DATASHEET

Seguridad del correo electrónico, protección basada en MX

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 de correo electrónico a las que debe enfrentarse su entidad. A las soluciones de seguridad del correo electrónico les cuesta seguir el ritmo y suelen pasar por alto intentos avanzados de ingeniería social, malware de día cero y ataques de suplantación de dominios, lo que pone en peligro las comunicaciones de su entidad. Y, a medida que los atacantes se centran más en plataformas como M365 y Google Workspace, se hace cada vez más esencial contar con un enfoque de seguridad del correo electrónico multicapa.

La solución

Al ser una solución de Secure Email Gateway basada en la nube, el sistema de protección basada en MX de Mimecast está diseñado para proteger hasta los entornos de correo electrónico más complejos gracias a sus capacidades de inspección multicapa, potenciadas por defensas tradicionales, inteligencia sobre 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, esta solución se integra a la perfección con su pila de seguridad existente y proporciona capacidades de corrección automatizadas. Esto permite a los equipos de TI y de seguridad controlar el riesgo de manera eficiente y reducir la complejidad para que, de esta forma, su entidad pueda defenderse de ataques sofisticados al correo electrónico sin poner en peligro la continuidad de la actividad.

6300 MILLONES DE DÓLARES

en pérdidas debido a ataques BEC en 2024[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 basadas en el correo electrónico con la detección líder del sector con IA, en la que ya confían 42 000 clientes.
- **Reduzca la complejidad**
  Gestione con facilidad entornos de correo electrónico complejos y consolide y simplifique los servicios de seguridad.
- **Simplifique las operaciones de seguridad**
  Reduzca la carga y mantenga a las personas informadas y capacitadas.

1 Verizon DBIR, 2025
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 en correos electrónicos vinculados a categorías de BEC, como solicitudes de ayuda para realizar tareas, transferencias bancarias falsas, urgencias, cambios de canal de comunicación, tarjetas regalo y estafas bancarias y financieras • Interpretación del contexto, los matices y las implicaciones del mensaje para determinar con precisión la verdadera intención • Banners de advertencias para correos electrónicos 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 usuarios internos comprometidos, negligentes y malintencionados
Malware	• Protección multicapa contra malware conocido y amenazas de día cero • Análisis estático de archivos y sandboxing de emulación completa • 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 en el momento del clic • Escaneo profundo de URL en varias fases 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 a través de una única consola web • Compatibilidad con M365, Google Workspace, entornos locales, híbridos 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

Casos de uso de la seguridad del correo electrónico

Ataques de phishing y de 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 identificar ataques sin carga útil con el fin de evitar 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 archivos 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 la 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 análisis estático rápido 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 completo. De manera opcional, 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 de un modo eficiente las amenazas sin depender de sistemas externos. Mediante las funciones de análisis y respuesta, los analistas pueden identificar rápido el alcance de la amenaza y buscar más indicadores de compromiso, lo que simplifica el proceso de categorización y de respuesta a las amenazas. La corrección de amenazas simplifica la eliminación de los correos electrónicos afectados directamente de las bandejas de correo 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.