Total **Fraud Protection®**

Cyxtera

DMARC Compass®

Liderando la **Autenticación de Emails**

El fraude vía email está en crecimiento

El canal de email continua siendo el principal vector de actividad maliciosa. La suplantación online de CEOs, el phishing dirigido a empleados, y las estafas para consumidores representan miles de millones de dólares en pérdidas para entidades gubernamentales, privadas y públicas. La protección del canal de email contra el fraude previene el robo de fondos y el deterioro de la reputación de una organización.

Protección de emails

DMARC Compass elimina el phishing vía email al bloquear mensajes no autorizados antes de que lleguen a los buzones de los empleados, socios y clientes. Adicionalmente, DMARC Compass brinda una tasa de entrega de mensajes más alta al permitir que los proveedores de email distingan más fácilmente entre phishing y campañas legítimas.

1 de cada 4.500 emails es un ataque de phishing.[1]

Las compañías pierden US$3.100 millones por causa de la afectación de emails.[2]

El número de sitios web de phishing se incrementó en 250% entre octubre de 2015 y marzo de 2016.[3]

Bloqueo de phishing en tiempo real

Las políticas de autenticación de emails identifican mensajes corporativos válidos y bloquean el phishing dirigido a empleados y usuarios. Nuestros clientes controlan si el phishing y los mensajes fraudulentos detectados son enviados al buzón de spam de los usuarios o eliminados del todo.

Desactivación de URLs maliciosas enviadas a empleados y usuarios

Los emails enviados a usuarios y empresas están disponibles para su evaluación en tiempo real en nuestro portal en la nube. Las URLs de phishing adjuntas, los enlaces de malware y las aplicaciones móviles maliciosas son analizadas y desactivadas en un tiempo líder en la industria de 3.6 horas.

Incremento del porcentaje de apertura de campañas de marketing

Utilice DMARC Compass para identificar y clasificar campañas de marketing genuinas, emails de facturación y remitentes de servicios. Ajuste las políticas de seguridad para incrementar la entrega de mensajes provenientes de terceros.

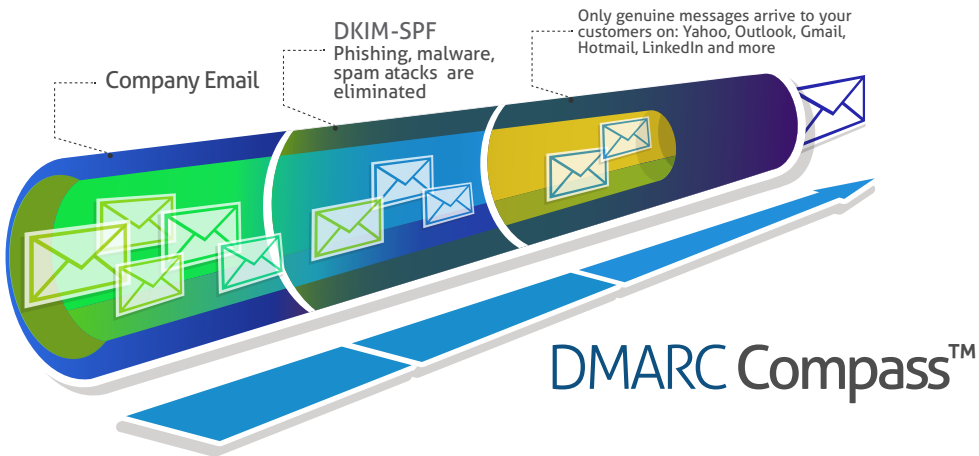
[1] http://www.gartner.com/document/code/300446?ref=ggrec&refval=3256818
[2] https://www.ic3.gov/media/2016/160614.aspx
[3] http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

Total Fraud **Protection®**

Cyxtera

¿Cómo DMARC Compass mejora la seguridad y entrega de emails?

DMARC Compass es un portal en la nube que reúne datos provenientes de los receptores de email. Este portal asiste en la implementación de tres protocolos - DMARC, SPF, y DKIM – permitiendo así que entidades receptoras como Microsoft y Gmail eviten que el phishing llegue a los usuarios, socios y empleados de su organización.



Obtenga resultados de los procesos de autenticación y entrega de emails

Todos los emails son autenticados y clasificados según el tipo de remitente. Los emails que fallen la autenticación pueden ser bloqueados o enviados a cuarentena.

Reciba los resultados de la autenticación

- **DMARC** provee reportes SPF, DKIM y sobre entrega de emails. Identifique fraudes & errores de configuración.
- **DKIM** suministra una clave única para cada email que certifica la legitimidad del mensaje.
- **SPF** declara públicamente los únicos servidores autorizados para el envío de email corporativo.

Clasifique remitentes

- **Los servidores internos** de email son monitoreados para asegurar la autenticación SPF y DKIM, y la entrega de mensajes.
- **Las entidades** que envían mensajes a su nombre son monitoreadas para permitir que sus mensajes sean entregados como si provinieran de servidores internos.
- **Los mensajes no autorizados** pueden ser bloqueados con el fin de prevenir la entrega de fraudes.

Evalúe los mensajes que fallen la validación DMARC

Aquellos emails que fallen la autenticación DMARC se encuentran disponibles en nuestro portal para su análisis.

- **Los contenidos de los mensajes** pueden ser desplegados fácilmente en el portal de DMARC Compass.
- **Los encabezados** proveen resultados de autenticación para cada etapa del proceso de entrega de emails.
- **Los archivos adjuntos** pueden ser examinados en busca de malware.
- **Las URLs incluidas en los mensajes** son rastreadas y analizadas para determinar si se tratan de phishing

Aproveche recursos adicionales

Una variedad de recursos adicionales permite que cada organización controle su entorno de email de acuerdo a sus necesidades.

- **El portal en la nube** suministra toda la información pertinente sin necesidad de instalar software localmente.
- **El equipo de soporte** se encuentra listo para resolver ágilmente cualquier tema o inquietud que nuestros clientes puedan tener.
- **Los reportes personalizables** permiten escoger que aspectos del trafico de email se quieren mostrar. Guarde los reportes y programe su entrega vía email.
- **Nuestros servicios profesionales** guían a las organizaciones hacia la exitosa implementación de la políticas de seguridad.

tfp@cyxtera.com