



## **Sicurezza e disponibilità dell'e-mail**

Come garantire la protezione e la disponibilità delle informazioni e dei sistemi di e-mail riducendo il costo di proprietà

Chris Miller  
Director of Product Management  
Symantec Network and Gateway Solutions



# Sicurezza e disponibilità dell'e-mail

## Indice generale

<b>Introduzione</b> .....	<b>4</b>
<b>Che cosa è il concetto di sicurezza e disponibilità dell'e-mail?</b> .....	<b>5</b>
<b>Fattori trainanti per la sicurezza e disponibilità dell'e-mail</b> .....	<b>6</b>
<b>Sicurezza e disponibilità dell'e-mail: come gestire in modo efficiente dati e sistemi</b> .....	<b>7</b>
Fase 1 – Sicurezza .....	8
Fase 2 – Archiviazione .....	13
Fase 3 – Realizzazione di una base resistente .....	16
<b>Introduzione della sicurezza e disponibilità dell'e-mail di Symantec</b> .....	<b>18</b>
Sicurezza dell'e-mail .....	18
Disponibilità per mezzo dell'archiviazione .....	23
Soluzione di Symantec per un sistema di e-mail resistente .....	24
<b>Conclusioni</b> .....	<b>30</b>

### Introduzione

La posta elettronica ha trasformato il modo di lavorare nelle aziende, influenzando radicalmente il modo di scambiare opinioni, idee, proposte e informazioni, nonché la velocità e l'efficienza con cui è possibile condurre gli affari. Nella nostra vita personale e lavorativa l'e-mail ha conquistato un'importanza pari, se non superiore, a quella del telefono.

Oltre a costituire un efficace mezzo di comunicazione, consentendo di interagire quasi in tempo reale con una o più persone contemporaneamente, è diventata di fatto la documentazione delle transazioni e delle operazioni interne di un'azienda. Allo stesso tempo, è diventata un veicolo per minacce e problemi che spesso mettono a repentaglio l'effettiva vitalità e redditività di un'azienda.

Nel corso degli ultimi dieci anni, l'e-mail si è evoluta da veicolo di comunicazione alternativo a strumento centrale da cui dipende la maggior parte delle applicazioni strategiche. Secondo Enterprise Strategy Group, più del 75% della proprietà intellettuale delle aziende è memorizzata nelle e-mail. Il fatto che l'e-mail svolga anche la funzione di documentazione dettagliata delle transazioni per un'azienda la rende preziosa come prova in ambito legale, dimostra che le aziende stanno seguendo le normative e fornisce una fonte per identificare le violazioni delle politiche aziendali interne. Il risultato è che un numero crescente di aziende sta decidendo di conservare le e-mail per periodi più lunghi e di verificare che in questo arco temporale non vengano modificate, sia perché ciò è imposto da normative o semplicemente per rispettare linee guida di regolamentazione interna. Questa tendenza ha anche aumentato i costi di archiviazione dei messaggi di e-mail e la complessità di gestione del ciclo di vita delle e-mail.

Dall'altro lato, gli elementi che rendono preziosa l'e-mail per un'organizzazione contribuiscono anche esporla a un elevato numero di rischi e svantaggi. Grazie alle sue caratteristiche di ubiquità e semplicità, è diventata il metodo preferito per trasmettere:

- Qualsiasi tipo di dati tra utenti, compresi contenuti non correlati al lavoro come file multimediali ed eseguibili o anche informazioni riservate all'esterno dell'azienda
- Minacce e problemi a migliaia di utenti, come virus e spamming, in modo assolutamente anonimo e poco costoso

Conseguentemente, vengono spese innumerevoli ore, budget e risorse nella difesa dei sistemi di e-mail e nello sforzo di garantirne un funzionamento efficiente. I professionisti IT tendono a porre l'attenzione su problemi della sicurezza quali la riduzione dello spamming o il blocco dei virus e su problemi di disponibilità quali la necessità garantire l'accesso in qualsiasi

momento ad applicazioni, sistemi e dati di e-mail. Tuttavia, se da una parte continua ad allungarsi la lista degli elementi necessari per gestire con maggiore efficienza ed efficacia volumi di e-mail in continua crescita, dall'altra i settori IT devono cercare un approccio più olistico per equilibrare i costi e i rischi associati a questa funzione. In situazioni quali la migrazione a nuovi server di e-mail o il consolidamento dei server di messaggistica, le organizzazioni hanno l'opportunità di rivedere i sistemi correnti e i piani per realizzare un'infrastruttura di e-mail che sia flessibile per rispondere a un ambiente IT in continua evoluzione. Il concetto di sicurezza e disponibilità dell'e-mail di Symantec può contribuire alla realizzazione di questo obiettivo.

### **Che cosa è il concetto di "sicurezza e disponibilità dell'e-mail"?**

In parole semplici, sicurezza e disponibilità dell'e-mail significa garantire con efficacia la sicurezza e la disponibilità dei sistemi di e-mail. Sicurezza e disponibilità sono attualmente due fonti di rischio critiche per l'e-mail. Questi concetti comportano la protezione dei dati e dei sistemi da abusi e attacchi, rendendo al contempo i sistemi e le informazioni altamente disponibili per l'azienda e rispondendo ai requisiti di conformità normativa e di presentazione di documenti legali. In questo contesto, il termine "sistemi" fa riferimento all'architettura di base dell'e-mail o al sistema di messaggistica stesso, dall'infrastruttura fisica (server, archiviazione e rete) al software applicativo (sistemi di posta, archivi dei messaggi e altro) e la sicurezza e la disponibilità delle informazioni che risiedono o vengono trasmesse al suo interno. Il termine "informazioni" si riferisce al contenuto effettivo che viene trasferito e memorizzato nei sistemi di messaggistica.

Di seguito viene definito l'impatto della disponibilità e della sicurezza sui dati e i sistemi:

Sicurezza e disponibilità sono aree molto ampie, quindi è utile comprendere gli specifici obiettivi che vengono affrontati in questo documento.

Garantire che l'e-mail sia "sicura" significa:

- Proteggere i sistemi di e-mail da attacchi e interruzioni intenzionali o accidentali. Gli utenti di e-mail devono essere protetti da minacce e interruzioni provenienti da Internet, come spamming e virus
- I dati scambiati con clienti, fornitori e partner sono liberi da contenuti nocivi o non appropriati.
- Proteggere la rete stessa dall'esposizione a infezioni di virus e worm che circolano per mezzo dell'e-mail e che possono colpire i sistemi degli utenti finali e i server interni.
- Proteggere i dati aziendali dalla trasmissione accidentale o intenzionale a persone non autorizzate e verificare che non violano alcuna limitazione della privacy (codici fiscali, informazioni sanitarie, ecc.).

Garantire che l'e-mail sia "disponibile" significa:

- Ridurre al minimo qualsiasi disagio operativo dell'infrastruttura di e-mail causato da un degrado delle prestazioni o da un errore improvviso
- Assicurare che i sistemi degli utenti finali non vengano compromessi o disattivati da attacchi trasmessi via e-mail
- Assicurare che le e-mail legittime siano disponibili e accessibili malgrado i volumi di spamming e altri contenuti indesiderati
- Conservare le e-mail a lungo termine in base a criteri normativi esterni o a politiche aziendali interne
- Fornire agli utenti finali l'accesso trasparente alle informazioni nelle e-mail, nei sistemi di posta o negli archivi
- Consentire a utenti finali e rappresentanti della legge di cercare in modo semplice e sicuro e-mail e allegati negli archivi
- Consentire alle organizzazioni di supervisionare le comunicazioni a fini di conformità con le politiche interne o esterne

Ovviamente, tutto ciò deve essere gestito dal settore IT a fronte di volumi di e-mail in continua crescita e di budget a disposizione sempre più ridotti.

### **Fattori trainanti per la sicurezza e disponibilità dell'e-mail**

Internet e e-mail hanno vissuto un'evoluzione rapida diventando potenti strumenti di supporto per la crescita delle aziende, ma non senza un prezzo. Vari fattori hanno creato l'esigenza di avere e-mail sicure e disponibili:

- La dimensione dei volumi di e-mail aziendali inviate annualmente in tutto il mondo è aumentata del 47% tra il 2003 e il 2004 (Fonte: IDC Worldwide Email Usage 2004.2008 Forecast: Spam Today, Other Content Tomorrow, IDC #31782, agosto 2004)
- Il volume dello spamming che entra nelle reti aziendali è in continua crescita, costituendo in media il 64% delle e-mail in entrata (Fonte: Brightmail Logistics and Operations Center monthly Spam Statistics Report)

## Sicurezza e disponibilità dell'e-mail

- Aumento degli attacchi di phishing.
- La crescita annua del numero di minacce a diffusione di massa continua ad aumentare.
- Riconoscimento negli Stati Uniti, Europa e altri mercati dell'e-mail come documentazione aziendale con valore legale che deve essere conservata.
- Nuove normative sul mantenimento, controllo e supervisione delle comunicazioni interne ed esterne.
- Perdita di informazioni a causa di furti o abusi da parte di dipendenti che colpisce l'immagine aziendale, la fiducia dei clienti e la responsabilità legale
- Aumento delle vertenze legali che richiedono la presentazione di e-mail.
- Aumento dei costi di archiviazione, il 65% delle organizzazioni considera la crescita dell'archiviazione della messaggistica come un problema serio o molto serio, leggermente più problematico dello spamming stesso. (Fonte: Osterman Research, *Messaging Security Market Trends, 2005-2008*, maggio 2005).

### **Sicurezza e disponibilità dell'e-mail: come gestire in modo efficiente dati e sistemi**

La sicurezza e disponibilità dell'e-mail inizia dal controllo e dalla gestione del flusso di informazioni di e-mail dall'inizio alla fine per proteggere l'azienda dai rischi e garantire un'operatività senza ostacoli. In termini pratici, si tratta di rimuovere i contenuti indesiderati o non necessari dall'infrastruttura di messaggistica nei momenti temporali più appropriati.

Questi "momenti più appropriati" sono:

- **E-mail in entrata:** in arrivo da Internet, tra cui attacchi di spamming e phishing, worm a diffusione di massa, contenuti non appropriati o non lavorativi
- **E-mail in uscita:** virus o contenuti riservati o non appropriati che escono dai confini aziendali
- **E-mail trasmessa internamente:** virus o contenuti riservati o non appropriati che vengono diffusi all'interno dell'organizzazione
- **E-mail archiviata:** e-mail che non viene più consultata spesso ma che deve essere conservata per periodi medio-lunghi

Per ottenere questo controllo, le organizzazioni hanno la necessità di un approccio su più livelli che inizia dal primo punto di ingresso nella rete, arriva fino all'utente finale e prosegue oltre fino ai sistemi di archiviazione e memorizzazione.

### **Fase 1 – Sicurezza**

Di norma, la prima fase consiste nella protezione dell'ambiente, che comprende le seguenti attività: evitare la ricezione di contenuti indesiderati, impedire che e-mail indesiderate provenienti da Internet raggiungano i server centrali e ispezionare il traffico di posta interno.

#### ***Riduzione sicura del volume***

Per garantire buone prestazioni del sistema di e-mail malgrado i maggiori volumi, specialmente di fronte all'attuale problema dello spamming, è importante evitare semplicemente la ricezione di contenuti indesiderati. Più facile da dire che da mettere in pratica, ovviamente, ma realizzabile con l'ausilio degli strumenti appropriati.

Una prima linea di difesa non tecnica può e deve essere costituita dall'educazione e dalla sensibilizzazione degli utenti sulle politiche e le best practices relative all'utilizzo dell'e-mail. Ad esempio, tutti gli utenti devono essere al corrente di politiche e procedure di base quali non rispondere ai messaggi di spamming, non utilizzare i collegamenti per disdire le comunicazioni, non selezionare i collegamenti presenti nelle e-mail fraudolente sospette, non aprire allegati di e-mail dei quali non è chiara l'attinenza lavorativa o che nascondono intenti sospetti, ovvero, l'allegato può contenere un virus o una patch di qualche vulnerabilità, ignorare virus fasulli e avvertimenti e non autorizzare contenuti basati su limiti di dimensione o di tipo di file, come EXE, MP3, AVI, ecc.

Tuttavia, anche se l'educazione deve svolgere un ruolo importante nel quadro della soluzione complessiva, per bloccare lo spamming e i messaggi indesiderati è necessario il contributo della tecnologia. La difficoltà di bloccare le e-mail in transito risiede nella paura che vengano perduti anche dati legittimi. Di conseguenza, i sistemi utilizzati per bloccare i contenuti prima che raggiungano la rete o i sistemi di posta interni devono essere estremamente affidabili, ovvero, devono essere efficaci e consentire un flusso costante delle e-mail legittime.

I vantaggi di una tecnologia in grado di bloccare i contenuti vicino alla fonte comprendono risparmi in termini di larghezza di banda e spazio di archiviazione che possono essere avvertiti in tutta la rete, dai moduli di scansione del gateway SMTP stesso fino agli archivi dei messaggi e anche al livello di archiviazione permanente della posta. Eliminando i contenuti non attinenti all'attività lavorativa, è possibile risparmiare preziosa larghezza di banda, potenza di elaborazione e spazio di memorizzazione.

Poche aziende offrono prodotti che garantiscono questo specifico vantaggio, fatta eccezione per la tecnologia brevettata di riconfigurazione del traffico di Symantec, che verrà discussa più avanti in questo documento.

### **Protezione del perimetro**

È possibile adottare vari provvedimenti per impedire che e-mail indesiderate provenienti da Internet raggiungano i server centrali, come i costosi dispositivi di storage dei messaggi e gli archivi dei dati, nonché gli utenti di e-mail. Le due minacce principali trasmesse nelle e-mail sono virus e spamming.

Innanzitutto, il contenuto virale più comune nelle e-mail sono i worm a diffusione di massa. Si tratta di programmi che utilizzano gli indirizzi di e-mail presenti nei sistemi compromessi per generare messaggi finalizzati a replicare e distribuire il proprio payload ad altri utenti e sistemi ignari. Poiché le e-mail dei worm a diffusione di massa non hanno un valore aziendale intrinseco, è possibile eliminarle automaticamente senza timore di perdere dati legittimi. Le scansioni antivirus a livello di gateway devono essere in grado di individuare e riconoscere i worm a diffusione di massa e consentire agli amministratori di eliminarli. Questa funzione, spesso indicata come "Mass-mailer Cleanup" o "Worm Purge", è un criterio importante nella valutazione delle soluzioni antivirus.

In secondo luogo, per distribuire i propri payload come allegati, i worm a diffusione di massa in genere utilizzano la stessa varietà di dati o di tipi di file. Questi sono tipi di file come .scr, .pif, .vbs e così via, che tipicamente non sono presenti nelle normali transazioni aziendali, ma possono comprendere anche file .exe e formati di compressione come .zip. In base a queste caratteristiche, è possibile adottare ulteriori provvedimenti per proteggere l'ambiente di rete dalle nuove minacce a diffusione di massa non ancora identificate. Il filtro degli allegati può svolgere questo compito per mezzo della creazione di politiche di eliminazione dei messaggi quando viene rilevata la presenza di un tipo di estensione sospetta, come .scr e .pif. Elemento cruciale è anche la capacità di identificare questi file all'interno di contenitori compressi, come i file .zip, e di adottare i provvedimenti appropriati.

In terzo luogo, i contenuti dello spamming possono essere eliminati o rimossi dai flussi della posta per ridurre ulteriormente il carico sui relativi sistemi. Le aree di quarantena dello spamming, ospitate generalmente su un server separato dall'infrastruttura di posta, costituiscono le posizioni ideali per spostare i contenuti indesiderati dello spamming dagli archivi attivi dei messaggi, e di conseguenza dalle caselle degli utenti, a supporti meno costosi che sono più facili da scalare e mantenere. Le aree di quarantena sono necessarie perché i sistemi antispamming non possono essere accurati al 100%. Poiché le aziende non possono rischiare la perdita di e-mail legittime, per gli utenti è necessaria una posizione in cui rivedere i messaggi contrassegnati come spamming. In ogni modo, l'affidabilità del sistema antispamming può giocare un ruolo significativo nella riduzione della quantità di dati che vengono conservati nella quarantena e che devono essere rivisti dagli utenti.

Le metriche standard per valutare l'affidabilità dei sistemi antispamming sono la percentuale di rilevazione, ovvero la quantità di spamming intercettato, e la percentuale di accuratezza rispetto ai falsi positivi, ovvero i messaggi legittimi identificati erroneamente come spamming. Una delle maggiori difficoltà che si presentano con molti sistemi antispamming è che

Le percentuali di rilevazione e di accuratezza sono spesso variabili dipendenti, vale a dire che si possono ottenere alte percentuali di rilevazione a scapito dell'accuratezza e viceversa. È importante cercare una soluzione antispamming che non sia un insieme di strumenti manuali, ma un meccanismo di risposta integrato, aggiornato regolarmente con definizioni di spamming molto precise e tecniche basate sui metodi più recenti di diffusione dello spamming.

Queste soluzioni antispamming avanzate garantiscono sia rilevazione che accuratezza. Il vantaggio principale, l'eliminazione di una larga parte dei messaggi di spamming in transito, riduce il carico sulla quarantena antispamming e sui revisori. Ulteriori vantaggi comprendono una maggiore fiducia degli utenti sulle difese antispamming dell'azienda.

Infine, per mantenere inalterata la fiducia di clienti e partner, è anche cruciale che un'organizzazione non venga percepita come fonte di contenuti non appropriati o nocivi. Questo problema può essere affrontato in molti modi.

- Tutte le e-mail in uscita devono essere esaminate alla ricerca di virus e contenuti non appropriati. Se vi sono informazioni riservate o interne che non devono essere comunicate all'esterno, è importante identificare questi contenuti e attuare le misure appropriate per filtrare i contenuti a livello del server o del gateway di posta e garantire che rimangano entro i confini dell'azienda. Sono importanti anche linee guida di politica e l'educazione e la sensibilizzazione dei dipendenti.
- Poiché per distribuire le proprie minacce gli attuali worm a diffusione di massa forniscono propri servizi di consegna SMTP e non dipendono più da noti programmi di e-mail o dall'architettura dei sistemi di posta delle aziende, è importante attivare misure in grado di bloccare il traffico SMTP non autorizzato, noto anche come traffico della porta 25. Queste comprendono regole del firewall di rete che limitano l'accesso alla porta 25 ai sistemi autorizzati e regole dei firewall desktop che impediscono l'utilizzo della porta 25 da parte degli utenti finali (questi ultimi inviano e ricevono le e-mail Internet per mezzo del server di posta, che è responsabile di tutte le trasmissioni SMTP).

Grazie all'implementazione di queste misure, un considerevole volume di dati può essere dirottato o eliminato dal flusso principale della posta, garantendo che i sistemi centrali non vengano oberati da contenuti non pertinenti all'azienda. A sua volta, questo produce un miglioramento significativo nel funzionamento globale dell'infrastruttura di e-mail.

Elemento chiave della protezione del perimetro è anche la scelta del formato della soluzione. Le alternative a disposizione comprendono:

- Soluzioni software, che richiedono l'installazione di software applicativo sull'hardware e il sistema operativo del cliente
- Soluzioni basate su appliance, nelle quali il software applicativo è fornito preinstallato in una combinazione di hardware e sistema operativo gestito dal produttore
- Soluzioni in hosting, nelle quali il software e i sistemi sono situati presso un provider all'esterno dell'azienda e i flussi della posta Internet vengono reindirizzati attraverso questo ambiente per essere esaminati

La disponibilità di risorse e competenze varia da azienda ad azienda, anche all'interno di grandi organizzazioni, pertanto la scelta del formato diventa una questione di preferenze e praticità. Di seguito sono indicati alcuni vantaggi e criteri per la scelta di una soluzione.

### **Software**

- Flessibilità di implementazione per mezzo del supporto di diversi sistemi operativi, tra cui Windows®, Solaris™ e Linux™. Questo consente alle aziende di implementare e mantenere la flessibilità e non richiede competenze su un sistema operativo specifico in tutte le sedi geografiche.
- Soluzioni altamente integrate che combinano tecnologie antispamming, protezione antivirus e filtro dei contenuti. Nelle situazioni di aggiornamento o upgrade di emergenza, un minor numero di componenti rende più semplice garantire la compatibilità e l'operatività.
- Il fornitore è responsabile di entrambi i componenti di tecnologia per la sicurezza e di risposta. Questo limita i conflitti tra prodotti di fornitori diversi in quanto la soluzione è unica.

### **Appliance**

- "Consolidamento" del sistema operativo a fini di sicurezza: i servizi non essenziali del sistema operativo vengono disattivati, o rimossi completamente, per limitare l'esposizione alle vulnerabilità del sistema.
- È disponibile un contratto di supporto globale con sostituzione dell'hardware entro quattro ore.
- Gli aggiornamenti delle applicazioni e del sistema operativo possono essere automatici.

### ***Soluzioni in hosting***

- Scansione basata su proxy, relay di posta per inoltro senza memorizzazione, significa che il provider esterno non deve mai assumere il possesso dei messaggi, fatta eccezione per la messa in quarantena dello spamming. Tutto ciò avviene operando come proxy tra il server di invio e quello di ricezione, tenendo aperta la connessione quanto basta per completare l'ispezione dei messaggi e chiudendo quindi la transazione nel modo più appropriato.

### ***Protezione del server di posta***

Oltre a disporre di una solida protezione perimetrale, è necessario comunque ispezionare il traffico di posta interno. Ciò è importante per varie ragioni:

- Scansione dei virus che entrano per mezzo di altri vettori, come le e-mail personali basate sul Web, supporti rimovibili come dispositivi USB, utenti di computer portatili con definizioni dei virus non aggiornate e altro.
- Prevenzione dell'invio di contenuti non autorizzati a utenti non autorizzati.
- Prevenzione dell'invio di contenuti indesiderati o di dimensioni eccessive per mezzo del sistema di posta interno.
- Pulizia dei virus dagli archivi dei messaggi in seguito a un attacco utilizzando le definizioni dei virus più recenti.
- Pulizia retroattiva degli archivi dei messaggi per rimuovere contenuti vecchi, non necessari come promemoria di gestione interna.

Il risultato è che le soluzioni per la protezione dei server di posta, come quelle per Microsoft® Exchange e Domino®, devono essere in grado di ispezionare i contenuti in tempo reale. Tali ispezioni devono avere luogo nel momento in cui l'e-mail viene assegnata all'archivio dei messaggi, quando viene richiamata dall'archivio e in base a una pianificazione o manualmente per operazioni di pulizia in base alla disponibilità di definizioni dei virus aggiornate o di regole dei contenuti specifiche progettate per identificare contenuti sospetti o non appropriati.

Nel caso di un numero elevato di minacce virali, la fase iniziale dell'epidemia lascia l'azienda esposta a infezioni nel momento in cui le e-mail entrano nell'archivio dei messaggi, dove le nuove infezioni non vengono ancora rilevate dalle definizioni correnti. Dopo avere aggiornato le definizioni, è importante eseguire scansioni periodiche dell'archivio dei messaggi per eliminare contenuti nocivi e proteggere gli utenti.

### Fase 2 – Archiviazione

Il progressivo utilizzo dell'e-mail come applicazione aziendale fa emergere sempre più la consapevolezza che i sistemi di e-mail non sono mai stati progettati per memorizzare la quantità di dati che deve essere gestita attualmente da un tipo sistema di messaggistica. A molte aziende viene richiesto di conservare una quantità di e-mail maggiore rispetto al passato, per esigenze di conformità normativa, di politica interna o per essere preparate nell'eventualità di controversie legali.

Quasi tutti gli amministratori dei sistemi di e-mail riconoscono il primo problema: la gestione dell'archiviazione delle e-mail. Ogni giorno arrivano nuovi messaggi e il volume cresce drasticamente anno dopo anno. L'impatto di questa crescita ha i seguenti effetti:

- Costo elevato dell'ambiente di e-mail derivante dai maggiori costi di archiviazione e backup
- Disponibilità e prestazioni inferiori dell'ambiente di e-mail perché i server di messaggistica vengono rallentati quando arrivano vicino all'esaurimento della capacità massima e perché sono necessari tempi più lunghi per eseguire il backup delle grandi quantità di dati delle e-mail

Per "risolvere" questo problema, la maggior parte delle organizzazioni IT implementa quote di e-mail, vincolando gli utenti a una quantità di archiviazione prestabilita, tipicamente tra i 25 e i 200 MB. Tuttavia, in vari modi questo sposta semplicemente il problema invece di risolverlo effettivamente:

- Gli utenti provvedono a garantire che la propria archiviazione di e-mail non superi la quota e memorizzano i messaggi in file separati, ad esempio, file PST in Microsoft Exchange o file .NSF in Domino
- In molti casi, questi file vengono conservati in file server di rete e quindi utilizzano ancora risorse di memorizzazione e di backup
- Inoltre, questi file sono estremamente soggetti a danni e agli stessi problemi di disponibilità e prestazioni osservati sui server di e-mail
- Infine, se gli utenti memorizzano questi file sui propri desktop o portatili, che spesso non vengono inclusi nelle procedure di backup, è possibile che dati aziendali critici diventino passibili di perdita o furto

Tutto questo si aggiunge al fatto che le quote di e-mail influiscono sulla produttività degli utenti, determinano numerose chiamate di supporto e costituiscono uno degli oneri negativi nella gestione dell'e-mail.

La soluzione concreta a questo problema è di fornire il vantaggio delle quote di e-mail (gestione dell'archiviazione) senza i problemi associati: consentire agli amministratori di ridurre al minimo la dimensione dell'archiviazione principale e sfruttare sistemi di archiviazione secondari meno costosi senza sovraccaricare gli utenti o perdere dati critici. I sistemi di archiviazione consentono agli amministratori dei sistemi di e-mail di:

- Eseguire automaticamente la migrazione dei messaggi e degli allegati di e-mail in base a criteri di politica, come la data e la dimensione, verso una posizione di archiviazione secondaria, spesso meno costosa
- Terminare o eliminare in modo attivo e automatico i messaggi o migrarli a un terzo livello di archiviazione in base ai criteri delle politiche aziendali.
- Comprimere le informazioni e implementare un'unica istanza di archiviazione per ridurre il volume delle informazioni sfruttando sistemi meno costosi di memorizzazione su disco o su nastro per i dati archiviati.
- Consentire agli utenti finali di accedere a messaggi e allegati in modo trasparente dall'archivio come se accedessero alle normali e-mail.
- Indicizzare i messaggi e gli allegati in modo che gli utenti possano cercare in qualsiasi momento le proprie e-mail negli archivi, anche di grandi dimensioni.

In tal modo, le soluzioni per l'archiviazione dei messaggi consentono alle organizzazioni di fornire agli utenti una casella postale praticamente infinita (senza quote) garantendo comunque il controllo dell'archiviazione nei server di messaggistica principali.

Tuttavia, l'archiviazione dei messaggi non è solo una questione di gestione dell'archiviazione. Numerose aziende considerano l'archiviazione come una best practice generale nel quadro della gestione delle informazioni, un modo per preservare le informazioni critiche dell'azienda in base alle esigenze di lavoro.

Molte aziende che sono soggette a potenziali vertenze riconoscono che l'e-mail è una documentazione con validità legale che è possibile esibire e che, in caso di controversia, può venire richiesta come prova in tribunale. L'affermazione che l'e-mail è stata semplicemente eliminata non è più ammissibile e, in molti casi, può comportare sanzioni nei confronti dell'azienda.

Inoltre, il vecchio metodo di produrre le e-mail ripristinando i relativi dati dai nastri è spesso proibitivo in termini di costi e tempi. In molti casi, il ripristino manuale si aggira tra 2.000 e 5.000 dollari per nastro, determinando costi totali che in alcune vertenze arrivano a superare

i 200.000 dollari per causa. Per le aziende che operano in settori facili a situazioni di contenzioso come i prodotti di largo consumo, ciò è insostenibile.

La conservazione delle e-mail è imposta anche da normative esterne, Ad esempio, la Securities and Exchange Commission Rule 17(a)–4(f) approvata negli Stati Uniti specifica che, per determinate aziende, le e-mail devono essere conservate su supporti non cancellabili per lunghi periodi di tempo. Sempre più, quindi, le aziende preferiscono essere preparate per affrontare correttamente nuove normative o interpretazioni di legge, invece di dover reagire in modo tardivo e spesso inefficace.

Infine, le organizzazioni stanno comprendendo che indipendentemente dai fattori esterni, il controllo e la conservazione delle informazioni è semplicemente una "best practice". L'e-mail è diventata la fonte e la destinazione di una gran parte della proprietà intellettuale delle aziende. Per questa ragione, molte realtà desiderano conservare le e-mail per finalità interne, come la possibilità di eseguire ricerche successive o semplicemente per monitorare utilizzi non appropriati o violazioni della politica aziendale.

In questo senso, la soluzione ideale per l'archiviazione dei messaggi consentirà anche di svolgere le seguenti funzioni:

- Archiviazione automatica delle e-mail "registrate" in modo da garantire che vengano acquisite
- Indicizzazione delle informazioni archiviate in modo da facilitare ricerche future
- Funzionalità di ricerca sicura nell'intera organizzazione, consentendo al personale autorizzato di effettuare richieste di informazioni a livello aziendale
- Strumenti specializzati per assistere nelle procedure di acquisizione, ricerca e revisione a fini di legge
- Campionatura e procedure di supervisione regolamentata delle e-mail dei dipendenti

Escludendo lo spamming e i virus, l'e-mail e altra proprietà intellettuale dell'azienda possono consumare il 30–50% delle risorse di archiviazione dell'organizzazione. Senza una gestione adeguata, ciò può comportare costi di milioni di dollari all'anno in archiviazione e amministrazione. L'archiviazione dei contenuti assume il controllo della gestione dei vecchi contenuti per ottenere quanto segue:

- Inferiore costo totale di proprietà degli ambienti di posta operativi
- Ricerca e recupero immediati dei contenuti da parte degli utenti
- Conformità con i requisiti di conservazione legali e aziendali
- Migrazioni di piattaforma più veloci
- Migliore consolidamento dei server e ottimizzazione dell'archiviazione

### Fase 3 – Realizzazione di una base resistente

Di analoga importanza nel mantenimento della sicurezza e della disponibilità delle informazioni di e-mail è la necessità di realizzare l'infrastruttura di e-mail su una base resistente, solida al punto da soddisfare le esigenze di crescita, resistente agli errori e in grado di recuperare rapidamente in caso di problemi. Molte aziende hanno l'opportunità di pianificare un'infrastruttura che supporti le esigenze di crescita dell'azienda, come nel caso sia necessario migrare verso una nuova versione dei server di messaggistica o quando è necessario valutare il consolidamento dei server.

Quando si considera in che modo realizzare un'infrastruttura che offra una maggiore disponibilità dell'e-mail:

- Gli amministratori dei sistemi di e-mail devono identificare, comprendere e rispondere a un'ampia gamma di problemi che potrebbero impedire l'accesso all'e-mail. Essi devono monitorare e rispondere automaticamente a potenziali interruzioni, in base a politiche di risposta ben definite.
- L'azienda deve disporre della capacità di garantire il funzionamento e la comunicazione nel caso si verifichi un disastro. È essenziale che siano disponibili piani e passaggi ben definiti per ripristinare il sistema e tecnologie per proteggere i dati e i sistemi in modo da ridurre al minimo i periodi di inattività e di interruzione.
- Le organizzazioni IT devono mantenere, aggiornare e gestire attivamente i vari componenti dell'infrastruttura IT che contribuiscono all'erogazione dei servizi, compresi i sistemi operativi server, i componenti di rete e i sistemi di archiviazione.

Uno degli elementi chiave per affrontare la disponibilità nell'infrastruttura di e-mail consiste nel garantire prima di tutto la protezione dei dati per mezzo di una soluzione consolidata di backup e ripristino. Le soluzioni di backup a livello aziendale devono garantire una protezione dei dati ad alte prestazioni che sia scalabile per gestire gli ambienti più grandi.

Per ridurre al minimo le interruzioni e proteggere i dati, il software di backup deve offrire un unico strumento di gestione per consolidare tutte le operazioni di backup e ripristino, fornendo al contempo tecnologie avanzate di gestione, avviso, reporting e risoluzione dei problemi. È anche importante che le organizzazioni sfruttino i vantaggi di entrambi i tipi di archiviazione su nastro e su disco con le relative innovazioni nella protezione basata sul disco e sulle istantanee, la gestione dei supporti fuori sede e il ripristino di emergenza automatico. Per ridurre l'impatto sui sistemi aziendali critici, le organizzazioni devono orientarsi verso una soluzione di backup e ripristino che sia compatibile con i database e le applicazioni on-line specifici per il sistema di messaggistica utilizzato nell'infrastruttura di e-mail.

Inoltre, è essenziale che il sistema venga protetto dalle interruzioni. Questi tipi di soluzioni, tra cui VERITAS Bare Metal Restore, automatizzano e razionalizzano il processo di ripristino dei server, eliminando la necessità di reinstallare manualmente i sistemi operativi o di configurare l'hardware. Per mezzo di semplici comandi, è possibile effettuare ripristini completi di server e dati in poco tempo e senza lunghe fasi di training o complicate attività amministrative.

Un'altra area chiave è la realizzazione di un ambiente di gestione dell'archiviazione altamente scalabile. Invece di seguire i metodi di adeguamento tradizionali che risultano lunghi e costosi, come ad esempio, l'aggiunta di altri server o di spazio su disco quando le prestazioni diminuiscono o viene esaurito lo spazio all'aumentare dei dati delle e-mail, è importante iniziare a considerare l'ambiente dell'e-mail in modo più complessivo come un sistema di risorse unificate e disponibili che può essere sfruttato e condiviso dall'intera rete di messaggistica.

Il software per la gestione dell'archiviazione e il clustering offre le tecnologie chiave da implementare per la realizzazione di questa infrastruttura di e-mail scalabile. Questi tipi di prodotti consentono di soddisfare esigenze in continuo aumento senza limitarsi alla semplice aggiunta di altri sistemi o volumi, ma identificando e utilizzando in modo intelligente le risorse esistenti inutilizzate, ottimizzando in definitiva il valore del costo totale di proprietà dell'intero ambiente di e-mail.

Grazie all'adozione della soluzione corretta per la gestione dell'archiviazione, gli amministratori sono anche in grado di svolgere on-line tutte le attività correlate, come la riconfigurazione dei sistemi RAID, la deframmentazione, il ridimensionamento del file system e dei volumi, senza la necessità di mettere i sistemi off-line per lo svolgimento di queste normali funzioni di manutenzione e senza alcun impatto sulle attività dell'azienda.

Inoltre, la tecnologia di clustering deve fornire funzioni di mirroring per garantire la ridondanza e la migrazione automatica dei dati dai dischi in cui si verificano problemi ad altri che funzionano correttamente per eliminare i tempi di inattività conseguenti a eventi non programmati o per spostare rapidamente un'applicazione da un server bloccato a uno funzionante.

## Introduzione della sicurezza e disponibilità dell'e-mail di Symantec

Grazie alla combinazione dei prodotti e dei servizi con VERITAS, il leader nelle soluzioni per la disponibilità, la nuova Symantec è in grado di offrire una soluzione completa per la realizzazione della sicurezza e della disponibilità dell'e-mail. Queste esclusive tecnologie e servizi consentono di controllare e gestire il flusso delle informazioni di e-mail dall'inizio alla fine, aiutando a proteggere un'organizzazione dai rischi, garantendo l'operatività dei sistemi e degli utenti, soddisfacendo i requisiti di conformità e conservazione dei documenti e contenendo al contempo il costo totale di proprietà dell'e-mail. Ecco in che modo le offerte di tecnologia e servizi di Symantec sono in grado di rispondere all'approccio su più livelli descritto in precedenza.

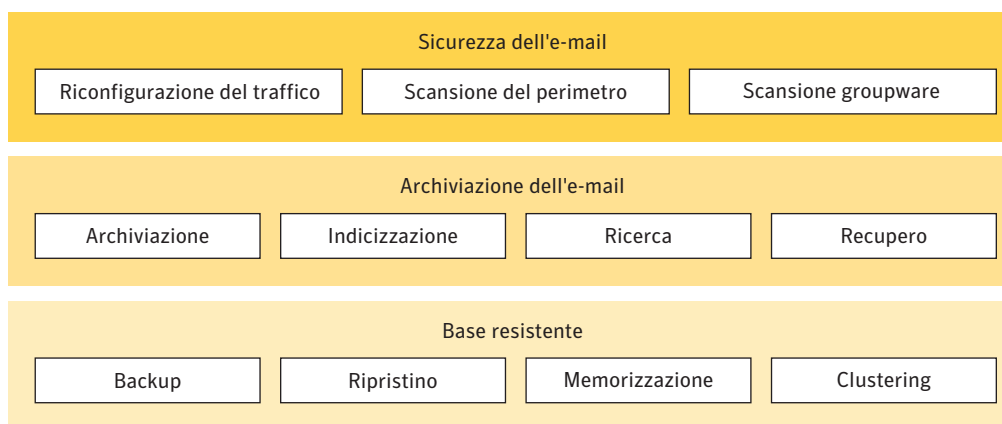


Figura 1. Approccio alla sicurezza e disponibilità dell'e-mail di Symantec

### Sicurezza dell'e-mail

La sicurezza dell'e-mail è composta da tre elementi chiave: riduzione del volume, protezione del perimetro e protezione groupware. Ma prima di discutere ciascun livello di protezione, è importante comprendere in che modo Symantec può essere all'avanguardia nel panorama delle minacce in costante evoluzione e aiutare i clienti a essere protetti dalle minacce trasmesse tramite e-mail.

### Global Intelligence Network e Security Response di Symantec

Al centro dell'organizzazione di Symantec opera l'infrastruttura di ricerca leader di settore, Symantec Global Intelligence Network, che aggrega, analizza e distribuisce in tutto il mondo avvisi sulle minacce per la sicurezza. Symantec Global Intelligence Network raccoglie dati sul codice nocivo da più di 150 milioni di desktop antivirus, 20.000 software per la rilevazione delle intrusioni (IDS), sensori firewall in oltre 180 paesi diversi con oltre 43.000 dispositivi per la

sicurezza gestiti. I Security Response Center globali di Symantec monitorizzano Probe Network, un insieme di oltre 2 milioni di indirizzi di e-mail con funzione di escan e analizzano le più recenti tattiche di spamming in tutto il mondo. Questa infrastruttura, combinata con le oltre 10.500 voci del database sulle vulnerabilità di Symantec, fornisce agli analisti di Symantec Security Response una fonte esclusiva di dati per identificare le linee di tendenza degli attacchi e delle attività del codice nocivo. Nei centri di Symantec Security Response, situati in Nord America, Asia, Australia, Cina ed Europa, sono presenti ricercatori considerati tra i migliori esperti nel settore della sicurezza che garantiscono una copertura 24x7 per qualsiasi importante evento riguardante la sicurezza. La varietà delle minacce e dei rischi per la sicurezza che vengono trattati dagli analisti di Symantec Security Response li pone all'avanguardia della ricerca sulla sicurezza.

La linea di prodotti Symantec Mail Security sfrutta i tempestivi aggiornamenti sulla sicurezza distribuiti da Symantec Security Response per aiutare le organizzazioni a prevedere e rispondere attivamente a qualsiasi minaccia alla sicurezza. Grazie al supporto di Global Intelligence Network e Security Response di Symantec, le informazioni e i provvedimenti consigliati sulle minacce più recenti possono essere aggiornati tramite l'efficiente rete dei sistemi LiveUpdate™ di Symantec, in grado di raggiungere i clienti in tutto il mondo indipendentemente dalla località geografica o dal fuso orario.

### ***Riduzione del volume***

#### **Appliance Symantec™ Mail Security Serie 8100**

Come è stato discusso precedentemente in questo documento, la prima linea di difesa per i contenuti di e-mail indesiderati deve essere situata all'esterno dell'infrastruttura di messaggistica, prima che i dati possano determinare effetti sui server interni, compresi i gateway di posta SMTP. Nella soluzione per la sicurezza e la disponibilità dell'e-mail di Symantec, questa prima linea di difesa è costituita dall'appliance Symantec Mail Security Serie 8100.

L'appliance Symantec Mail Security Serie 8100 impiega un approccio esclusivo per il contenimento dello spamming basato sulla valutazione della reputazione del mittente e sull'utilizzo di tecniche di riconfigurazione del traffico per il flusso SMTP in entrata. I pacchetti SMTP vengono campionati e analizzati in tempo reale, viene presa una decisione in merito alla "reputazione" di un mittente, quindi viene applicata la riconfigurazione del traffico per dissuadere i mittenti "indesiderati" dall'invio di contenuti alla rete aziendale protetta. In questo contesto, la "reputazione del mittente" viene desunta dal fatto che il server di origine, determinato tramite gli indirizzi IP, invia e-mail "legittime" o prevalentemente e-mail spamming.

Diversamente dalle tipiche scansioni antispamming a livello di gateway, l'appliance Symantec Mail Security Serie 8100 non intraprende alcuna azione sulle singole e-mail, ma considera la storia e la reputazione del percorso di posta stesso. Il risultato è che può utilizzare un elevato numero di input statistici per determinare una reputazione e, una volta stabilita, applica la "riconfigurazione del traffico" alla connessione del mittente. Questo significa che al mittente dello spamming viene assegnata una connessione all'ambiente protetto molto lenta, rendendo decisamente poco conveniente l'invio di e-mail.

Ironicamente, invece di lasciare che l'autore dello spamming sia in grado di controllare le risorse di sistema e la larghezza di banda di un ambiente legittimo, la situazione viene capovolta controllando le risorse del sistema mittente con un costo trascurabile per il cliente. Il risultato finale è che i server di posta del cliente vengono recepiti come se fossero sull'orlo di un collasso inducendo gli autori dello spamming a rimuovere il dominio dall'invio di futuri messaggi, con l'effetto di una significativa riduzione del volume di spamming.

### **Vantaggi dell'appliance Symantec Mail Security Serie 8100**

Se si considera che il 60–70% dell'e-mail in entrata è spamming, la pratica della riconfigurazione mirata del traffico si traduce in una riduzione del 50% del volume complessivo delle e-mail, senza alcun rischio di perdita della posta. Il risultato è una corrispondente riduzione dei messaggi che:

- Devono essere elaborati dalle scansioni e dai gateway di e-mail a livello centrale
- Vengono memorizzati in costosi archivi di messaggi sensibili ai problemi di volume
- Richiedono la revisione da parte degli utenti per mezzo di una quarantena dello spamming
- Devono essere archiviati, nel caso vi siano requisiti legali che impongono la conservazione di tutte le e-mail ricevute, compreso lo spamming, per un determinato periodo di tempo

Queste significative riduzioni dei volumi possono tradursi in ulteriori risparmi nel numero e nella dimensione complessiva dei server necessari per rispondere al problema, compresi i dispositivi di scansione gateway e i server di posta. In termini pratici, la riduzione dello spamming dal 70% del traffico a meno del 20% equivale a ritornare ai livelli di spamming esistenti intorno all'anno 2000. Come minimo, ciò consentirà di migliorare le prestazioni complessive e la scalabilità dei sistemi esistenti e allevierà il carico sui sistemi back-end e sugli utenti.

Il passo successivo nella realizzazione della sicurezza e della disponibilità dell'e-mail si focalizza sulla protezione del perimetro.

### **Protezione del perimetro**

Le soluzioni per il perimetro di Symantec abbracciano i formati chiave (software, appliance e soluzioni in hosting) e i sistemi operativi principali (Windows, Solaris e Linux), offrendo la flessibilità di scegliere il taglio adeguato alle esigenze di ogni organizzazione.

Inoltre, tutte le offerte di soluzioni Symantec hanno in comune i seguenti elementi:

- Tecnologie e funzioni di risposta antispamming di Symantec leader di settore, che offrono una percentuale di efficacia del 95% (fonte: eWeek 2003) e un livello di precisione del 99,9999% (Yankee Group Report 2004), ottenuti per mezzo di oltre 20 tecnologie di filtro, l'infrastruttura di risposta globale dei BLOC (fonte: Brightmail Logistics and Operations Centers) e aggiornamenti frequenti a intervalli tra 5 e 10 minuti. Inoltre, le liste di reputazione dei mittenti sfruttano la Probe Network™ per identificare le fonti di spamming note in Internet e fornire maggiore certezza insieme a un sistema di valutazione fondato.
- Le note tecnologie e funzioni di risposta antivirus NAVEX™ di Symantec, che assicura una protezione e un aggiornamento coerenti su tutte le piattaforme supportate, utilizza diverse tecnologie di rilevazione, tra cui quelle euristiche, ed è supportato dai centri operativi globali di Symantec™ Security Response, con aggiornamenti pianificati e manuali resi disponibili con frequenza settimanale, giornaliera e oraria
- Funzionalità Mass-Mailer Cleanup per rimuovere interi messaggi e impedire notifiche di virus non necessarie basate sulla presenza di worm a diffusione di massa
- La capacità di attuare blocchi tramite regole personalizzabili in base ai nomi e alle estensioni degli allegati o per dimensione dei messaggi, riga di oggetto e contenuto del corpo dei messaggi in modo da fermare sul nascere gli attacchi o impedire la trasmissione di contenuti di e-mail indesiderati o non appropriati
- La flessibilità di trattare lo spamming in modo diverso in base alla valutazione del motore antispamming, ad esempio, l'eliminazione dei messaggi riconosciuti come spamming e la quarantena di quelli sospetti per consentire che vengano ulteriormente esaminati
- La Spam Quarantine basata sul Web di Symantec, che rimuove i messaggi di spamming dall'ambiente di messaggistica lasciandoli però a disposizione degli amministratori e degli utenti finali per essere elaborati ed ulteriormente esaminati

### **Vantaggi della protezione del perimetro di Symantec**

Come seconda linea di difesa dopo l'appliance Symantec Mail Security Serie 8100, le soluzioni software e appliance per il perimetro di Symantec offrono i seguenti vantaggi:

- I contenuti dannosi trasmessi tramite e-mail in Internet non raggiungono i desktop degli utenti finali, non diffondono infezioni e non causano interruzioni nella rete
- Nell'ambiente centrale della posta entra un numero significativamente inferiore di messaggi indesiderati
- Grazie a una gestione flessibile dello spamming e a un elevato grado di precisione, gli utenti devono rivedere un minor numero di messaggi
- Viene archiviato un numero inferiore di e-mail non correlate all'attività

Chiaramente, l'applicazione di un'ulteriore 95% di riduzione sui volumi di spamming rimanenti consente di ridurre al minimo l'impatto negativo sugli archivi dei messaggi centrali e secondari e sugli utenti finali. Inoltre, la rimozione delle e-mail dei worm a diffusione di massa può limitare i picchi di volumi causati da questi tipi di attacchi e impedire che altri dati indesiderati intasino gli archivi dei messaggi e le caselle postali. La protezione del perimetro è chiaramente uno dei livelli più critici per aumentare la sicurezza della rete e migliorare la disponibilità dell'e-mail.

### ***Protezione dell'ambiente groupware***

Laddove la protezione del perimetro di Symantec svolge un ruolo chiave nella riduzione degli effetti negativi del traffico di e-mail Internet, Symantec™ Mail Security per Microsoft® Exchange e Symantec™ Mail Security per Domino® garantiscono che anche il traffico interno dei messaggi sia libero da contenuti nocivi o non appropriati.

Entrambe le soluzioni sono strettamente integrate nei rispettivi ambienti di posta grazie all'utilizzo delle API supportate dai fornitori e alla garanzia della massima funzionalità e di conflitti minimi con l'architettura di messaggistica sottostante.

Simili alle soluzioni per la protezione del perimetro, Symantec Mail Security per Exchange e per Domino sfruttano la stessa tecnologia e le stesse funzioni di risposta antivirus, nonché la stessa flessibilità di aggiornamento. Per le organizzazioni più piccole o anche per alcune realtà maggiori che hanno standardizzato server di posta e gateway adottando un'infrastruttura Domino o Exchange, è disponibile anche l'opzione di attivare le stesse tecnologie antispamming e di risposta che vengono utilizzate nelle soluzioni per la protezione del perimetro, fornendo la flessibilità di implementazione richiesta da organizzazioni eterogenee.

Oltre ai servizi di scansione centrali, Symantec Mail Security per Microsoft Exchange e per Domino offrono funzionalità di ispezione dei contenuti analoghe, quali il filtro della riga di

oggetto e del corpo dei messaggi, rimozione degli allegati e limitazioni alla dimensione dei messaggi. Tali funzionalità possono essere utilizzate per applicare politiche di utilizzo dell'e-mail e per contenere l'esposizione a sanzioni normative o vertenze legali conseguenti a contenuti non appropriati inviati tramite l'e-mail interna.

### ***Vantaggi della protezione groupware di Symantec***

Questo terzo livello della soluzione per la sicurezza e la disponibilità dell'e-mail contribuisce ulteriormente alla riduzione dei dati eliminando i contenuti indesiderati che vengono trasmessi internamente e i messaggi di worm a diffusione di massa in fase di propagazione iniziale.

È particolarmente adatto per la rilevazione preventiva delle violazioni delle politiche di e-mail, quali l'invio di contenuti non appropriati o non autorizzati a utenti interni o esterni.

Seguendo questo passaggio finale della scansione e pulizia della memorizzazione dei messaggi, i sistemi di archiviazione possono aggiungere il proprio valore alla catena della sicurezza e disponibilità dell'e-mail.

### **Disponibilità per mezzo dell'archiviazione**

Symantec Enterprise Vault è la soluzione leader di settore per svolgere funzioni automatiche e trasparenti di archiviazione, indicizzazione, ricerca e recupero delle informazioni, garantendo al contempo il funzionamento ottimale dei server Microsoft® Exchange e fornendo agli utenti un facile accesso ai propri dati archiviati. Enterprise Vault fornisce le seguenti funzionalità:

- **Memorizzazione** – Spostamento automatico dei contenuti di e-mail, file system, Microsoft SharePoint® e messaggistica istantanea dalle costose posizioni di archiviazione operative ad archivi on-line meno costosi senza influire sull'accesso ai dati da parte degli utenti. Gli utenti possono accedere direttamente alle informazioni archiviate dai propri client di e-mail come Outlook o dai browser Web e possono anche consultarli off-line mediante la funzione opzionale Offline Vault. Il settore IT è inoltre in grado di reperire, rilevare, migrare ed eliminare i file PST spostandone il contenuto nell'archivio. Oltre alle caselle e-mail, Enterprise Vault è anche in grado di archiviare i diari e le cartelle pubbliche di Microsoft Exchange.
- **Gestione** – I dati archiviati vengono compressi automaticamente, le copie duplicate vengono rimosse e i dati vengono conservati in base alle politiche aziendali. Col tempo, i dati possono essere migrati verso un sistema di memorizzazione terziario, comprendente archivi su nastro gestiti da Symantec NetBackup.
- **Reperimento** – Utenti finali, settori addetti alla conformità, esperti legali e funzioni addette alla gestione del rischio aziendale possono effettuare in tutta sicurezza ricerche nei messaggi, file e allegati con il minimo sforzo. Inoltre, gli uffici legali sono in grado di gestire le procedure di revisione legale per mezzo del modulo opzionale Discovery Accelerator, mentre le persone che si occupano di conformità possono supervisionare le comunicazioni dei dipendenti per mezzo del modulo Compliance Accelerator.

### ***Vantaggi di Symantec Enterprise Vault***

Come è stato descritto in precedenza, le soluzioni per l'archiviazione dei messaggi forniscono vantaggi in tre aree centrali:

- **Maggiore disponibilità dell'e-mail** – Enterprise Vault contribuisce a diminuire la quantità di dati memorizzati nei server di messaggistica e nei file server principali, riducendo i problemi di danni e prestazioni che si verificano quando tali server raggiungono le soglie limite di capacità. Non solo, l'archiviazione dei dati, il mantenimento della disponibilità per il periodo di conservazione a lungo termine e la fornitura di funzionalità di ricerca garantiscono l'accesso ai dati per gli utenti finali.
- **Minori costi dell'e-mail** – Enterprise Vault riduce i costi dell'intero ambiente di e-mail. Innanzitutto, grazie all'archiviazione dei dati vecchi o utilizzati raramente in sistemi di archiviazione meno costosi, Enterprise Vault riduce i costi dei sistemi di archiviazione principali nell'ambiente. Non meno importante, i costi di backup vengono ridotti in quanto i dati statici archiviati non devono più essere inclusi nelle consuete operazioni di backup. Il settore IT riduce i costi di supporto grazie all'eliminazione dei file PST e delle quote di e-mail, diminuendo, ad esempio, anche i costi e i tempi di migrazione dei dati da spostare nel passaggio a una nuova versione di Microsoft Exchange o nel consolidamento dei server di e-mail.
- **Rischio di e-mail controllato** – Tramite la conservazione dell'e-mail in base alle politiche aziendali, Enterprise Vault consente alle organizzazioni di affrontare anche i problemi riguardanti i rischi normativi o interni. Questi comprendono la riduzione dei rischi associati all'impossibilità di produrre informazioni correlate a vertenze legali, alla mancanza di conformità con le normative per la conservazione dei dati o a comunicazioni del personale non autorizzate.

### **Soluzione di Symantec per un sistema di e-mail resistente**

#### ***Protezione dei dati***

La necessità di recuperare i dati è un elemento cruciale in qualsiasi ambiente di e-mail, sia a causa di un'interruzione del sistema sia di un qualsiasi altro evento non programmato. Come è stato discusso precedentemente in questo documento, una buona parte dei dati strategici può risiedere nell'infrastruttura di e-mail. In un ambiente Exchange o Notes® è possibile utilizzare VERITAS NetBackup per il backup e il ripristino delle informazioni.

NetBackup™ per Microsoft Exchange Server semplifica il backup e il ripristino dei database senza interrompere il funzionamento del server Exchange o dei sistemi locali o remoti. Un approccio multilivello al backup e al ripristino garantisce una disponibilità costante dei servizi e dei dati di Exchange durante i backup. Amministrazione centralizzata, opzioni di automazione e il supporto dei più diffusi dispositivi di memorizzazione creano la flessibilità necessaria agli amministratori per massimizzare le prestazioni.

NetBackup™ per Lotus Notes fornisce funzioni di backup e ripristino ad alte prestazioni degli ambienti Lotus Notes/Domino. I servizi e i dati Lotus rimangono disponibili durante le operazioni di backup perché il database non viene posto off-line. Gli amministratori possono pianificare backup automatici per i client Lotus Notes® locali e remoti nella rete ed eseguire il backup e il ripristino a livello di database e registro delle transazioni.

NetBackup fornisce:

- Protezione completa e senza interferenze dei database e delle caselle e-mail di Exchange, compreso il backup incrementale delle caselle e-mail.
- Metodi flessibili per eseguire backup pianificati senza controllo dell'operatore.
- Ripristino immediato e capillare dei database e delle caselle e-mail, compreso il supporto per il ripristino di singoli messaggi.
- Funzionalità avanzate, tra cui Single Instance Store (SIS), esclusione globale e multiplexing di gruppi di memorizzazione. In combinazione con NetBackup™ Advanced Client è possibile anche disporre dell'integrazione con Volume Shadow Copy Services (VSS) e di funzioni di backup off-host.
- Tecniche alternative consentono di ripristinare i dati Lotus su un sistema o una directory alternativi.
- Supporto avanzato dell'integrazione di Lotus per server Lotus partizionati e il clustering Lotus.

### ***Vantaggi di Symantec (VERITAS) NetBackup***

Quale leader riconosciuto per il backup e il ripristino aziendale, VERITAS NetBackup™ è progettato per aiutare a fornire protezione completa dei dati per gli ambienti UNIX, Windows, Linux e NetWare® più complessi. Interfacce grafiche intuitive aiutano le organizzazioni a gestire tutti gli aspetti del backup e del ripristino e a mantenere politiche di backup coerenti a livello aziendale. Il software VERITAS NetBackup fornisce soluzioni di backup e ripristino compatibili con database e applicazioni negli ambienti Oracle®, IBM® DB2, UDB, Microsoft® SQL Server, Microsoft Exchange Server, Microsoft SharePoint Portal Server, SAP NetWeaver, Sybase, Informix e Lotus Notes e Domino Server.

### Dati principali del prodotto

- **Protezione dei dati end-to-end** – Protezione dei dati per tutti gli ambienti, dai desktop al centro dati all'archivio.
- **Unica soluzione per tutte le piattaforme** – NetBackup aiuta a consolidare e standardizzare le operazioni di backup e ripristino, proteggendo tutti i sistemi nelle principali varianti di UNIX, Windows, Linux e NetWare.
- **Scalabilità illimitata** – Gestione e controllo centralizzati, tecnologia ad alte prestazioni e architettura multilivello flessibile consentono al software NetBackup di adattarsi alle crescenti esigenze dei moderni centri dati.
- **Prestazioni uniche** – Backup sintetici utilizzano minore larghezza di banda della rete e riducono l'impatto sugli host applicativi in quanto i file vengono inclusi nel backup una sola volta. Il multiplexing di un massimo di 32 flussi di dati diversi su una singola unità nastro aiuta a ottenere il massimo throughput dall'hardware di memorizzazione.
- **Gestione e reporting** – NetBackup Operations Manager offre funzioni di gestione e reporting basate sul Web per grandi utenze aziendali di NetBackup. Fornisce monitoraggio in tempo reale, reporting cronologico, amministrazione, gestione degli avvisi e assistenza nella risoluzione dei problemi.
- **Protezione avanzata dei dati** – Esecuzione di backup e ripristini con impatto minimo e prestazioni elevate tramite NetBackup Advanced Client. Questa suite consolidata di tecnologie basate sull'uso di istantanee consente la protezione dei dati di FlashBackup, Instant Recovery, Offhost e Block-Level Incremental.
- **Ripristino di emergenza automatico** – L'opzione NetBackup Vault automatizza il processo di ripristino di emergenza contribuendo a semplificare la rotazione dei nastri e la creazione e la gestione di duplicati dei nastri per l'archiviazione fuori sede. NetBackup Bare Metal Restore razionalizza il processo di ripristino dei server. NetBackup Administration Console fornisce un singolo punto per la gestione che consente agli amministratori del backup di gestire un elevato numero di server con maggiore efficienza.
- **Ampia gestione dei supporti** – Consente agli utenti di condividere una libreria di nastri automatizzata tra sistemi eterogenei comprendenti UNIX, Windows, Linux, NetWare o dispositivi NAS (Network Attached Storage), consentendo agli utenti di NetBackup di sfruttare con maggiore efficacia le costose risorse di nastri e unità.

- **Sicurezza** – Protezione dei dati di backup selezionando la crittografia a 40, 56, 128 o 256 bit del software NetBackup. L'opzione di crittografia a impatto minimo di NetBackup garantisce che i dati siano sicuri prima di lasciare il client. NetBackup Access Control offre la flessibilità di limitare o fornire livelli di accesso specifici alle funzionalità amministrative del software NetBackup.
- **Sistemi di memorizzazione di rete** – Il software NetBackup supporta un'ampia gamma di librerie a nastro, unità a nastro e tecnologie di interconnessione SAN (Storage Area Network) dei principali fornitori. È possibile condividere in modo dinamico singole unità a nastro su connessioni SCSI o su una SAN, oppure utilizzare l'agente opzionale NetBackup per NDMP per aiutare a proteggere i dispositivi NAS (Network Attached Storage) più diffusi.

### ***Gestione di sistemi di archiviazione e clustering***

Symantec (VERITAS) Storage Foundation High Availability (HA) per Windows estende le funzionalità native di gestione dei dati di Windows® 2000 e Windows Server 2003. Le funzionalità disco/volume logico risultanti forniscono la base per un ambiente di archiviazione per Microsoft Exchange estremamente scalabile. Inoltre, Global Cluster e Volume Replicator assicurano il ripristino dell'infrastruttura di Exchange.

La rapida crescita dei volumi di archiviazione è un dato normale per la maggior parte delle implementazioni di Exchange. Storage Foundation HA per Windows offre un approccio modulare per affrontare l'ampia gamma di minacce potenziali alla disponibilità dell'e-mail. Le organizzazioni possono implementare i diversi componenti con un approccio graduale o in base alle esigenze specifiche. Mediante VERITAS Storage Foundation HA per Windows, è possibile creare un ambiente di archiviazione altamente disponibile e resistente grazie alle seguenti funzionalità:

- Creazione di un sistema di archiviazione che può essere espanso automaticamente per soddisfare crescenti esigenze di dati, quali ad esempio, un volume di archiviazione per un registro di transazioni.
- Progettazione di configurazioni di archiviazione che utilizzano il mirroring o combinazioni mirroring/striping per proteggere dalla perdita di un singolo disco.
- Identificazione e risoluzione degli "hotspot" di archiviazione che rallentano le prestazioni globali dell'applicazione.
- Creazione di immagini relative a specifici punti nel tempo per il ripristino immediato da errori logici o danni ai dati.

Per proteggere l'infrastruttura di Exchange da disastri che coinvolgono un intero sito, è possibile utilizzare le opzioni Global Cluster e Volume Replicator per creare un ambiente di ripristino di emergenza che consente il failover veloce dell'intero ambiente Exchange o di un intero centro dati. Poiché il sito di ripristino di emergenza secondario non deve coincidere esattamente con quello primario e può essere utilizzato per altri scopi, le aziende possono sfruttare gli investimenti in ripristino di emergenza e controllare i relativi costi di supporto con i seguenti criteri:

- Utilizzo di un sistema di archiviazione a costo o capacità inferiore nella posizione di ripristino fuori sede.
- Utilizzo di un singolo centro dati come posizione di ripristino fuori sede per varie altre sedi di centri dati.
- Utilizzo del sito di ripristino per eseguire servizi non critici, come lo sviluppo e test, che possono essere interrotti, fermati e sostituiti con applicazioni critiche in caso di failover globale. Di seguito viene illustrato come utilizzare Storage Foundation HA per Windows per affrontare in modo specifico differenti tipi di minacce per la disponibilità di Exchange.

Tuttavia, non è possibile proteggere i dati di Exchange da tutte le fonti di errori logici. Danni ai dati, errori degli utenti e virus presentano rischi che sono quasi impossibili da eliminare. La migliore difesa è di annullare l'effetto di questi errori in modo rapido ed efficace, con perdita minima di dati. VERITAS Storage Foundation offre un'altra alternativa: istantanee relative a punti specifici nel tempo dei database e dei registri delle transazioni di Exchange mediante l'opzione FlashSnap. Un'istantanea di FlashSnap è un volume indirizzabile in modo indipendente che esegue il mirroring dei volumi di produzione. Grazie alla suddivisione del mirroring, l'opzione FlashSnap crea un'immagine dei dati in un punto temporale specifico che può essere utilizzata come origine di backup, scaricando il processo di backup dall'ambiente di produzione, oppure può essere utilizzata per creare immagini di ripristino immediato.

Le organizzazioni possono proteggere gli ambienti di Exchange da un'ampia gamma di errori dei componenti implementando funzioni di clustering locali e aziendali per garantire la disponibilità. Storage Foundation HA per Windows integra la tecnologia VERITAS Cluster Server (VCS), che fornisce opzioni di clustering del failover flessibili e scalabili con funzionalità di gestione del carico di lavoro. In un cluster VCS, vari server sono collegati con un sistema di archiviazione condiviso e con heartbeat Ethernet privati. Ciascun sistema nel cluster è in grado di accedere all'archiviazione di qualsiasi altro sistema.

Per garantire l'operatività aziendale in caso di interruzione generalizzata, la protezione migliore è la possibilità di riprendere le operazioni, quasi istantaneamente e senza perdita di dati, in un sito alternativo situato a una distanza significativa da quello primario. L'utilizzo di Storage Foundation con le opzioni Global Cluster e Volume Replicator consente di replicare i dati tra due siti separati e di scambiare i servizi applicativi tra di essi con un semplice clic del mouse.

La combinazione di VERITAS NetBackup e Storage Foundation HA per Windows, con le opzioni Global Cluster e Replication, offre alle organizzazioni che dipendono da Microsoft Exchange un'unica soluzione per realizzare una base resistente per il sistema di e-mail.

### **Vantaggi principali di Storage Foundation HA:**

- Massimizzazione dell'efficienza operativa dei dati e delle applicazioni di messaggistica
- Riduzione dei tempi di inattività pianificati o meno
- Attivazione di una soluzione di alta disponibilità per il clustering locale, metropolitano o globale dall'interno di un unico prodotto
- Possibilità di testare la soluzione di ripristino di emergenza senza impatto sulle applicazioni di produzione
- Ottimizzazione e pianificazione della configurazione e delle politiche dei cluster per mezzo di uno strumento portatile di modellizzazione e simulazione

### **Conclusioni**

Nella maggior parte delle organizzazioni, l'ambiente di e-mail è diventato il centro delle attività. L'efficacia e l'efficienza di questo centro possono influire sulla produttività degli utenti finali e sulla capacità dell'azienda di funzionare. Nel corso degli ultimi anni, le arterie dell'e-mail sono diventate letteralmente intasate da spamming, virus e qualsiasi altra cosa che può essere trasmessa per mezzo di questo veicolo. La sua vitalità è messa a rischio da tutto ciò che ne ha sfruttato le prerogative.

La sicurezza e disponibilità dell'e-mail è la strada che consente di recuperare l'efficienza dei sistemi di e-mail riducendo la quantità di contenuti indesiderati e potenzialmente pericolosi che entrano nel sistema e ottimizzando gli archivi tramite l'eliminazione dei volumi in eccesso che possono determinare possibili sovraccarichi ed errori.

Le soluzioni per la sicurezza e la disponibilità dell'e-mail di Symantec offrono l'esclusiva capacità di ridurre i rischi per i sistemi e i dati di e-mail e garantire l'efficienza e le prestazioni di sistemi e utenti soddisfacendo al contempo i requisiti normativi e le politiche aziendali. Particolarmente importante è l'impatto che le soluzioni di Symantec offrono per contenere i costi di proprietà complessivi grazie alla riduzione del carico a tutti i livelli dell'infrastruttura di e-mail, compresi i costi di archiviazione e i costi operativi associati al tentativo di scalare l'infrastruttura e massimizzare le prestazioni. Opzioni di implementazione flessibili su un'ampia gamma di formati, punti di integrazione e ambienti operativi consentono alle aziende di adattare le soluzioni alle proprie esigenze, invece di rivolgersi a soluzioni mirate di diversi fornitori. Il raggiungimento di livelli più elevati di sicurezza e disponibilità per le applicazioni aziendali strategiche è l'elemento chiave per realizzare l'infrastruttura resistente che consente alle organizzazioni di garantire l'operatività, l'efficienza e la crescita delle aziende qualunque cosa accada.



## Informazioni su Symantec

Symantec è il leader mondiale nella fornitura di soluzioni che aiutano utenti privati e aziende a garantire la sicurezza, disponibilità e integrità delle informazioni. Con sede principale a Cupertino, California, Symantec svolge attività in oltre 40 paesi. Ulteriori informazioni sono disponibili all'indirizzo [www.symantec.it](http://www.symantec.it).

Symantec ha filiali operative in oltre 40 paesi. Per informazioni sui contatti in ogni specifico paese, visitate il nostro sito Web.

### Sede principale

20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
408 517 8000  
800 721 3934  
[www.symantec.com](http://www.symantec.com)

### Italia (Milano)

Symantec srl  
Via Rivoltana, 2D  
20090 Segrate (MI)  
Italia  
Tel: +39 02 7033 21  
Servizio Clienti  
Tel: +39 02 48270000  
Sito Web: [www.symantec.it](http://www.symantec.it)

Symantec e il logo Symantec sono marchi registrati negli Stati Uniti di Symantec Corporation. Live Update, Symantec Mail Security, Symantec Mail Security 8100 Series, Symantec Mail Security for Domino, Symantec Mail Security for Microsoft Exchange e Symantec Security Response sono marchi di Symantec Corporation. Domino, IBM, Lotus Notes e Notes sono marchi di International Business Machines Corporation negli Stati Uniti, in altri paesi o in entrambi. Microsoft, Microsoft Exchange, Microsoft SharePoint, Windows e Windows 2000 sono marchi o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri paesi. NetWare è un marchio registrato di Novell, Inc., negli Stati Uniti e in altri paesi. Oracle è un marchio registrato di Oracle Corporation e/o delle sue consociate. Solaris è un marchio o marchio registrato di Sun Microsystems, Inc., negli Stati Uniti e in altri paesi. Altri nomi e prodotti sono marchi dei rispettivi proprietari. Qualsiasi informazione tecnica che viene resa disponibile da Symantec Corporation è prodotto coperto da diritto d'autore di Symantec Corporation ed è di proprietà di Symantec Corporation. Le informazioni tecniche sono fornite come tali e Symantec Corporation non fornisce alcuna garanzia sulla relativa accuratezza o sul relativo utilizzo. Qualsiasi utilizzo della documentazione tecnica o delle informazioni qui contenute è a rischio dell'utente. Copyright © 2005 Symantec Corporation. Tutti i diritti riservati. 07/05 WP-00068-IT