

		Escudo de entrada Avanzado	Trustifi Suite Completa
Integración rápida y sencilla Sin cambios de arquitectura. Realizamos el proceso contigo		>	~
Buzones de correo libres de amenazas Escaneo completo de todos los componentes del correo electrónico (encabezados, enlaces, archivos adjuntos), utilizando los motores súper sofisticados de Trustifi que se actualizan diariamente contra los últimos ataques de correo electrónico.		>	▽
Sistema de cuarentena de correo electrónico Sistema completo y conveniente para poner en cuarentena correos electrónicos sospechosos/maliciosos. El administrador y/o los revisores reciben toda la información por correo electrónico con una opción conveniente y segura para tomar medidas inmediatas (liberar/eliminar/lista blanca/etc.) desde cualquier lugar y en tiempo real, incluso desde su teléfono móvil.		•	♥
Sistema de gestión mejorado Una plataforma basada en web para administrar usuarios/buzones de correo, configurar preferencias y adaptar el sistema a sus necesidades únicas eligiendo cómo manejar los correos electrónicos percibidos como sospechosos/maliciosos/otros, definiendo los revisores de seguridad de su organización que revisarán y tomarán medidas para correos electrónicos en cuarentena, decidiendo qué tipos de archivos se bloquean automáticamente, definiendo el umbral de detección de los motores de análisis y mucho más		>	♥
Personalización Configure una lista de permitidos/lista de bloqueo para dominios/direcciones/enlaces/archivos que afectan a todos sus usuarios, mientras que los usuarios individuales pueden configurar esas listas solo para ellos (y usted puede revisar/editar esas listas en cualquier momento)		>	♥
	ore correos electrónicos incorrectos, directamente a usted o a nosotros, mediante un banner en el stro complemento. Los administradores y revisores también pueden informar posibles falsos positivos	>	~
Registros de auditoría Sistema de registro interno para m	onitorear y rastrear cada acción administrativa realizada en el sistema.	>	▽
Buzones libres de spam Sistema de inteligencia artificial para detectar spam o correos electrónicos no deseados y evitar que lleguen a sus buzones de correo.		>	~
Elimina los ataques BEC sistema de inteligencia artificial of financieras) y evita que lleguen a su	que identifica textos que instan a los destinatarios a realizar acciones sensibles (principalmente	>	•
Sofisticado motor de reglas entrantes Mejore la seguridad y la eficiencia creando reglas de correo electrónico entrante personalizadas diseñadas para cumplir con cualquier requisito específico.		>	♥
Herramienta de respuesta a amenazas Escanee e identifique correos electrónicos potencialmente peligrosos que ya hayan recibido sus usuarios y elimine de manera efectiva estas amenazas eliminando los correos electrónicos de sus bandejas de entrada.		>	♥
Período de retención (datos en cuarentena/detectados) l año: mantenemos todos sus correos electrónicos en cuarentena hasta por l año (luego se eliminarán automáticamente, pero tiene la opción de guardar correos electrónicos específicos)		>	▽
Protección a un clic Realiza escaneos de enlaces en el momento de hacer clic (no cuando se envía el correo electrónico) Y evita la entrada a páginas maliciosas que han cambiado después del escaneo inicial o no han sido detectadas.		>	~
Gráficos de tendencias y conocimientos Supervise fácilmente las tendencias de los buzones de correo y las amenazas potenciales con visualizaciones y gráficos informativos. Los administradores pueden identificar rápidamente posibles inquietudes y recibir orientación sobre cómo abordarlas.		>	•
Servicios descubiertos Detecte automáticamente qué servicios web están utilizando sus usuarios para evitar casos de TI oculta y minimizar la exposición de datos confidenciales en su organización a terceros.		>	•
	nte firmas digitales únicas para sus dominios internos y los dominios de sus socios y clientes, para n ataques de suplantación de identidad o suplantación de identidad, incluso si fallan las medidas de	•	•
Escudo de Salida	Control de contenido inapropiado • Detecta y bloquea cualquier blasfemia o contenido relacionado con violencia, consumo de droga etc. enviado por tus usuarios. Gestión de cuarentena saliente • Los administradores y equipos de TI pueden establecer políticas para bloquear y poner en cuar		•
	Cifrado Cifrado Cifrado Cifrado Cifrado Cifrado Cifrado Cifrado Cifrado de correo electrónico de nivel NSA, además de DLP completo con un sofisticado motor de admitir cualquier caso de uso. Retransmisión móvil segura para una protección total en cualquier dispositivo. Recuperar, bloquear, modificar y establecer vencimientos para correos electrónicos ya enviados: Tokenización: en lugar de cifrar un correo electrónico completo, solo se reemplaza la información un cadena aleatoria de caracteres, conocida como token. Este método mejora la productividad, la apertura y facilita la búsqueda de correos electrónicos desde su bandeja de entrada Cestión de permisos	e reglas para / entregados n confidencial con as tasas de	•
▽	Configure revisores altamente específicos para tareas específicas como administrar correos e cuarentena, archivar casos o administrar usuarios del sistema. Aspecto personalizados	electrónicos en	
	 Personalice cada aspecto de sus correos electrónicos cifrados y su portal web de Trus agregando el logotipo de su empresa, combinación de colores, exenciones de responsabilidad más. 		
Archivado	Gestión de retención Los usuarios pueden elegir la cantidad de tiempo que se puede conservar un correo electrónico antes eliminarlo automáticamente.	de	•
en la nube con	Descubrimiento electrónico Los datos se conservarán en su estado original para que puedan usarse como evidencia para los regula cumplimiento o los equipos legales.	adores de	
indexación inteligente	Restaurar correos electrónicos eliminados restaurar correos electrónicos después de que fueron eliminados y moverlos nuevamente a la bandeja usuario	de entrada del	
	Compartir de forma segura la capacidad de compartirlo de forma segura (MFA, seguimiento, etc.), incluso con un destinatario/ider	tidad ———	•
	externo, y por un tiempo limitado Capacidades específicas para compartir consultas la capacidad de compartir solo un subconjunto específico de datos con opciones de filtrado.		~
	Visualización del estado del correo electrónico y de la información de seg mostrar el estado del correo electrónico (en cuarentena, liberado, ext.), seguimiento de correo electrónicos salientes (si el destinatario abrió el correo electrónico, ext.)	uimiento onico para correos	•
Servicio de detección y respuesta gestionada por correo electrónico (EMDR)	Seguridad del correo electrónico administrada por expertos. El equipo de ciberseguridad de Trustifi puede eliminar la carga de trabajo de su equip realizando las tareas necesarias para mantener su entorno de seguridad electrónico. • Revisión diaria de correos electrónicos en cuarentena para identificar posibles falsos positivos o forma electrónico de posibles puntos débiles en la postura de seguridad de su organización. • Actualización y mantenimiento de listas permitidas y listas de bloqueo • Encontrar y corregir errores de configuración relacionados con la seguridad del correo electrónicos.	o de TI de correo alsos negativos.	•



Proteja los correos electrónicos de su empresa con seguridad impulsada por IA info@ig.technology

