HOJA DE DATOS

Email Security Cloud Gateway

Su aliado en seguridad y resistencia del correo electrónico con IA para M365 y Google Workspace

El Problema

Los ataques avanzados de phishing, las estafas de compromiso del correo electrónico empresarial (BEC) y las tácticas maliciosas son solo algunas de las amenazas que su entidad debe enfrentar. Las soluciones de seguridad del correo electrónico tratan de mantener el ritmo y suelen pasar por alto intentos avanzados de ingeniería social, malware de día cero y ataques de suplantación de dominios, que ponen en peligro sus comunicaciones empresariales. Y a medida que los atacantes se centran más en plataformas como M365 y Google Workspace, es esencial contar un enfoque de seguridad del correo electrónico multicapa.

La solución

C omo Secure Email Gateway basado en la nube, Mimecast Email Security Cloud Gateway está diseñado para mantener seguros hasta los entornos de mensajes más complejos gracias a sus capacidades de inspección multicapa, potenciadas por defensas tradicionales, inteligencia de amenazas e IA avanzada. Nuestra solución integral inspecciona cada elemento de un correo electrónico en tiempo real y detiene las amenazas antes de que lleguen al usuario. Con políticas personalizables, controles granulares y una amplia gama de soluciones complementarias, Cloud Gateway se integra a la perfección con su pila de seguridad existente y proporciona capacidades de corrección automatizadas. Permite a los equipos de TI y de seguridad controlar con eficacia el riesgo y la complejidad, lo que permite a su entidad defenderse de ataques sofisticados al correo electrónico sin poner en peligro la continuidad de la actividad.

2900 MILLONES

en pérididas a debido a BEC en 2023[1]

EL 40 %

de los ataques por correo electrónico incluyen bec y pretexto[2]

Valor de Mimecast

- **Obtenga la mejor protección**
  Bloquee todas las amenazas del correo electrónico con la detección líder del sector con tecnología de IA, en la que confían 40 000 clientes.
- **Domine la complejidad**
  Gestione fácilmente entornos de correo electrónico complejos; consolide y simplifique los servicios de seguridad.
- **Simplifique las operaciones de seguridad**
  Reduzca la carga, mantenga a la gente informada y capacitada.

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

Característica	Detalles
BEC	• Protección contra ataques de ingeniería social, engaño por homoglifo/homografía y suplantación de identidad • Análisis de la fuerza de las relaciones entre el remitente y los destinatarios dentro de la entidad* • Detección de lenguaje específico de amenazas dentro de mensajes relacionados con categorías de BEC, como pedidos de ayuda para realizar tareas, transferencias bancarias falsas, urgencias, cambios de canal de comunicación, tarjetas regalo, estafas bancarias y financieras* • Centrarse en comprender el contexto, los matices y las implicaciones del mensaje para interpretar con precisión la verdadera intención* • Banners de advertencias para mensajes con tecnología de IA que aparecen y se actualizan en tiempo real en todos los dispositivos en función del nivel de riesgo*
Amenazas internas	• Detección de direcciones potencialmente erróneas para defenderse de las filtraciones de datos* • Análisis de correos electrónicos internos y salientes para protegerse contra personas internas comprometidas, descuidadas y malintencionadas
Malware	• Protección multicapa contra malware conocido y amenazas de día cero • Análisis estático de archivos y sandboxing de emulación total • Conversión segura de archivos adjuntos en documentos PDF benignos • El portal de descifrado permite escanear malware y URL protegidos por contraseña
Phishing	• Reescritura de URL de todos los enlaces de los mensajes, con análisis de la hora del clic • Escaneo multifase profundo de URL con detección de amenazas basada en aprendizaje automático y protección de credenciales • Protección de códigos QR en correos y archivos adjuntos con escaneo profundo de URL • Escaneo de enlaces de descarga directa con análisis estático de archivos y sandboxing
Administración	• Administración central con una única consola basada en web • Compatibilidad con M365, Google Workspace, local, híbrido y otros • Administración avanzada y federada de cuentas para actividades frecuentes de FyA • Enrutamiento inteligente del correo basado en indicadores, destinatarios o políticas • Sincronización automatizada con IAM para control de políticas y acceso • Información centralizada sobre amenazas y flujos de trabajo administrativos simplificados • Corrección automatizada o manual de correos no seguros, no deseados o maliciosos • Ingesta de fuentes de amenazas específicas para el usuario y tendencias de amenazas regionales en SIEM, SOAR o TIP • Fácil integración con proveedores como Splunk, CrowdStrike, Netskope y otros
Complementos disponibles	• Cloud Archive • Continuity • DMARC Analyzer • Large File Send • Mimecast Engage • Mimecast Email Incident Response • Secure Messaging

*requiere Protección Advanced BEC

Casos de uso de seguridad del correo electrónico

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

La defensa de Mimecast contra los sofisticados ataques de phishing y BEC está muy integrada. Las fuentes de amenazas y los protocolos de autenticación del correo inspeccionan los mensajes. Luego, el Procesamiento del Lenguaje Natural (PLN) extrae el texto y emplea el modelado de amenazas para analizar pistas contextuales e identifica ataques sin carga antes de que lleguen a los usuarios. La tecnología de grafos sociales crea un grafo de identidad de las relaciones remitente-receptor, que permite detectar actividades anómalas con banners dinámicos que alertan a los usuarios de posibles amenazas. Las funciones de escaneo de adjuntos y URL de la plataforma, incluidas la protección contra el robo de credenciales y la detección multifase de ataques, escanean todos los enlaces para detectar páginas de phishing.

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 y se puede integrar con los datos de inteligencia sobre amenazas específicos del cliente. Para mayor seguridad, se utilizan varios motores antivirus para detectar una gama más amplia de amenazas de malware. 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. Como opción, con la conversión segura de archivos, se pueden eliminar los ejecutables potencialmente peligrosos antes de entregar el archivo.

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. Mediante análisis y respuesta, los analistas 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 los correos electrónicos afectados directamente de las bandejas de los usuarios, minimiza los posibles daños y garantiza una respuesta rápida. Además, estas capacidades de corrección se pueden utilizar con herramientas integradas como las plataformas SOAR o XDR.