

Email Security Cloud Integrated

Proteja su inversión en M365 con una solución de seguridad del correo electrónico con tecnología de IA.

El problema

Las funciones de seguridad nativas de Microsoft 365, incluidas Exchange Online Protection (EOP) y Microsoft Defender para Office 365, tienen cada vez más problemas con el sofisticado panorama de amenazas actual. Aunque estas herramientas ofrecen seguridad fundamental para la colaboración, se les dificulta detectar y detener ataques avanzados que aprovechan la arquitectura de seguridad estandarizada de Microsoft. Los actores de amenazas eluden las defensas de Microsoft con sofisticadas técnicas de ingeniería social, ataques al correo electrónico empresarial y ataques con tecnología de IA que parecen legítimos para los sistemas de detección basados en reglas. Los recientes incidentes de seguridad destacan las limitaciones de confiar solo en la seguridad nativa de Microsoft. Las entidades se enfrentan a nuevos retos con los complejos requisitos de configuración de seguridad de Microsoft y la restricción de las funciones de protección avanzadas a las licencias Premium. Para esta brecha de seguridad se necesita un enfoque más sofisticado.

La solución

Email Security Cloud Integrated de Mimecast ofrece una protección completa al aumentar las capacidades nativas de seguridad del correo electrónico de Microsoft 365 con un enfoque avanzado multicapa. Con tecnología de IA avanzada, Cloud Integrated se integra a la perfección con Microsoft 365 para ofrecer las mejores funciones de detección que bloquean hasta los ataques de correo electrónico más sofisticados. Las capacidades avanzadas de análisis del comportamiento controlan los patrones de comunicación, aprovechan los grafos sociales para detectar anomalías y detectan el lenguaje NLP de amenazas para detener los intentos de ataques al correo electrónico empresarial antes de que lleguen a los usuarios. Las entidades se benefician

de una solución optimizada desde el primer momento, con una administración simplificada a través de una interfaz intuitiva que se puede implementar en menos de cinco minutos.

Valor de Mimecast

- **Obtenga la mejor seguridad del correo electrónico con tecnología de IA**
Proteja a su entidad con la mejor detección del sector con tecnología de, en la que confían 42 000 clientes.
- **Cierre las brechas en la protección del correo electrónico M365**
Detenga las amenazas que Microsoft pasa por alto: el equivalente a un malware, phishing o correo electrónico no fiable reciben los empleados cada siete horas.
- **Simplifique drásticamente la seguridad del correo electrónico**
Dedique menos tiempo a gestionar la seguridad del correo electrónico con una solución optimizada y lista para usar, muy intuitiva y que se implementa por completo en menos de cinco minutos.

2900 MILLONES EN PÉRDIDAS debido a BEC en 2023¹

El **40 % DE LOS ATAQUES POR CORREO ELECTRÓNICO** incluyen BEC y pretexto²

¹ www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report
² www.verizon.com/business/resources/reports/dbir/

Característica:	Detalles:
BEC	<ul style="list-style-type: none"> • Analizar la fuerza de la relación entre el remitente y los destinatarios • Detectar lenguaje específico de amenazas dentro de correos electrónicos relacionados con categorías de BEC, como: <ul style="list-style-type: none"> • Solicitudes de ayuda para realizar tareas • Transferencias bancarias falsas • Indicadores de urgencia • Conmutadores de canales de comunicación • Estafas con tarjetas regalo • Estafas bancarias y financieras • Interpretar el contexto, el tono y las implicaciones de los mensajes para determinar la verdadera intención • Actualizar los banners de advertencia para correo electrónico con IA en tiempo real en todos los dispositivos
Amenazas internas	<ul style="list-style-type: none"> • Análisis de correos electrónicos internos y salientes para proteger contra la propagación lateral de malware y enlaces de phishing
Malware	<ul style="list-style-type: none"> • Poner en cuarentena los archivos maliciosos conocidos con detección automática • Analizar los archivos adjuntos protegidos por contraseña en busca de posibles amenazas • Inspección mediante protección multicapa contra malware para defenderse de las amenazas conocidas y los ataques de día cero • Realizar análisis estáticos de archivos y ejecutar pruebas sandbox para archivos sospechosos
Phishing	<ul style="list-style-type: none"> • Reescribir todos los enlaces en los correos electrónicos y los asuntos para el escaneo al hacer clic • Escanear enlaces con análisis multifase y detección de amenazas basada en aprendizaje automático • Proteger contra el robo de credenciales y códigos QR maliciosos en correos electrónicos y adjuntos • Aislar los navegadores al acceder a dominios desconocidos • Analizar enlaces de descarga directa con escaneo de archivos estáticos y pruebas sandbox
Administración	<ul style="list-style-type: none"> • Gestionar la administración de forma centralizada con una única consola web • Configurar notificaciones de detecciones para administradores y usuarios finales • Acceder a información detallada por detección para facilitar el análisis • Crear políticas personalizables que se adapten a los requisitos de la entidad • Habilitar la creación de informes nativos de usuario final en Microsoft Outlook • Corregir los mensajes maliciosos con un solo clic • Restaurar la configuración de Mimecast en caso de error de configuración • Integración perfecta con proveedores como Splunk, Microsoft y otros
Escaneo de vulnerabilidades	<ul style="list-style-type: none"> • Buscar amenazas sin interrumpir el flujo de correo • Escaneo retrospectivo de 30 días
Complementos disponibles	<ul style="list-style-type: none"> • Collaboration Security • DMARC Analyzer • Mimecast Engage • Sync and Recover

Casos de uso

Ataques de phishing y compromiso del correo electrónico empresarial (BEC)

La defensa de Mimecast contra los sofisticados ataques de phishing y BEC actúa como una plataforma integrada. El proceso comienza cuando las fuentes de amenazas y los protocolos de autenticación del correo electrónico analizan los mensajes entrantes. Luego, el Procesamiento del Lenguaje Natural (PLN) extrae el texto y emplea el modelado de amenazas para analizar las pistas contextuales e identifica los ataques sin carga antes de que lleguen a los usuarios. El grafo social construye un grafo de identidad basado en las relaciones remitente-receptor, que le permite detectar actividades anómalas. Cuando se identifican posibles amenazas, los banners dinámicos alertan a los usuarios de estos riesgos. Las funciones de escaneo de adjuntos y enlaces funcionan juntas, incluso la protección contra el robo de credenciales y la detección de ataques multifase, que analizan todos los enlaces para identificar páginas de phishing ocultas y contenido malicioso.

Amenazas de malware y ransomware

El completo sistema de detección de malware de Mimecast emplea múltiples capas de protección para garantizar máxima seguridad. Los archivos se comparan con la base de datos propia de Mimecast, que mantiene un registro de los archivos escaneados previamente. Para mayor seguridad, se utilizan varios motores antivirus para detectar una gama más amplia de amenazas. Se realiza un rápido análisis estático de los archivos, para buscar características sospechosas como código oculto, estructuras inusuales o conexiones a sitios maliciosos conocidos. Por último, los archivos se analizan en detalle en un entorno sandbox de emulación completa, que simula un sistema informático integral.

Mitigar un ataque de phishing

Ante un ataque de phishing, se pueden utilizar herramientas de corrección nativas de Mimecast para gestionar y mitigar con eficacia las amenazas sin depender de sistemas externos. En la página de inicio de detección, los administradores pueden identificar rápido el alcance de la amenaza y buscar más indicadores de compromiso, simplificando el proceso de categorización de amenazas y respuesta. La corrección de amenazas permite la eliminación racionalizada de correos electrónicos afectados, minimiza los posibles daños y garantiza una respuesta rápida.

Descubra y corrija las amenazas con la seguridad avanzada de Mimecast

Comience hoy su análisis gratuito de 30 días para descubrir las amenazas que Microsoft pasa por alto. Se implementa en pocos minutos sin afectar a las comunicaciones por correo electrónico.

<https://www.mimecast.com/free-trial/>