

Presentación del producto y de las licencias

	Licencia	Descripción de funciones	Sophos Email Standard	Sophos Email Advanced
	Proveedores de servicios de correo electrónico compatibles	Compatible con todos los servicios de correo electrónico, incluidos Gmail de Google Workspace y Microsoft 365: <ul style="list-style-type: none"> • Microsoft Exchange Online y Microsoft 365 • Microsoft Exchange 2003 o posterior • Gmail de Google Workspace Estas no son las únicas plataformas compatibles: una sencilla configuración de MX es todo lo necesario y Sophos Email es compatible con cualquier servicio del que sea propietario del dominio y controle los registros DNS asociados.	✓	✓
	Integración de reglas de flujo de correo de Microsoft 365	Las reglas de Sophos Mailflow crean una conexión directa con Microsoft 365 desde la consola de Sophos Central, sin necesidad de redireccionamientos de registros MX. Esto garantiza un menor tiempo de procesamiento en todo el correo electrónico, al tiempo que se proporciona la misma protección avanzada. Disponibile para clientes de Sophos Email Advanced que utilicen Microsoft 365.		✓
	Sincronización de Active Directory y Sincronización de Azure Active Directory	Sincronización de Active Directory y Sincronización de Azure Active Directory ofrecen a las organizaciones una forma sencilla de trasladar a la nube entornos Active Directory o Exchange locales. <ul style="list-style-type: none"> • Mantenga a los usuarios sincronizados automáticamente con Sophos Email utilizando Sincronización de AD • Soporte completo para actualizar automáticamente los datos de AD en las empresas que se han trasladado totalmente a la nube 	✓	✓
	Introducir registros de alias manualmente	Acceso de administrador para añadir manualmente registros de alias de direcciones de correo electrónico cuando Active Directory no está disponible	✓	✓
	Portal de autoservicio para usuarios	Sophos Email proporciona a sus usuarios finales acceso a las siguientes herramientas: <ul style="list-style-type: none"> • Gestión de correo electrónico en cuarentena (aceptar/eliminar mensajes) • Edición de las reglas de las listas de permitidos y bloqueados • Consulta de mensajes en caso de que se produzca una interrupción utilizando la bandeja de entrada de emergencia 	✓	✓
	Políticas de usuario/grupo/dominio	Crear políticas de seguridad del correo electrónico únicas para usuarios, grupos o todo el dominio puede hacerse en minutos.	✓	✓
	Ubicaciones de centros de datos	Ajústese a las normativas de cumplimiento de datos y mejore la experiencia del usuario final con varias opciones de centros de datos globales: <ul style="list-style-type: none"> • Reino Unido • Estados Unidos • Alemania 	✓	✓
CONTINUIDAD DE LA ACTIVIDAD	Spool de correo para garantizar que no se pierdan nunca los mensajes*	Si se produce una interrupción en el servicio de correo electrónico de Microsoft o Google Cloud, los mensajes del destinatario se ponen en cola automáticamente con Sophos Email y se entregan cuando se restablece el servicio (período de reintentos de 5 días).	✓	✓
	Acceso del usuario a una bandeja de entrada de emergencia 24/7*	El acceso de lectura al correo electrónico en cola se proporciona desde una bandeja de entrada de emergencia 24/7 dentro del portal para usuarios finales.	✓	✓
	Alertas de administrador*	En el caso de que se produzcan interrupciones del proveedor del servicio de correo electrónico en la nube externo, se reciben alertas si el correo no puede entregarse a un servidor o servicio.	✓	✓

	Licencia	Descripción de funciones	Sophos Email Standard	Sophos Email Advanced
PROTECCIÓN CONTRA AMENAZAS	Actualizaciones en directo contra amenazas para detener los últimos ataques	Gracias al respaldo de SophosLabs, Sophos Email proporciona actualizaciones en directo para proteger contra las últimas amenazas.	✓	✓
	Detección antispam, antivirus y antiphishing	Filtrado de correo electrónico entrante y saliente para bloquear correo electrónico no deseado: <ul style="list-style-type: none"> • El filtrado por reputación bloquea el 90 % del spam • Nuestro motor antispam captura el resto, incluyendo los ataques de phishing más recientes • Sender Genotype, nuestra tecnología de filtrado por reputación next-gen, elimina el spam de redes de bots en el nivel de la conexión IP supervisando las solicitudes de conexión y rechazando aquellas con indicios de conexiones a redes de bots • Retraso de cola de Sophos ofrece protección frente al spam "snowshoe" 	✓	✓
	Cuarentena de correo electrónico	Gracias a los sencillos controles predefinidos de Sophos Email, las políticas de cuarentena de mensajes se configuran para proteger su negocio en cuestión de segundos. Luego el portal para usuarios finales permite a estos liberar mensajes a demanda, y los mensajes de resúmenes de cuarentena proporcionan a diario un compendio del correo en cuarentena, con la opción de liberarlo directamente desde la bandeja de entrada.	✓	✓
	Listas de permitidos y bloqueados	La política de remitentes permitidos y bloqueados permite a los administradores restringir mensajes de o a direcciones de correo electrónico, direcciones IP y dominios específicos, y admite el uso de comodines, lo que hace posible bloquear dominios de nivel superior (TLD) por países. Con los banners inteligentes los usuarios finales pueden actualizar sus listas de remitentes permitidos y bloqueados personalizadas desde el mismo correo electrónico, mientras que el portal de autoservicio permite administrar estas listas.	✓	✓
	Autenticación SPF, DKIM y DMARC entrante	<ul style="list-style-type: none"> • Sender Policy Framework (SPF): para identificar direcciones IP autorizadas para enviar correos electrónicos desde el dominio • Domain Keys Identified Mail (DKIM): ofrece pruebas criptográficas de que un mensaje lo ha enviado un remitente específico y que no se ha manipulado • Domain Message Authentication Reporting and Conformance (DMARC): determina qué hacer cuando un mensaje no supera las comprobaciones SPF o DKIM del remitente 	✓	✓
PROTECCIÓN CONTRA AMENAZAS	Comprobaciones de anomalías de encabezado	<ul style="list-style-type: none"> • La detección de anomalías de encabezado identifica si el nombre del remitente mostrado es el mismo que un nombre de usuario interno 	✓	✓
	Protección posentrega para Microsoft 365	La protección continua posentrega para Microsoft 365 elimina automáticamente los correos electrónicos de phishing que contienen nuevas URL infectadas tan pronto como cambia el estado de la amenaza		✓
	Protección contra la suplantación de identidad con phishing	<ul style="list-style-type: none"> • Compare el nombre mostrado de los mensajes entrantes con el nombre mostrado de marcas de servicios en la nube que se utilizan comúnmente de forma malintencionada, y con los VIP de la empresa, a fin de detectar coincidencias • Análisis de dominios de imitación para identificar nombres de dominio parecidos al dominio corporativo • Los mensajes sospechosos se pueden bloquear, poner en cuarentena, etiquetar con una advertencia en el asunto o añadir un banner con un enlace directo a la lista de bloqueo a nivel de usuario 		✓
	Protección de direcciones URL en el momento del clic	Reescritura de direcciones URL para comprobar la reputación del sitio web de los enlaces de correo electrónico antes de su entrega y en el momento en que se hace clic en ellos, con lo que se bloquean ataquesfurtivos diferidos.		✓
	Espacio seguro de Sophos	Espacio seguro basado en la nube capaz de detectar aplicaciones no deseadas y malware conocido y desconocido antes de que se ejecuten.		✓
PROTECCIÓN DE LA INFORMACIÓN	Cifrado del correo electrónico (TLS, S/MIME, basado en imposición)	Escanea los mensajes y los adjuntos de forma automática para detectar datos sensibles, lo que le permite establecer fácilmente políticas para bloquear o cifrar los mensajes con solo unos clics. Si lo prefiere, puede permitir que los usuarios cifren los mensajes personalmente con nuestro complemento de M365. <ul style="list-style-type: none"> • El cifrado basado en imposición protege todo el correo electrónico o solo los archivos adjuntos • El cifrado TLS impuesto evita interceptar los mensajes en tránsito • Añada una firma digital para verificar la identidad del remitente con S/MIME 		✓
	Cifrado del correo electrónico (basado en extracción)	Disponibile con Sophos Email Advanced, el cifrado integral de portal web opcional permite a los usuarios gestionar, leer y responder a mensajes cifrados en un portal web seguro.		Complemento
	Prevención de pérdida de datos	La prevención de pérdida de datos y el control de contenido ofrecen una prevención de filtraciones de datos avanzada con cifrado del correo electrónico basado en políticas. Cree políticas DLP de múltiples reglas para grupos y usuarios individuales a fin de garantizar la protección de información sensible gracias a la detección de información financiera, contenido confidencial, información médica y datos de información personal en todos los correos y adjuntos.		✓

*Función no disponible con la integración de reglas de flujo de correo de Microsoft 365.