Cisco Email Security Appliance

Negli ultimi vent'anni l'e-mail si è evoluta, passando da strumento impiegato principalmente da tecnici e professionisti della ricerca fino a diventare la colonna portante delle comunicazioni aziendali. Sono oltre 100 miliardi al giorno i messaggi e-mail che si scambiano le aziende. Con l'aumentare dell'utilizzo di e-mail, la sicurezza è diventata una priorità sempre maggiore. Le campagne spam di massa non sono più l'unico problema. Oggi lo spam e il malware costituiscono solo una parte di un quadro più complesso che include le minacce in entrata e i rischi in uscita.

Le soluzioni Cisco® Email Security offrono una protezione e-mail a elevata disponibilità contro le minacce dinamiche e in rapido mutamento che colpiscono le aziende. Grazie alle soluzioni di appliance, virtuali, cloud e ibride, Cisco Email Security è riconosciuta da terzi come la soluzione leader che offre:

- **Protezione e-mail veloce e completa,** spesso in anticipo di ore o giorni rispetto alla concorrenza
- **Un delle principali reti di informazioni di intelligence sulle minacce, grazie a Cisco Talos,** basata sulle analisi della sicurezza collettiva ad ampio raggio
- **Protezione dei messaggi in uscita** attraverso Data Loss Prevention (DLP) integrata, crittografia e-mail e integrazione facoltativa con la soluzione DLP aziendale RSA
- **Minore costo totale di proprietà** con ingombro ridotto, implementazione semplificata e amministrazione automatizzata e conseguente risparmio sul lungo periodo

Panoramica del prodotto

La soluzione completa Cisco offre un'implementazione semplice e rapida, con pochi requisiti di manutenzione, bassa latenza e costi operativi ridotti. La tecnologia "set-and-forget", una volta attivate le impostazioni di policy automatiche, lascia libero il personale di dedicarsi ad altro. Dopodiché, la soluzione inoltra automaticamente gli aggiornamenti della sicurezza alla soluzione di intelligence sulle minacce basata su cloud di Cisco. I dati sull'intelligence delle minacce vengono aggiornati in Cisco Email Security Appliance (ESA) ogni 3-5 minuti, fornendo una soluzione di difesa dalle minacce aggiornata e di alto livello ore o giorni prima di altri fornitori. Opzioni di implementazione flessibili e integrazione fluida con l'infrastruttura di sicurezza esistente rendono Cisco Email Security ideale per le esigenze di un'azienda.

Appliance virtuale

Cisco Email Security Virtual Appliance (ESAV) riduce in modo significativo il costo di implementazione della sicurezza e-mail, soprattutto nelle reti altamente distribuite. L'appliance consente al gestore di rete di creare le istanze quando e dove necessario, sfruttando l'infrastruttura di rete esistente. Cisco ESAV è una versione software di Cisco ESA e funziona su un hypervisor VMware ESXi e sui server Cisco Unified Computing System™ (Cisco UCS®). Con l'acquisto di pacchetti software Cisco Email Security si riceve una licenza illimitata per Cisco ESAV

Con Cisco ESAV è possibile soddisfare immediatamente le esigenze di crescita del traffico grazie alla pianificazione semplificata delle capacità. Non è necessario acquistare e spedire le appliance, quindi è possibile supportare nuove opportunità commerciali senza aggiungere ulteriore complessità al data center o dover assumere personale aggiuntivo.

Funzionalità e vantaggi

Cisco Email Security difende i sistemi e-mail mission-critical con soluzioni basate su appliance, virtuali, cloud e ibride. Cisco Email Security è riconosciuto da terze parti come la migliore fonte di soluzioni di sicurezza e-mail. Nella Tabella 1 sono illustrate le principali funzionalità e vantaggi delle soluzioni Cisco Email Security.

Tabella 1. Funzionalità e vantaggi

Funzionalità	Vantaggio
Intelligence globale sulle minacce	Protezione e-mail rapida e completa grazie a una delle più grandi reti di rilevamento di minacce al mondo. Cisco Email Security fornisce ampia visibilità e footprint, tra cui: • 100 terabyte (TB) di intelligence di sicurezza al giorno • 1,6 milioni di dispositivi di sicurezza implementati, inclusi firewall, sensori Cisco Intrusion Prevention System (IPS) e appliance Web ed e-mail • 150 milioni di endpoint • 13 miliardi di richieste Web al giorno • Il 35% del traffico e-mail aziendale globale Cisco Talos consente di controllare l'attività del traffico globale 24 ore su 24. Analizza le anomalie, scopre le nuove minacce e monitora le tendenze del traffico. Cisco Talos consente di evitare gli attacchi zero-hour generando in continuazione nuove regole che consentono di aggiornare Cisco ESA. Questi aggiornamenti si verificano ogni 3-5 minuti, assicurando una difesa dalle minacce leader del settore.
Blocco di spam	Lo spam è un problema complesso, che richiede una soluzione sofisticata: Cisco lo semplifica. Per impedire ai messaggi di spam di raggiungere le caselle di posta dell'azienda, una difesa multilivello combina due livelli di filtri: uno esterno, basato sulla reputazione del mittente, e uno interno, che esegue un'analisi approfondita del messaggio. Con i filtri basati sulla reputazione, oltre l'80% dello spam viene bloccato prima che raggiunga la rete. I miglioramenti recenti includono analisi contestuale e automazione avanzata, nonché classificazione automatica, per fornire una robusta protezione dalle campagne snowshoe. I clienti che devono gestire grandi volumi di e-mail in poco tempo possono applicare i filtri in base al mittente o all'oggetto, con la possibilità di bloccare i relativi messaggi o di metterli in quarantena.
Advanced Malware Protection (AMP)	Cisco ESA ora include Advanced Malware Protection (AMP), una soluzione antimalware che sfrutta la vasta intelligence di sicurezza cloud di Sourcefire (parte di Cisco). Fornisce protezione durante le varie fasi dell'attacco: prima, durante e dopo un attacco. Dispone inoltre delle funzionalità di valutazione della reputazione e blocco dei file, file sandboxing e analisi retrospettiva dei file per eseguire l'analisi continua delle minacce, anche dopo che hanno superato il gateway e-mail. Gli utenti possono bloccare altri attacchi, monitorare i file sospetti, ridurre l'ambito di un attacco e risolvere rapidamente i problemi. AMP è disponibile per tutti i clienti Cisco ESA come funzionalità su licenza aggiuntiva.
Controllo dei messaggi in uscita	Cisco ESA controlla i messaggi in uscita tramite DLP, crittografia e-mail e integrazione opzionale con RSA Enterprise Manager. Con questo controllo i messaggi più importanti sono conformi agli standard del settore e sono protetti durante il transito. Inoltre, la scansione antispam e antivirus, insieme alla limitazione della velocità in uscita, possono essere utilizzate per evitare che i sistemi o gli account violati dell'azienda vengano inseriti nelle blacklist dell'e-mail. Novità: ora ESA supporta la crittografia e le firme Secure/Multipurpose Internet Mail Extensions (S/MIME), oltre aTransport Layer Security (TLS).
Prestazioni eccellenti	Cisco ESA blocca rapidamente i nuovi virus in entrata. Le code di consegna di dominio evitano che le e-mail non recapitabili provochino un backup delle consegne critiche per gli altri domini.
DLP	È possibile utilizzare una o più policy predefinite (tra le 100 disponibili) per impedire che i dati riservati escano dalla rete. Se si preferisce, è possibile utilizzare le parti di tali policy predefinite per creare policy personalizzate. Il motore DLP e-mail RSA integrato utilizza strutture di dati predefinite insieme a punti di dati opzionali personalizzati, come parole, frasi, dizionari ed espressioni frequenti, per creare rapidamente policy accurate con un numero minimo di falsi positivi. Il motore DLP valuta le violazioni in base alla gravità, in modo da poter applicare diversi livelli di azioni correttive a seconda delle esigenze.

Funzionalità	Vantaggio
Basso costo	Footprint ridotto, configurazione facile e gestione automatizzata degli aggiornamenti consentono di prolungare la durata della soluzione Cisco Email Security. La soluzione Cisco ha uno dei TCO più bassi in assoluto.
Implementazione flessibile	Tutte le soluzioni Cisco Email Security condividono un approccio semplice all'implementazione. La configurazione guidata del sistema può gestire anche ambienti complessi e fornisce protezione in pochi minuti, garantendo maggiore sicurezza e velocità. Le licenze sono basate sull'utente, non sul dispositivo, quindi è possibile applicarle per utente invece che per il dispositivo, in modo da fornire protezione del gateway e-mail sia in uscita che in entrata, senza costi aggiuntivi. Questa funzionalità consente di eseguire la scansione dei messaggi in uscita con motori antispam e antivirus per supportare completamente le esigenze aziendali. Cisco ESAV offre le stesse funzionalità di Cisco ESA, con l'ulteriore comodità e risparmio consentiti da un modello di un'implementazione virtuale. Cisco ESAV offre provisioning self-service istantaneo. Con una licenza Cisco ESAV è possibile implementare gateway virtuali di sicurezza e-mail nella rete senza connessioni Internet. Acquistando la licenza Cisco ESAV è possibile ottenere le licenze software acquistate. Si possono applicare in qualsiasi momento le licenze a un nuovo file immagine virtuale Cisco ESAV archiviato localmente. I file di immagine virtuali incontaminati possono essere clonati, se necessario, fornendo la possibilità di implementare immediatamente diversi gateway di sicurezza e-mail. È possibile eseguire soluzioni hardware e virtuali Cisco Email Security nella stessa implementazione. Pertanto, le piccole filiali o le postazioni remote possono avere la stessa protezione disponibile nella sede centrale senza dover eseguire l'installazione e predisporre il supporto presso quella sede. È possibile gestire facilmente le implementazioni personalizzate con Cisco Content Security Management Appliance (SMA) o Cisco Content Security Management Appliance (SMAV).
Soluzioni su misura dell'azienda	La soluzione basata su cloud è un servizio completo ed estremamente affidabile che mette a disposizione software, potenza di elaborazione e supporto. L'interfaccia utente co-gestita è identica a quella di Cisco ESA e di ESAV. Pertanto, si ottiene una protezione eccezionale con operazioni di amministrazione ridotte e senza hardware in sede da monitorare e gestire. La soluzione ibrida assicura un controllo in uscita avanzato di messaggi sensibili in sede, consentendo al tempo stesso di approfittare della praticità e della convenienza economica del cloud. L'hardware e le appliance virtuali in sede sono prontamente collegabili. È possibile scegliere il modello più adatto per il proprio ambiente in modo da proteggere i messaggi in entrata e in uscita nel gateway.

Specifiche del prodotto

La Tabella 2 indica le specifiche delle prestazioni per Cisco ESA, la Tabella 3 indica le specifiche hardware per Cisco ESA, la Tabella 4 indica le specifiche per Cisco ESAV e la Tabella 5 indica le specifiche per la Cisco Security Management Appliance (SMA).

Tabella 2. Specifiche delle prestazioni Cisco ESA

Implementazione	Modello	Spazio su disco	Mirroring RAID	Memoria	CPU
Grandi imprese	Cisco ESA C680	1,8 TB (600 x 3)	Sì (RAID 10)	32 GB	2 x 6 (2 core hexa)
Medie imprese	Cisco ESA C380	1,2 TB (600 x 2)	Sì (RAID 1)	16 GB	1 x 6 (1 core hexa)
Piccole e medie aziende o filiali	Cisco ESA C170	500 GB (250 x 2)	Sì (RAID 1)	4 GB	1 x 2 (1 dual core)

Nota: per un dimensionamento accurato, verificare la propria scelta controllando le velocità di picco del flusso di messaggi e la dimensione media dei messaggi con uno specialista Cisco per la sicurezza dei contenuti.

Tabella 3. Specifiche hardware Cisco ESA

Modello	Cisco ESA C680	Cisco ESA C380	Cisco ESA C170
Unità rack (RU)	2 RU	2 RU	1 RU
Dimensioni (A x L x P)	3,5 x 19 x 29 pollici (8,9 x 48,3 x 73,7 cm.)	3,5 x 19 x 29 pollici (8,9 x 48,3 x 73,7 cm.)	1,67 pollici x 16,9 pollici x 15,5 pollici (1,67 x 16,9 x 15,5 pollici)
Opzione di alimentazione CC	Sì	Sì	No
Accensione e spegnimento in remoto	Sì	Sì	No
Alimentatore ridondante	Sì	Sì	No
Disco rigido hot-swap	Sì	Sì	Sì
Interfacce Ethernet	Schede di interfaccia di rete a 4 gigabit (NIC), RJ45-45	NIC a 4 gigabit, RJ-45	NIC a 2 gigabit, RJ45-45
Velocità (Mbps)	10/100/1000, negoziazione automatica	10/100/1000, negoziazione automatica	10/100/1000, negoziazione automatica
Opzione in fibra 10 Gigabit Ethernet	Sì (accessorio)	No	No

Tabella 4. Specifiche Cisco ESAV

Utenti e-mail				
Utenti e-mail	**Modello**	**primario**	**Memoria**	**Core**
Solo valutazioni	Cisco ESAV C000v	250 GB (SAS 10.000 giri/min.)	4 GB	1 (2,7Ghz)
Piccola impresa (fino a 1.000)	Cisco ESAV C100v	250 GB (SAS 10.000 giri/min.)	6 GB	2 (2,7 Ghz)
Media impresa (fino a 5.000)	Cisco ESAV C300v	1024 GB (SAS 10.000 giri/min.)	8 GB	4 (2,7 Ghz)
Grandi imprese o service provider	Cisco ESAV C600v	2032 GB (SAS giri/min.)	8 GB	8 (2,7 Ghz)
Server				
Cisco UCS	VMware ESXi 5.0, 5.1 e 5.5 Hypervisor			

Tabella 5. Specifiche piattaforma Cisco SMA serie M

Modello	Cisco SMA M680	Cisco SMA M380	Cisco SMA M170
Numero di utenti	10.000 o più	Fino a 10.000	Fino a 1000

Destinazioni di implementazione

È possibile implementare soluzioni Cisco Email Security:

- **In sede:** Cisco ESA è un gateway e-mail che in genere viene implementato in una zona demilitarizzata (DMZ) del firewall. Il traffico Simple Mail Transfer Protocol (SMTP) in ingresso è indirizzato verso l'interfaccia dati Cisco ESA in base alle specifiche impostate dai record di scambio di posta. Cisco ESA filtra il traffico e lo riconsegna al server di posta di rete. Il server di posta reindirizza anche la posta in uscita verso l'interfaccia dati Cisco ESA, in cui viene filtrato in base alle policy in uscita e quindi consegnato alle destinazioni esterne.
- **Virtuale:** con Cisco UCS in esecuzione nella filiale di piccole dimensioni, Cisco ESAV può essere ospitato con altri prodotti Cisco come Cisco Web Security Virtual Appliance (WSAV). Insieme, offrono lo stesso livello di protezione dei loro equivalenti hardware, ma consentono di risparmiare su spazio e alimentazione. Con Cisco SMA o SMAV questa implementazione personalizzata può essere gestita a livello centrale.

Opzioni per Cloud Security

Cisco Cloud Email Security fornisce un modello di implementazione flessibile per la sicurezza e-mail. Consente di ridurre i costi mediante la co-gestione e senza infrastruttura di sicurezza e-mail in loco.

Cisco Hybrid Email Security offre i vantaggi di Cisco Cloud Email Security uniti a un controllo avanzato dei dati in uscita, crittografia dei messaggi e DLP in loco. Questa soluzione ibrida consente di passare a una soluzione cloud a seconda delle proprie esigenze.

Cisco Email Security: licenze per appliance fisiche e virtuali

Una licenza Cisco ESAV è inclusa per tutti i pacchetti software di Cisco Email Security: Cisco Email Security Inbound, Cisco Email Security Outbound o Cisco Email Security Premium. Questa licenza prevede le stesse condizioni degli altri servizi software inclusi nel pacchetto e può essere utilizzata per tutte le istanze virtuali desiderate, purché ci si attenga al numero di utenti previsto. Le licenze Cisco ESA sono incluse in tutti i pacchetti software di Cisco Email Security. È sufficiente acquistare le licenze appropriate per il numero di caselle postali da

supportare, quindi acquistare le appliance in sede appropriate. Per le appliance virtuali, ordinare semplicemente le licenze software per ottenere il diritto.

Licenze in abbonamento basate sulla durata

Le licenze sono costituite da abbonamenti della durata di 1, 3, o 5 anni.

Licenze con abbonamento basate sulla quantità

Il portafoglio Cisco Email Security utilizza prezzi distinti in base al numero di caselle postali. I rappresentanti di vendite e partner sono a disposizione dei clienti per determinare l'implementazione corretta.

Licenze software di sicurezza e-mail

Sono disponibili tre pacchetti di licenze software di sicurezza e-mail, nonché un'offerta personalizzata: Cisco Email Security Inbound, Cisco Email Security Outbound, Cisco Email Security Premium e Advanced Malware Protection. I componenti principali di ciascuna offerta software sono forniti nella tabella 6.

Tabella 6. Componenti software

Pacchetti	Descrizione
Cisco Email Security Inbound Essentials	Il pacchetto Cisco Email Security Inbound Essentials offre protezione contro le minacce basate su e-mail, tra cui antispam, la soluzione antivirus Sophos, i filtri delle epidemie di virus e il clustering.
Cisco Email Security Outbound Essentials	Il pacchetto Cisco Email Security Outbound Essentials fornisce protezione contro la perdita di dati grazie alla conformità DLP, alla crittografia e-mail e al clustering.
Cisco Email Security Premium	Il pacchetto Cisco Email Security Premium combina le protezioni in entrata e in uscita incluse nelle due licenze Cisco Email Security Essentials sopra riportate, per la protezione contro le minacce basate su e-mail e la prevenzione contro la perdita di dati essenziali.
Offerte personalizzate	**Descrizione**
Cisco Advanced Malware Protection	Cisco Advanced Malware Protection (AMP) può essere acquistato in modalità personalizzata con il pacchetto software Cisco Email Security. AMP è una soluzione completa anti-malware che permette di rilevare e bloccare il malware, eseguire un'analisi continua e ricevere avvisi retrospettivi. AMP potenzia le funzionalità di rilevamento e blocco antimalware già disponibili in Cisco Email Security, quali la valutazione della reputazione e il blocco dei file, file sandboxing e analisi retrospettiva dell'analisi continua delle minacce, anche dopo che esse hanno superato il gateway e-mail.

Contratti di licenza software

Il contratto di licenza con l'utente finale (EULA) di Cisco e il Contratto di Licenza con l'utente finale supplementare (SEULA) di Cisco Web Security vengono forniti con tutti gli acquisti di licenze software.

Supporto per gli abbonamenti al software

Tutte le licenze Cisco Email Security comprendono il supporto essenziale per l'abbonamento al software, affinché le applicazioni business-critical siano disponibili, estremamente sicure e funzionino con prestazioni ottimali. Questo supporto fornisce agli utenti il diritto di usufruire dei servizi sottoelencati per l'intero periodo dell'abbonamento al software acquistato.

- Aggiornamenti software e aggiornamenti importanti per assicurare il funzionamento ottimale delle applicazioni con le funzionalità più recenti
- Cisco Technical Assistance Center (TAC) fornisce un supporto rapido e specializzato
- Strumenti online che sfruttano e ampliano le competenze interne all'azienda, migliorandone l'agilità.
- Apprendimento collaborativo che offre ulteriori competenze e opportunità di formazione.

Servizi Cisco

Nella Tabella 7 sono riepilogati i servizi Cisco disponibili per le soluzioni Cisco Email Security.

Tabella 7. Servizi Cisco per le soluzioni Cisco Email Security

Servizio	Descrizione
Servizi a marchio Cisco	• Cisco Security Planning and Design Service consente di implementare rapidamente e in modo economicamente conveniente una soluzione di sicurezza robusta. • Cisco Email Security Configuration and Installation Remote Service consente di ridurre i rischi di sicurezza mediante l'installazione, la configurazione e i test della soluzione. • Cisco Security Optimization Service supporta un sistema di sicurezza in evoluzione in grado di affrontare le nuove minacce alla sicurezza, con progetti, prestazioni e supporto ai cambiamenti del sistema.
Servizi di collaborazione e partner	• Cisco Collaborative Professional Services Network Device Security Assessment Service consente di mantenere un ambiente di rete avanzato identificando le lacune di sicurezza. • Cisco Smart Care Service assicura il funzionamento ottimale dell'azienda grazie al monitoraggio proattivo e mediante l'intelligence legata alla verifica estremamente sicura delle prestazioni della rete. • Inoltre, i partner Cisco forniscono un'ampia gamma di servizi aggiuntivi attraverso il ciclo di vita di pianificazione, progettazione, implementazione e ottimizzazione.
Finanziamenti Cisco	Cisco Capital® è in grado di realizzare soluzioni di finanziamento personalizzate in base alle esigenze specifiche delle aziende. Acquisendo subito la tecnologia Cisco è possibile usufruire immediatamente dei vantaggi che essa offre per l'azienda.

Servizi di assistenza Cisco SMARTnet

Per sfruttare al meglio l'investimento tecnologico, è possibile acquistare Cisco SMARTnet® Service per utilizzarlo con Cisco ESA. Cisco SMARTnet Service consente di risolvere rapidamente i problemi di rete grazie al supporto diretto e costante degli esperti Cisco, agli strumenti per il self-help e alla sostituzione rapida dell'hardware. Per ulteriori informazioni, visitare http://www.cisco.com/go/smartnet.

Come valutare le piattaforme Cisco ESA

Il modo migliore per comprendere i vantaggi delle piattaforme Cisco ESA servie C e serie X consiste nel partecipare al programma "Try Before You Buy". Per ricevere un'appliance di valutazione completamente funzionante da testare nella propria rete gratuitamente per 45 giorni, visitare il sito http://www.cisco.com/go/esa.

Come valutare Cisco Cloud Email Security Services

La soluzione basata su cloud è un servizio affidabile, tutto compreso, che fornisce un modello di implementazione flessibile per la sicurezza e-mail. Esso consente di ridurre i costi personali mediante la co-gestione e senza alcuna infrastruttura di sicurezza e-mail in loco. Il team responsabile dei clienti o il rivenditore Cisco possono agevolare la configurazione di una valutazione gratuita di 45 giorni.

Come valutare le piattaforme Cisco ESAV

1. Accedere a http://www.cisco.com/go/esa.
2. Sotto “Support”, sul lato destro, fare clic su “Software Downloads, Release and General Information”. Fare clic su “Download Software” e quindi sul collegamento relativo a un modello per visualizzare le immagini della macchina virtuale scaricabili e disponibili. Sarà anche disponibile una licenza di valutazione XML scaricabile. Sarà necessario scaricare una delle immagini e la licenza di valutazione XML.
3. Scaricare la seguente documentazione da Cisco.com:
   a. Guida di installazione di Cisco Security Virtual Appliance
   b. Documentazione per Cisco IronPort® Manufacturing - AsyncOS 9,0

4. Per iniziare, seguire le istruzioni fornite nella Guida di installazione di Cisco Security Virtual Appliance. Notare che le valutazioni di Cisco Content Security Virtual Appliance non sono coperte in Cisco SMARTnet Service e pertanto non sono supportate.

Informazioni sulla garanzia

Le informazioni sulla garanzia sono disponibili sul sito Cisco.com alla pagina Garanzie dei prodotti.

Perché scegliere Cisco?

Oggi la sicurezza della rete è di importanza fondamentale. La presenza continua di minacce e rischi, nonché le problematiche relative alla riservatezza e al controllo, rendono la sicurezza indispensabile per garantire la continuità aziendale, la protezione delle informazioni fondamentali e il mantenimento della reputazione del marchio. Le soluzioni di sicurezza Cisco integrate nella rete forniscono maggiore visibilità e controllo per proteggere costantemente l'azienda. La leadership di mercato, la protezione avanzata contro le minacce prima, durante e dopo un attacco, i prodotti innovativi e la longevità fanno di Cisco il fornitore ideale per rispondere alle esigenze di sicurezza.

Ulteriori informazioni

Per ulteriori informazioni, visitare http://www.cisco.com/go/emailsecurity.

Sede centrale Americhe
Cisco Systems, Inc.
San Jose, California (USA)

Sede centrale Asia e Pacifico
Cisco Systems (USA) Pte. Ltd.
Singapore

Sede centrale Europa
Cisco Systems International BV Amsterdam,
Paesi Bassi

Le filiali Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito Web Cisco all'indirizzo **www.cisco.com/go/offices**.

Stampato negli Stati Uniti C78-729751-05 12/14