Sophos Email

SOPHOS
Cybersecurity delivered.

Panoramica del prodotto e delle licenze

	Licenza	Descrizione delle caratteristiche	Sophos Email Standard	Sophos Email Advanced
	Compatibilità con provider di posta elettronica	Compatibile con tutti i servizi di posta elettronica, inclusi Gmail di Google Workspace e Microsoft 365: • Microsoft Exchange Online e Microsoft 365 • Microsoft Exchange 2003 o versione successiva • Gmail di Google Workspace Il supporto non è limitato solo a queste piattaforme: basta una semplice configurazione MX e Sophos Email è compatibile con qualsiasi servizio per il quale si controllano i domini e i record DNS.	✓	✓
	Integrazione delle regole del flusso di posta per Microsoft 365	Le regole di Sophos Mailflow creano una connessione diretta a Microsoft 365 dalla console di Sophos Central, senza bisogno di reindirizzare i record MX. Questo garantisce tempi di elaborazione più rapidi per tutte le e-mail, pur garantendo la stessa protezione avanzata. Disponibile per i clienti Sophos Email Advanced che usano Microsoft 365		✓
	Sincronizzazione con Active Directory e sincronizzazione con Azure Active Directory	La sincronizzazione con Microsoft Active Directory (AD Sync) e Azure AD Sync offre alle aziende un metodo semplicissimo per trasferire nel cloud i propri ambienti on-premise di Active Directory o Exchange. • AD Sync sincronizza automaticamente gli utenti con Sophos Email • Supporto completo dell'aggiornamento automatico dei dati di AD una volta che le aziende hanno completato il passaggio al cloud	✓	✓
	Immissione manuale dei record alias	Accesso amministratore per aggiungere manualmente record alias di indirizzi e-mail quando Active Directory non è disponibile	✓	✓
	Portale self-service per gli utenti finali	Sophos Email permette agli utenti finali di accedere ai seguenti strumenti: • Gestione delle e-mail in quarantena (per accettare/eliminare i messaggi di posta) • Modifica delle regole degli elenchi di autorizzazione/blocco • Visualizzazione dei messaggi in caso di interruzione del servizio, con la casella di posta di emergenza	✓	✓
	Policy per dominio/gruppo/utente	La creazione di policy di sicurezza specifiche per singoli utenti, gruppi o per il dominio intero può essere completata entro pochi minuti	✓	✓
	Ubicazione dei data center	Una scelta di data center a livello globale, per ottemperare ai requisiti di conformità alle normative sui dati e per migliorare l'esperienza degli utenti finali: • Regno Unito • Stati Uniti • Germania	✓	✓
CONTINUITÀ DEL BUSINESS	Spooling, per garantire che nessun messaggio venga smarrito*	Nell'eventualità di un'interruzione del servizio di posta Microsoft o Google Cloud, le e-mail dei destinatari vengono automaticamente inserite in una coda di Sophos Email, per poi essere consegnate una volta ripristinato il servizio (i tentativi di consegna vengono ripetuti per un massimo di 5 giorni)	✓	✓
	Accesso per gli utenti a una casella di posta di emergenza disponibile 24/7*	Accesso in lettura alle e-mail in coda, da una casella di posta di emergenza disponibile 24/7 nel portale utenti	✓	✓
	Avvisi per gli amministratori*	In caso di interruzione dei servizi dei provider di posta elettronica nel cloud di terze parti, vengono visualizzati avvisi di mancato recapito dei messaggi a un server/servizio	✓	✓

Sophos Email Panoramica del prodotto e delle licenze

	Licenza	Descrizione delle caratteristiche	Sophos Email Standard	Sophos Email Advanced
PROTEZIONE CONTRO LE MINACCE	Aggiornamenti delle minacce in tempo reale per bloccare i più recenti tipi di attacco	Gestita dai SophosLabs, Sophos Email è una soluzione che offre aggiornamenti in tempo reale per proteggere i sistemi delle minacce più recenti	✓	✓
	Rilevamento antispam, antivirus e antiphishing	Filtro delle e-mail in entrata e in uscita per bloccare i messaggi indesiderati: • Il filtro basato sulla reputazione blocca il 90% dello spam • Il nostro motore anti-spam si occupa del resto, inclusi i nuovi attacchi di phishing • Sender Genotype, la nostra tecnologia next-gen che filtra i messaggi in base alla reputazione, elimina lo spam inviato dalle botnet a livello di connessione IP, monitorando le richieste di connessione e respingendo quelle che danno prova di essere state inviate da botnet • Sophos Delay Queue offre protezione contro lo spam snowshoe	✓	✓
	Quarantena delle e-mail	I controlli preimpostati e facili da utilizzare di Sophos Email garantiscono la configurazione rapida delle policy per la quarantena, proteggendo l'azienda in pochi secondi. Successivamente, il portale per gli utenti finali consente agli utenti stessi di rilasciare le e-mail su richiesta, mentre i riepiloghi della quarantena integrati nei messaggi offrono un resoconto quotidiano dei messaggi mandati in quarantena, con l'opzione di rilasciarli direttamente dalla casella di posta	✓	✓
	Elenchi di autorizzazione/ blocco	Le policy di autorizzazione e blocco dei mittenti permettono agli amministratori di imporre restrizioni per i messaggi inviati o ricevuti da indirizzi e-mail, indirizzi IP e domini specifici, e supportano l'uso di caratteri jolly per consentire il blocco di domini di primo livello in base al paese. I banner intelligenti permettono agli utenti finali di personalizzare i propri elenchi di autorizzazione e blocco dei mittenti direttamente dal messaggio e-mail, mentre il Self Service Portal aiuta a gestire questi elenchi	✓	✓
	Autenticazione SPF, DKIM e DMARC in entrata	• Sender Policy Framework (SPF) per identificare gli indirizzi IP autorizzati a inviare e-mail dal dominio. • DKIM (Domain Keys Identified Mail) fornisce prova crittografica che i messaggi sono stati inviati da un mittente specifico e che non hanno subito manomissioni DMARC (Domain Message Authentication Reporting & Conformance) determina l'azione da intraprendere quando i messaggi non superano le verifiche SPF o DKIM del mittente	✓	✓
	Controlli delle anomalie nell'intestazione	• Il rilevamento delle anomalie nell'intestazione identifica se il nome del mittente che viene visualizzato corrisponde a uno dei nomi degli utenti interni	✓	✓
	Protezione post-recapito per Microsoft 365	La protezione post-recapito per Microsoft 365 è sempre attiva e rimuove automaticamente le e-mail di phishing contenenti URL che cambiano stato e diventano pericolosi		✓
	Protezione contro gli attacchi di phishing e imitazione	• Confronto tra il nome visualizzato nelle e-mail in entrata e il nome dei brand dei servizi cloud più frequentemente utilizzati a sproposito, con verifica dei nomi degli utenti VIP delle organizzazioni, per individuare eventuali corrispondenze • Analisi dei domini simili a domini legittimi, per identificare i domini che fingono di essere quelli di aziende legittime • I messaggi sospetti possono essere bloccati, messi in quarantena, taggati con un avviso nella riga dell'oggetto, oppure dotati di un banner che include un link diretto all'elenco di blocco a livello dell'utente		✓
	Protezione Time-of-Click degli URL	Riscrittura degli URL per verificare la reputazione dei siti web dei link inclusi nelle e-mail sia prima della consegna del messaggio, sia al momento del clic, bloccando gli attacchi nascosti e quelli ad azione ritardata		✓
	Sophos Sandbox	Una sandbox basata sul cloud, in grado di rilevare applicazioni indesiderate e malware noti e non, prima che abbiano la possibilità di eseguirsi		✓
PROTEZIONE DELLE INFORMAZIONI	Cifratura delle e-mail (TLS, S/MIME, con push)	Analizza automaticamente corpo del messaggio e allegati, alla ricerca di dati di natura sensibile, per semplificare la compilazione di policy per il blocco o la cifratura dei messaggi con pochissimi clic. In alternativa, è possibile fornire agli utenti l'opzione di cifrare le e-mail in maniera indipendente, grazie al nostro plugin per M365. • La cifratura con push protegge l'intero messaggio di posta oppure solamente gli allegati • L'implementazione della cifratura TLS previene l'intercettazione dei messaggi in transito • Aggiungi una firma digitale per verificare l'identità del mittente con S/MIME		✓
	Cifratura delle e-mail (con pull)	Disponibile con Sophos Email Advanced, è una cifratura opzionale completa dei portali web, che permette agli utenti di gestire, leggere e rispondere ai messaggi cifrati in un portale web sicuro.		**Add-on**
	Data Loss Prevention (prevenzione della perdita di dati)	La prevenzione della perdita dei dati e il controllo dei contenuti aiutano a prevenire i tentativi avanzati di violazione dei dati, utilizzando la cifratura delle e-mail basata sulle policy. Crea policy DLP con regole multiple per gruppi e singoli utenti, e garantisci la sicurezza dei dati di natura sensibile, grazie all'individuazione di informazioni finanziarie, sanitarie, riservate e personali in ogni e-mail e allegato.		✓

*Opzione non disponibile con l'integrazione delle regole del flusso di posta per Microsoft 365.

22-02-19 LG-IT (PS)

SOPHOS