potrà compilare e pubblicare liste di parole predefinite ottenute dalle liste di termini del Cliente.

7.3. Il Cliente riconosce che, qualora E-mail CC venga usato insieme all'azione di quarantena del Servizio Anti-Spam E-mail, ciò può portare a sottoporre lo Spam sospetto a quarantena prima che questa sia stata filtrata da E-mail CC.

7.4. E-mail CC è in grado di scansionare il contenuto nascosto di alcune versioni di documenti Word, Excel, PowerPoint e pdf, ma non di altri documenti.

7.5. Symantec sottolinea che la configurazione di E-mail CC è completamente sotto il controllo del Cliente, e che l'accuratezza di tale configurazione stabilirà l'accuratezza del Servizio E-mail CC; di conseguenza, Symantec non accetta alcuna responsabilità per danni o perdite derivanti direttamente o indirettamente da qualunque mancato rilevamento da parte del Servizio o da una identificazione erronea di un'E-mail contenente contenuto sospetto che successivamente venga dimostrato lecito.

7.6. Symantec raccomanda che il Cliente disponga di adeguati termini d'uso per i computer del Cliente (o suo equivalente) mirati a regolare l'uso delle E-mail fatto dagli Utenti e che qualunque modello di regole fornito da Symantec supporti tale politica. In alcuni paesi, potrebbe essere necessario ottenere il consenso di ciascun singolo dipendente. Symantec consiglia al Cliente di controllare sempre le normative locali prima di attivare E-mail CC. Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento di E-mail CC.

Appendice 5 - Servizio Symantec MessageLabs Email Boundary Encryption.cloud

1. Panoramica

1.1. Il Servizio Symantec MessageLabs Email Boundary Encryption.cloud ("Boundary Encryption, BE") fornisce canali di comunicazione crittografata che consentono al Cliente di formare una rete di E-mail privata sicura (secure private E-mail network, SPEN) con organizzazioni partner individuate ("Partner SPEN"). Tale configurazione è nota come crittografia "Applicata".

1.2. Inoltre, il Cliente può anche ricevere E-mail crittografate inviate in modo opportunistico da organizzazioni che abbiano server di posta TLS-compatibili per i quali non esista crittografia Applicata con il Cliente, se tali organizzazioni dispongono di server di posta compatibili con TLS. Tale configurazione è nota come crittografia "Opportunistica".

1.3. Se il Cliente ha sottoscritto a BE ma non ha identificato esplicitamente alcun Partner SPEN, il Cliente può ricevere E-mail inviate in modo opportunistico in entrata su TLS, e inviare le E-mail crittografate in modo opportunistico in uscita a organizzazioni non Partner SPEN.

1.4. Inoltre, il Cliente può configurare i propri server e-mail per il modello "Connessione Sicura" di BE, in tal caso:

1.4.1 Gli scambi di E-mail fra Symantec e i server di posta della Connessione Sicura del Cliente saranno protetti da crittografia TLS. Se il routing sarà eseguito in formato crittografato o meno dipenderà da (i) applicazioni TLS specificate dal Cliente e (ii) capacità del server di destinazione di ricevere le E-mail su TLS Opportunistico.

1.4.2 IL CLIENTE RICONOSCE E ACCETTA CHE, SE IL MODELLO DI CONNESSIONE SICURA NON VIENE APPLICATO A UN SERVER DI POSTA PARTICOLARE, LE E-MAIL IN ENTRATA E IN USCITA DEL CLIENTE, CHE ABBIANO ORIGINE O SIANO RICEVUTE DA QUEL SERVER DI POSTA, NON POSSONO ESSERE PROTETTE DALLA CRITTOGRAFIA TLS. DI CONSEGUENZA, IL CLIENTE RICONOSCE E ACCETTA CHE NON DEVE INVIARE O RICEVERE DATI SENSIBILI ATTRAVERSO TALI SERVER DI POSTA E CHE LO FA A SUO COMPLETO RISCHIO.

1.5 Se il Cliente sta utilizzando BE insieme al Servizio PBE, la pratica migliore raccomandata da Symantec è che il Cliente implementi il modello di Connessione Sicura di BE su tutti i propri server di posta.

1.6 **BE FUNZIONA SOLO QUANDO UTILIZZATO INSIEME A UNO DEI SEGUENTI SERVIZI E NON PUÒ OPERARE COME SERVIZIO SINGOLO: E-MAIL AV, E-MAIL AS, E-MAIL IC E/O E-MAIL CC.**

2. Fornitura e fatturazione

2.1. Symantec inizierà l'addebito di BE a partire dalla data in cui Symantec verifica che la rete del Cliente è tecnicamente in grado di supportare BE ("Data di approvazione tecnica").

2.2 La Clausola 5.2 del Allegato 1 non verrà applicata a BE. L'obiettivo di Symantec sarà di soddisfare gli ordini BE e le richieste di modifica BE entro 4 settimane dalla Data di approvazione tecnica, a condizione che il Cliente abbia soddisfatto tutti i requisiti preliminari.

2.3 Nel caso in cui Symantec debba allocare risorse tecniche aggiuntive per la fornitura di BE, a causa della mancata esecuzione della due diligence necessaria da parte del Cliente, Symantec si riserva il diritto di addebitare i servizi professionali aggiuntivi al prezzo di £1500/€1500 (a seconda della valuta di fatturazione del Cliente) a persona al giorno.

3. Configurazione

3.1. Il Cliente definirà per dominio i Partner SPEN con i quali desidera comunicare in modo sicuro. I Partner SPEN possono essere clienti o meno di BE, tuttavia Symantec non supporterà i Partner SPEN direttamente. Le organizzazioni non Partner SPEN possono ricevere E-mail Opportunistiche su TLS in uscita come descritto nella Clausola 1 precedente, nel caso in cui i loro server di posta supportino la ricezione di posta crittografata.

3.2. BE si basa sullo standard 'SMTP su TLS' (Simple Mail Transfer Protocol over Transport Layer Security) ("STARTTLS").

3.3. I server di posta, sia del Cliente che del Partner SPEN, devono supportare STARTTLS per essere abilitati all'uso di BE.

3.4. BE è supportato dalle Tower selezionate attraverso le quali tutte le E-mail STARTTLS vengono instradate. Di conseguenza, il Cliente stabilisce quali domini utilizzare in BE.

3.5. Quando si utilizza BE insieme alla funzionalità del sistema di firma di E-mail AS, Symantec raccomanda al Cliente di includere nella lista di mittenti approvati E-mail AS tutti i domini dei Partner SPEN. Nel caso in cui questa migliore prassi raccomandata non sia seguita, il Cliente riconosce e accetta che, in alcune circostanze che coinvolgono la non disponibilità del sistema di firma locale, le E-mail possono essere ridirette a un sistema di firma remoto attraverso una rete pubblica.

4. Certificati e Autenticazione

4.1. Laddove il Cliente dia origine a una connessione STARTTLS, il server di posta ricevente deve fornire il proprio certificato di autenticazione. Se il server di posta ricevente desidera autenticare il Servizio, Symantec fornirà il suo certificato client per l'autenticazione. Se il server di posta ricevente non è in grado di autenticare, l'E-mail sarà restituita al Cliente.

4.2. Laddove un server di posta esterno dia origine a una connessione STARTTLS, il Servizio fornirà il proprio certificato server per l'autenticazione, ma non insisterà con il server di posta esterno per la fornitura di un certificato client per l'autenticazione.

4.3. La convalida di qualunque certificato si basa sull'Autorità Certificatrice che ha firmato il certificato. Per ciascun certificato inviato da un server di posta remoto, come parte della connessione STARTTLS, il Servizio confermerà che un'Autorità Certificatrice riconosciuta abbia firmato il certificato. Se un certificato non può essere convalidato con un'Autorità di Certificato riconosciuta, la connessione sarà interrotta e l'E-mail sarà restituita al mittente.

5. Termini e Condizioni della Crittografia

5.1. Symantec non si assume alcuna responsabilità relativamente al mancato adempimento da parte del Cliente o di qualunque terzo (compreso, senza limitazioni, qualunque Partner SPEN) degli obblighi relativamente alla registrazione dei certificati o della tempestività o accuratezza di tali informazioni.

5.2. BE deve essere utilizzata esclusivamente per consentire al Cliente di implementare adeguati termini d'uso per i computer del Cliente (o suo equivalente) già esistenti. L'utilizzo di servizi di crittografia in alcuni paesi può essere soggetto a normative. Si consiglia al Cliente di controllare sempre le normative rilevanti prima di attivare il Servizio BE. Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento di BE.

Appendice 6 - Servizio Symantec MessageLabs Web v2 Protect.cloud

1. Panoramica

1.1. Una volta eseguiti i cambiamenti rilevanti nella configurazione, le richieste relative a pagine Web e allegati vengono instradati elettronicamente attraverso il Servizio Anti-Virus e Anti Spyware del Web di Symantec ("Web v2 Protect"), e vengono poi esaminati in modo digitale per il rilevamento di virus.

1. Descrizione del Servizio

2.1. Le richieste esterne del Cliente HTTP e FTP-su-HTTP, compresi tutti gli allegati, le macro e i file eseguibili, vengono indirizzate attraverso Web v2 Protect.

2. Configurazione

3.1. Le impostazioni di configurazione necessarie per dirigere questo traffico esterno attraverso Web v2 Protect sono effettuate e manutenute dal Cliente, e dipendono dall'infrastruttura tecnica del Cliente. Il Cliente deve assicurare che il traffico interno HTTP/FTP-su-HTTP (ad es., all'Intranet aziendale) non sia diretto attraverso Web v2 Protect. Laddove il Cliente abbia servizi Internet che richiedano una connessione diretta piuttosto che tramite proxy, è responsabilità del Cliente apportare le modifiche necessarie alla propria infrastruttura, per facilitare tale processo.

3.2. L'accesso a Web v2 Protect è limitato attraverso Scanning IP, i.e. l'indirizzo/gli indirizzi IP dal quale/dai quali ha origine il traffico web del Cliente. Gli Scanning IP sono usati anche per identificare il cliente e per selezionare in modo dinamico le impostazioni specifiche per il cliente.

3.3. Web v2 Protect scansionerà gli elementi appropriati della pagina Web e i suoi allegati che possono contenere virus, codici nocivi, spyware o adware. Potrebbe non essere possibile scansionare alcune pagine Web, alcuni contenuti o allegati (ad es., se protetti da password). Gli allegati identificati in modo specifico come non scansionabili non saranno bloccati. Il traffico in streaming e crittografato (ad es., Media streaming e/o HTTPS/SSL) non può essere scansionato e attraverserà Web v2 Protect senza essere sottoposto a scansione.

3.4. Il Supporto Utente in Roaming è una caratteristica opzionale che estende il Servizio Web ASAV v2 agli Utenti che non si trovano all'interno della rete aziendale (ad es., ad un Utente che lavora da casa). Il Cliente deve installare un file PAC nel PC dell'Utente, in modo che l'Utente venga indirizzato al portale web di Symantec, quando il browser viene avviato. Per accedere al portale web, l'Utente deve inserire password e nome utente. Il Cliente può scaricare un modello di file PAC da ClientNet e modificarlo.

3. Avvisi

4.1. Se si scopre che la pagina Web di un Cliente o gli allegati contengono un oggetto identificato come Virus, Spyware o Adware, l'accesso a tale pagina Web o allegato viene negato e l'utente di Internet visualizzerà automaticamente una pagina Web di avviso. In rari casi, e qualora uno o più elementi del contenuto richiesto siano bloccati, potrebbe non essere possibile visualizzare la pagina Web di avviso e la pagina di avviso potrebbe sostituire il contenuto dell'articolo richiesto, ma l'accesso alla pagina infetta o all'allegato infetto potrebbe comunque essere ancora negato.

4.2. Vi è una sezione all'interno delle pagine Web di avviso automatico che può essere personalizzata dai clienti attraverso ClientNet.

4. Reporting

5.1 Il reporting relativo all'efficacia di Web v2 Protect viene fornito su ClientNet.

5.2 Per abilitare il reporting per Utente o per gruppo, il Cliente dovrà installare l'applicazione software rilevante (il "Proxy Sito Client"), seguendo le linee guida per l'installazione. L'uso del Proxy Sito Client è soggetto al Contratto di Licenza per Utente Finale fornito con il Proxy Sito Client.

5.3 Il Cliente riconosce che i dati di reporting dettagliati di ClientNet vengono memorizzati solo per un periodo massimo di quaranta (40) giorni e che non saranno disponibili al Cliente dopo tale periodo. I dati riassuntivi di ClientNet sono disponibili per un periodo di dodici (12) mesi.

5.4 Il Cliente può richiedere un periodo di reporting più lungo per il rapporto dettagliato ClientNet, fino a un massimo di sei (6) mesi, sottoscrivendo al Trattenimento dei Dati Superiore WSS.

6. Termini e Condizioni generali

6.1. NESSUN SOFTWARE DI SCANSIONE È IN GRADO DI GARANTIRE UN TASSO DI RILEVAMENTO DEL 100% E, DI CONSEGUENZA, SYMANTEC NON ACCETTA ALCUNA RESPONSABILITÀ PER DANNI O PERDITE DERIVANTI DIRETTAMENTE O INDIRETTAMENTE DA QUALUNQUE MANCATO RILEVAMENTO DI VIRUS, CODICI NOCIVI, SPYWARE O ADWARE DA PARTE DI Web v2 Protect.

6.2. Symantec sottolinea che la configurazione di Web v2 Protect è completamente sotto il controllo del Cliente. Web v2 Protect deve essere usato esclusivamente per consentire al Cliente di implementare i previgenti adeguati termini d'uso per i computer del Cliente (o suo equivalente). In alcuni paesi, potrebbe essere necessario ottenere il consenso di ciascun singolo dipendente. Symantec consiglia al Cliente di controllare sempre le normative locali prima di attivare Web v2 Protect. Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento di Web v2 Protect.

6.3 Il traffico web del Cliente, quando usa Web v2 Protect, non dovrà essere superiore a trenta megabyte (30 MB) per Utente al giorno (calcolato come media per ciascun Utente nell'Uso Registrato totale del Cliente per Web v2 Protect). Nel caso di superamento di tale limite quotidiano, Symantec si riserva il diritto di:

6.3.1 rifiutare la fornitura o sospendere in tutto o in parte Web v2 Protect immediatamente e fino all'interruzione di tale uso in eccesso; o

6.3.2 richiedere al Cliente di acquistare Utenti aggiuntivi per riflettere l'uso del traffico web reale del Cliente ed emettere fatture aggiuntive e/o apportare modifiche alle fatture successive, a copertura dei costi per l'Uso Registrato superiore su base pro-rata, per la parte rimanente del periodo di fatturazione in vigore.

Appendice 7 - Servizio Symantec MessageLabs Web v2 URL.cloud

1. Panoramica

1.1. Una volta eseguiti i cambiamenti rilevanti alla configurazione, le richieste di pagine Web e di allegati vengono instradate elettronicamente attraverso il Servizio Symantec MessageLabs Web v2 URL.cloud ("Web v2 URL") e vengono esaminate digitalmente.

2. Descrizione del Servizio

2.1. Le richieste esterne HTTP e FTP-su-HTTP del Cliente, compresi tutti gli allegati, le macro o i file eseguibili, sono indirizzate attraverso Web v2 URL.

3. Configurazione

3.1. Le impostazioni di configurazione necessarie per indirizzare questo traffico esterno attraverso Web v2 URL vengono eseguite e manutenute dal Cliente, e dipendono dall'infrastruttura tecnica del Cliente. Il Cliente deve accertare che il traffico interno HTTP/FTP-su-HTTP (ad es., all'Intranet aziendale) non sia inviato attraverso Web v2 URL. Laddove il Cliente abbia servizi Internet che richiedano una connessione diretta piuttosto che tramite proxy, è responsabilità del Cliente apportare le modifiche necessarie alla propria infrastruttura, per facilitare tale processo.

3.2. L'accesso a Web v2 URL è limitato attraverso Scanning IP (ad es., l'indirizzo/gli indirizzi IP dai quali il traffico web del Cliente ha origine). Gli Scanning IP sono usati anche per identificare il Cliente e per selezionare in modo dinamico le impostazioni specifiche del Cliente.

3.3. Il Cliente è in grado di configurare Web v2 URL per creare le regole della politica di accesso limitato attraverso ClientNet (in base sia a categorie che a tipi di contenuto) e di utilizzarle in momenti specifici con Utenti specifici o gruppi specifici, usando il Proxy Sito Client descritto nella Clausola 5.1.

3.4. IL CLIENTE RICONOSCE CHE Web v2 URL SARÀ FORNITO CON LE IMPOSTAZIONI PREDEFINITE DI SYMANTEC APPLICATE DALL'INIZIO E CHE È ESCLUSIVA RESPONSABILITÀ DEL CLIENTE CONFIGURARE Web v2 URL ATTRAVERSO CLIENTNET SECONDO LE PROPRIE ESIGENZE. Le impostazioni predefinite comprendono una funzione di "Blocco e Registrazione " per le seguenti Categorie URL:

3.4.1 Contenuto per adulti / sessualmente esplicito; e
3.4.2 Spyware; e
3.4.3 URL di Spam; e
3.4.4 Attività illegali.

3.5 Il Supporto Utente in Roaming è una caratteristica opzionale che estende il Servizio Web v2 URL agli Utenti che non si trovano all'interno della rete aziendale (ad es., ad un Utente che lavori da casa). Il Cliente deve installare un file PAC nel PC dell'Utente, in modo che l'Utente venga indirizzato al portale web di Symantec, quando il browser viene avviato. Per accedere al portale web, l'Utente deve inserire password e nome utente. Il Cliente può scaricare un modello di file PAC da ClientNet e modificarlo.

4. Avvisi

4.1. Se un Utente richiede una pagina Web o un allegato, laddove si applichi la politica di restrizione dell'accesso, l'accesso a tale pagina Web o allegato viene negato e l'Utente visualizzerà una pagina Web di avviso automatico. In rari casi, e qualora uno o più elementi del contenuto richiesto siano bloccati, potrebbe non essere possibile visualizzare la pagina Web di avviso e la pagina di avviso può sostituire il contenuto dell'articolo richiesto, ma l'accesso alla pagina rilevante sarà ancora negato.

4.2. Vi è una sezione all'interno delle pagine Web di avviso automatico che può essere personalizzata dai clienti attraverso ClientNet.

5. Reporting

5.1. Il reporting sui risultati delle regole della politica di accesso limitato di un Cliente, creato in conformità con la precedente Clausola 3.3, viene fornito attraverso ClientNet.

5.2 Per consentire un'amministrazione e reporting per Utente o per gruppo, il Cliente dovrà installare l'applicazione software rilevante (il "Proxy Sito Client") in conformità con le linee guida per l'installazione. L'uso del Proxy Sito Client è soggetto al Contratto di Licenza Utente Finale fornito con il Proxy Sito Cliente.

5.3 Il Cliente riconosce che i dati di reporting dettagliati di ClientNet vengono memorizzati da Symantec solo per un periodo massimo di quaranta (40) giorni e non saranno disponibili al Cliente alla scadenza di tale periodo. I dati riassuntivi di ClientNet sono disponibili per un periodo di dodici (12) mesi.

5.4 Il Cliente può richiedere un periodo di reporting più lungo per il rapporto dettagliato ClientNet, fino a un massimo di sei (6) mesi, sottoscrivendo al Trattenimento dei Dati Superiore WSS.

6. Termini e Condizioni generali

6.1. NESSUN SOFTWARE DI SCANSIONE È IN GRADO DI GARANTIRE UN TASSO DI RILEVAMENTO DEL 100% E, DI CONSEGUENZA, SYMANTEC NON ACCETTA ALCUNA RESPONSABILITÀ PER DANNI O PERDITE DERIVANTI DIRETTAMENTE O INDIRETTAMENTE DA QUALUNQUE MANCATO RILEVAMENTO DI URL BLOCCATI O CONTENUTO BLOCCATO DA PARTE DI Web v2 URL.

6.2. Symantec sottolinea che la configurazione di Web v2 URL è completamente sotto il controllo del Cliente. Web v2 URL deve essere usato esclusivamente per consentire al Cliente di implementare gli adeguati termini d'uso per i computer del Cliente (o suo equivalente) previgenti .In alcuni paese, potrebbe essere necessario ottenere il consenso di ciascun singolo dipendente. Symantec consiglia al Cliente di controllare sempre le normative locali prima di attivare Web v2 URL. Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento di Web v2 URL.

6.3 Il traffico web del Cliente durante l'uso di Web v2 URL non dovrà superare i trenta megabyte (30 MB) per Utente al giorno (calcolato come media per ciascun Utente per l'Uso Registrato totale del Cliente per WebURL v2). Nel caso di superamento di tale limite quotidiano, Symantec si riserva il diritto di:

6.3.1 rifiutare la fornitura o sospendere in tutto o in parte Web v2 URL immediatamente e fino all'interruzione di tale eccesso; o
6.3.2 richiedere al Cliente di acquistare Utenti aggiuntivi per riflettere l'uso di traffico web reale del Cliente ed emettere fatture aggiuntive e/o apportare modifiche alle fatture successive, a copertura dei costi per l'Uso Registrato superiore, su base pro-rata, per la parte rimanente del periodo di fatturazione in vigore.

Appendice 8 - Servizio Symantec MessageLabs Email Archiving.cloud (P)

1. Panoramica del Servizio

1.1 I Servizi Symantec MessageLabs Email Archiving.cloud (P), Symantec MessageLabs Email Archiving.cloud Lite (P) e Symantec MessageLabs Email Archiving.cloud Premium (P) (collettivamente, il "Servizio di Archiviazione (P)") di Symantec sono servizi di archiviazione ibridi per l'archiviazione e il ripristino di E-mail.

1.2 Per i Clienti con *500 Utenti o meno*, il *Servizio Symantec MessageLabs Email Archiving.cloud Lite (P)* comprende:

(i) caratteristiche standard, come descritto nella Clausola 3 riportata di seguito;

(ii) periodo di trattenimento di 3 anni;

(iii) memorizzazione massima di 3 GB per Utente (calcolata come media per ciascun Utente sulla base del numero totale di Utenti).

Per i Clienti con *più di 500 Utenti*, il *Servizio Symantec MessageLabs Email Archiving.cloud Lite (P)* comprende:

(i) caratteristiche standard, come descritto nella Clausola 3 riportata di seguito;

(ii) periodo di trattenimento di 1 anno;

(iii) memorizzazione massima di 1,5 GB per Utente (calcolata come media per ciascun Utente sulla base del numero totale di Utenti).

1.3 Per i Clienti con *500 Utenti o meno*, il *Servizio Symantec MessageLabs Email Archiving.cloud (P) Service* comprende:

(i) caratteristiche standard, come descritto nella Clausola 3 riportata di seguito;

(ii) periodo di trattenimento di 10 anni;

(iii) memorizzazione massima di 10 GB per Utente (calcolata come media per ciascun Utente sulla base del numero totale di Utenti).

Per i Clienti con *più di 500 Utenti*, il *Servizio Symantec MessageLabs Email Archiving.cloud (P)* comprende:

(i) caratteristiche standard, come descritto nella Clausola 3 riportata di seguito;

(ii) periodo di trattenimento illimitato;

(iii) memorizzazione massima di 6 GB per Utente (calcolata come media per ciascun Utente sulla base del numero totale di Utenti).

1.4 Per i Clienti con *500 Utenti o meno*, il *Servizio Symantec MessageLabs Email Archiving.cloud Premium (P)* comprende:

(i) caratteristiche standard, come descritto nella Clausola 3 riportata di seguito;

(ii) caratteristiche premium come descritte nella Clausola 4 riportata di seguito;

(iii) periodo di trattenimento di 10 anni;

(iv) memorizzazione massima di 10 GB per Utente (calcolata come media per ciascun Utente sulla base del numero totale di Utenti).

Per i Clienti con *più di 500 Utenti*, il *Servizio Symantec MessageLabs Email Archiving.cloud Premium (P)* comprende:

(i) caratteristiche standard, come descritto nella Clausola 3 riportata di seguito;

(ii) caratteristiche premium come descritte nella Clausola 4 riportata di seguito;

(iii) periodo di trattenimento illimitato;

(iv) memorizzazione massima di 6 GB per Utente (calcolata come media per ciascun Utente sulla base del numero totale di Utenti).

1.5 Il Cliente deve configurare le caratteristiche del diario di Scambio, per depositare una copia delle E-mail interne ed esterne in una casella di posta locale sul server di Scambio. L'applicazione/Le applicazioni che si trovano dietro al firewall, all'interno della rete aziendale del Cliente (la/le "Applicazione/i di Archiviazione E-mail"), può/possono essere usata/e per ritirare dati da questa casella di posta per l'invio al Servizio di Archiviazione (P). Le E-mail vengono cancellate dalla casella di posta del diario soltanto quando viene confermata la memorizzazione nel Servizio di Archiviazione (P).

1.6 Symantec monitorerà l'uso del Servizio di Archiviazione (P) da parte del Cliente e, nel caso in cui la memorizzazione reale fosse superiore alla quantità di spazio di archiviazione acquistato, il Cliente dovrà acquistare un blocco aggiuntivo di spazio per archiviazione ai prezzi applicati da Symantec in quel momento. Symantec emetterà ulteriori fatture e/o apporterà modifiche alle fatture successive, a copertura dei costi per l'aumento della memorizzazione su base pro-rata, per la parte rimanente del periodo di fatturazione attuale.

1.7 Il Cliente riconosce e acconsente che una volta archiviata, l'E-mail non può essere cancellata fino alla scadenza del periodo di trattenimento assegnato. Ciò significa che non è possibile cancellare le E-mail singole in modo selettivo.

1.8 Il Cliente riconosce e concorda che Symantec non è in grado di agire come esecutore del download di terzi. Nel caso in cui il Cliente debba nominare un esecutore di download di terzi per scopi di conformità, Symantec farà quanto ragionevolmente possibile per facilitare un accordo diretto e indipendente fra il Cliente e il fornitore di servizi terzo di Symantec pertale scopo. Il Cliente riconosce che il fornitore di servizi terzo può imporre costi per tale servizio.

2. Attivazione del Servizio

2.1 Il Cliente deve completare il modulo di fornitura di Symantec in modo accurato.

2.2 Il Cliente deve acquistare l'Applicazione/le Applicazioni di Archiviazione E-mail per ricevere il Servizio di Archiviazione (P). L'Applicazione/Le Applicazioni di Archiviazione E-mail acquistata/e (e la documentazione allegata) sarà/saranno spedita/e al Cliente per l'installazione e la configurazione. Il Cliente è responsabile di tutti i costi relativi a spedizione, oneri, assicurazione e imposte sull'Applicazione di Archiviazione E-mail.

2.3 Symantec contatterà il Cliente per programmare una chiamata iniziale con il client.

2.4 Le azioni delineate nel Documento di Installazione Client di Symantec devono essere completate dal Cliente prima della chiamata iniziale con il client e comprendono, fra le altre cose:

2.4.1 Installazione di un nuovo account utente per la directory attiva;

2.4.2 Installazione di gruppi di directory attive aggiuntive;

2.4.3 Aggiunta di utenti ai gruppi di Scambio;

2.4.4 Configurazione dei Firewall (se necessaria);

2.4.5 Abilitazione del Diario di Scambio Microsoft (non prima di 48 ore dall'installazione dell'Applicazione di Archiviazione E-mail);

2.4.6 Installazione dell'Applicazione di Archiviazione E-mail (in rack e in avvio);

2.4.7 Accertarsi che tutte le caselle di posta necessarie per l'archiviazione siano "abilitate per la posta";

2.4.8 Configurazione dell'accesso remoto di Symantec.

Il Cliente può chiamare un Manager del Servizio Clienti Symantec qualora abbia bisogno di assistenza in relazione alle azioni precedentemente elencate.

2.5 La chiamata iniziale con il client deve essere eseguita attraverso WebEx. Nel corso di questa chiamata, le parti dovranno:

2.5.1 Verificare che tutte le azioni nel Documento di Installazione Client siano state completate;

2.5.2 Installare il software di archiviazione e altri software usando il Documento delle Procedure di Installazione di Archiviazione di Symantec;

2.5.3 Revisionare l'installazione della directory attiva;

2.5.4 Attivare il servizio;

2.5.5 Verificare l'accessibilità all'interfaccia utente;

2.5.6 Verificare l'archiviazione (site-to-site);

2.5.7 Generare copie delle chiavi di crittografia, in conformità con il Documento delle Procedure di Backup Chiave di Symantec.

2.6 Una sessione di formazione è disponibile durante o in seguito alla chiamata iniziale con il client, e comprende sessioni focalizzate su: (i) tecnologia informatica (IT), (ii) Politica, (iii) Supervisione, (iv) Utente finale.

2.7 Una chiamata post-revisione viene eseguita all'incirca una (1) settimana dopo l'attivazione. In seguito al completamento soddisfacente della chiamata post-revisione, il Cliente può seguire le procedure di supporto standard, nel caso in cui fosse necessaria ulteriore assistenza.

3. Caratteristiche standard

3.1 *Determinazione dell'indirizzo ed Espansione della Lista/del Gruppo di Distribuzione*. Tutti gli indirizzi e-mail identificati da Exchange come indirizzi interni saranno così definiti nella casella di posta dell'Utente corrispondente. Per ciascuna lista di distribuzione indicata come destinataria del messaggio, una lista dei membri al momento attivi sarà indicata come metadato aggiuntivo sul messaggio E-mail.

3.2 *Indice a testo pieno*. L'Applicazione di Archiviazione E-mail può estrarre contenuto di testo da diversi tipi di allegati e campi comuni nel messaggio, per supportare la creazione di un indice a testo pieno e per la ricerca all'interno del Servizio di Archiviazione (P).

3.3 *Crittografia.* I dati relativi al contenuto del messaggio e i dati dell'indice (ad eccezione di campi come date e altre informazioni non di identificazione personale) sono crittografati usando tecnologie di crittografia standard dell'industria basate sulla chiave di crittografia specifica per cliente in possesso esclusivo del Cliente. Il Cliente ha l'esclusivo possesso di tutte le password, le chiavi di crittografia, e le impostazioni di configurazione, e di conseguenza il Cliente deve accertarsi che siano manutenute con sicurezza e a garanzia o in altra posizione adeguata. Symantec non accetta responsabilità per la perdita di nessuna password, chiave di crittografia o impostazione di configurazione. Il Cliente comprende che la perdita di password e di chiavi di crittografia renderà l'archivio inaccessibile.

3.4 *Politiche di conservazione*. Il Cliente può definire e aggiornare le politiche di conservazione attraverso l'interfaccia utente. Ciascuna politica di conservazione può tenere conto dei criteri, comprese le parti coinvolte, le parole chiave/frasi nel contenuto e i tipi di file allegati. Quando ciascun messaggio viene archiviato, è valutato rispetto a ciascun insieme di politiche di conservazione attive in quel momento. Se un messaggio corrisponde a più di una politica di conservazione si applica la politica con il periodo di conservazione più lungo. Se

nessuna politica di conservazione specifica corrisponde al messaggio, viene applicata la politica di conservazione predefinita.
3.5 *InfoTag (metadati)*. Il Cliente può definire e aggiornare gli InfoTag attraverso l'interfaccia utente. Ciascun InfoTag può tenere in considerazione criteri, comprese le parti coinvolte, le parole chiave/frasi nel contenuto, il tipo di file allegati. Quando ciascun messaggio viene archiviato, viene valutato rispetto all'insieme attivo di InfoTag e viene segnalato con ciascuno di quelli applicabili.
3.6 *Tracking della politica*. I cambiamenti apportati alle politiche di trattenimento e supervisione sono mantenuti dal sistema in forma inalterabile a scopo di riferimento. Il Cliente può generare un file in formato pdf delle versioni attuali o precedenti delle politiche attraverso l'interfaccia utente.
3.7 *Tracking Utente storico*. Una lista di tutti gli Utenti in possesso di una casella di posta all'interno di Exchange viene inviata al sistema ogni notte, per mantenere una lista aggiornata di tutte le caselle di posta che sono esistite dall'implementazione del Servizio di Archiviazione (P). Queste informazioni possono essere usate per creare politiche ed archivi che facciano riferimento agli Utenti che sono stati cancellati dalla Directory Attiva, e anche per fornire ad altri Utenti l'accesso alle e-mail degli ex dipendenti.
3.8 *Stub degli allegati*. Il Cliente può abilitare la funzionalità che sostituisce il contenuto dell'allegato all'interno del sistema di posta del Cliente ("Dati della casella di posta") con un indicatore alla copia appropriata all'interno dell'archivio. Il Cliente può definire e aggiornare le politiche di stub con diverse regole per ciascun gruppo di caselle di posta, sulla base di età e dimensione del messaggio e sulla base della cartella in cui si trova. Per facilitare il ripristino automatico dell'allegato originale dall'archivio, quando gli Utenti inoltrano la posta, il Cliente può installare il modulo Stub Allegati alla sua Library di Moduli dell'Organizzazione (una cartella pubblica speciale sul server di Scambio). Outlook installerà automaticamente il modulo dal server. Per facilitare l'accesso per il recupero dei documenti al di fuori della rete del Cliente, il Cliente può reinstallare il Proxy Archivio nei server Exchange front-end (OWA). Come impostazione predefinita, solo i Dati della Casella di posta che sono stati archiviati precedentemente saranno soggetti a stub. Il Cliente può abilitare un'opzione di archiviazione di una copia degli allegati non archiviati precedentemente, per facilitare lo stub degli allegati contenuti nella casella di posta. Il Cliente può configurare le politiche di trattenimento per ciascuna casella di posta, per stabilire per quanto tempo gli allegati memorizzati in tal modo debbano essere trattenuti. Se non specificato, la politica di trattenimento predefinita si applicherà a tali articoli. Gli allegati memorizzati tramite questo processo non sono ricercabili all'interno dell'archivio.
3.9 *Accesso dell'Utente Finale*. Il Cliente può scegliere di fornire agli Utenti individuali l'accesso per la ricerca nell'archivio, o all'interno dell'interfaccia utente web, o direttamente all'interno di Outlook.
3.10 *Accesso alla scoperta legale*. Il Cliente può eseguire ricerche sull'intero archivio all'interno dell'interfaccia utente. Il Cliente può creare un "archivio", ovvero un deposito di informazioni per i messaggi rilevanti per una questione particolare. Il Cliente può eseguire l'attività di ricerca all'interno dell'archivio nello stesso modo in cui può eseguire una ricerca nell'archivio attivo.
3.11 *Archivi ad-hoc*. Il Cliente può usare l'interfaccia utente della politica per stabilire e aggiornare gli archivi ad-hoc. L'archivio può basarsi su criteri come le parti coinvolte, le parole chiave/frasi nel contenuto, e i tipi di file allegati. Quando ciascun messaggio viene archiviato, è valutato rispetto all'insieme di archivi attivi in quel momento. Il messaggio viene associato a ciascun archivio a cui corrisponde. Per inserire i dati archiviati esistenti in archivi ad-hoc, il Cliente può eseguire una ricerca per criteri simili, copiare i risultati in una cartella, quindi copiare i contenuti della cartella nell'archivio. Ciascun archivio ad-hoc ha un periodo di trattenimento indefinito: tutti i messaggi in un dato archivio ad-hoc sono trattenuti fino a quando il controllo non viene cancellato.
3.12 *Archivi basati su persone*. Il Cliente può usare l'interfaccia utente della politica, per stabilire e aggiornare archivi basati sulle persone. Ciascun archivio basato sulle persone definisce un insieme di Utenti. Quando un messaggio viene archiviato, se coinvolge una delle persone elencate nel controllo indicato, viene associato a quel controllo. Inoltre, il sistema registra automaticamente le mail esistenti che appartengono agli Utenti che attualmente sono indicati dal controllo e crea una nuova copia dei messaggi in tale controllo. Quando gli Utenti sono eliminati dalla definizione di un archivio basato sulle persone, i messaggi che appartengono esclusivamente a tali Utenti non più elencati saranno automaticamente eliminati dal controllo. I messaggi per gli Utenti attualmente elencati coperti dal controllo sono trattenuti fino al rilascio di tale controllo.
3.13 *Esportazione dei dati*. I messaggi dell'archivio attivo e non, possono essere esportati ai file PST. Il sistema creerà file PST multipli se necessario a causa delle restrizioni delle dimensioni del file.
3.14 *Reporting*. I rapporti relativi alle dimensioni e alla crescita dell'archivio sono a disposizione del Cliente all'interno dell'interfaccia utente e possono essere visualizzati in HTML o esportati come PDF o CSV (solo dati).
3.15 *Traccia di controllo*. Le attività di ricerca, visualizzazione dei messaggi, esportazione, ripristino e supervisione sono soggette a tracking. La traccia di controllo può essere visualizzata quale proprietà di qualunque specifico messaggio. Un visualizzatore della traccia di controllo in tutti i messaggi consente visualizzazioni filtrate basate sul tipo di attività, sulla persona che ha eseguito l'attività e/o sulla data dell'attività.
3.16 *Integrazione con la Directory Attiva.* L'accesso all'archivio è gestito aggiungendo Utenti (o gruppi esistenti di Utenti) a un insieme di gruppi di sicurezza predefiniti all'interno della Directory Attiva. Ciascuno di questi gruppi è composto da un insieme di privilegi associati. Un Utente può eseguire diversi ruoli grazie alla sua appartenenza a diversi di questi gruppi di sicurezza. L'autenticazione viene eseguita direttamente sulla Directory Attiva. Gli Utenti vi accedono inserendo il loro nome utente e password standard della Directory Attiva e gli account disabilitati perdono i diritti di accesso all'archivio. I gruppi della Directory Attiva possono essere indicati con diversi altri aspetti del sistema per facilitarne l'amministrazione di elementi come le politiche. Un processo di sincronizzazione notturna viene usato per registrare i cambiamenti nei membri del gruppo.
3.17 *Gestione della conservazione e dell'eliminazione*. Sulla base delle politiche di conservazione definite dal Cliente all'interno dell'interfaccia utente, il Servizio di Archiviazione (P) suddividerà i messaggi per categoria e assegnerà una data di eliminazione o registrerà il mese in cui il messaggio è stato archiviato per essere trattenuto per un tempo indefinito. Le date di eliminazione programmata si allineano all'inizio di ciascun mese. Quando i messaggi raggiungono la data di eliminazione programmata, l'Utente/gli Utenti autorizzato/i del Cliente possono approvare formalmente l'eliminazione di tutti i messaggi associati a tale data di eliminazione programmata. Per i messaggi archiviati con un periodo di conservazione indefinito, l'Utente/gli Utenti autorizzato/i del Cliente possono approvare formalmente l'eliminazione di tutti i messaggi che sono stati archiviati nel corso di un mese specifico. Il Cliente riconosce e concorda che quando i dati sono destinati all'eliminazione, non possono essere ripristinati in una forma leggibile ad occhio umano da qualunque supporto di memorizzazione (compresi, senza limitazione alcuna, i sistemi di backup).

4. Caratteristiche Premium
Le seguenti caratteristiche sono comprese esclusivamente nel *Servizio Symantec MessageLabs Email Archiving.cloud Premium (P)*:
4.1 *Supervisione.*
4.1.1 *Selezione automatica per la Revisione della Supervisione.* Il Cliente può stabilire e aggiornare le politiche tramite l'interfaccia utente che aggiunge messaggi a una coda di revisione. Ciascuna politica può tenere in considerazione le parti coinvolte, le parole chiave/frasi nel contenuto e i tipi di file. Inoltre, politiche campione casuali possono essere configurate per Utenti specifici.
4.1.2 Revisione della Supervisione. Il Cliente può assegnare i diritti di accesso ai revisori per leggere i messaggi che sono stati aggiunti alla coda di revisione e indicarli come accettabili o meno.
4.2 *Archiviazione Bloomberg*
4.2.1 Il Servizio Symantec MessageLabs Email Archiving.cloud Premium (P) utilizza funzioni di registrazione del Servizio Professionale Bloomberg che registra e-mail e conversazioni fatte con messaggistica istantanea in file XML che vengono pubblicati ogni notte nel sito FTP Bloomberg.
4.2.2 Se il Cliente sottoscrive il Servizio Professionale Bloomberg, l'Applicazione di Archiviazione E-mail può essere usata per recuperare una copia di questi file XML dal sito FTP per la conversione in messaggi formattati HTML e per l'invio all'archivio.
4.2.3 Il formato FIRM è supportato, ma non sono supportati i formati ACCOUNT né l'estratto storico delle registrazioni Bloomberg.
4.2.4 L'integrazione dell'archiviazione Bloomberg non elimina il contenuto dal sito FTP Bloomberg, ma tiene traccia di quali file siano stati elaborati. Poiché Bloomberg elimina il contenuto dal proprio sito FTP regolarmente, e il processo di integrazione di archiviazione di Bloomberg elimina le copie che ha effettuato nelle Applicazioni di Archiviazione E-mail, il Cliente deve accertarsi che l'integrazione di archiviazione stia funzionando regolarmente, in modo che i file non siano cancellati prima che l'integrazione di archiviazione di Bloomberg sia stata in grado di recuperarli ed elaborarli completamente.
4.2.5 Una lista degli identificatori FIRM Bloomberg viene usata per identificare quali utenti indicati nell'XML siano dipendenti interni. L'integrazione dell'archiviazione Bloomberg fornisce un'interfaccia utente di mappatura basata sul web che consente a un amministratore di associare ciascun account utente Bloomberg agli account utenti della Directory Attiva corrispondenti. Quando i file XML vengono elaborati, se un messaggio fa riferimento a un utente interno non ancora presente nella mappatura, l'indirizzo viene aggiunto alla lista di indirizzi non in mappatura e il messaggio non viene elaborato. Quando l'amministratore ha eseguito la mappatura di tali indirizzi, può avviare

la rielaborazione dei messaggi associati. Gli indirizzi e-mail aziendali stabiliti sono usati come mittenti/destinatari del messaggio.
4.2.6 Un blocco informativo all'interno del corpo del messaggio fornisce informazioni aggiuntive relativamente agli indirizzi/nomi visualizzati delle parti del messaggio/della conversazione, comprese le informazioni di account Bloomberg dell'utente.

5. Importazione dei dati acquisiti
5.1 Il Cliente può importare i dati acquisiti nel Servizio di Archiviazione (P), fatto salvo il pagamento di una quota basata sulla quantità di dati da importare. Nel caso in cui la quantità di dati effettivi sia superiore alla quantità di dati da importare acquistata, Symantec si riserva il diritto di applicare a tali dati aggiuntivi i propri prezzi standard di quel momento.
5.2 Nel caso in cui il Cliente decida di usare un software indipendente di terzi per facilitare l'importazione dei dati nell'archivio, il Cliente riconosce e accetta che Symantec non è responsabile di tale software di terzi e che il Cliente lo fa a proprio rischio e a proprie spese.

6. Conclusione del servizio
6.1 Al termine del Servizio di Archiviazione (P), Symantec eliminerà i dati del Cliente dall'archivio. Prima del termine, il Cliente può estrarre i propri dati dall'archivio, oppure può richiedere che una terza parte nominata da Symantec trasferisca i dati archiviati al Cliente in formato file PST conformemente alla Clausola 6.2 di seguito.
6.2 Se il Cliente richiede che una terza parte nominata da Symantec trasferisca i dati al termine:
6.2.1 Il Cliente deve stipulare un accordo diretto con la terza parte nominata. Symantec non farà parte di tale accordo.
6.2.2 Poiché i dati sono archiviati in formato crittografato, il Cliente dovrà fornire alla terza parte una chiave di crittografia per decodificare le e-mail in un formato liberamente accessibile.
6.2.3 Il Cliente sarà responsabile dei costi del trasferimento. I costi saranno pattuiti al momento dell'accordo con la terza parte. I costi dipendono dai seguenti fattori: (i) quantità di dati; (ii) formato/supporto di trasferimento; (iii) costi di configurazione del processo di trasferimento; (iv) tempo e materiali utilizzati per completare il trasferimento.
6.2.4 Symantec si riserva il diritto di addebitare le proprie tariffe in vigore per l'archiviazione se i dati non sono stati esportati ed eliminati dall'archivio alla data di termine effettiva.

7. Termini e Condizioni del Servizio
7.1 Symantec può, a sua esclusiva discrezione, porre termine al Servizio di Archiviazione (P) immediatamente e senza notifica, e intraprendere le azioni difensive che ritiene necessarie:
7.1.1 Se indicato da un tribunale o da un'autorità competente;
7.1.2 In caso di attacco del Servizio di Archiviazione (P) o della rete;
7.1.3 Nel caso in cui il Cliente, o qualunque dei suoi Utenti, violi la Politica di Uso Accettabile della Clausola 7.3 riportata di seguito.
7.2 Il Cliente sarà responsabile di assicurare che esso stesso e tutti i suoi Utenti siano a conoscenza e si conformino con la Politica d'Uso Accettabile descritta nella Clausola 7.3 riportata di seguito.
7.3 *Politica d'Uso Accettabile*. Gli Utenti non possono, in nessuna circostanza, commettere, o tentare di commettere, o aiutare o istigare a commettere, qualunque azione che possa minacciare il Servizio di Archiviazione (P), sia deliberatamente, che con colpa o a titolo di responsabilità oggettiva. Questo comprende, fra le altre cose:
7.3.1 Qualunque tentativo di arrestare un service host o una rete;
7.3.2 Attacchi di tipo "Denial of service" o "flooding" contro un service host o una rete;
7.3.3 Qualunque tentativo di aggirare l'autenticazione di un utente o la sicurezza di un service host o di una rete;
7.3.4 Qualunque uso dissoluto del Servizio di Archiviazione (P);
7.3.5 La creazione, trasmissione, memorizzazione o pubblicazione di qualunque tipo di Virus o programma di corruzione o di dati corrotti;
7.3.6 Qualunque altra azione che possa influire in modo negativo sul Servizio di Archiviazione (P) o il suo funzionamento.
7.5 NESSUN SERVIZIO DI ARCHIVIAZIONE E-MAIL È IN GRADO DI GARANTIRE UN'ACCURATEZZA DEL 100% E DI CONSEGUENZA SYMANTEC NON ACCETTA ALCUNA RESPONSABILITÀ PER DANNI O PERDITE DERIVANTI DIRETTAMENTE O INDIRETTAMENTE DA QUALUNQUE MANCANZA DEL SERVIZIO, AD ECCEZIONE DEI RIMEDI ESPRESSAMENTE INDICATI NEL CONTRATTO DI LIVELLO DEL SERVIZIO.
7.6 Il Cliente riconosce che le e-mail possono contenere informazioni di identificazione personale e che l'archiviazione delle e-mail potrebbe, quindi, implicare l'elaborazione di dati personali. Inoltre, il Cliente riconosce che il Servizio di Archiviazione (P) è un servizio che può essere configurato e che il Cliente è unicamente responsabile per la configurazione del Servizio di Archiviazione (P), in conformità con gli adeguati termini d'uso per i computer del Cliente (o suo equivalente) previgenti e di tutte le leggi o le normative. Qualunque modello fornito da Symantec è per l'uso esclusivo come guida, per consentire al Cliente di creare le sue politiche e altri modelli personalizzati. Di conseguenza, Symantec consiglia al Cliente di controllare sempre le normative locali prima di attivare il Servizio di Archiviazione (P), e di accertarsi che esso stesso, e tutti i suoi dipendenti, siano a conoscenza e si conformino con qualunque responsabilità relativa alla tutela dei dati e alle leggi e/o normative sulla privacy, in relazione all'uso da parte del Cliente del Servizio di Archiviazione (P). In alcuni paesi può essere necessario ottenere il consenso di ciascun dipendente, prima di usare il Servizio di Archiviazione (P). Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento del Servizio di Archiviazione (P) da parte del Cliente. Il Cliente deve tenere presente questo nel corso della configurazione del Servizio di Archiviazione (P).
7.6 Il Cliente deve selezionare la sede del centro dati per l'archiviazione al momento dell'ordine, e i prezzi vengono calcolati in base a tale selezione. SE VIENE SELEZIONATO UN CENTRO ARCHIVIAZIONE DATI NEGLI STATI UNITI D'AMERICA, IL CLIENTE ACCONSENTE A FARE TUTTO QUANTO NECESSARIO PER (I) INFORMARE I SUOI DIPENDENTI, AGENTI E APPALTATORI, NONCHÉ I TERZI CHE USANO IL SISTEMA DI COMUNICAZIONE COPERTO DAL SERVIZIO DI ARCHIVIAZIONE (P), DEL FATTO CHE QUALUNQUE INFORMAZIONE, COMPRESE, SENZA LIMITAZIONI, LE INFORMAZIONI DI IDENTIFICAZIONE PERSONALE DEGLI INDIVIDUI, POSSONO ESSERE ELABORATE NEGLI STATI UNITI D'AMERICA; E (II) DEVE OTTENERE IL CONSENSO DI TALI DIPENDENTI, AGENTI, APPALTATORI E TERZI A TALE ELABORAZIONE, PRIMA DELL'ATTIVAZIONE DEL SERVIZIO DI ARCHIVIAZIONE (P) DA PARTE DEL CLIENTE.
7.7 Il Cliente riconosce e acconsente che (i) i servizi di scansione di Symantec (E-mail AV, E-mail AS, E-mail IC e E-mail CC) non eseguono la scansione di tutte le e-mail che entrano nell'archivio e (ii) i servizi di scansione di Symantec (E-mail AV, E-mail AS, E-mail IC e E-mail CC) non eseguono la scansione delle e-mail che vengono rilasciate dall'archivio per il loro reinserimento nella casella di posta dell'Utente. Di conseguenza, Symantec non può essere ritenuta responsabile di alcun virus, spam, immagini o contenuto inappropriato che tali e-mail reinserite potrebbero contenere, e, inoltre, il Contratto di Livello di Servizio non si applica a tali e-mail ripristinate.

8. Licenza del Software
8.1 I seguenti termini e le seguenti condizioni riguardano il software installato nell'Applicazione di Archiviazione E-mail (il "Software"):
8.1.1 Il Cliente riconosce e concorda che, in qualunque momento, il rapporto esistente fra il Cliente e Symantec è il seguente: Symantec, e/o i suoi fornitori, è/sono proprietario/i del Software. Il presente Contratto garantisce al Cliente una licenza limitata non esclusiva sull'uso del Software, in relazione al Servizio di Archiviazione (P) descritto nella presente Appendice, e non implica la vendita del Software o di qualunque altra proprietà intellettuale. Tutti i diritti non espressamente garantiti dal presente Contratto sono riservati di Symantec e dei suoi fornitori.
8.1.2 Il Cliente può usare una copia del Software con una Applicazione di Archiviazione E-mail. Per gli scopi del presente Contratto, "uso" indica l'esecuzione, il funzionamento, la visualizzazione e l'archiviazione del Software, per la durata della fornitura del Servizio di Archiviazione (P).
8.1.3 Il Software è protetto dalle leggi sui diritti d'autore di Canada e Stati Uniti e dai trattati internazionali. Il Cliente non può noleggiare o dare in leasing il Software o una copia della documentazione di accompagnamento del Software. Il Cliente non può copiare, eseguire reverse-engineering, disassemblare, decompilare, decodificare o tentare di creare il codice sorgente dal Software.
8.1.4 Il Cliente riconosce che una violazione di tali disposizioni porterà ad un danno irreparabile per Symantec e i suoi fornitori e con il presente acconsente che Symantec e/o i suoi fornitori potranno far entrare in vigore direttamente la presente sezione comprese (senza limitazioni) prestazioni specifiche o provvedimento ingiuntivo, oltre a qualunque rimedio cui tale parte avrà diritto secondo i termini di legge o secondo equità.
8.1.5 Tutta la tecnologia, il software, la documentazione e i processi usati dal Symantec per fornire il Servizio di Archiviazione (P) sono di proprietà esclusiva di Symantec o dei suoi fornitori.

Appendice 9 – Servizio Symantec MessageLabs EIM.cloud

1. Descrizione del Servizio

1.1 Il Servizio Symantec MessageLabs EIM.cloud ("EIM") è un servizio gestito che consente il controllo amministrativo, la memorizzazione centralizzata e la gestione di dominio della messaggistica istantanea.

1.2 Ad eccezione delle versioni MSI e Java, il client EIM (il "POD") è installato su ciascuna stazione di lavoro dell'Utente. Tutte le istanze consentono all'Utente di connettersi in modo sicuro alla piattaforma EIM e di usare EIM. Il POD ha la seguente funzionalità:

(a) Condivisione di file;
(b) Conferenza con messaggistica istantanea sicura;
(c) Interoperabilità con le reti pubbliche di messaggistica istantanea (solo con pacchetto CONNECT).

1.3 Lo strumento di amministrazione EIM, una console basata su web, consente agli amministratori definiti di gestire la struttura del loro dominio e la base di utenti.

2. Caratteristiche del Servizio EIM

Caratteristiche del Servizio – Symantec MessageLabs EIM Communicate.cloud ("COMMUNICATE")

(i) Condivisione di file integrata (capacità 100 mb per Utente);
(ii) Soluzione di back-up del desktop;
(iii) Capacità di condividere le informazioni con gli Utenti EIM online o offline;
(iv) Liste di controllo degli accessi;
(v) Comunicazioni sicure, 168-bit 3DES SSL crittografate POD-to-POD;
(vi) Console amministrativa basata su web;
(vii) Interfaccia con opzioni utente completa;
(viii) Rilevamento e tracking della presenza avanzati;
(ix) Supporto per un'ampia varietà di server proxy;
(x) Capacità di HTTP tunnelling;
(xi) Notifiche di avviso per i nuovi file;
(xii) Sistema di file orientati all'oggetto con capacità di ricerca estese.

Caratteristiche del Servizio – Symantec MessageLabs EIM Connect.cloud ("CONNECT")

Si applicano tutte le caratteristiche del pacchetto COMMUNICATE, con l'aggiunta di:

(i) Instant Messenger interoperabile (AOL, MSN, Yahoo!);
(ii) Messaggi SMS (2 messaggi per Utente, o "Quota Utente");
(iii) Capacità di registrazione di Messaggistica Istantanea.

Caratteristiche del Servizio - COLLABORATE

Si applicano tutte le caratteristiche del pacchetto CONNECT, con l'aggiunta di:

(i) Integrazione con WebEx;
(ii) Integrazione con Salesforce.com.

3. Responsabilità per il Numero/Password dell'Account.

3.1 Il Cliente è responsabile di tutti gli usi dei sito web di amministrazione, autorizzati o meno dal Cliente, e il Cliente è responsabile di mantenere la riservatezza del login e delle password dell'account del Cliente. Il Cliente acconsente di notificare a Symantec immediatamente qualunque uso non autorizzato dell'account del Cliente.

4. Responsabilità del contenuto delle comunicazioni nell'Account del Cliente.

4.1 Symantec non rilascia alcuna garanzia espressa o implicita in merito alla fornitura del Servizio EIM, ad eccezione di quanto indicato nel presente Contratto. Symantec non garantisce un tasso di rilevamento del 100% di Virus o Spam e, di conseguenza, Symantec non accetta responsabilità per alcun danno o alcuna perdita derivanti direttamente o indirettamente da qualunque mancato rilevamento di EIM di Virus o Spam o per aver identificato erroneamente un messaggio come Virus o Spam che successivamente non si sia rivelato tale. 4.2 Symantec non rilascia alcuna garanzia implicita o esplicita in merito alla disponibilità di EIM, o all'abilità di EIM di trattenere tutti i dati.

4.3 Symantec sottolinea che la configurazione di EIM è completamente sotto il controllo del Cliente. In alcuni paesi, potrebbe essere necessario ottenere il consenso di ciascun singolo dipendente. Symantec consiglia al Cliente di controllare sempre le normative locali prima di attivare EIM. Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente quale risultato del funzionamento di EIM.

5. Obblighi

5.1 Il Cliente acconsente a quanto segue:

5.1.1 non trasmetterà o archivierà tramite POD o EIM alcun dato, testo, video, audio, software, o altro contenuto illegale;

5.1.2 non trasmetterà o archivierà tramite POD o EIM qualunque contenuto che violi qualsiasi brevetto, marchio commerciale, diritto d'autore, diritto all'immagine o altro diritto di proprietà intellettuale;

5.1.3 non trasmetterà o archivierà alcun contenuto che violi qualunque legge locale, statale, nazionale, o internazionale applicabile, che potrebbe comportare responsabilità civile o penale;

5.1.4 non trasmetterà o archivierà alcun contenuto promozionale non richiesto, materiale pubblicitario, Spam, "spim", catene di S. Antonio, o altro materiale del genere;

5.1.5 non userà POD o EIM per trasmettere o visualizzare pubblicamente contenuti per scopi diversi dagli scopi di comunicazione della società;

5.1.6 non userà POD o EIM per trasmettere intenzionalmente contenuto comprendente un Virus, worm, cancelbot, time bomb, cavallo di troia, sniffer, o altro codice programmato per acquisire informazioni sugli altri utenti o per interrompere la funzionalità o la disponibilità di qualunque programma informatico, database, EIM o di qualsiasi altro host di Internet; o

5.1.7 non maschererà l'identità dell'Utente POD tramite spoofing, falsificando intestazioni, usando relay di terzi, o altrimenti oscurando le origini del contenuto trasmesso, compreso, senza limite alcuno, impersonare un'altra persona o entità.

6. Interoperabilità

6.1 Il Cliente riceverà la funzionalità di interoperabilità come indicato nella precedente Clausola 2 (vedere il pacchetto CONNECT precedentemente descritto). Symantec non fornisce alcuna garanzia relativamente alla capacità di EIM di interoperare con qualunque fornitore IM, compresi, fra gli altri, AOL, MSN e Yahoo!.

7. Memorizzazione di Dati solo USA

7.1 SI RICHIAMA L'ATTENZIONE SUL FATTO CHE TUTTI I MESSAGGI SARANNO MEMORIZZATI NEGLI STATI UNITI E CHE SYMANTEC NON ACCETTA ALCUNA RESPONSABILITÀ PER QUALUNQUE VIOLAZIONE DELLE LEGGI O DELLE NORMATIVE APPLICABILI. IL CLIENTE RICONOSCE CHE LA CONFIGURAZIONE E L'USO DI EIM È A SUO COMPLETO CONTROLLO E DISCREZIONE. Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento di EIM. Il Cliente deve tenere presente questo quando esegue la configurazione di EIM.

8. Registrazione e conformità

8.1 Il Cliente può scegliere di registrare i messaggi istantanei elaborati dal Servizio EIM, soggetto al pagamento delle tariffe corrispondenti per la funzionalità di registrazione.

8.2 Symantec invia i file di registro al Cliente con frequenza giornaliera in modo che il Cliente abbia la possibilità di memorizzare tali registri su un archivio compatibile.

8.3 Symantec conserva i registri per un periodo di tre (3) anni, dopodiché vengono eliminati in modo definitivo. Il rappresentante autorizzato del Cliente può richiedere per iscritto (i) una copia di tali registri o (ii) l'eliminazione di tali registri, in qualsiasi momento prima della scadenza del periodo di conservazione di tre (3) anni.

8.4 Il Cliente è informato che la console di amministrazione permette di disattivare in qualsiasi momento la registrazione per gruppo o sottogruppo e quindi i registri potrebbero non fornire una registrazione completa dell'utilizzo del Servizio EIM.

8.5 Symantec può comunicare per iscritto con preavviso di sei (6) mesi l'intenzione di cessare l'erogazione e il supporto del Servizio EIM. Alla scadenza di tale periodo di preavviso, il Servizio EIM cesserà.

8.6 Alla cessazione del Servizio EIM, il Cliente può richiedere la restituzione o l'eliminazione dei propri registri. Se il Cliente non indica la sua preferenza entro novanta (90) giorni dalla cessazione, Symantec eliminerà i registri in modo definitivo.

8.7 Il Cliente riconosce e accetta che ai fini delle normative SEC, Symantec non può agire in nessun caso come soggetto terzo per il download.

9. Licenza del software

9.1 Concessione della Licenza

Fatti salvi i termini e le condizioni del presente Contratto, Symantec garantisce al Cliente il diritto non esclusivo e non trasferibile di installare e usare il Software per il Servizio EIM, esclusivamente per le operazioni commerciali interne del Cliente ("Software" indica ciascun programma software di Symantec per il Servizio EIM in oggetto formato codice in licenza da Symantec e governato dai termini del Contratto, comprese, senza limitazioni, nuove emissioni o nuovi aggiornamenti rilasciati in base al presente). Tutti i diritti di proprietà intellettuale nel Software sono e rimarranno di proprietà di Symantec (e/o dei suoi fornitori). Il Software viene fornito in licenza da Symantec, non venduto. Il Cliente riconosce che il Software e tutte le relative

informazioni, compresi, senza limitazione alcuna, gli Aggiornamenti, sono di proprietà di Symantec e dei suoi fornitori. Il Cliente sarà pienamente responsabile per la conformità di ciascun Utente Finale con i termini del Contratto, o della violazione degli stessi. Il Cliente notificherà immediatamente a Symantec qualunque uso non autorizzato o violazione dei termini della presente licenza.

9.2. Restrizioni relative a copie e uso

Il Cliente può scaricare e installare il Software alle seguenti condizioni:

9.2.1. Il Cliente non può scaricare o installare il Software su un numero di licenze per Utente Finale superiore a quello delle licenze ottenute dal Cliente stesso ("Utente Finale" indica il computer fisico su cui viene installato il software).

9.2.2. Il Cliente può copiare il Software, come ragionevolmente necessario, per scopi di backup, archiviazione o recupero in seguito a guasto. La Documentazione Stampata può essere riprodotta dal Cliente esclusivamente per uso interno ("Documentazione" indica le guide utente e/o i manuali per il funzionamento del Software di Symantec, allegati al Software scaricato).

9.2.3 Il Cliente non può, né può consentire a terzi di: (i) decompilare, disassemblare, o eseguire reverse engineering del Software, ad eccezione di quanto espressamente consentito dalla legge in vigore, senza il previo consenso scritto di Symantec; (ii) rimuovere qualunque notifica di identificazione del prodotto o dei diritti di autore; (iii) dare in leasing o a prestito il Software o in multiproprietà o per uso da parte di un'agenzia di servizio; (iv) modificare la traduzione, adattare o creare lavori derivati del Software, o (v) altrimenti usare o copiare il Software, ad eccezione di quanto espressamente indicato nel presente.

9.3. Trasferimento dei diritti

Il Cliente non può trasferire, assegnare o delegare la licenza del software derivante dal presente Contratto senza il previo consenso scritto di Symantec. Qualunque trasferimento, assegnazione o delega di tale tipo, in violazione di quanto precedentemente esposto, sarà nullo.

9.4. Garanzia limitata e rinuncia

9.4.1 Symantec garantisce che, al momento del download, il Software sarà conforme in tutti gli aspetti materiali all'attuale Documentazione Symantec.

9.4.2 La garanzia precedentemente indicata non si applicherà nel caso in cui: (i) il Software non viene usato in conformità con il presente Contratto o la Documentazione; (ii) il Software, o parte dello stesso, è stato modificato da qualunque soggetto diverso da Symantec; o (iii) un malfunzionamento del Software è stato causato da apparecchiatura del Cliente o da software di terzi.

9.4.3 SYMANTEC NON GARANTISCE CHE IL FUNZIONAMENTO DEL SOFTWARE SARÀ SENZA INTERRUZIONI O PRIVO DI ERRORI. SYMANTEC NEGA E DISCONOSCE ESPRESSAMENTE OGNI GENERE DI GARANZIE DI QUALUNQUE TIPO, SIA ESPRESSE, CHE IMPLICITE CHE ALTRIMENTI, COMPRESE, FRA LE ALTRE, LA GARANZIA DI COMMERCIABILITÀ, DI QUALITÀ SODDISFACENTE O DI ADEGUATEZZA PER UNO SCOPO PARTICOLARE.

9.5. Termine

Al termine del Servizio EIM o del Contratto, tutti i diritti del Cliente di uso del Software, garantiti dal presente, cesseranno immediatamente e il Cliente restituirà prontamente a Symantec, o distruggerà, tutte le copie del Software e della Documentazione.

Appendice 10 – Servizio Symantec MessageLabs Policy Based Encryption.cloud

1. Descrizione del Servizio

1.1 Il Servizio Symantec MessageLabs Policy Based Encryption.cloud ("PBE") fornisce la capacità di inviare e ricevere E-mail crittografate basate sulla politica di sicurezza e-mail del Cliente.

1.2 Per ricevere la PBE, il Cliente deve inoltre sottoscrivere ai seguenti Servizi:

- **Symantec MessageLabs Email Boundary Encryption.cloud ("BE** - Boundary Encryption") come descritto in dettaglio nell'Allegato 2 Appendice 5; e
- **Symantec MessageLabs Email Content Control.cloud ("Email CC")** come descritto in dettaglio nell'Allegato 2 Appendice 4.

1.3 PBE fornisce la seguente funzionalità:

- Capacità di usare E-mail CC per definire le politiche di crittografia in uscita per le E-mail;
- Consegna di E-mail Crittografate alla casella di posta del destinatario esterno;
- Accesso del destinatario alla E-mail crittografata attraverso un portale web sicuro;
- Accesso del destinatario al portale web sicuro per rispondere all'E-mail in formato crittografato.

2. Caratteristiche di PBE

2.1 PBE consente al Cliente di inviare un'E-mail crittografata direttamente nella casella di posta di un destinatario, senza bisogno che il destinatario scarichi il software.

2.2 Il Cliente può configurare il metodo di crittografia, che può essere Push o Pull. Per Symantec MessageLabs Policy Based Encryption.cloud (Z) ("PBE Z"), in base alla regola di E-mail CC, viene scelto Push o Pull. Per Symantec MessageLabs Policy Based Encryption.cloud (E) ("PBE E"), il metodo di crittografia predefinito è Pull ma può essere cambiato in Push dal destinatario scaricando la funzionalità Secure Reader all'interno del portale web sicuro del destinatario.

2.2.1 La variante "PBE Push" del Servizio PBE invia al destinatario una notifica di e-mail con l'E-mail originale salvata all'interno come allegato crittografato. Dopo aver eseguito una registrazione online iniziale, il destinatario è in grado di visualizzare l'E-mail decrittografata offline usando un'applicazione Java sul desktop.

2.2.2 La variante "PBE Pull" del Servizio invia al destinatario una notifica per e-mail. Il destinatario è in grado di visualizzare l'E-mail decrittografata online attraverso una sessione SSL sicura nel proprio browser, quando esegue il login in un portale web sicuro e inserisce la password.

2.3 PBE, inoltre, consente al destinatario di accedere a un portale web sicuro e di rispondere a un'E-mail crittografata in formato crittografato.

2.4 Il Cliente può personalizzare il portale usato dai destinatari per leggere le E-mail crittografate (ad es., inserendo il logo e i numeri di supporto del Cliente).

2.5 Il destinatario di un'E-mail crittografata può inoltre inviare una nuova E-mail a qualunque Utente PBE del Cliente.

2.6 Se il Cliente sottoscrive a PBE E, è disponibile un Plug-In di Outlook di terzi che aggiunge un' icona "crittografia" alla barra degli strumenti di Outlook del destinatario. Il Cliente riconosce e accetta che Symantec non è responsabile di tale software di terzi.

2.7 Se il Cliente sottoscrive a PBE E, sono disponibili le seguenti caratteristiche aggiuntive:

a) un destinatario può scegliere la lingua del portale web sicuro del destinatario e le e-mail di notifica da una lista di lingue supportate;

b) i destinatari possono eseguire il login nei propri account senza aprire un messaggio specifico, anche se non hanno messaggi attivi;

c) i destinatari possono visualizzare tutti i messaggi precedenti (che non sono stati cancellati in modo permanente) nella loro casella di posta, compresi i messaggi inviati;

d) se si usa il metodo Pull, un messaggio composto nel portale web può avere destinatari multipli, a condizione che tali destinatari condividano il dominio dal quale l'Utente ha ricevuto precedentemente un'e-mail sicura;

e) se si usa il metodo Push, i destinatari possono rispondere a qualunque indirizzo e-mail dello stesso dominio;

f) notifiche iniziali ai nuovi Utenti sono disponibili in più di una lingua;

g) è possibile usare un certificato/chiave di terzi per crittografare un'E-mail in uscita, usando la chiave pubblica del destinatario, e decrittografare un'E-mail in entrata usando la chiave privata del destinatario, anziché i certificati/chiavi predefiniti generati dal Servizio PBE.

3. Fornitura, fatturazione e richieste di cambiamenti

3.1. Symantec inizierà l'addebito di PBE a partire dalla data in cui Symantec verifica che la rete del Cliente è tecnicamente in grado di supportare PBE ("Data di approvazione tecnica").

3.2 La Clausola 5.2 del Allegato 1 non verrà applicata a PBE. L'obiettivo di Symantec sarà di soddisfare gli ordini PBE e le richieste di modifica PBE entro 4 settimane dalla Data di approvazione tecnica, a condizione che il Cliente abbia soddisfatto tutti i requisiti preliminari.

3.3 Il Cliente acconsente a fornire tutte le risorse, le informazioni e le autorizzazioni necessarie come richiesto, e ad attivare o correggere i servizi mail DNS per la connettività alla PBE.

3.4 Il Cliente può modificare la personalizzazione del portale fino a un massimo di due volte all'anno.

4. Configurazione

4.1 Il Cliente è responsabile di implementare la configurazione di PBE secondo le necessità del Cliente. Il Cliente configura PBE attraverso ClientNet, selezionando le opzioni disponibili nel Servizio E-mail CC.

4.2 Symantec sottolinea che la configurazione di PBE è completamente sotto il controllo del Cliente e che l'accuratezza di tale configurazione determinerà l'accuratezza di PBE. Symantec non accetta, quindi, alcuna responsabilità per danni o perdite derivanti direttamente o indirettamente da un mancato adempimento da parte di PBE degli obblighi di crittografia del Cliente

5. Parametri di Servizio

5.1 A PBE si applicano le seguenti limitazioni:

5.1.1 Il numero di E-mail sicure che il Cliente può inviare in un mese usando PBE Z non può superare di trecento (300) volte l'Uso Registrato di PBE. Il numero di E-mail sicure che il Cliente può inviare in un mese usando PBE E non può superare di quattrocentottanta (480) volte l'Uso Registrato di PBE. Quando si invia un'E-mail a destinatari multipli, ciascun indirizzo unico sarà conteggiato come E-mail sicura. Nel caso in cui il Cliente superi il numero di E-mail sicure consentite in un mese, Symantec incrementerà l'Uso Registrato di conseguenza. Laddove Symantec incrementi l'Uso Registrato, Symantec potrà a sua discrezione esclusiva emettere fatture aggiuntive e/o apportare cambiamenti a fatture successive, a copertura dei prezzi per l'Uso Registrato superiore su base pro-rata, per la parte rimanente del periodo di fatturazione attuale.

5.1.2 Le E-mail instradate attraverso PBE Z sono limitate a una dimensione massima di cinquanta megabyte (50 MB) per E-mail, una volta compresse. Le E-mail instradate attraverso PBE E sono limitate a una dimensione massima di cinquanta megabyte (50 MB) per E-mail post-crittografia.

5.1.3 Il livello di servizio Latenza E-mail nel Contratto Livello di Servizio non si applica a PBE.

5.1.4 Il numero minimo di Utenti per PBE Z è 50 Utenti. Gli ordini iniziali e successivi di PBE Z possono essere passati per blocchi minimi di 50 Utenti o con incrementi di 10 Utenti per gli ordini superiori a 50 Utenti.

5.1.4 **PBE FUNZIONA ESCLUSIVAMENTE QUANDO USATO INSIEME AI SERVIZI BE E E-MAIL CC, E NON PUÒ FUNZIONARE COME SERVIZIO INDIPENDENTE. CIASCUN UTENTE PBE INDIVIDUALE DEVE ESSERE UN UTENTE E-MAIL CC.**

6. Termini e Condizioni

6.1 IL CLIENTE RICONOSCE E ACCETTA CHE L'USO DI PBE È COMPLETAMENTE SOTTO IL SUO CONTROLLO E DISCREZIONE. PBE deve essere usato esclusivamente per consentire al Cliente di implementare i previgenti ed adeguati termini d'uso per i computer del Cliente (o suo equivalente). L'utilizzo di servizi di crittografia in alcuni paesi può essere soggetto a normative. Si consiglia al Cliente di controllare sempre le normative rilevanti prima di attivare PBE. Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento di PBE.

Appendice 11 - Symantec Email Continuity.cloud ("EC")

1. Panoramica di EC

1.1 EC è un sistema di messaggi in stand-by per gli ambienti Microsoft Exchange e Lotus Notes. EC sincronizza il sistema chiave e le informazioni Utente comprese, fra le altre, la directory E-mail e i contatti personali degli Utenti individuali. Il Cliente può inoltre configurare EC a supporto dei dispositivi BlackBerry®, attraverso l'inoltro wireless e usando il Client Web BlackBerry® o il Servizio Internet BlackBerry®, e un'esperienza Outlook integrata per gli Utenti su Outlook 2003 Cached Mode o Outlook 2007 Cached Mode, attraverso l'installazione di Outlook Extension.

1.2. *Versioni supportate*: Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007, Lotus Notes Versione 6, Lotus Notes Versione 7.

1.3 *Versioni supportate per Outlook Extension*: Microsoft Outlook 2003 in Cached Mode; Microsoft Outlook 2007 in Cached Mode.

1.4 Il Cliente è responsabile della fornitura e manutenzione dei componenti hardware e software necessari (come indicato nel modulo di fornitura).

2. Descrizione del Servizio EC

2.1. *Attivazione.* Il Cliente può richiedere l'attivazione di EC telefonicamente alla squadra di supporto Symantec o attraverso il portale dei Servizi di Gestione E-mail ("EMS"). All'attivazione di EC, il Cliente riceverà notifiche via SMS ai numeri di telefono cellulare indicati e agli indirizzi e-mail personali. In quel momento, EC inizierà a ricevere e a selezionare le E-mail in entrata, a filtrarle (in conformità con la Clausola 4.4 riportata di seguito) secondo tutti gli altri Servizi E-mail Symantec al quale il Cliente abbia sottoscritto (ad es., il Servizio E-mail AV), e direzionarli alle caselle di posta dell'Utente appropriato. EC memorizzerà e tratterrà il traffico E-mail ricevuto e inviato nel corso dell'attivazione fino a trenta (30) giorni dopo la disattivazione, per consentire al Cliente di unire tali E-mail nel suo sistema mail primario, se lo desidera.

2.2 *Conservazione.* Il Cliente ha la responsabilità di designare gli Utenti le cui E-mail debbano essere conservate e il periodo di trattenimento specifico per ciascun Utente. Le E-mail conservate saranno cancellate alla prima data fra (a) la scadenza del periodo di conservazione indicato per tale Utente o (b) il termine del servizio EC. Il Cliente deve acquistare spazio sufficiente per la memorizzazione, per soddisfare i requisiti di conservazione, in conformità con la Clausola 5.1 riportata di seguito.

2.3 *Manager Autenticazione.* Il Cliente può estendere le politiche di sicurezza del Cliente per l'autenticazione della Directory Attiva di Microsoft a EC, per consentire agli Utenti di eseguire il login nelle proprie caselle di posta EC usando la loro password di Windows, e di conseguenza eliminando la necessità di avere password EC separate. L'autenticazione di Windows richiede la disponibilità di un controllore di dominio Windows accessibile al Manager Autenticazione al momento dell'attivazione EC, che sia in grado di autenticare gli Utenti che tentano di eseguire il login nelle caselle di posta EC. Versioni supportate: Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007

2.4 Il numero minimo di Utenti di EC che può essere acquistato dal Cliente è il numero superiore fra (a) il numero di Utenti uguale al numero di caselle di posta nell'organizzazione del Cliente in Microsoft Exchange o (b) dieci (10) Utenti.

3. Riservato.

4. Configurazione

4.1 *Attivazione parziale*: Per alcuni sistemi/versioni e-mail (ambienti Microsoft Exchange 2000, 2003 e 2007), EC può essere attivato per sottogruppi dell'ambiente del Cliente (uno o più individui, server e/o sedi), l'"Attivazione Parziale", per gestire periodi di interruzione di e-mail con più localizzazioni.

4.2 *Attivazione*: La sottoscrizione EC consente al Cliente di disporre di ventiquattro (24) attivazioni all'anno, ciascuna per una durata fino a dodici (12) ore consecutive ("Attivazioni Incluse"). (A scopo illustrativo, un'attivazione singola della durata di sei (6) ore conterebbe come una (1) attivazione, e un'attivazione singola della durata di diciannove (19) ore conterebbe come due (2) attivazioni). Nel caso in cui il Cliente abbia usato la sua quota di Attivazioni Incluse, il Cliente potrà acquistare attivazioni aggiuntive (ciascuna della durata massima di dodici (12) ore consecutive) ai prezzi di Symantec in vigore in quel momento.

4.3 Test del Sistema: Il Test di Sistema comprende (a) un (1) test trimestrale di EC per tutti gli Utenti, tale test sarà della durata massima di quattro (4) ore e (b) per gli ambienti Microsoft Exchange 2000, Microsoft Exchange 2003 or Microsoft Exchange 2007, test parziali illimitati fino al dieci percento (10%) degli Utenti. Il Cliente deve programmare tali test con Symantec non meno di sette (7) giorni lavorativi prima della data del test desiderata dal Cliente.

4.4 **IL CLIENTE RICONOSCE E ACCETTA CHE, LADDOVE IL CLIENTE SI TROVI IN STATO ATTIVATO, E IL CLIENTE INVII E-MAIL O RICEVA E-MAIL DA UN'ALTRA ORGANIZZAZIONE, ANCH'ESSA IN STATO ATTIVATO, LE E-MAIL BYPASSERANNO I SERVIZI DI SCANSIONE IN ENTRATA E IN USCITA DI SYMANTEC CHE IL CLIENTE HA SOTTOSCRITTO**.

4.5 Se il Cliente usa i Servizi E-mail AV, E-mail AS, E-mail CC e/o E-mail IC, Symantec è in grado di configurare il direzionamento del failover per le e-mail del Cliente all'ambiente EC all'interno di ClientNet. Questo direzionamento di failover sarà utilizzato quando il servizio EC viene attivato.

4.6 **SE IL CLIENTE NON USA E-MAIL AV, E-MAIL AS, E-MAIL CC O E-MAIL IC, È RESPONSABILITÀ DEL CLIENTE CONFIGURARE E TESTARE IL DIREZIONAMENTO FAILOVER PER LE E-MAIL DEL CLIENTE NELL'AMBIENTE EC. QUESTI FAILOVER DEVONO ESSERE INSTALLATI SECONDO LE ISTRUZIONI DI SYMANTEC NEL CORSO DEL PROCESSO DI FORNITURA E DEVONO ESSERE MANTENUTI SUCCESSIVAMENTE. NEL CASO IN CUI IL CLIENTE NON RIESCA A INSTALLARE O MANTENERE TALI FAILOVER, IL CLIENTE RICONOSCE E ACCETTA CHE LE E-MAIL NON POSSONO ESSERE INSTRADATE A EC.**

5. Opzioni

5.1 *Symantec Email Continuity.cloud Storage Option*.

5.1.1 Il Cliente deve acquistare spazio sufficiente per la memorizzazione a scopo di conservazione.

5.1.2 Se il Cliente sottoscrive ai bundle Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud o Symantec MessageLabs Ultimate Safeguard.cloud, questi bundle comprendono un massimo di 0,7 GB di spazio per nuove e-mail per ciascun Utente all'anno, per il Servizio EC e di Symantec Email Continuity Archive.cloud combinati. Nel caso in cui il Cliente superi lo spazio di memorizzazione, Symantec addebiterà i costi di tale spazio aggiuntivo ai suoi prezzi correnti in quel momento.

5.1.3 Se il Cliente non sottoscrive a uno dei bundle elencati nella Clausola 5.1.2, non viene incluso alcuno spazio di memorizzazione nel prezzo per Utente e il Cliente deve acquistare spazio di archiviazione sufficiente per il Servizio ai prezzi correnti in quel momento di Symantec.

5.1.4 Laddove il Cliente debba acquistare spazio di memorizzazione aggiuntivo, Symantec emetterà fatture aggiuntive e/o apporterà modifiche alle fatture successive, a copertura dei prezzi per l'incremento dell'archiviazione su base pro-rata per la parte rimanente del periodo di fatturazione attuale.

5.2 *Symantec Email Continuity.cloud Wireless Option.*

5.2.1 Se il Cliente sottoscrive il servizio Symantec Email Continuity.cloud Wireless Option, gli amministratori del sistema possono fornire dispositivi BlackBerry® specifici gestiti dai Server Aziendali BlackBerry® RIM (BES). Quando EC viene attivato, i dispositivi BlackBerry® forniti continueranno a inviare e a ricevere E-mail comunicando con EMS, attraverso un canale sicuro definito dal server BES.

5.2.2. Versioni supportate: Microsoft Exchange 2000, Microsoft Exchange 2003 o Microsoft Exchange 2007; BlackBerry® Enterprise Server versione 4.0 (o superiore); BlackBerry® Handheld Devices versione firmware 4.1 (o superiore).

6. Termini e Condizioni EC

6.1 NESSUN SERVIZIO DI CONTINUITÀ E-MAIL PUÒ GARANTIRE UNA SINCRONIZZAZIONE AL 100%, E, DI CONSEGUENZA, SYMANTEC NON PUÒ ACCETTARE ALCUNA RESPONSABILITÀ PER DANNI O PERDITE DERIVANTI DIRETTAMENTE O INDIRETTAMENTE DA UNA MANCATA SINCRONIZZAZIONE DI EC CON I SISTEMI E-MAIL.

6.2 Symantec sottolinea che la configurazione di EC è completamente sotto il controllo del Cliente. Symantec raccomanda al Cliente di disporre di adeguati termini d'uso per i computer del Cliente (o suo equivalente) . In alcuni paesi, potrebbe essere necessario ottenere il consenso di ciascun singolo dipendente. Symantec consiglia al Cliente di controllare sempre le normative locali prima di attivare EC. Symantec non accetta responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento di EC.

7. Licenza Software per EC

7.1 Concessione della licenza

Fatti salvi i termini e le condizioni del presente Contratto, Symantec garantisce al Cliente il diritto non esclusivo e non trasferibile di installare e usare il Software per EC come applicabile esclusivamente per le operazioni commerciali interne del Cliente. ("Software" indica ciascun programma di software di Symantec per EC in formato codice oggetto concesso in licenza da Symantec e governato dai termini del Contratto, compresi, senza limiti, le nuove versioni o gli aggiornamenti indicati nel presente). Tutti i diritti di proprietà intellettuale nel Software sono e rimarranno di proprietà di Symantec (e/o dei suoi fornitori). Il Software viene dato in licenza da Symantec, non viene venduto. Il

Cliente riconosce che il Software e tutte le informazioni correlate, compresi, senza limitazione alcuna, tutti gli aggiornamenti, sono di proprietà di Symantec e dei suoi fornitori. Il Cliente sarà completamente responsabile della conformità di ciascun Utente o della violazione dei termini del presente Contratto. Il Cliente notificherà immediatamente a Symantec qualunque uso non autorizzato o violazione dei termini della presente licenza.

7.2. Restrizioni relative a copie e uso

Il Cliente può scaricare e installare il Software alle seguenti condizioni:

7.2.1. Il Cliente non può scaricare o installare il Software su un numero di licenze superiore a quello di licenze per Utente Finale concesse in licenza al Cliente. ("Utente Finale" indica il computer fisico sul quale il software è installato).

7.2.2. Il Cliente può copiare il Software, come ragionevolmente necessario, per scopi di backup, archiviazione o recupero in seguito a guasto. La Documentazione Stampata può essere riprodotta dal Cliente esclusivamente per uso interno. ("Documentazione" indica le guide utente e/o i manuali per il funzionamento del Software di Symantec compresi con il Software scaricato).

7.2.3 Il Cliente non può, né può consentire a terzi di: (i) decompilare, disassemblare, o eseguire reverse engineering del Software, ad eccezione di quanto espressamente consentito dalla legge in vigore, senza il previo consenso scritto di Symantec; (ii) rimuovere qualunque notifica di identificazione del prodotto o dei diritti di autore; (iii) dare in leasing o a prestito il Software o in multiproprietà o per uso da parte di un'agenzia di servizio; (iv) modificare la traduzione, adattare o creare lavori derivati del Software, o (v) altrimenti usare o copiare il Software, ad eccezione di quanto espressamente indicato nel presente.

7.3. Trasferimento dei diritti

Il Cliente non può trasferire, assegnare o delegare la licenza del software relativa al presente Contratto senza il previo consenso scritto di Symantec. Qualunque trasferimento, assegnazione o delega di tale tipo, in violazione di quanto precedentemente esposto, sarà nullo.

7.4. Garanzia limitata e rinuncia

7.4.1 Symantec garantisce che, al momento del download, il Software sarà conforme, dal punto di vista materiale, alla Documentazione attuale di Symantec.

7.4.2 La garanzia precedente non si applica se: (i) il Software non viene usato in conformità con il presente Contratto o la Documentazione; (ii) il Software, o parte dello stesso, è stato modificato da qualunque soggetto diverso da Symantec; o (iii) un malfunzionamento del Software è stato causato da apparecchiatura del Cliente o da software di terzi.

7.4.3 SYMANTEC NON GARANTISCE CHE IL FUNZIONAMENTO DEL SOFTWARE SARÀ SENZA INTERRUZIONI O SENZA ERRORI. SYMANTEC DISCONOSCE E NEGA ESPRESSAMENTE OGNI GENERE DI GARANZIE DI QUALUNQUE TIPO, SIA ESPRESSE, CHE IMPLICITE CHE ALTRIMENTI, COMPRESE, FRA LE ALTRE, LA GARANZIA DI COMMERCIABILITÀ, DI QUALITÀ SODDISFACENTE O DI ADEGUATEZZA PER UNO SCOPO PARTICOLARE.

7.5. Rescissione

Al momento della rescissione di EC, tutti i diritti del Cliente di usare il Software garantiti nel presente cesseranno immediatamente e il Cliente restituirà tempestivamente a Symantec, o distruggerà, tutte le copie del Software e della Documentazione.

Appendice 12 - Strumento Schemus

1.1 Lo Strumento Schemus è un software che sincronizza i dati fra il server della directory del Cliente e i servizi Symantec sottoscritti dal Cliente.
1.2 Lo Strumento Schemus viene dato in licenza al Cliente da Schemus Limited attraverso un contratto di licenza di utente finale ("EULA di Terzi").
1.3 Il Cliente riconosce e accetta che l'accesso e l'uso dello Strumento Schemus è soggetto all'accettazione e alla conformità da parte del Cliente con i termini e le condizioni dell'EULA di Terzi (una copia dei quali sarà fornita da Symantec su richiesta).
1.4 Lo Strumento Schemus è una tecnologia controllata soggetta alle leggi e normative di importazione ed esportazione applicabili , come più dettagliatamente specificato nelle disposizioni di controllo delle esportazioni della sezione "Clausole generali" del Contratto. **IL CLIENTE RICONOSCE E ACCONSENTE CHE DOVRÀ FIRMARE UNA DICHIARAZIONE DI CONFORMITÀ (UNA COPIA DELLA QUALE È DISPONIBILE PRESSO SYMANTEC SU RICHESTA) (I) PRIMA DEL DOWNLOAD DEL SOFTWARE, (II) PRIMA DELL'EMISSIONE DELLA CHIAVE DI LICENZA E (III) SUCCESSIVAMENTE OGNI ANNO, SE RICHIESTO DA SYMANTEC.**
1.5 Symantec non fornisce ulteriori garanzie (sia espresse che implicite, statutarie o altrimenti) in merito allo Strumento Schemus. In caso di guasto relativo allo Strumento Schemus, Symantec farà tutto quanto ragionevolmente possibile, dal punto di vista commerciale, per aiutare ad individuare la fonte del problema e, laddove applicabile, per inoltrare il problema a Schemus Limited.
1.6 La responsabilità massima di Symantec verso il Cliente, per quanto riguarda lo Strumento Schemus, sarà limitata a una somma uguale all'importo pagato dal Cliente a Symantec per lo Strumento Schemus, o £250 (o €350, laddove il Cliente paghi in Euro), a seconda di quale sia l'importo maggiore.

Appendice 13 - Servizio Symantec MessageLabs Instant Messaging Security.cloud ("IMSS")

1 Panoramica

1.1 Il Cliente deve sincronizzare la sua directory utente con Symantec, al fine di creare una lista di nomi utente della Directory Attiva e nomi utente corrispondenti di messaggistica istantanea (IM) all'interno di ClientNet. Un "Utente Interno" è un utente noto della directory del Cliente e caricato nell'interfaccia amministrativa IMSS. Un "Utente Esterno" è un utente non noto della directory del Cliente e/o non caricato nell'interfaccia amministrativa IMSS.

1.2 Il Cliente deve anche eseguire i cambiamenti di base al firewall per gestire le proprie conversazioni IM attraverso Symantec.

1.3 Una volta che IMSS è stato configurato in conformità con le Clausole 1.1 e 1.2 precedentemente specificate, gli IM che passano da Utenti Interni a Utenti Esterni, e vice versa, sono inviati attraverso IMSS per la scansione da parte di prodotti leader, compreso lo scanner euristico di Symantec, Skeptic™.

1.4 IMSS è in grado di scansionare esclusivamente alcune versioni di client IM pubblici. Symantec pubblicherà una lista di versioni supportate di client IM pubblici su ClientNet. Il Cliente riconosce e accetta che Symantec può aggiornare e modificare tale lista regolarmente senza notifica.

1.5 Se un **IM** in entrata:
1.5.1 sembra contenere un Virus o altro codice nocivo, sarà bloccato;
1.5.2 contiene un URL per una pagina web in cui un Virus o altro codice nocivo sia stato rilevato, l'accesso a tale pagina web sarà negato.

1.6 IMSS fornisce, inoltre, una funzionalità di base anti-Phishing che bloccagli **IM** in entrata considerati attacchi di Phishing.

1.7 IMSS è in grado di scansionare alcune versioni di documenti Word, Excel, e PowerPoint, ma non altri allegati.

1.8 IMSS non è in grado di scansionare IM crittografati.

2. Riservato.

3. Controllo del Contenuto IMSS

3.1 IMSS consente al Cliente di configurare la propria strategia di filtraggio del contenuto basata sulle proprie regole per gli IM in entrata e in uscita.

3.2 Il Cliente è responsabile di implementare le opzioni di configurazione, in conformità con gli adeguati termini d'uso per i computer del Cliente (o suo equivalente) attraverso ClientNet. Le regole possono essere configurate per gruppo o individuo. I cambiamenti apportati alle regole dal Cliente entreranno in vigore entro quattro (4) ore.

3.3 Sono disponibili opzioni per definire l'azione da intraprendere al momento del rilevamento del contenuto controllato all'interno di un IM. Tali opzioni sono descritte in maggiore dettaglio su ClientNet e nella versione attuale della Guida dell'Amministratore.

3.4 Il Cliente può revisionare i risultati delle sue regole attraverso ClientNet in forma di riassunti quotidiani, settimanali, mensili e annuali, organizzati sia per regola che per Utente.

4 Registrazione e memorizzazione

4.1 Se il Cliente ha abilitato la funzionalità di registrazione, Symantec compilerà registrazioni quotidiane degli IM scansionati. Ciascuna registrazione comprenderà la data e l'ora, il contenuto e i nomi dei file trasferiti. Tutte le registrazioni non in grado di passare al Cliente saranno memorizzate per un periodo di trentuno (31) giorni, dopodiché saranno distrutte.

4.2 Il Cliente può inoltre configurare IMSS per inviare una copia di ciascun IM nell'archivio compatibile o nella soluzione di memorizzazione del Cliente.

5 Notifiche

5.1 Il Cliente può configurare IMSS per inviare una notifica automatica:
5.1.1 al mittente e al destinatario designato, nel caso in cui un IM venga bloccato poiché si ritiene che possa contenere un Virus, una attacco di Phishing o contenuto controllato; o
5.1.2 al destinatario, se l'accesso a una pagina web è stato negato poiché si ritiene che contenga un Virus o contenuto nocivo.

5.2 Il Cliente può attivare, personalizzare e disattivare le notifiche usando ClientNet.

6 Supporto

6.1 Il Supporto comprende:

6.1.1 Una descrizione dettagliata dell'interfaccia IMSS, compresa una descrizione del servizio e una sessione di Domande e Risposte. (Questo non comprende assistenza per l'installazione di regole o analisi dell'efficacia delle regole);
6.1.2 Guida dell'Amministratore;
6.1.3 la Guida Utente

7 Termini e Condizioni IMSS

7.1 Le liste dei termini di controllo del contenuto e le regole modello suggerite, fornite dal Symantec, comprendono termini che potrebbero essere considerati offensivi. Il Cliente accetta e riconosce che Symantec potrà compilare e pubblicare liste di parole predefinite ottenute dalle liste di termini del Cliente.

7.2 Il Cliente riconosce che gli IM possono contenere informazioni di identificazione personale e che la registrazione e l'intercettazione degli IM potrebbero, quindi, implicare l'elaborazione di dati personali. Inoltre, il Cliente riconosce che IMSS è un servizio configurabile e che il Cliente è esclusivamente responsabile per la configurazione di IMSS in conformità con gli adeguati termini d'uso per i computer del Cliente (o suo equivalente) e con tutte le leggi o normative applicabili. Di conseguenza, Symantec consiglia al Cliente di controllare sempre le normative locali prima di attivare IMSS, e di accertarsi che il Cliente stesso e tutti i suoi dipendenti siano a conoscenza e si conformino a tutte le responsabilità che abbiano relativamente alla tutela dei dati e alle leggi e/o normative sulla privacy, in concomitanza con l'uso da parte del Cliente di IMSS. In alcun paesi può essere necessario ottenere il consenso dei singoli dipendenti prima di eseguire l'intercettazione e la registrazione degli IM. Comeminimo, il Cliente implementerà, con personalizzazione ragionevole e minima, la notifica predefinita di Symantec per IMSS, per coloro che usano qualunque sistema di comunicazione coperto da IMSS che (i) indichi che le comunicazioni trasmesse attraverso tale sistema sono registrate e possono essere intercettate, (ii) indichi gli scopi di tale registrazione e intercettazione, e (iii) ottenga un consenso preventivo dell'utente per tali registrazione e intercettazione. Il Cliente può tradurre, ma non modificherà altrimenti, qualsivoglia linguaggio relativo agli articoli (i), (ii) e (iii) nella frase precedente, come parte di una personalizzazione delle notifiche predefinite per IMSS. Symantec non accetta alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa dell'attivazione di IMSS da parte del Cliente. Il Cliente riterrà indenne Symantec da qualunque reclamo da parte dei suoi dipendenti, di qualunque terza parte e/o di agenzie governative, in merito all'intercettazione o alla registrazione degli IM da parte di Symantec o alla mancata conformità del Cliente con le leggi e/o le normative.

7.3 **SI FA NOTARE AL CLIENTE CHE GLI IM CHE PASSANO ATTRAVERSO IMSS POSSONO ESSERE SCANSIONATI E MEMORIZZATI SU HARDWARE UBICATO NEGLI STATI UNITI D'AMERICA. DI CONSEGUENZA, IL CLIENTE ACCETTA DI FARE TUTTO IL POSSIBILE PER (I) INFORMARE TUTTI I SUOI DIPENDENTI, AGENTI E APPALTATORI E I TERZI CHE UTILIZZANO IL SISTEMA DI COMUNICAZIONE COPERTO DA IMSS DEL FATTO CHE QUALUNQUE INFORMAZIONE, COMPRESE ANCHE INFORMAZIONI DI IDENTIFICAZIONE PERSONALE DEGLI INDIVIDUI, CHE PASSINO ATTRAVERSO IMSS POSSONO ESSERE ELABORATE NEGLI STATI UNITI D'AMERICA; E (II) PER OTTENERE IL CONSENSO DI TALI DIPENDENTI, AGENTI, APPALTATORI E TERZI A TALE ELABORAZIONE PRIMA DI, O IN CONCOMITANZA CON, L'ATTIVAZIONE DI IMSS DA PARTE DEL CLIENTE. INOLTRE, TUTTI I DATI PERSONALI CHE IL CLIENTE FORNISCE A SYMANTEC POSSONO ESSERE TRASFERITI ALLE AFFILIATE DI SYMANTEC E/O AI SUBAPPALTATORI CHE AGISCONO PER CONTO DI SYMANTEC. TALI AFFILIATE O SUBAPPALTATORI POSSONO ESSERE SITUATI NEGLI STATI UNITI O IN ALTRI PAESI CHE POTREBBERO AVERE LEGGI SULLA TUTELA DEI DATI CHE OFFRONO PROTEZIONE MINORE RISPETTO A QUELLE DELLA REGIONE IN CUI SI TROVA IL CLIENTE, NEL CUI CASO SYMANTEC FARÀ**

QUANTO POSSIBILE PER GARANTIRE CHE I DATI RACCOLTI, SE TRASFERITI, RICEVANO UN LIVELLO ADEGUATO DI TUTELA. IL CLIENTE ACCONSENTE A FARE TUTTO QUANTO IL POSSIBILE PER (I) INFORMARE TUTTI I SUOI DIPENDENTI, AGENTI E APPALTATORI, NONCHÉ I TERZI, I CUI DATI PERSONALI SIANO FORNITI DAL CLIENTE A SYMANTEC, DEL FATTO CHE I LORO DATI POTREBBERO ESSERE ELABORATI IN TALI PAESI; E (II) PER OTTENERE IL CONSENSO DI TALI DIPENDENTI, AGENTI, APPALTATORI E TERZI A TALE ELABORAZIONE. SYMANTEC NON ACCETTA ALCUNA RESPONSABILITÀ PER ALCUNA VIOLAZIONE CORRISPONDENTE DELLE LEGGI O DELLE NORMATIVE IN VIGORE.

7.4 **NESSUN SOFTWARE O SERVIZIO È IN GRADO DI GARANTIRE UN TASSO DI RILEVAMENTO IM DEL 100%, DI CONSEGUENZA SYMANTEC NON ACCETTA ALCUNA RESPONSABILITÀ PER ALCUNA PERDITA O DANNO RISULTANTE DIRETTAMENTE O INDIRETTAMENTE DA QUALUNQUE MANCATO RILEVAMENTO DI IMSS DI SPIM, VIRUS, ATTACCHI DI PHISHING, CODICI NOCIVI, URL BLOCCATI O CONTENUTO CONTROLLATO, O PER AVER IDENTIFICATO ERRONEAMENTE IM COME CONTENENTI SPIM, VIRUS, ATTACCHI DI PHISHING, CODICI NOCIVI, URL BLOCCATI O CONTENUTI CONTROLLATI.** Inoltre, la configurazione delle regole di controllo del contenuto IMSS sono completamente sotto il controllo del Cliente e l'accuratezza di tale configurazione influenzerà l'accuratezza di IMSS.

Appendice 14 - Symantec Email Continuity Archive.cloud e Symantec Email Continuity Archive Lite.cloud

1. Panoramica

1.1 I Servizi Symantec Email Continuity Archive.cloud e Symantec Email Continuity Archive Lite.cloud sono sistemi di memorizzazione di e-mail offerti che consentono agli amministratori del sistema del Cliente di impostare politiche di conservazione di e-mail specifiche per la memorizzazione delle e-mail storiche per un insieme di caselle di posta e-mail stabilite.

2. Obblighi del Cliente

2.1 Il Cliente è responsabile delle seguenti azioni per quanto riguarda il Servizio:
2.1.1 Fornire ed eseguire la manutenzione dell'hardware e del software necessari (come identificati nel modulo di fornitura);
2.1.2 Accertarsi che le risorse tecniche dedicate con i diritti d'amministrazione siano disponibili per la fornitura del Servizio;
2.1.3 Designare quali Utenti abbiano il diritto di ricevere il Servizio e il periodo di conservazione specificato per ciascun Utente;
2.1.4 Designare e proteggere i privilegi di accesso all'archivio attraverso l'interfaccia cliente;
2.1.5 Impostare e gestire le politiche di conservazione dell'archiviazione;
2.1.6 Eseguire ricerche per il recupero dei dati archiviati.
2.2 Nel caso in cui il Cliente non abbia eseguito le azioni richieste per fornire il Servizio entro trenta (30) giorni dalla data dell'ordine del Cliente, Symantec potrà iniziare ad addebitare il costo del Servizio.

3. Caratteristiche

3.1 Il *Servizio Symantec Email Continuity Archive.cloud* comprende le seguenti caratteristiche di servizio:
3.1.1 *Registrazione e Archiviazione di E-mail*: l'e-mail viene registrata, quando inviata all'ambiente e-mail primario del Cliente, e viene trasferita in un archivio e-mail per l'indicizzazione e la memorizzazione. L'E-mail viene crittografata e memorizzata nel Servizio. Le politiche di trattenimento delle E-mail possono essere impostate in modo che gli Utenti stabiliscano quando le e-mail saranno eliminate dal Servizio.
3.1.2 *Recupero*: fornisce la capacità di recuperare le e-mail dall'archivio e-mail e di posizionarle nell'archivio messaggi Scambio del Cliente.
3.1.3 *E-Discovery*: fornisce la capacità agli amministratori del sistema del Cliente di specificare alcuni Utenti come "Revisori", dando loro la capacità di revisionare le e-mail in caselle di posta diverse dalle loro per scoperte elettroniche e altri scopi. I Revisori possono creare un archivio di scoperte contenente i risultati di una ricerca nelle caselle di posta degli Utenti. L'archivio delle scoperte può essere esportato a una casella di posta singola.
3.1.4 *Autenticazione Windows*: consente a un Cliente che usa Microsoft Exchange 2000, Microsoft Exchange 2003 e/o Microsoft Exchange 2007 di estendere le politiche di sicurezza del Cliente per l'autenticazione della Directory Attiva di Microsoft agli Utenti del Servizio, consentendo agli Utenti di eseguire il login nel Servizio usando la password della Directory Attiva.
3.1.5 *Archivio Utente Finale*: consente agli Utenti che fanno parte di una politica di conservazione di accedere al proprio archivio personale contenente e-mail dalla loro casella di posta attraverso un'interfaccia basata sul web. Gli amministratori e-mail del Cliente possono inoltre specificare se gli Utenti possano o meno inoltrare e-mail dal proprio archivio personale.
3.1.6 *Gestione della Memorizzazione*: l'amministratore del sistema del Cliente può stabilire una politica di gestione dell'archivio che sposterà gli allegati dai messaggi di Scambio del Cliente al Servizio, con lo scopo di ridurre i requisiti di archiviazione.
3.2 Il *Servizio Symantec MessageLabs Email Archiving.cloud Lite (D)* comprende le seguenti caratteristiche di sistema (come maggiormente descritte in precedenza):
3.2.1 *Registrazione e Memorizzazione E-mail*
3.2.2 *Recupero*
3.2.3 *E-Discovery*
3.2.4 *Autenticazione Windows*
Il Servizio Symantec Email Continuity Archive Lite.cloud non comprende le caratteristiche di Archiviazione Utente Finale o di Gestione della Memorizzazione. Il Cliente può includere la caratteristica di servizio Archivio Utente Finale sottoscrivendo il *Symantec Email Continuity Archive Lite.cloud End User Pack*.
3.3 *Importazione*: il Cliente può importare dati acquisiti nel Servizio dai file pst, scaricando e usando uno strumento di importazione, fatto salvo il pagamento di una quota di importazione basata sulla quantità di dati che devono essere importati. Nel caso in cui la quantità di dati effettivi sia superiore alla quantità di dati da importare acquistata, Symantec si riserva il diritto di applicare a tali dati aggiuntivi i propri prezzi standard di quel momento.

4. Symantec Email Continuity.cloud Storage Option

4.1 La memorizzazione del Cliente sarà misurata per mezzo della quantità grezza di e-mail trasferite al Servizio e attualmente memorizzate.
4.2 Se il Cliente sottoscrive ai bundle Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud o Symantec MessageLabs Ultimate Safeguard.cloud:
4.2.1 Questi bundle comprendono un massimo di 0,7 GB di nuovo spazio per memorizzazione di e-mail per ciascun Utente all'anno, per i Servizi EC e Symantec Email Continuity Archive.cloud combinati. Nel caso in cui il Cliente superi lo spazio di memorizzazione, Symantec addebiterà i costi di tale spazio aggiuntivo ai suoi prezzi correnti in quel momento.
4.2.2 Il bundle non comprende spazio di memorizzazione per i dati acquisiti importati in conformità con la precedente Clausola 3.3, e il Cliente deve acquistare uno spazio di memorizzazione aggiuntivo sufficiente a soddisfare i requisiti ai prezzi applicati da Symantec in quel momento.
4.3 Se il Cliente non sottoscrive a uno dei bundle elencati nella Clausola 4.2, non viene incluso spazio di memorizzazione nel prezzo per l'Utente e il Cliente deve acquistare spazio di archiviazione sufficiente per il Servizio ai prezzi applicati in quel momento da Symantec.
4.4 Laddove il Cliente debba acquistare spazio di memorizzazione aggiuntivo, Symantec emetterà ulteriori fatture e/o apporterà modifiche alle fatture successive, a copertura dei prezzi per l'incremento dello spazio di archiviazione su base pro-rata, per la parte rimanente del periodo di fatturazione attuale.

5. Termini e Condizioni

5.1 NESSUN SERVIZIO DI ARCHIVIAZIONE E-MAIL È IN GRADO DI GARANTIRE UN'ACCURATEZZA DEL 100% E, DI CONSEGUENZA, SYMANTEC NON ACCETTA ALCUNA RESPONSABILITÀ RELATIVA A DANNI O PERDITE RISULTANTI DIRETTAMENTE O INDIRETTAMENTE DA QUALUNQUE MANCANZA DEL SERVIZIO, AD ECCEZIONE DEI RIMEDI ESPRESSAMENTE INDICATI NEL CONTRATTO DI LIVELLO DI SERVIZIO.
5.2 Symantec non sarà responsabile per alcuna incapacità di fornire il Servizio come qui indicato che sia causata da (a) incapacità di Symantec di applicare le pratiche standard nell'attivare e gestire il Servizio al Cliente, (b) la mancata conformità del Cliente con le linee guida di Symantec indicate nel manuale utente o nel modulo di fornitura, o (c) la mancata attivazione o uso del Servizio da parte del Cliente.
5.3 Symantec sottolinea che la configurazione e l'uso del Servizio è interamente sotto il controllo del Cliente. Symantec raccomanda al Cliente di disporre di una politica d'uso accettabile per i computer (o suo equivalente). In alcuni paesi, potrebbe essere necessario ottenere il consenso di ciascun singolo dipendente. Symantec consiglia al Cliente di verificare sempre le normative locali prima di attivare il Servizio. Symantec non può accettare alcuna responsabilità civile o penale che possa essere attribuita al Cliente a causa del funzionamento del Servizio. **5.4 IL CLIENTE RICONOSCE E ACCONSENTE CHE PARTE O TUTTO IL SERVIZIO PUÒ ESSERE ESEGUITO NEGLI STATI UNITI D'AMERICA E CHE IL CLIENTE È RESPONSABILE DELL'OTTENIMENTO DI TUTTI I CONSENSI E LE APPROVAZIONI NECESSARI PER RENDERE EFFICACE IL TRASFERIMENTO DEI DATI. INOLTRE, IL CLIENTE RICONOSCE E ACCONSENTE CHE SYMANTEC NON PUÒ ACCETTARE RESPONSABILITÀ PER ALCUNA VIOLAZIONE CORRISPONDENTE DELLA LEGGE O DELLE NORMATIVE APPLICABILI.**
5.5 Il Cliente riconosce e acconsente che (i) i servizi di scansione di Symantec (E-mail AV, E-mail AS, E-mail IC e E-mail CC) non sottopongono a scansione tutte le e-mail che entrano originariamente nell'archivio, e che (ii) i servizi di scansione di Symantec (E-mail AV, E-mail AS, E-mail IC e E-mail CC) non sottopongono a scansione tutte le e-mail che sono rilasciate dall'archivio per il loro reinserimento nella casella di posta dell'Utente. Di conseguenza, Symantec non può essere ritenuta responsabile di alcun virus, spam, immagini o contenuto inappropriato che tali e-mail reinserite potrebbero contenere, e, inoltre, il Contratto di Livello di Servizio non si applica a tali e-mail ripristinate.
5.6 Il Cliente riconosce e acconsente che Symantec non può agire come esecutore del download terzo in ogni caso ai sensi delle le normative SEC.

6. Licenza del Software

6.1 Concessione della licenza
Fatti salvi i termini e le condizioni del presente Contratto, Symantec garantisce al Cliente il diritto non esclusivo e non trasferibile di installare e usare il Software per il Servizio di Symantec Email Continuity Archive.cloud o Symantec Email Continuity Archive Lite.cloud, come applicabile esclusivamente per le operazioni

commerciali interne del Cliente. ("Software" indica ciascun programma software di Symantec per il Servizio di Symantec Email Continuity Archive.cloud o Symantec Email Continuity Archive Lite.cloud nel formato codice oggetto fornito in licenza da Symantec e governato dai termini del Contratto, compresi, senza limitazioni, le nuove distribuzioni o gli aggiornamenti come indicato nel presente). Tutti i diritti di proprietà intellettuale nel Software sono e rimarranno di proprietà di Symantec (e/o dei suoi fornitori). Il Software viene dato in licenza da Symantec, non viene venduto. Il Cliente riconosce che il Software e tutte le informazioni correlate, compresi, senza limitazione alcuna, tutti gli aggiornamenti, sono proprietà di Symantec e dei suoi fornitori. Il Cliente sarà completamente responsabile della conformità di ciascun Utente o della violazione dei termini del presente Contratto. Il Cliente notificherà immediatamente a Symantec qualunque uso non autorizzato o violazione dei termini della presente licenza.

6.2. Restrizioni relative a copie e uso

Il Cliente può scaricare e installare il Software alle seguenti condizioni:

6.2.1. Il Cliente non può scaricare o installare il Software su un numero di licenze superiore a quello di licenze per Utente Finale concesse in licenza al Cliente. ("Utente Finale" indica il computer fisico sul quale il software è installato).

6.2.2. Il Cliente può copiare il Software, come ragionevolmente necessario, per scopi di backup, archiviazione o recupero in seguito a guasto. La Documentazione Stampata può essere riprodotta dal Cliente esclusivamente per uso interno. ("Documentazione" indica le guide utente e/o i manuali per il funzionamento del Software di Symantec compresi con il Software scaricato).

6.2.3 Il Cliente non può, né può consentire a una terza parte di: (i) decompilare, disassemblare, o eseguire reverse engineering del Software, ad eccezione di quanto espressamente consentito dalla legge in vigore, senza il previo consenso scritto di Symantec; (ii) rimuovere qualunque notifica di identificazione del prodotto o dei diritti di autore; (iii) dare in leasing, a noleggio o usare il Software per scopi di suddivisione di tempo o per agenzia di servizio; (iv) modificare la traduzione, adattare o creare lavori derivati del Software, o (v) altrimenti usare o copiare il Software, ad eccezione di quanto espressamente indicato nel presente.

6.3 Trasferimento dei diritti

Il Cliente non può trasferire, assegnare o delegare la licenza del software relativa al presente Contratto senza il previo consenso scritto di Symantec. Qualunque trasferimento, assegnazione o delega di tale tipo, in violazione di quanto precedentemente esposto, sarà nullo.

6.4 Garanzia limitata e rinuncia

6.4.1 Symantec garantisce che, al momento del download, il Software sarà conforme dal punto di vista materiale con l'attuale Documentazione di Symantec.

6.4.2 La garanzia precedente non si applica se: (i) il Software non viene usato in conformità con il presente Contratto o la Documentazione; (ii) il Software, o parte dello stesso, è stato modificato da qualunque entità diversa da Symantec; o (iii) un malfunzionamento del Software è stato causato da apparecchiatura del Cliente o da software di terzi.

6.4.3 SYMANTEC NON GARANTISCE CHE IL FUNZIONAMENTO DEL SOFTWARE SIA SENZA INTERRUZIONI O SENZA ERRORI. SYMANTEC DISCONOSCE E NEGA ESPRESSAMENTE OGNI GENERE DI GARANZIE DI QUALUNQUE TIPO, SIA ESPRESSE, CHE IMPLICITE CHE ALTRIMENTI, COMPRESE, FRA LE ALTRE, LA GARANZIA DI COMMERCIABILITÀ, DI QUALITÀ SODDISFACENTE O DI ADEGUATEZZA PER UNO SCOPO PARTICOLARE.

6.5. Rescissione

Al termine del Servizio di Symantec Email Continuity Archive.cloud o Symantec Email Continuity Archive Lite.cloud, tutti i diritti del Cliente di utilizzare il Software garantiti dal presente cesseranno immediatamente e il Cliente restituirà tempestivamente a Symantec, o distruggerà, tutte le copie del Software e della Documentazione.

7. Termine del servizio ed estrazione dei dati

7.1 Al termine del Servizio Symantec Email Continuity Archive.cloud o Symantec Email Continuity Archive Lite.cloud, Symantec eliminerà i dati del Cliente dall'archivio.

7.2 Il Cliente può estrarre i propri dati dall'archivio in qualsiasi momento prima del termine.

Appendice 15 - Servizio Symantec MessageLabs Volume Mail ("Posta di Grosso Volume")

1. Se il Cliente sottoscrive al Servizio Volume di Posta, il Cliente può inviare e ricevere Mail di Grosso Volume secondo le seguenti condizioni:

1.1 La Posta di Grosso Volume deve comprendere esclusivamente destinatari confermati e prescelti. Su richiesta di Symantec, e sulla base delle normative applicabili, il Cliente dovrà fornire prove di tali conferme.

1.2 Le dimensioni di ciascuna Posta di Grosso Volume, compresi gli allegati, non devono superare i 500 kilobyte.

1.3 La casella 'Destinatari' per ciascuna Posta di Grosso Volume non deve contenere più di cinquecento (500) indirizzi E-mail.

1.4 Il Cliente deve operare attraverso un efficace sistema di gestione della lista, compresa la tempestiva rimozione degli indirizzi e-mail non validi e cancellazione della sottoscrizione.

1.5 Il Cliente deve ricevere il Servizio Symantec MessageLabs Email Anti-Virus.cloud per le sue E-mail standard.

1.6 La Posta di Grosso Volume del Cliente deve aver origine da, o essere diretta a, un dominio separato rispetto alle E-mail standard, per consentire alla Posta di Grosso Volume di essere indirizzata verso un server Tower di Controllo particolare.

1.7 Il banner in uscita predefinito notificherà al destinatario che la Posta di Grosso Volume è stata scansionata alla ricerca di virus, ma non conterrà il logo Symantec.

1.8 Se il Cliente sottoscrive al Servizio Posta di Grosso Volume Banda F o G nella Sezione B "Servizio e Costi", il Cliente deve inviare o ricevere Posta di Grosso Volume in volumi non superiori a 250.000 destinatari al giorno.

1.9 Il Cliente riconosce e accetta che l'invio di Posta di Grosso Volume può avere un effetto variabile sul flusso del traffico E-mail. Tali effetti sono al di fuori del controllo di Symantec, e per questa ragione i Livelli di Servizio indicati nel Contratto di Livello di Servizio non si applicano alla Posta di Grosso Volume.

1.10 Se, in qualunque momento, (i) i sistemi E-mail del Cliente entrano a far parte della lista nera, o (ii) il Cliente fa entrare i sistemi di Symantec nella lista nera a causa dell'invio di Spam, o (iii) il Cliente non soddisfa gli obblighi indicati nella presente Appendice, Symantec informerà il Cliente e si riserva il diritto a sua esclusiva discrezione di trattenere la fornitura, sospendere o terminare in tutto o in parte i Servizi immediatamente.

1.11 Ciascuna Banda di Servizio di Posta di Grosso Volume ha una quota massima di Destinatari consentiti al Mese. Tali quote non sono trasferibili o cumulative, e, di conseguenza, i Destinatari non utilizzati non possono essere messi da parte per i mesi successivi.

1.12 Il Cliente avvertirà Symantec se, in qualunque momento, l'utilizzo di Posta di Grosso Volume supererà il numero di Destinatari al Mese consentiti per la Banda attuale del Cliente, e Symantec incrementerà il costo alla Banda appropriata in conformità con il listino prezzi applicato in quel momento da Symantec. Inoltre, Symantec monitorerà l'utilizzo di Posta di Grosso Volume reale del Cliente e se il numero di Destinatari al Mese supererà il numero consentito per la Banda attuale del Cliente, Symantec incrementerà il costo in conformità con il listino prezzi applicato in quel momento da Symantec. Symantec emetterà, a sua esclusiva discrezione, fatture aggiuntive e/o apporterà le modifiche alle fatture successive a copertura di tali incrementi.

Appendice 15 – Symantec Enterprise Vault.cloud

1. Panoramica

EV.cloud è il nome collettivo per un certo numero di Servizi di archiviazione (secondo la descrizione di ciascuno nelle Clausole da 1.1 a 1.10 inclusiva di seguito) sottoscritti dal Cliente. Tutti i Servizi nella serie EV.cloud sono compatibili con le versioni approvate dei server Exchange utilizzati internamente e dei servizi Exchange in hosting.

1.2 Quanto segue è applicabile ai Servizi Symantec Enterprise Vault Personal.cloud e Symantec Enterprise Vault Discovery.cloud:

1.2.1 La dimensione massima delle e-mail che può essere accettata dal Servizio Symantec Enterprise Vault Personal.cloud e Symantec Enterprise Vault Discovery.cloud è di 50 MB.

1.2.2 Per entrambi i Servizi Symantec Enterprise Vault Personal.cloud e Symantec Enterprise Vault Discovery.cloud si applica quanto segue:

1.2.3 I Clienti possono rispondere a e inoltrare direttamente i messaggi che si trovano nell'archivio creato da entrambi i servizi. Ciò consente al Cliente di creare regolarmente file di backup in caso di problemi con le proprie e-mail.

1.2.4 Nessuno dei due servizi sostituisce la necessità del Cliente di eseguire il backup locale del proprio server di posta. Nell'eventualità che il Cliente debba ricostruire il proprio server di posta, l'operazione deve essere eseguita in base ai dati gestiti a livello locale e non a quelli presenti nell'archivio.

1.1. Symantec Enterprise Vault Personal.cloud

Il Servizio Symantec Enterprise Vault Personal.cloud è il servizio di archiviazione delle e-mail basato su Internet di Symantec progettato per fornire agli Utenti individuali del Cliente l'accesso ai propri archivi di e-mail personali direttamente da Microsoft Outlook o Outlook Web Access (laddove supportato) al fine di trovare e ripristinare e-mail perdute o eliminate.

1.1.1 Le e-mail in entrata e in uscita del Cliente, compresi gli allegati, vengono acquisite in un repository online ("Archivio personale"), nel quale gli Utenti possono cercare messaggi di e-mail perduti o eliminati.

1.1.2 Gli Utenti possono inoltre accedere all'Archivio personale da Microsoft Outlook, Outlook Web Access (laddove supportato), IBM Lotus Notes, dispositivi BlackBerry® e tramite browser su un sito Web sicuro.

1.1.3 Gli Utenti possono cercare nell'Archivio personale specifiche e-mail e allegati secondo due modalità: Ricerca rapida e Ricerca avanzata. L'opzione Ricerca avanzata fornisce agli Utenti la possibilità di personalizzare le ricerche in base a vari criteri, quali parole chiave dei messaggi, destinatario, mittente, oggetto, data(e) e tipo di allegato.

1.1.4 Se la funzione è attivata, gli Utenti possono comporre, rispondere e inoltrare messaggi direttamente dal Servizio Symantec Enterprise Vault Personal.cloud , analogamente a quanto avverrebbe in Outlook o Notes.

1.1.5 Gli Utenti possono creare ricerche personalizzate in base a vari criteri (ad esempio, intervallo di date, mittente dell'e-mail, tipo di allegato, ecc.) e quindi salvarle in modo da riutilizzarle all'occorrenza.

1.1.6 Il trasferimento delle e-mail precedenti del Cliente nell'Archivio personale e la rimozione degli archivi locali aiuta a recuperare spazio sulle unità condivise e sui server di e-mail del Cliente.

1.1.7 L'Archivio personale del Cliente può essere utilizzato per recuperare e-mail storiche nel caso un computer o dei portatili vengano smarriti o rubati.

1.1.8 I Clienti possono acquisire i file PST nel Servizio Symantec Enterprise Vault Personal.cloud mantenendo opzionalmente la struttura delle dopo l'acquisizione iniziale.

1.2. Symantec Enterprise Vault Discovery.cloud

Il Servizio Symantec Enterprise Vault Discovery.cloud è il servizio di archiviazione delle e-mail basato su Internet di Symantec progettato per accelerare le richieste di reperimento legale (e-discovery), applicare policy di utilizzo delle e-mail e coadiuvare la mitigazione della perdita di dati. Discovery Archive assiste i clienti nella conservazione delle e-mail correlata a riferimenti di carattere legale, e ha l'obiettivo di proteggere le comunicazioni riservate tra legali e clienti.

1.2.1 Symantec Enterprise Vault Discovery.cloud memorizza e indicizza e-mail, allegati e messaggi su BlackBerry® (testo SMS, PIN-to-PIN, registri delle chiamate) in un repository online centralizzato.

1.2.2 I Clienti possono associare riferimenti legali a comunicazioni specifiche (in base a criteri di ricerca) per contribuire a evitare che il personale o le policy di eliminazione automatiche del Cliente eliminino accidentalmente e-mail pertinenti a casi specifici. Amministratori e revisori possono contrassegnare comunicazioni riservate tra legali e cliente, che possono essere escluse dalle richieste di e-discovery.

1.2.3 Il registro delle ricerche di Symantec Enterprise Vault Discovery.cloud acquisisce le attività dei revisori, in modo che gli amministratori possano svolgere le verifiche appropriate.

1.2.4 Gli amministratori hanno la possibilità di raggruppare gli Utenti in base a criteri personalizzati. I revisori sono quindi in grado di effettuare ricerche tra questi gruppi.

1.2.5 I Clienti possono eseguire ricerche nei contenuti delle e-mail e allegati archiviati utilizzando vari criteri di ricerca, tra cui destinatario, mittente, data, oggetto, corpo del messaggio, allegati del messaggio e altre proprietà dei messaggi.

1.2.6 I revisori del Cliente possono consultare agevolmente i risultati di ricerca, individuare i termini di ricerca evidenziati e contrassegnare e-mail potenzialmente dannose, in modo che siano facilmente recuperabili per un'ulteriore verifica.

1.2.7 I Clienti possono contrassegnare e-mail legate a uno specifico caso o questione legale ed esportarle successivamente in una soluzione di terze parti per la gestione dei casi o di altro tipo per consentire ulteriori verifiche e analisi.

1.2.8 I revisori del Cliente possono creare e salvare ricerche di e-mail personalizzate in base alle policy di e-mail del Cliente, quindi eseguirle nuovamente all'occorrenza.

1.2.9 I revisori del Cliente possono configurare avvisi di policy per ricevere notifiche quando un'e-mail soddisfa i criteri di una "ricerca salvata" (ad esempio, contiene parole o frasi specifiche).

1.3. Symantec Enterprise Vault.cloud BlackBerry® Option

Il Servizio Symantec Enterprise Vault.cloud BlackBerry® Option è il servizio basato su Internet di Symantec progettato per consentire ai singoli Utenti del Cliente di accedere e cercare e-mail archiviate, allegati, SMS, messaggi PIN-to-PIN e file di registro delle chiamate tramite i propri dispositivi BlackBerry®. Gli utenti possono trovare e ripristinare e-mail perdute o eliminate e continuare a utilizzare il proprio dispositivo BlackBerry® per comporre, rispondere e inviare messaggi in tempo reale nel caso in cui il server di e-mail principale del Cliente subisca un'interruzione operativa. Symantec Enterprise Vault.cloud BlackBerry® Option è un servizio aggiuntivo opzionale del Servizio Symantec Enterprise Vault Personal.cloud.

1.3.1 Symantec Enterprise Vault.cloud BlackBerry® Option può essere distribuito dagli amministratori agli Utenti da un BlackBerry® Enterprise Server (BES) o dagli Utenti tramite BlackBerry® Desktop Manager.

1.3.2 Gli Utenti possono accedere all'Archivio personale per BlackBerry® facendo clic sull'icona visualizzata nella finestra principale del dispositivo.

1.3.3 Quando l'Utente fa clic sull'applicazione, viene visualizzata una schermata iniziale per tre secondi e viene quindi chiesto all'utente di immettere le proprie credenziali.

1.3.4 Dopo avere effettuato correttamente l'accesso, viene visualizzata la schermata principale (ovvero, la schermata List View) dell'Archivio personale.

1.3.5 Dalla schermata List View (casella postale), gli Utenti possono eseguire varie funzioni, tra cui: composizione di nuovi messaggi, risposta o inoltre di e-mail, ed esecuzioni di ricerche semplici o avanzate.

1.3.6 Gli Utenti possono trovare e-mail vecchie, perdute o eliminate utilizzando ricerche semplici o avanzate su tutti i messaggi e i file di registro delle chiamate memorizzati nel proprio Archivio personale e poi ripristinare tali messaggi nella propria casella della posta in arrivo.

1.3.7 L'Utente può immettere testo nella casella di ricerca e premere l'icona di ricerca per avviare l'operazione. I risultati di ricerca possono essere filtrati in base ai criteri "Data", "Mittente" e "Destinatario".

1.3.8 L'Utente può utilizzare il proprio Archivio personale per comporre, rispondere e inviare messaggi anche se la piattaforma

di e-mail principale del Cliente (ad esempio, Microsoft Exchange) non è disponibile.

1.4 AdvisorMail on Symantec.cloud™
Il Servizio AdvisorMail on Symantec.cloud™ (AdvisorMail) è il servizio di archiviazione delle e-mail basato su Internet di Symantec che si occupa di accelerare il processo di revisione delle e-mail imposto da alcuni requisiti normativi. Il Servizio AdvisorMail archivia le e-mail in un unico repository. I messaggi vengono esaminati automaticamente e contrassegnati in base alle policy specifiche del Cliente. Messaggi o allegati contenenti parole chiave o frasi specificate possono essere esaminati da professionisti della conformità per verificare l'applicazione delle policy.
1.4.1 AdvisorMail acquisisce automaticamente i messaggi inviati e ricevuti senza alcun intervento da parte del Cliente e li trasmette in modo sicuro a diversi data center per la conservazione utilizzando la crittografia TLS o VPN.
1.4.2 Gli strumenti di amministrazione e reporting di AdvisorMail comprendono modalità di revisione preliminare e a posteriori, campionamento casuale, regole personalizzabili per specifici domini o indirizzi di e-mail e report di riepilogo.
1.4.3 AdvisorMail offre due livelli di autorizzazione distinti per la revisione delle e-mail: Amministratore (accesso completo) e Revisore (diritti di supervisione per caselle postali selezionate).
1.4.4 AdvisorMail offre vari strumenti per semplificare il processo di supervisione, tra cui il contrassegno automatico delle e-mail sospette per la revisione dell'auditor.
1.4.5 I Clienti possono preselezionare la cartella iniziale (ad esempio, revisione a posteriori), intervallo di date e visualizzazione dei messaggi (ad esempio, List o Snippet View).
1.4.6 I Clienti possono utilizzare la funzionalità Next Click per saltare alla violazione successiva nei messaggi di e-mail e allegati con un singolo clic del mouse mentre le azioni, tramite il clic con il pulsante destro, consentono di scegliere i comandi direttamente da un menu di scelta rapida (ad esempio, aggiunta di parole chiave al dizionario).
1.4.7 La funzionalità di supervisione a livelli di AdvisorMail consente ai Clienti di attivare con un unico comando un dizionario aziendale (elenco di parole chiavi e frasi vietate) per le sedi remote.
1.4.8 L'editor di liste bianche di AdvisorMail consente ai Clienti di creare elenchi di parole chiave e frasi autorizzate che si trovano spesso in dichiarazioni di rinuncia (ovvero, le dichiarazioni di esonero da responsabilità che si trovano in fondo alle e-mail) per ridurre il numero di violazioni di conformità falsi positivi.
1.4.9 AdvisorMail consente ai Clienti di aggiungere indirizzi di e-mail, spostare utenti in altre sedi, modificare regole e verificare più e-mail.
1.4.10 Il registro di ricerca di AdvisorMail acquisisce le attività di controllo dei revisori dell'Azienda, coadiuvando gli amministratori nella soddisfazione dei requisiti di conformità.
1.4.11 I Revisori possono aggiungere note ai messaggi in base alle esigenze.

1.5 AdvisorMail IM Option on Symantec.cloud™
Il Servizio AdvisorMail IM Option on Symantec.cloud™ è il servizio di archiviazione basato su Internet di Symantec per le piattaforme di messaggistica istantanea supportate. I messaggi istantanei vengono acquisiti, archiviati e indicizzati in AdvisorMail e poi monitorati in base alla policy di conformità specifiche del Cliente. Messaggi istantanei contenenti parole chiave o frasi specificate possono essere esaminati da professionisti della conformità per verificare l'applicazione delle policy. Il Servizio AdvisorMail IM Option on Symantec.cloud™ è un servizio aggiuntivo opzionale di AdvisorMail.
1.5.1 Il Servizio AdvisorMail IM Option on Symantec.cloud™ interagisce con le reti e i clienti di messaggistica istantanea supportati che attualmente comprendono reti di messaggistica istantanea pubbliche come AOL, MSN, Yahoo e Google Talk, reti private (Reuters) e client di messaggistica istantanea aziendali (Microsoft Office Communicator, Lotus Sametime e Jabber).
1.5.2 I messaggi istantanei vengono indicizzati e copiati nel formato originale su supporti che consentono di effettuare rapidamente ricerche.
1.5.3 Il Cliente può cercare e recuperare conversazioni di messaggistica istantanea specifiche in base a vari criteri di ricerca, tra cui intervallo di date, parole chiave o frasi e mittente/destinatario.
1.5.3 Non è disponibile una cronologia di registrazione per finalità di controllo.

1.6 AdvisorMail Bloomberg Option on Symantec.cloud™
Il Servizio AdvisorMail Bloomberg Option on Symantec.cloud™ è il servizio di archiviazione basato su Internet di Symantec per Instant Bloomberg (messaggi istantanei) ed e-mail Bloomberg. I messaggi di Bloomberg vengono acquisiti, archiviati e indicizzati in AdvisorMail e poi monitorati in base alla policy specifiche dell'Azienda. I messaggi di Bloomberg contenenti parole chiave o frasi specifiche possono essere quindi riveduti da professionisti della conformità. Il Servizio AdvisorMail Bloomberg Option on Symantec.cloud™ è un servizio aggiuntivo opzionale di AdvisorMail.
1.6.1 Il Servizio AdvisorMail Bloomberg Option on Symantec.cloud™ acquisisce i messaggi di Instant Bloomberg e le e-mail di Bloomberg in AdvisorMail nel relativo formato proprietario.
1.6.2 I messaggi di Bloomberg vengono indicizzati e copiati nel formato originale su supporti di storage che consentono di effettuare rapidamente ricerche.
1.6.3 Il Cliente può cercare e recuperare messaggi di Bloomberg specifici in base a vari criteri di ricerca, tra cui intervallo di date, parole chiave o frasi e mittente/destinatario.
1.6.4 Non è disponibile una cronologia di registrazione per finalità di controllo.

1.7 Riservato.

1.8 Symantec Enterprise Vault.cloud Data Import Option
Il Servizio Symantec Enterprise Vault.cloud Data Import Option è il servizio basato su Internet di Symantec progettato per migrare e acquisire vecchie versioni di dati di e-mail esistenti nel repository di archivio del Cliente. Il servizio di importazione consente quindi al Cliente di eseguire ricerche nel proprio archivio di e-mail (ad esempio, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud e AdvisorMail) comprendente sia le e-mail precedenti acquisite, sia i nuovi flussi di e-mail.
1.8.1 Il Servizio Symantec Enterprise Vault.cloud Data Import Option richiede che un Cliente invii tramite S-FTP o corriere sicuro i dati di e-mail in formato file PST o EML.
1.8.2 Il Cliente può estrarre manualmente i dati e fornirli in formato PST o EML o utilizzare servizi professionali per l'estrazione automatizzata dai repository supportati.
1.8.3 Seguendo le indicazioni del Cliente, il Servizio Symantec Enterprise Vault.cloud Data Import Option assegna la proprietà di ciascun messaggio che è stato individuato. I messaggi che non possono essere assegnati direttamente a un individuo specifico vengono archiviati in una casella postale "generica" all'interno dell'archivio di e-mail.
1.8.4 Tutte le attività di migrazione possono essere registrate e controllate per garantire l'integrità dei record di e-mail del Cliente e mantenere i criteri "Chain of Custody".
1.8.5 Il Servizio Symantec Enterprise Vault.cloud Data Import Option comporta la partecipazione attiva del Cliente nella pianificazione, analisi e attuazione di un piano di acquisizione con interferenze minime per il business.
1.8.6 La dimensione massima delle e-mail che può essere accettata dal Servizio è di 40 MB.

1.9 Symantec Enterprise Vault Mailbox Continuity.cloud
SE SYMANTEC NON È IN GRADO DI STABILIRE UNA CONNESSIONE SMTP CON IL CLIENTE, LE E-MAIL DEL CLIENTE SARANNO INSTRADATE AL SERVIZIO SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD PER CONTO DEL CLIENTE ("EVENTO DI CONTINUITÀ"). A SCANSO DI EQUIVOCI: (I) SE IL FIREWALL DEL CLIENTE OPERA IN FUNZIONE DI PROXY E RISPONDE PER CONTO DEL SERVER DI POSTA, O (II) SE IL SERVER DI POSTA DEL CLIENTE FORNISCE UNA RISPOSTA (COMPRESI SENZA LIMITAZIONE CODICI DI ERRORE), CIÒ COSTITUIRÀ UNA CONNESSIONE SMTP E NON SARÀ CONSIDERATO UN EVENTO DI CONTINUITÀ.

1.9.1 Durante un Evento di continuità, gli Utenti del Cliente possono accedere alle proprie e-mail tramite una cartella dedicata in Microsoft Outlook® o un'interfaccia utente basata sul Web. L'Utente può: (i) visualizzare fino a novanta (90) giorni di e-mail storiche, comprese le nuove e-mail inviate e ricevute durante l'Evento di continuità; (ii) creare, rispondere a e inoltrare e-mail; e (iii) utilizzare comuni strumenti per le e-mail quali controllo ortografico, inserimento di allegati e formattazione del testo.
1.9.2 Se il Cliente è abbonato solamente a Symantec Enterprise Vault Mailbox Continuity.cloud, le E-mail di continuità saranno archiviate all'interno di tale servizio per un periodo di novanta (90) giorni. Se il Cliente ha acquistato un servizio di archiviazione aggiuntivo nel quadro della presente Appendice 17, le E-mail di continuità saranno conservate in base al periodo di conservazione scelto dal Cliente in tale servizio.
1.9.3 Le E-mail di continuità saranno recapitate al server e-mail primario del Cliente nel momento in cui tale server inizia nuovamente ad accettare le e-mail, ad eccezione delle e-mail che sono rimaste in coda per più di sette (7) giorni che non saranno recapitate e il Cliente dovrà recuperare tali e-mail dall'archivio di continuità descritto nella Clausola 1.9.2 sopra riportata.
1.9.4 Per il recapito delle e-mail, il Servizio Symantec Enterprise Vault Mailbox Continuity.cloud utilizza una connessione Transport Layer Security ("TLS") di tipo opportunistico invece che imposta. TLS è un protocollo di sicurezza avanzato progettato per proteggere/crittografare le -e-mail durante il trasporto in Internet. **TUTTI I CLIENTI DI BOUNDARY ENCRYPTION E POLICY BASED ENCRYPTION CHE SCELGONO ANCHE IL SERVIZIO SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD RICONOSCONO E ACCETTANO CHE VERRÀ TENTATA UNA CONNESSIONE TLS MA CHE QUESTA POTREBBE NON ESSERE OTTENUTA NEL QUAL CASO LE E-MAIL NON SARANNO CRITTOGRAFATE. DI CONSEGUENZA, IL CLIENTE RICONOSCE CHE NON DEVE INVIARE O RICEVERE DATI SENSIBILI TRAMITE IL SERVIZIO SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD E CHE TALI OPERAZIONI SONO INTERAMENTE A SUO RISCHIO.**
1.9.5 Obblighi di Symantec Enterprise Vault Mailbox Continuity.Cloud
Il Servizio Symantec Enterprise Vault Mailbox Continuity.Cloud recapita le e-mail solamente a un unico server designato per dominio specificato e i Clienti di tipo "routing per Utente" accettano qui questo aspetto del servizio. Il Cliente accetta di configurare il Servizio Symantec Enterprise Vault Mailbox Continuity.Cloud come route di recapito di failover con l'interfaccia ClientNet e di indicare inoltre a Symantec la posizione di recapito (nome o indirizzo IP dell'host di posta) per dominio dei propri server di posta all'inizio del servizio. Durante il periodo del Servizio Symantec Enterprise Vault Mailbox Continuity.Cloud, il Cliente riconosce e accetta l'obbligo costante di aggiornare Symantec in merito a qualsiasi modifica di tale posizione di recapito. Il Cliente riconosce che la mancata esecuzione di tali configurazioni o la mancata fornitura di tali informazioni di recapito a Symantec influirà negativamente sulla funzionalità del Servizio Symantec Enterprise Vault Mailbox Continuity.Cloud.

1.10 Symantec Enterprise Vault.cloud Folder Sync Option

1.10.1 Symantec Enterprise Vault.cloud Folder Sync Option è un servizio aggiuntivo del Servizio Symantec Enterprise Vault Personal.cloud descritto unicamente nella Sezione 1.1 della presente Appendice. Il Servizio Symantec Enterprise Vault.cloud Folder Sync Option consente al Cliente di visualizzare le e-mail nel Servizio Symantec Enterprise Vault Personal.cloud in modo simile all'organizzazione delle e-mail nelle cartelle Outlook del Cliente. Il Servizio Symantec Enterprise Vault.cloud Folder Sync Option consente agli amministratori di sincronizzare le strutture delle cartelle di Outlook del Cliente all'interno di Symantec Enterprise Vault Personal.cloud. Quando i Clienti spostano messaggi e-mail tra le cartelle di Outlook e creano e spostano la posizione delle cartelle di Outlook, il servizio di sincronizzazione replica di conseguenza la–struttura delle cartelle all'interno di Symantec Enterprise Vault Personal.cloud.
1.10.2 Symantec Enterprise Vault.cloud Folder Sync Option viene distribuito dagli amministratori per il Cliente tramite un servizio locale che tiene traccia degli spostamenti di cartelle ed elementi.
1.10.3 Dopo la sincronizzazione iniziale, Symantec Enterprise Vault.cloud Folder Sync Option fornisce una sincronizzazione incrementale tra le cartelle di Outlook e Symantec Enterprise Vault Personal.cloud.
1.10.4 Le sincronizzazioni incrementali possono essere pianificate con frequenza oraria, giornaliera o settimanale in base alle preferenze del Cliente.
1.10.5 Il Cliente può filtrare i risultati di una ricerca dell'archivio attivando la funzionalità di 'filtro' e selezionando una cartella nell'elenco restituito nei filtri di ricerca.
Il servizio è supportato solamente sulle piattaforme Microsoft Exchange Server 2003, 2007 o 2010.

2. Termini aggiuntivi.

2.1 Symantec sottolinea che la configurazione e l'utilizzo del Servizio è interamente sotto il controllo del Cliente. Symantec consiglia che presso il Cliente sia in vigore una policy di utilizzo accettabile dei computer (o equivalente). In certi paesi può essere necessario ottenere l'autorizzazione delle singole persone. Symantec consigli al Cliente di verificare sempre la legislazione locale prima di implementare il Servizio. Symantec non accetta alcun obbligo per responsabilità civili o penali in cui può incorrere il Cliente per effetto dell'utilizzo del Servizio.
2.2 **IL CLIENTE RICONOSCE E ACCETTA CHE TUTTO IL SERVIZIO O UNA SUA PARTE VENGA EFFETTUATO NEGLI STATI UNITI D'AMERICA E CHE IL CLIENTE HA LA RESPONSABILITÀ DI OTTENERE TUTTE LE AUTORIZZAZIONI E APPROVAZIONI NECESSARIE PER EFFETTUARE IL TRASFERIMENTO DEI DATI. IL CLIENTE RICONOSCE E ACCETTA INOLTRE CHE SYMANTEC NON PUÒ ACCETTARE ALCUNA RESPONSABILITÀ PER QUALSIASI VIOLAZIONE CONSEGUENTE DELLA LEGGE O DELLE NORMATIVE VIGENTI.**
2.3 Il Cliente riconosce e accetta che (i) i servizi di scansione di Symantec (Email AV, Email AS, Email IC e Email CC) non esaminano tutte le e-mail che entrano originariamente nell'archivio e che (ii) i servizi di scansione di Symantec (Email AV, Email AS, Email IC e Email CC) non esaminano le e-mail che vengono rilasciate dall'archivio per essere reintegrate nella casella postale di un Utente. Di conseguenza, Symantec non può essere responsabile di virus, spam, immagini o contenuti non appropriati che tali e-mail reintegrate potrebbero contenere, e inoltre, il Contratto di servizio non avrà valore per tali e-mail reintegrate.
2.4 Soggetto ai termini e condizioni del presente Contratto, Symantec concede al Cliente il diritto non esclusivo e non trasferibile di installare e utilizzare qualsiasi software pertinente ai suddetti Servizi come applicabile esclusivamente alle operazioni aziendali interne del Cliente. Tutti i diritti di proprietà intellettuale su questo software sono e rimarranno di proprietà di Symantec (e/o dei suoi fornitori). Tale software non viene venduto ma è concesso in licenza da Symantec. Il Cliente riconosce che il software e tutte le informazioni correlate, compresi senza limitazione gli aggiornamenti, sono di proprietà di Symantec e dei suoi fornitori. Il Cliente avrà la responsabilità e l'intero obbligo di garantire la conformità di ciascun Utente riguardo la violazione dei termini del presente Contratto. Il Cliente dovrà segnalare immediatamente a Symantec qualsiasi utilizzo non autorizzato o violazione dei termini della presente licenza.
2.5 Il Cliente riconosce e accetta che ai fini delle normative SEC, Symantec non può agire in nessun caso come soggetto terzo per il download.
2.6 Tutti i dati del Cliente memorizzati o archiviati in virtù del presente atto da Symantec o dai suoi fornitori di terze parti sono di esclusiva proprietà del Cliente ("Dati del cliente"), e nulla qui trasferisce a Symantec o ai suoi fornitori alcun diritto, titolo o interesse legale o equitativo sui Dati del cliente.
2.7 I Dati del cliente saranno memorizzati o archiviati durante il Periodo del Servizio, e per un periodo di centoventi (120) giorni dopo il Periodo del Servizio, o centoventi (120) giorni dopo la data di rescissione se il Servizio viene rescisso prima della scadenza del Termine (collettivamente, il "Periodo di conservazione successivo al termine"). Durante o prima del Periodo di conservazione successivo al termine, il Cliente dovrà richiedere per iscritto a Symantec di: (i) eliminare i dati del

Cliente senza alcun addebito (salvo diversa prescrizione disposta dalla legge o da una corte); o (ii) fornire una copia offline in formato PST tramite supporto su disco rigido alle tariffe in vigore di Symantec e a un volume non superiore a due (2) terabyte recapitati al mese fino alla completa restituzione al Cliente di tutti i Dati del cliente. Nel caso in cui il Cliente non fornisca istruzioni scritte a Symantec come stabilito nella frase precedente, Symantec eliminerà i Dati del cliente (salvo diversa prescrizione disposta dalla legge o da una corte) alla scadenza del Periodo di conservazione successivo al termine.

Appendice 17 – Symantec Endpoint Protection.cloud

1. Panoramica

1.1 Per ricevere il Servizio Symantec Endpoint Protection.cloud, il Cliente deve installare un agente sui computer degli utenti finali designati e assegnare la policy appropriata per l'utilizzo del Servizio. Il portale di gestione di Symantec Endpoint Protection.cloud è riservato all'amministratore per gestire computer, policy, avvisi e report ("Portale di gestione").

1.2 È possibile che il Cliente debba apportare alcune semplici modifiche al firewall per consentire all'agente di comunicare e funzionare con l'infrastruttura di Symantec Hosted Services.

1.3 Una volta che il servizio è stato configurato secondo le clausole 1.1 e 1.2, il Portale di gestione verrà utilizzato per gestire gli agenti.

1.4 Symantec pubblicherà un elenco dei sistemi operativi supportati per l'agente e dei browser supportati per il Portale di gestione. Il Cliente riconosce e accetta che Symantec può aggiornare e modificare periodicamente questo elenco senza preavviso.

1.5 L'agente sul computer:

1.5.1 Proteggerà il computer dai programmi malware rilevati in base ai metodi conosciuti come previsto dal servizio

1.5.2 Bloccherà attacchi nocivi conosciuti dalla rete verso il computer

1.5.3 Farà il possibile per fornire funzionalità antiphishing sui browser supportati che bloccheranno gli attacchi ritenuti phishing.

2. Portale di gestione

2.1 Il Portale di gestione consente al Cliente di configurare la sicurezza in base alle sue policy per gli agenti.

2.2 Il Cliente è responsabile dell'implementazione delle opzioni di configurazione in linea con la propria policy di utilizzo accettabile dei computer (o equivalente) tramite il Portale di gestione. Le policy vengono configurate sul gruppo di computer.

2.3 Le modifiche apportate alla policy sono visibili immediatamente nel Portale di gestione e vengono raggruppate per la trasmissione agli agenti. L'impostazione effettiva della policy sul singolo agente può essere visualizzata sul Portale di gestione o sull'agente in esecuzione nel computer dell'utente finale.

3. Registri e report

3.1 Tutti i registri e i report prodotti dall'agente sono archiviati sul Portale di gestione, dove possono essere consultati e scaricati per un periodo di dodici (12) mesi prima della loro eliminazione.

4. Notifiche

4.1 Il Cliente può configurare il Servizio Symantec Endpoint Protection.cloud per l'invio di una notifica automatica ai destinatari di e-mail configurati in base alla regola degli avvisi, configurabile sul Portale di gestione.

4.2 Il Cliente può creare, eliminare e personalizzare le notifiche sul Portale di gestione.

5. Supporto

5.1 Il supporto include:

5.1.1 Panoramica del Portale di gestione con una descrizione del servizio e una sessione di domande e risposte. (L'assistenza per l'impostazione delle policy o l'analisi della loro efficacia non sono incluse);

5.1.2 Manuale dell'amministratore;

5.1.3. Manuale dell'utente.

6. Riservatezza dei dati di Symantec Endpoint Protection.cloud

6.1 Il Cliente riconosce che i registri possono contenere informazioni di carattere personale e che la registrazione e acquisizione dei registri può pertanto comportare il trattamento di dati personali. Inoltre, il Cliente riconosce che Symantec Endpoint Protection.cloud è un servizio configurabile e che il Cliente è l'unico responsabile della configurazione di Symantec Endpoint Protection.cloud in base alla policy di utilizzo accettabile dei computer (o equivalente) e a tutte le leggi o normative vigenti. Pertanto, Symantec consiglia al Cliente di verificare sempre la legislazione locale prima di distribuire Hosted Endpoint Protection, e di assicurarsi che tutti i dipendenti conoscano e si attengano a tutte le responsabilità riguardanti le leggi e/o normative sulla protezione e la riservatezza dei dati correlate all'utilizzo di Symantec Endpoint Protection.cloud da parte del Cliente. In alcuni paesi può essere necessario ottenere il consenso di personale individuale prima di procedere all'acquisizione e registrazione dei dati. Il Cliente dovrà installare qualsiasi agente Symantec Endpoint Protection.cloud con un livello di personalizzazione minimo e ragionevole. Il Cliente riconosce e accetta che i dispositivi coperti dal Servizio Symantec Endpoint Protection.cloud (i) registrano le informazioni relative alle operazioni del Servizio Symantec Endpoint Protection.cloud (ii) che tali informazioni verranno trasmesse a Symantec allo scopo di fornire informazioni di gestione e reporting al Cliente, e (iii) il Cliente acconsente a tale registrazione e trasmissione. Symantec non accetta alcuna responsabilità riguardo eventuali responsabilità civili o penali a cui può andare incontro il Cliente che utilizza Hosted Endpoint Protection.

7. Configurazione

7.1 Se il Cliente ha acquistato il Servizio tramite un rivenditore Symantec, il Cliente autorizza espressamente tale rivenditore Symantec a (i) modificare la configurazione del Servizio con l'obiettivo di ottenere la funzionalità ottimale del Servizio stesso, e (ii) presentare le richieste di Supporto per conto del Cliente.

Appendice 18 – Servizio Symantec MessageLabs Web v2 Smart Connect.cloud ('Smart Connect')

1. **Panoramica**

1.1. Una volta che l'agente dell'utente in roaming è stato installato e le modifiche di configurazione pertinenti sono state apportate, le richieste di pagine Web e allegati vengono instradate elettronicamente tramite l'agente dell'utente al Servizio Symantec MessageLabs Web v2 URL.cloud ("Web v2 URL") e al Servizio Symantec MessageLabs Web v2 Protect.cloud ("Web v2 Protect") per essere sottoposte a un esame digitale.

2. **Descrizione del servizio**

2.1. Quando l'utente si connette a Internet nei paesi 'coperti dal servizio' designati, le richieste HTTP e FTP-over-HTTP esterne del Cliente compresi allegati, macro o file eseguibili vengono indirizzate tramite i servizi Web v2 URL e Web v2 Protect.

3. **Configurazione**

3.1. Le impostazioni di configurazione richieste per indirizzare questo traffico Web esterno al software agente dell'utente in roaming, e per inoltrare il traffico in entrata ai servizi Web v2 URL e Web v2 Protect, vengono eseguite e mantenute dal Cliente e dipendono dalle caratteristiche dell'infrastruttura tecnica del Cliente. Il Cliente deve installare un file PAC nel PC dell'Utente in modo che il browser, quando viene avviato, punti all'agente di roaming Symantec. In ClientNet è disponibile un modello di file PAC che può essere scaricato e modificato dal Cliente. Il Cliente deve assicurarsi che il traffico HTTP/FTP-over-HTTP interno (ad esempio, l'intranet aziendale) non sia indirizzato al software dell'agente di roaming.

3.2. L'accesso a Web v2 URL e Web v2 Protect è limitato ai sistemi autorizzati che contengono una versione valida del software dell'agente di roaming del Cliente e agli utenti autorizzati che sono stati attivati per questi servizi in ClientNet. L'agente software di roaming e le informazioni degli utenti autorizzati sono utilizzati per identificare il Cliente e selezionare in modo dinamico le impostazioni specifiche corrispondenti.

3.3. Le regole delle policy per il servizio Web v2 URL e la scansione dei contenuti per il servizio Web v2 Protect utilizzate nel servizio agente di roaming saranno le stesse applicate alle connessioni nelle posizioni di rete configurate, ad esempio, la LAN aziendale.

3.4. Il Cliente riconosce che l'agente di roaming sarà fornito con impostazioni predefinite di Symantec applicate fin dall'inizio che comprendono l'adozione di misure ragionevoli per instradare il traffico Web dell'utente verso un punto di accesso 'ottimale' dell'infrastruttura di servizio. Tale inoltro è basato sulla conoscenza della posizione dell'utente in roaming basata sull'indirizzo IP e sull'utilizzo di un database di localizzazione geografica di terze parti per identificare il paese dal quale l'utente si sta connettendo. Symantec instraderà gli utenti con la designazione di paese appropriata verso quello che è ritenuto il punto di accesso ottimale del servizio per il paese specificato. Ciò avrà luogo indipendentemente da qualsiasi valutazione delle probabili prestazioni della connessione del singolo utente finale e solo per i paesi per i quali Symantec è ritenuta in grado di fornire un livello di servizio accettabile.

Per tutti gli altri paesi al di fuori dei paesi di servizio accettabile, il Cliente riconosce che Symantec non sarà in grado di fornire le funzionalità del servizio Web v2 URL o Web v2 Protect. In queste situazioni, dopo avere stabilito che l'utente finale si trova in un paese 'non coperto dal servizio', l'agente di roaming non verrà aperto in modo che l'utente finale possa connettersi a Internet senza i vantaggi del servizio Symantec disponibili nei paesi con livello di servizio accettabile.

IL CLIENTE RICONOSCE E ACCETTA CHE IL TRAFFICO WEB DELL'UTENTE PUÒ ESSERE INDIRIZZATO A UN'INFRASTRUTTURA SITUATA IN UNA LOCALITÀ GEOGRAFICA ESTERNA ALL'UE PER ESSERE ELABORATO IN BASE ALLA PRESENTE CLAUSOLA 3.4. IL CLIENTE HA LA RESPONSABILITÀ DI OTTENERE TUTTI I PERMESSI E LE APPROVAZIONI RICHIESTE PER IL TRASFERIMENTO DI TALE TRAFFICO WEB. IL CLIENTE RICONOSCE E ACCETTA INOLTRE CHE SYMANTEC NON PUÒ ACCETTARE ALCUNA RESPONSABILITÀ PER QUALSIASI VIOLAZIONE CONSEGUENTE DELLA LEGGE O DELLE NORMATIVE VIGENTI.

4. **Termini di esportazione aggiuntivi per Smart Connect.cloud**

4.1 Il Cliente o il Partner non dovrà, e non dovrà permettere a terze parti, di vendere, rivendere, esportare, riesportare, cedere, deviare, distribuire, disporre, divulgare o gestire in altro modo la Tecnologia controllata, direttamente o indirettamente, in alcuno dei seguenti paesi: Afghanistan, Angola, Armenia, Azerbaijan, Bosnia ed Erzegovina, Burma, Burundi, Cina, Cuba, Repubblica Democratica del Congo, Eritrea, Etiopia, Iran, Iraq, Corea del Nord, Liberia, Libia, Nigeria, Ruanda, Sierra Leone, Somalia, Sudan, Siria, Tanzania, Uganda e Zimbabwe.

4.2 Il Cliente o il Partner non potranno cedere Web Roaming Agent a qualsiasi altra azienda o individuo che non sia dipendente del Cliente o del Partner tranne nei casi seguenti: (i) il Cliente o il Partner può cedere o consentire il download di Web Roaming Agent a propri subappaltatori terzi per essere utilizzato per conto del Cliente o del Partner; e/o (ii) il Cliente o il Partner può cedere o consentire il download di Web Roaming Agent a propri clienti finali ai quali rivende il Servizio Symantec, a condizione che il Cliente o il Partner comunichi a tali terze parti gli obblighi della presente Clausola.

Allegato 3
Contratto del Livello di Servizio

1. Definizioni

1.1. I seguenti termini avranno i seguenti significati per gli scopi del presente Contratto di Livello di Servizio:

"**Richiesta di Credito**" indica la notifica che il Cliente deve inviare a Symantec via E-mail all'indirizzo support@messagelabs.com con la riga dell'oggetto "Richiesta di Credito" (a meno che non sia altrimenti notificato da Symantec);

"**Cluster Tower Designato**" indica due (2) o più Tower, distribuite su un minimo di due (2) sedi, programmate per fornire il Servizio al Cliente;

"E-mail Falsa Positiva a Virus" indica un'E-mail legittima erroneamente indicata/marcata come contenente un Virus;

"**E-mail Services**" indica i Servizi E-mail AV, E-mail AS, E-mail IC, E-mail CC, Crittografia basata sulla Politica e Crittografia di Delimitazione;

"Virus Conosciuto" indica un Virus per il quale, al momento della ricezione da parte di Symantec: (i) sia già stata resa pubblicamente disponibile una firma per un minimo di una (1) ora per la configurazione di scanner commerciali di terzi usati da Symantec; o (ii) sia compresa nella "Wild List" che si trova presso http://www.wildlist.org e identificato come "In the wild" da almeno due partecipanti alla Wild List.

"Tracker Symantec" indica uno strumento di Symantec con cui vengono misurate Disponibilità del Servizio e Latenza del Servizio;

"**Costo mensile**" indica il costo mensile per i Servizi coinvolti, come indicato in dettaglio nel Contratto;

"**Livello di Servizio**" indica ciascuno dei parametri di Servizio definiti nel Contratto del Livello di Servizio;

"Falso Negativo Spam" indica un'E-mail Spam che non viene identificata come Spam;

"Falso Positivo Spam" indica un'E-mail legittima erroneamente indicata/contrassegnata come Spam;

"Impostazioni Raccomandate Spam" indica le linee guida di configurazione di migliori prassi di Symantec per il Servizio E-mail AS; e

"Tower" indica una serie di server a carico bilanciato;

"**Servizi Web**" indica i Servizi Web v2 Protect e Web v2 URL collettivamente.

2. Clausole generali

2.1. Nel caso in cui il Cliente ritenga di avere diritto a un'indennità in conformità con il presente Contratto di Livello di Servizio, il Cliente deve inviare una Richiesta di Credito entro dieci (10) giorni lavorativi dalla fine del mese di calendario in questione. Il Cliente riconosce che le registrazioni vengono mantenute esclusivamente per un numero limitato di giorni, e, di conseguenza, qualunque Richiesta di Credito inviata al di fuori del tempo indicato sarà considerata non valida.

2.2. Tutte le Richieste di Credito saranno soggette a verifica da parte di Symantec, in conformità con le disposizioni applicabili del presente Contratto di Livello di Servizio.

2.3. Il presente Contratto di Livello di Servizio non è in vigore: (i) nel corso di periodi di Manutenzione Programmata o di manutenzione di emergenza, nei periodi di non disponibilità causati da forza maggiore o atti od omissioni del Cliente o di terzi; (ii) nel corso di periodi di sospensione del servizio di Symantec, in conformità con i termini del Contratto; (iii) laddove il Cliente violi il Contratto (compreso senza limitazione nel caso il Cliente abbia fatture scadute); (iv) in relazione a qualsiasi e-mail che non è passata attraverso il Servizio (compreso senza limitazione il caso in cui il Cliente non abbia impostato il proprio router per puntare tutto il traffico di e-mail verso Symantec); o (v) in relazione a qualsiasi E-mail in entrata o in uscita che è stata inviata inizialmente a Symantec con più di 500 destinatari per sessione SMTP.

2.4. Le indennità indicate nel Contratto di Livello del Servizio saranno l'unico ed esclusivo rimedio del Cliente per contratto, per atti illeciti (compresa, senza limitazioni, la negligenza) o altrimenti in relazione a tutti i livelli di Servizio.

2.5. La responsabilità massima cumulativa di Symantec, in conformità con il presente Contratto di Livello di Servizio nel corso di un mese di calendario, non sarà superiore al cento percento (100%) del Costo Mensile pagabile dal Cliente per il/i Servizi/o coinvolti.

2.6 Laddove il Servizio coinvolto faccia parte di un bundle di Servizi non divisibile:

a) al fine di calcolare i crediti di servizio, il Costo Mensile del Servizio interessato sarà calcolato come costo mensile totale del bundle di Servizio non divisibile diviso per il numero di Servizi costitutivi che costituiscono tale bundle; e

b) se il Cliente termina il Servizio interessato in conformità con il presente Contratto di Livello di Servizio, il costo riconteggiato del bundle di Servizio non divisibile sarà calcolato come il costo mensile totale originale per il bundle di Servizio non divisibile, diviso per il numero originale di Servizi costitutivi che fanno parte di tale bundle, e moltiplicato per il numero di Servizi costituenti rimanenti che fanno parte di tale bundle.

2.7 I Livelli di Servizio per i Servizi E-mail non si applicano al Servizio EC e, di conseguenza, i Livelli di Servizio per i Servizi E-mail nelle Clausole dalla 3 alla 5 riportate di seguito saranno sospesi nel corso di qualunque periodo in cui il Servizio di EC sia in stato attivato.

3. Disponibilità al 100% del Servizio

3.1 Il Livello di Servizio della Disponibilità del Servizio sarà in funzione solo se il Cliente utilizza uno o più Servizi E-mail o Servizi Web.

3.2 In relazione ai Servizi E-mail, il presente Livello di Servizio di Disponibilità di Servizio indica la capacità di stabilire una sessione SMTP sulla porta 25 del Cluster Tower Designato, come misurato dal Tracker di Symantec. Questo Livello di Servizio si applica esclusivamente al Cluster Tower Designato in grado di:

3.2.1 ricevere le E-mail in arrivo del Cliente per conto del dominio del Cliente, 24 ore su 24, 7 giorni su 7; e

3.2.2 accettare le E-mail in uscita del Cliente con un host SMTP Cliente configurato per conto del/dei domini/o del Cliente 24 ore su 24, 7 giorni su 7.

3.3 Relativamente ai Servizi Web, il presente Livello di Servizio dellaDisponibilità di Servizio indica la disponibilità dei Servizi Web ad accettare le richieste web in uscita del Cliente e sarà in vigore esclusivamente se l'host del Cliente, i dispositivi gateway o proxy sono configurati correttamente 24 ore su 24, 7 giorni su 7.

3.4 Se nel corso di un mese di calendario la Disponibilità del Servizio sarà inferiore al cento percento (100%), il Cliente può avere diritto alla seguente percentuale di credito:

Disponibilità di Servizio Percentuale per mese di calendario	Credito percentuale del Costo Mensile
< 100% ma >= 99%	25
< 99% ma >= 98,0%	50
< 98,0%	100 e termine del Servizio coinvolto a discrezione del Cliente

3.5 Nel caso in cui la Disponibilità del Servizio sia inferiore al novantotto percento (98%), nel corso di qualunque mese di calendario, il Cliente avrà diritto di terminare il Servizio coinvolto immediatamente e di ricevere un rimborso pro rata dei costi pagati in anticipo per il Servizio in questione per il periodo successivo alla rescissione.

4. Consegna E-mail 100%

4.1 Il presente Livello di Servizio di Consegna E-mail funzionerà esclusivamente se il Cliente utilizza uno o più dei Servizi E-mail.

4.2 Symantec consegnerà il 100% delle E-mail inviate dal o al Cliente alle seguenti condizioni:

4.2.1 l'E-mail deve essere stata ricevuta dal Cluster Tower Designato del Cliente; e

4.2.2 l'E-mail non deve contenere Virus, Spam o altro contenuto che la abbia fatta bloccare dai Servizi E-mail.

4.3 Fatto salvo quanto indicato alle precedenti Clausole 4.1 e 4.2, e nel caso in cui Symantec non consegnasse un'E-mail al Cliente e il Cliente non avesse violato i termini del Contratto, il Cliente avrà diritto a terminare i Servizi E-mail con una notifica scritta con trenta (30) giorni di anticipo.

5. Latenza E-mail - 60 secondi

5.1. Fatto salvo quanto indicato alla Clausola 5.2, il presente Livello di Servizio di Latenza E-mail sarà in funzione solo se il Cliente utilizza uno o più dei Servizi E-mail.

5.2. Il presente Livello di Servizio di Latenza E-mail **non**si applicherà al Servizio di Crittografia Basata sulla Politica.

5.3. Se, nel corso di qualunque mese di calendario, il tempo medio di consegna (come misurato dal Tracker di Symantec), per le E-mail inviate ogni 5 minuti dalla e alla Tower dei Servizi E-mail all'interno del Cluster Tower Designato dal Cliente, saràsuperiore ai ritardi indicati nella tabella riportata di seguito, il Cliente potrà inviare una Richiesta di Credito in conformità con la tabella seguente:

Tempo medio di consegna del 100% delle misurazioni (in minuti e secondi)	Credito percentuale del Costo Mensile
> 1 min ma <= 1 min 30 sec	25
> 1 min 30 sec ma <= 2 min	50
> 2 min ma <= 2 min 30 sec	75
> 2 min 30 sec	100

5.4. Il presente Livello di Servizio di Latenza E-mail non sarà in funzione:
5.4.1. Se il Cliente non ha fornito a Symantec una lista di indirizzi E-mail specifici per ricevere il Servizio (la "Lista di Convalida") e il Cliente subisce un attacco del tipo Denial of Service;
5.4.2. Nel corso dei periodi di ritardo causati da un loop di mail dai/ai sistemi del Cliente.

6. Latenza Web - 0,1 secondi

6.1 Il presente Livello di Servizio di Latenza Web funzionerà esclusivamente se il Cliente utilizza uno o più Servizi Web.
6.2. Se il tempo di scansione medio di un contenuto Web, misurato da quando Symantec riceve il contenuto al punto di tentata trasmissione del contenuto di Symantec, calcolato nel corso di un mese di calendario, è inferiore al 100%, secondo la tabella riportata di seguito, il Cliente può inviare una Richiesta di Credito:

Percentuale media della scansione di contenuto web all'interno di 100 millisecondi	Credito percentuale del Costo Mensile
< 100% ma >= 99%	25
< 99% ma >= 98%	50
< 98% ma >= 97%	75
< 97%	100 e rescissione dal Servizio coinvolto a discrezione del Cliente

6.3 Il presente Livello di Servizio di Latenza Web si applica solo a oggetti di 1 MB o inferiori.

7. Spam - Falsi Positivi 0,0003%

7.1. Il presente Livello di Servizio Falsi Positivi Spam funziona solo se il Cliente utilizza il Servizio Anti Spam E-mail e implementa le Impostazioni Raccomandate Spam di Symantec.
7.2. Laddove il tasso di Falso Positivo Spam sia superiore allo 0,0003%, per tutto il traffico E-mail del Cliente nel corso di qualunque mese di calendario, il Cliente può avere diritto a un credito in conformità con la seguente tabella:

Tasso di Falso Positivo Spam percentuale nel corso del mese di calendario	Credito percentuale del Costo Mensile
>0,0003 ma <= 0,003	25
> 0,003 ma <= 0,03	50
>0,03 ma <= 0,3	75
>0,3	100

7.3. Le seguenti E-mail non costituiranno E-mail Falso Positivo Spam per gli scopi del Livello di Servizio:
7.3.1. E-mail che non costituiscono E-mail commerciali legittime;
7.3.2. E-mail con più di 20 destinatari;
7.3.3. Laddove il mittente dell'E-mail si trovi nella lista di mittenti bloccati del Cliente, compreso, senza limite alcuno, quelli definiti dall'Utente individuale se il Cliente ha abilitato le impostazioni a livello di Utente;
7.3.4. E-mail inviate da un macchinario compromesso;
7.3.5. E-mail inviate da un macchinario che si trovi su una lista di blocco di una terza parte;
7.3.6. E-mail che sono state inviate a più di 20 destinatari (in una singola operazione o in una serie di operazioni) e che abbiano almeno l'80% di contenuto uguale.

8. Tasso di blocco di Spam 99%

8.1. Il presente Livello di Servizio di blocco di Spam funziona solo se il Cliente utilizza il Servizio E-mail Anti Spam e implementa le Impostazioni Raccomandate Spam. Le disposizioni della presente Clausola 8 corrispondono al numero di Falsi Negativi Spam misurati in un mese.
8.2. Il Cliente può avere diritto a un credito in conformità con la tabella seguente:

Tasso di blocco di Spam percentuale nel corso del mese di calendario	Credito percentuale di Costo mensile
>98% - <= 99%	25
> 97% - <= 98%	50
> 96% - <= 97%	75
< 96%	100

8.3. Questo Livello di Servizio di blocco di Spam non funzionerà qualora le E-mail non siano state inviate a un indirizzo legittimo.
8.4 Alle E-mail contenenti caratteri asiatici si applicherà un tasso di blocco di Spam del 95%. Nel caso in cui tale tasso di blocco di Spam fosse inferiore al 95%, il Cliente avrà diritto a un credito del 25% del Costo Mensile. Nel caso in cui il tasso di blocco di Spam sia inferiore al 90%, il Cliente avrà diritto a un credito del 100% del Costo Mensile.

9. Richieste di Credito per Servizio Spam

9.1. Per avere diritto al credito, in conformità con le Clausole 7 e 8, il Cliente deve inviare le E-mail False Positive o False Negative all'indirizzo support@Symantec.com entro 5 giorni dalla ricezione dell'E-mail. Symantec eseguirà indagini e confermerà se l'E-mail sia un Falso Positivo Spam o un Falso Negativo Spam e documenterà quanto scoperto. Al termine del mese di calendario, se il Cliente ritiene che il numero di Falsi Positivi Spam o Falsi Negativi Spam confermati gli conferisca il diritto di ricevere un credito ai sensi della tabella precedente, il Cliente dovrà inviare una Richiesta di Credito a Symantec in conformità con la Clausola 2.1 del presente Allegato.

10. Protezione da Virus E-mail - 100%

10.1 Il presente Livello di Servizio di Protezione da Virus E-mail funzionerà solamente se il Cliente utilizza il Servizio Anti Virus E-mail.
10.2 Nel caso in cui i sistemi del Cliente fossero infetti da uno o più Virus, nel corso di un mese di calendario, come notificato a Symantec in una chiamata di supporto validata e soggetta a registrazione, a conferma che un Virus sia stato passato al Cliente attraverso il Servizio E-mail AV, il Cliente può fatturare a Symantec i danni liquidati per un importo pari al 100% del Costo Mensile esistente al momento, oppure £5.000/€10.000 (in base alla valuta di fatturazione per quel Cliente), a seconda di quale sia l'importo inferiore. Il rimedio indicato nella presente Clausola 10.2 sarà l'unico ed esclusivo rimedio ai sensi del contratto per atti illeciti (compresa, senza limitazioni, la negligenza) o altrimenti per qualunque infezione di Virus passata al Cliente o a una terza parte tramite il Servizio. Per evitare qualunque dubbio, il rimedio indicato nella presente Clausola 10.2 non si applicherà nei caso di auto-infezione eseguita volontariamente.
10.3. I sistemi del Cliente sono considerati infetti se un Virus contenuto in un'E-mail ricevuta attraverso il Sistema E-mail AV è stato attivato all'interno dei sistemi del Cliente o automaticamente o per mezzo di intervento manuale.
10.4. Nel caso in cui Symantec rilevi ma non fermi un'E-mail infetta da Virus, Symantec avvertirà immediatamente il Cliente, fornendo informazioni a sufficienza per consentire al Cliente di identificare e cancellare l'E-mail infetta dal Virus. Se tale notifica garantirà la prevenzione di un'infezione, il rimedio indicato nella precedente Clausola 10.2 non sarà applicabile. La mancata azione tempestiva del Cliente a seguito di tale informazione invaliderà il Livello di Servizio contenuto nella precedente Clausola 10.2.
10.5. Il Servizio E-mail AV scansionerà il più possibile le E-mail e gli allegati. Potrebbe non essere possibile scansionare gli allegati con contenuti sotto il diretto controllo del mittente (ad es., allegati protetti da password e/o crittografati). Tali E-mail e/o allegati sono esclusi dal Livello di Servizio della precedente Clausola 10.2.
10.6. Il presente Livello di Servizio Protezione E-mail da Virus non funzionerà in relazione a Virus che siano stati rilasciati intenzionalmente dal Cliente.

11. E-mail con Virus Falsi Positivi 0,0001%

11.1 Il presente Livello di Servizio Falso Positivo E-mail con Virus funzionerà esclusivamente se il Cliente utilizza il Servizio Anti Virus E-mail.
11.2. Laddove il tasso di Falso Positivo E-mail con Virus sia superiore allo 0,0001%, rispetto a tutto il traffico E-mail del Cliente nel corso di un mese di calendario, il Cliente potrebbe avere diritto a un credito in conformità con la tabella seguente:

Tasso percentuale di Falsi Positivi E-mail con Virus nel corso del mese di calendario	Credito percentuale del Costo Mensile
>0,0001 ma <= 0,001	25
> 0,001 ma <= 0,01	50
>0,01 ma <= 0,1	75
>0,1	100

12. Protezione Web da Virus - Conosciuto al 100%

12.1 Il presente Livello di Servizio Protezione Web da Virus funzionerà esclusivamente se il Cliente utilizza il Servizio Web v2 Protect.
12.2. Nel caso in cui i sistemi del Cliente dovessero essere infetti da uno o più Virus Conosciuti nel corso di un mese di calendario, come notificato a Symantec in una chiamata di supporto validata e soggetta a registrazione, compresi i dettagli dell'URL dal quale è stato scaricato l'articolo, a conferma che un Virus Conosciuto sia stato passato al Cliente attraverso il Servizio Web v2 Protect, il Cliente può fatturare a Symantec i dati liquidati pari al 100% del Costo Mensile in essere al quel momento, o £5.000/€10.000 (in base alla valuta di fatturazione del Cliente), a seconda di quale sia inferiore. Il rimedio indicato nella presente Clausola 12.2 sarà il solo ed esclusivo rimedio per contratto, per atti illeciti (compresa, senza limiti alcuno, la negligenza) o altrimenti in merito a qualunque infezione da Virus Conosciuto passato al Cliente o a una terza parte attraverso il Sistema Web v2 Protect. Per evitare tutti i dubbi, il rimedio indicato nella presente Clausola 12.2 non si applicherà nei casi di auto-infezione o download volontario di un codice nocivo noto da parte del Cliente.
12.3 I sistemi del Cliente sono considerati infetti se un Virus Conosciuto, contenuto in una transazione web ricevuta attraverso il

Servizio Web v2 Protect, è stato attivato all'interno dei sistemi del Cliente o automaticamente o tramite intervento manuale.
12.4 Nel caso in cui Symantec rilevi ma non fermi un Virus Conosciuto, come parte di una transazione sul web, attraverso il Servizio Web v2 Protect di Symantec, Symantec avvertirà immediatamente il Cliente, fornendo informazioni sufficienti per consentire al Cliente di identificare e cancellare l'articolo. Se tale notifica porta alla prevenzione dell'infezione, il rimedio indicato nella precedente Clausola 12.2 non sarà applicabile. La mancata azione tempestiva del Cliente a seguito di tale informazione invaliderà il Livello di Servizio contenuto nella precedente Clausola 12.2.
12.5. Il Servizio Web v2 Protect scansionerà quanti più articoli web possibili. Potrebbe non essere possibile scansionare gli articoli che siano contenuti o inseriti per scopi comunicativi attraverso i Protocolli Web supportati (HTTP, e FTP su HTTP), trasferiti sugli HTTPS, compressi o modificati dalla forma originale per la distribuzione, soggetti a protezione della licenza del prodotto, download o update, o i contenuti che siano sotto il diretto controllo del mittente (ad es., articoli protetti da password e/o crittografati). Tali articoli e/o allegati sono esclusi dal Livello di Servizio nella Clausola 12.2.

13. Supporto tecnico e risposta ai guasti 24 ore su 24, 7 giorni su 7

13.1 Ventiquattro (24) ore al giorno, sette (7) giorni alla settimana, Symantec:
a) fornirà supporto tecnico al Cliente in caso di problemi con il Servizio; e
b) interagirà con il Cliente al fine di risolvere tali problemi.
13.2 Qualora un Cliente presenti un problema, un guasto o una richiesta, per l'ottenimento di informazioni di servizio telefonicamente o via e-mail da Symantec, il livello di priorità verrà stabilito e la risposta sarà fornita in base alle definizioni riportante nella tabella in basso:

Livello di priorità	Definizioni	Target della risposta
Critico	Perdita di Servizio	95% delle chiamate ricevono risposta entro 2 ore
Grave	Perdita parziale di Servizio o danneggiamento del Servizio	85% delle chiamate ricevono risposta entro 4 ore
Minimo	Richiesta di informazione che potenzialmente influisce sul Servizio o non influisce sul Servizio	75% delle chiamate ricevono risposta entro 8 ore

13.3 I guasti che hanno origine da azioni del Cliente o che richiedono le azioni di altri fornitori di servizi sono al di fuori del controllo di Symantec e come tali sono specificatamente esclusi dai tempi di risposta citati nella precedente Clausola 13.2
13.4 Fatto salvo quanto indicato nella Clausola 13.3, se il Cliente ritiene di aver sofferto un ritardo nella risposta di Symantec a una richiesta (al di fuori dei parametri definiti nella precedente Clausola 13.2), può aver diritto a un credito. Le Richieste di Credito devono indicare l'ora, la data e il numero di registrazione dell'incidente. Se idoneo, il Cliente riceverà l'accredito ai sensi della seguente tabella:

Priorità	Mancata conformità con il target	Credito percentuale di Costo mensile
Critico	Più di una volta nel corso di un mese di calendario	15
Grave	Più di due volte nel corso di un mese di calendario	10
Minimo	Più di tre volte nel corso di un mese di calendario	5

14. Servizio di Archiviazione (P)

14.1 Le disposizioni della presente Clausola 14 si applicano esclusivamente al Servizio di Archiviazione (P).

14.1 Disponibilità del Servizio di Archiviazione (P)

14.1.1 Il Servizio di Archiviazione (P) sarà Disponibile al 99,9% per ciascun mese di calendario, ad eccezione delle finestre di Manutenzione Programmata e di manutenzione di emergenza. In tale caso, "Disponibile" indica il momento in cui l'infrastruttura offerta da Symantec è pronta ad accettare e archiviare E-mail. Per gli scopi del calcolo della non disponibilità si applicano i seguenti criteri: a) la misurazione sarà eseguita dai sistemi di monitoraggio di Symantec (tali misurazioni possono essere fornite al Cliente su richiesta scritta), b) il monitoraggio avrà luogo in intervalli di 5 minuti con due guasti successivi necessari per essere considerato un periodo di interruzione, c) solo l'infrastruttura offerta da Symantec sarà misurata, e tale misurazione escluderà qualunque non disponibilità come risultato di un periodo di interruzione dell'Applicazione di Archiviazione E-mail, periodo di interruzione della rete del Cliente o periodo di interruzione di Internet.
14.1.2 Per ogni uno (1) percento o parte dello stesso di non disponibilità oltre la disponibilità target del 99,9%, in conformità con la presente Clausola 14.1 nel corso del mese di calendario in questione, il Cliente avrà diritto a un credito equivalente al dieci percento (10%) dei costi mensili dovuti a Symantec in relazione al Servizio di Archiviazione (P), fatto salvo un massimo del 100% dei costi mensili dovuti in relazione al Servizio di Archiviazione (P) per qualunque mese di calendario. Il Cliente può rescindere dal Servizio di Archiviazione (P) a sua esclusiva opzione se in qualunque momento tale disponibilità sia inferiore al novanta percento (90%) nel corso di un mese di calendario.

14.2 Servizio di Archiviazione (P) - Livello di Servizio di Applicazione

14.2.1 Se un'Applicazione di Archiviazione E-mail si guasta nel corso del periodo di garanzia per ragioni coperte dalla Garanzia Limitata di Symantec (come definito nella documentazione ricevuta dall'Applicazione di Archiviazione E-mail), Symantec lavorerà, senza costi per il Cliente, con il Cliente per risolvere il problema dell'Applicazione di Archiviazione E-mail (che può richiedere accesso VPN all'Applicazione di Archiviazione E-mail) entro quattro (4) ore dalla ricezione della notifica del problema dal Cliente nel corso del Normale Orario Lavorativo e entro otto (8) ore dalla ricezione della notifica del problema al di fuori del Normale Orario Lavorativo. Entro venti (20) ore del Normale Orario Lavorativo dalla ricezione delle notifica del problema, Symantec dovrà:
14.2.1.1 avvertire il Cliente che l'Applicazione di Archiviazione E-mail sta funzionando in modo appropriato e che il problema non ha avuto origine dall'Applicazione di Archiviazione E-mail o dal Software; o
14.2.1.2 riparare l'Applicazione di Archiviazione E-mail con hardware e/o software; o
14.2.1.3 notificare al Cliente che è necessaria un'Applicazione di Archiviazione E-mail sostitutiva; oppure
14.2.1.4 se Symantec non è in grado di riparare o sostituire l'Applicazione di Archiviazione E-mail, risarcire i costi mensili per il Servizio di Archiviazione (P) per il Periodo attuale e rescindere dal Servizio di Archiviazione (P).
14.2.2 Nel caso in cui Symantec fosse obbligato, in conformità con la precedente Clausola 14.2.1.3, a fornire un'Applicazione di Archiviazione E-mail sostitutiva, Symantec consegnerà tale Applicazione di Archiviazione E-mail sostitutiva alla sede del Cliente entro quarantotto (48) ore del Normale Orario Lavorativo, dal momento della notifica di Symantec al Cliente della necessità di una nuova Applicazione di Archiviazione E-mail.
14.2.3 Nel caso in cui Symantec fosse obbligato, in conformità con le precedenti Clausole 14.2.1.2 e 14.2.1.3, a riparare o sostituire l'Applicazione o Software di Archiviazione E-mail e non lo facesse entro i tempi indicati nelle Clausole 14.2.1 e 14.2.2, Symantec rimborserà al Cliente il cinque percento (5%) dei costi mensili per il Servizio di Archiviazione (P) per ciascun giorno di ritardo successivo a tale tempistica.
14.2.4 I termini precedenti della presente Clausola 14.2 saranno il solo ed esclusivo rimedio del Cliente per quanto riguarda qualunque difetto o violazione della garanzia relativamente all'Applicazione di Archiviazione E-mail.

15. Servizio di EC

15.1 Le disposizioni della presente Clausola 15 si applicano esclusivamente al Servizio di EC.
15.1.1 EC sarà Disponibile al 99,9% per ciascun mese di calendario, ad eccezione delle finestre di Manutenzione Programmata e manutenzione di emergenza. In tal caso, "Disponibile" vuol dire che l'infrastruttura offerta da Symantec è pronta per sincronizzare il sistema chiave e le informazioni Utente. Per gli scopi del calcolo della non disponibilità si applicano i seguenti criteri: a) la misurazione sarà eseguita dai sistemi di monitoraggio di Symantec (tali misurazioni possono essere fornite al Cliente su richiesta scritta), b) solo l'infrastruttura offerta da Symantec sarà misurata, e tale misurazione esclude qualunque non disponibilità come risultato di un periodo di interruzione della rete del Cliente, periodo di interruzione di terzi problemi DNS al di fuori del diretto controllo di Symantec.
15.1.2 Per ogni un (1) percento, o parte dello stesso, di non disponibilità oltre la disponibilità target del 99,9%, in conformità con la presente Clausola 15.1 del mese di calendario in questione, il Cliente avrà diritto a un credito equivalente al dieci percento (10%) dei costi mensili dovuti a Symantec in relazione al Servizio EC, fatto salvo un massimo del 100% dei costi mensili dovuti, in relazione al Servizio EC per qualunque mese di calendario. Il Cliente può rescindere dal Servizio EC a sua esclusiva opzione se in qualunque momento tale disponibilità sia inferiore al novanta percento (90%) nel corso di un mese di calendario.

16. Servizio Symantec Email Continuity Archive.cloud o Symantec Email Continuity Archive Lite.cloud

16.1 Le disposizioni della presente Clausola 16 si applicano esclusivamente al Servizio di Symantec Email Continuity Archive.cloud e di Symantec Email Continuity Archive Lite.cloud.
16.1.1 I Servizi di Symantec Email Continuity Archive.cloud e di Symantec Email Continuity Archive Lite.cloud saranno disponibili al 99,95% per ciascun mese di calendario. La disponibilità sarà calcolata dividendo il numero totale di ore in cui il Servizio di Symantec Email

Continuity Archive.cloud e di Symantec Email Continuity Archive Lite.cloud (come applicabile) è risultato non disponibile (ad eccezione dei periodo di interruzione della rete Cliente, di manutenzione o di problemi DNS al di fuori del diretto controllo di Symantec) per il numero totale di ore disponibili programmate del Servizio di Symantec Email Continuity Archive.cloud e di Symantec Email Continuity Archive Lite.cloud (come applicabile) nel mese di calendario in questione.
16.1.2 Per ciascuno un (1) percento di non disponibilità, al di fuori del target di disponibilità del 99,95% in conformità con la presente Clausola 16 nel mese di calendario in questione, il Cliente avrà diritto a un credito equivalente ai costi pagati a Symantec in relazione al Servizio di Symantec Email Continuity Archive.cloud e di Symantec Email Continuity Archive Lite.cloud (come applicabile) per un giorno del Servizio di Symantec Email Continuity Archive.cloud o Symantec Email Continuity Archive Lite.cloud.

17. Symantec EV.cloud

17.1 Symantec garantirà il 99,99% di disponibilità del server per EV.cloud. Se la disponibilità del server nell'arco di un mese di calendario scende al di sotto del 99,99%, Symantec emetterà un accredito al Cliente come previsto di seguito:

Disponibilità del server	Accredito percentuale della tariffa mensile
Dal 99,9% al 99,98%	5% della tariffa mensile
Dal 98,0% al 99,8%	10% della tariffa mensile
Dal 95,0% al 97,9%	15% della tariffa mensile
Dal 90,0% al 94,9%	25% della tariffa mensile
89,9% o meno	2,5% della tariffa mensile per ogni 1% di disponibilità mancata fino a un massimo del 100% della tariffa mensile

17.2 Le richieste di accredito devono comprendere le date e gli orari di mancata disponibilità del server. Symantec confronterà le informazioni sulla mancata disponibilità del server fornite dal Cliente con i dati di monitoraggio della disponibilità del server mantenuti da Symantec. Se la mancata disponibilità del server rientra nei criteri della tabella alla Clausola 17.1 precedente, verrà emesso un accredito. L'accredito descritto in questa Clausola 17.2 costituirà l'unico ed esclusivo rimedio del Cliente in relazione a qualsiasi mancata disponibilità del server. La mancata disponibilità del server a fini di manutenzione è esclusa dai calcoli della disponibilità.

18. Symantec Endpoint Protection.cloud

18.1 Le disposizioni della presente Clausola 18 si applicano solo al Servizio Symantec Endpoint Protection.cloud.
18.1.1 Symantec Endpoint Protection.cloud sarà disponibile al 100% di ogni mese civile, esclusi i periodi di Manutenzione pianificata e di manutenzione di emergenza. In questo caso, la definizione di "Disponibile" indica che l'infrastruttura in hosting di Symantec è pronta per sincronizzare le informazioni delle policy. Ai fini del calcolo della non disponibilità avranno valore i seguenti criteri: a) la misurazione sarà eseguita dai sistemi di monitoraggio di Symantec (tale misurazione può essere fornita al Cliente previa richiesta scritta), b) verrà misurata solamente l'infrastruttura in hosting di Symantec e tale misurazione esclude qualsiasi non disponibilità derivante da un'interruzione della rete del Cliente, da un'interruzione di terze parti o da problemi DNS al di fuori del controllo diretto di Symantec.
18.1.2 Per ogni uno (1) percento o relativa parte di non disponibilità oltre l'obiettivo di disponibilità del 99,9% ai sensi della presente Clausola 18.1 nel mese civile in questione, il Cliente avrà diritto a un credito equivalente al dieci percento (10%) della tariffa mensile dovuta a Symantec in relazione al Servizio Hosted Endpoint Protection, subordinato a un massimo del 100% della tariffa mensile dovuta in relazione al Servizio Symantec Endpoint Protection.cloud Service in qualsiasi mese civile. Il Cliente può scegliere di rescindere il Servizio Symantec Endpoint Protection.cloud se in qualsiasi momento tale disponibilità scende al di sotto del novanta percento (90%) in qualsiasi mese civile.
18.1.3 Il credito descritto nella Clausola 18.1.2 costituirà l'unico ed esclusivo rimedio del Cliente in relazione a qualsiasi mancata disponibilità del server per il Servizio Endpoint Protection.cloud. I Livelli di servizio nelle Sezioni 3.1, 3.4 e 11.1 del presente Contratto di servizio non si applicano al Servizio Symantec Endpoint Protection.cloud.