Trustifi

www.trustifi.com

	Trustifi Full Suite	Trustifi Full Suite +
Escudo de Entrada™		
1. **Fuentes de Inteligencia de Amenazas:** Aprovecha fuentes de datos globales para identificar y bloquear amenazas emergentes.	✓	✓
2. **Inteligencia Artificial para SPAM:** Utiliza inteligencia artificial para detectar y filtrar correos electrónicos no deseados.	✓	✓
3. **Inteligencia Artificial para GRAYMAIL:** Identifica y gestiona correos grises, que incluyen correos no deseados pero no maliciosos.	✓	✓
4. **Inteligencia Artificial para BEC:** Detecta y previene ataques de compromiso de correo electrónico empresarial.	✓	✓
5. **Control de Dominio de Suplantación:** Bloquea correos de dominios suplantados para prevenir la suplantación de identidad.	✓	✓
6. **Protección contra Phishing en URLs:** Escanea y bloquea URLs de phishing dentro de correos electrónicos.	✓	✓
7. **Protección contra Malware (Adjuntos):** Detecta y elimina archivos adjuntos maliciosos.	✓	✓
8. **Analizador de DMARC:** Monitorea y aplica políticas de DMARC para prevenir la suplantación de correos electrónicos.	✓	✓
9. **Respuesta a Amenazas:** Proporciona herramientas para una respuesta rápida a amenazas detectadas.	✓	✓
10. **Escaneo al Hacer Clic:** Escanea URLs en correos electrónicos en tiempo real al hacer clic.	✓	✓
11. **Búsqueda de URLs Maliciosas:** Busca activamente y neutraliza URLs maliciosas.	✓	✓
12. **Gestión de Cuarentena:** Aísla correos electrónicos sospechosos para un análisis y acción adicionales.	✓	✓
13. **Configuración Avanzada Personalizada:** Permite configuraciones para satisfacer necesidades organizacionales específicas.	✓	✓
Escudo de Salida™	✓	✓
1. **Cifrado AES256 a Demanda:** Cifra correos electrónicos utilizando AES256 para una mayor seguridad.	✓	✓
2. **Clasificación de Datos:** Categoriza y protege la información sensible en los correos electrónicos.	✓	✓
3. **Reglas de Prevención de Pérdida de Datos (DLP):** Aplica políticas de prevención para asegurar datos sensibles.	✓	✓
4. **Autenticación Multifactor para Destinatarios:** Requiere autenticación multifactor para los destinatarios de correos .	✓	✓
5. **Gestión de Cuarentena:** Aísla correos electrónicos salientes que activan políticas de seguridad para su revisión.	✓	✓
Smart Indexing Archivado en la Nube		
1. Gestión de Retención: Los usuarios pueden elegir el tiempo que un correo puede ser retenido antes de ser eliminado automáticamente	–	✓
2. eDiscovery: Los datos se conservarán en su estado original para que puedan ser utilizados como evidencia por los reguladores de cumplimiento o equipos locales	–	✓
3. Restauración de Correos eliminados: Recupera correos luego de su eliminación y los regresa a la bandeja	–	✓
4. Compartición segura: La capacidad de compartir de forma segura (con autenticación multifactor, seguimiento, etc.), incluso con un destinatario o identidad externa, y por un tiempo limitado.	–	✓
5.Capacidades de compartición de consultas específicas: La capacidad de compartir solo un subconjunto específico de datos con opciones de filtrado.	–	✓
6.Visualización del estado y seguimiento de correos: Muestra el estado del correo electrónico (en cuarentena, liberado, etc.), y el seguimiento de correos electrónicos salientes (si el destinatario abrió el correo, etc.).	–	✓

FUNCIONES OPCIONALES DE PAGO

Simulación de Amenazas

1. Plantillas personalizables: Utiliza plantillas dinámicas que replican los correos electrónicos de ataques de phishing más recientes y comunes, asegurando sesiones de entrenamiento excepcionalmente realistas.

2. Amplia gama de técnicas sofisticadas

3. Analíticas detalladas: Recibe informes completos sobre las interacciones de los usuarios y realiza un seguimiento de las mejoras a lo largo de múltiples campañas.

4. Entrenamiento y evaluación integrados: Involucra a los usuarios en ataques simulados de correo electrónico seguidos de evaluaciones específicas.

5. Banners inteligentes: Adjunta banners a los correos electrónicos de usuarios que fallaron en simulaciones de phishing, ofreciendo consejos para mejorar la concienciación sobre la seguridad del correo electrónico.

Protección de Cuentas Comprometidas

1. Detección de Anomalías de Usuario: Identifica comportamientos inusuales que pueden indicar una cuenta comprometida.

2. Monitoreo de Geolocalización: Rastrea las ubicaciones de inicio de sesión para detectar actividad sospechosa.

3. Gestión de Dispositivos: Monitorea y controla los dispositivos que acceden a la red.

4**. Escaneo de la Web Oscura:** Busca en la web oscura credenciales comprometidas y amenazas.

5. Monitoreo de la Red: Observa continuamente la actividad de la red en busca de señales de toma de cuentas.

Servicio de Detección y Respuesta Administrada de Correos Electrónicos (EMDR)

Seguridad de correo electrónico gestionada por expertos. El equipo de expertos en ciberseguridad de Trustifi puede reducir la carga de trabajo de tu equipo de TI al realizar las tareas necesarias para mantener tu entorno de seguridad de correo

1. Revisión diaria de correos electrónicos en cuarentena para identificar posibles falsos positivos o falsos negativos.

2. Identificación de posibles puntos débiles en la postura de seguridad de tu organización.

3. Actualización y mantenimiento de listas de permitidos y bloqueados.

4. Detección y corrección de configuraciones incorrectas relacionadas con la seguridad del correo electrónico.

Trustifi facilita a su personal de seguridad de TI obtener la protección que necesitan, incluyendo alertas, trazabilidad, monitoreo y concienciación, al mismo tiempo que es sencillo, transparente y lo suficientemente fácil para que sus usuarios finales puedan aplicar toda esta seguridad con solo hacer clic en un botón.

www.trustifi.com

info@ig.technology

1 844-249-6328

www.ig.technology

technologies