proofpoint.

GUÍA DE PLANIFICACIÓN

Migración de un gateway de correo electrónico tradicional a Proofpoint

Los gateways de correo electrónico (SEG) tradicionales se crearon para bloquear el spam y el malware conocido. Sin embargo, en la actualidad, los ciberdelincuentes recurren a amenazas sofisticadas y técnicas multivectoriales, como las estafas Business Email Compromise (BEC), la usurpación de cuentas (ATO, Account Takeover), el phishing mediante códigos QR y la elusión de la autenticación multifactorial (MFA), amenazas que los gateways de correo electrónico no estaba diseñadas para neutralizar. Por lo tanto, cuando utiliza un gateway tradicional de este tipo, su organización corre un mayor riesgo de sufrir un incidente y de ver cómo se disparan sus costes operativos.

Si desea adoptar Proofpoint para reforzar su seguridad, esta guía de planificación le ayudará a preparar su proceso de migración. Está diseñada para clientes de Barracuda, Cisco (IronPort), Forcepoint (Websense), Symantec Email Security.cloud (MessageLabs), Trellix (FireEye/McAfee) y Trend Micro.

Estas instrucciones paso a paso le ayudarán a evaluar la eficacia de su gateway tradicional (heredado), calcular sus costes y establecer un calendario para la migración. Proofpoint ofrece opciones de despliegue flexibles (migración completa al gateway, despliegue de API o un enfoque gradual) para que pueda elegir la que mejor se adapte a su entorno. Para simplificar este proceso, su equipo de Proofpoint puede proporcionarle herramientas gratuitas (evaluación rápida de riesgos, informe de desviaciones, evaluación del valor añadido) para que pueda cuantificar la reducción de riesgos y el retorno de la inversión.

Paso 1: Cuantificar la eficacia de su protección actual

Comience por la visibilidad. Mida la eficacia de sus defensas actuales (y lo que se les escapa) para establecer una base de referencia clara.

- Revise los informes de falsos negativos, que se encuentran en los registros de administración y en las incidencias de SIEM/IR. Esto puede ayudarle a comprender la magnitud y el alcance de las detecciones perdidas.
- Documente el porcentaje de correos electrónicos denunciados por los usuarios que se han confirmado como verdaderos positivos, ya que estos datos le ayudarán a cuantificar el tiempo que dedican los analistas a resolver los falsos positivos.
- Identifique los incidentes de usurpación de cuentas (ATO) detectados por otros sistemas. Por ejemplo, el uso indebido de las reglas del buzón de correo electrónico, las alertas relacionadas con la imposibilidad de desplazamiento o la geolocalización, así como la elusión de la autenticación multifactorial.
- Revise los intentos de phishing interno o lateral detectados por otros sistemas o denunciados por los usuarios.
- Realice una evaluación rápida de riesgos de Proofpoint. Este servicio le proporcionará visibilidad basada en datos sobre las amenazas que su gateway de correo electrónico existente o su sistema Microsoft 365 podrían no detectar.

Este conjunto de soluciones forma parte de la plataforma Human-Centric Security, que mitiga las cuatro principales áreas de riesgo asociado a las personas.

Paso 2: Calcular el coste de mantener la situación actual

La seguridad no solo se mide en términos de elementos bloqueados, sino también en términos de eficacia de las operaciones. Evalúe el tiempo, el esfuerzo y el nivel de atención que dedican los analistas a la clasificación manual, los falsos positivos y los flujos de trabajo fragmentados para poner de relieve el coste real que supone mantener su gateway tradicional.

- Documente el número de clics y los minutos/horas que necesitan sus analistas para examinar un solo incidente de phishing. (No es raro que los analistas utilicen más de 12 clics y dediquen varias horas a resolver cada incidente). Identifique también los lugares donde suelen producirse retrasos.
- Realice un seguimiento de las horas que dedican los analistas a clasificar el buzón de correo malicioso. Calcule cuánto tiempo dedican los analistas a examinar los correos electrónicos denunciados por los usuarios cada semana. Determine también qué porcentaje de estos mensajes son amenazas reales en comparación con las falsas alarmas.
- Calcule el tiempo que su equipo dedica a preparar informes. Ante el tiempo que le lleva a su equipo recopilar y dar formato a las métricas de seguridad para elaborar informes destinados a los directivos o al consejo de administración. Esta tarea suele requerir exportaciones manuales de datos y operaciones en hojas de cálculo.
- Hable con los analistas de seguridad y averigüe cuáles son sus motivos de frustración. ¿Cuáles son los problemas más frecuentes? Por ejemplo: el ruido, los falsos positivos y la multiplicación de consolas.

Paso 3: Elegir su ruta de migración

Su entorno y sus prioridades cambiarán, y la seguridad de su correo electrónico debe hacer lo propio. Proofpoint le ofrece una flexibilidad que los proveedores con un único modelo no pueden proporcionarle. Nos diferenciamos por ofrecer tres vías de migración.

- **Opción 1: Refuerzo de la seguridad con protección basada en API.** Esta opción requiere poco esfuerzo y tiene un gran impacto. Integre Proofpoint Core Email Protection - API con Microsoft 365 para obtener protección inmediata contra amenazas como las estafas Business Email Compromise (BEC), la usurpación de cuentas (ATO) y el phishing. Este modelo también admite la transición de un gateway de correo electrónico tradicional a un modelo Microsoft + Proofpoint, garantizando una protección continua durante y después de la migración.
- **Opción 2: Despliegue de la API seguida de la migración del gateway.** Esta opción requiere un esfuerzo moderado, pero tiene un impacto mayor. Comience por desplegar la API de Proofpoint para obtener rápidos beneficios operativos y reducir los riesgos. A continuación, realice una transición gradual al gateway de correo electrónico seguro de Proofpoint para tener control sobre el enrutamiento, responder a las necesidades cambiantes en materia de cumplimiento normativo o garantizar una defensa avanzada de múltiples capas.
- **Opción 3: Sustitución completa del gateway.** Desactive por completo su gateway de correo electrónico tradicional y migre sus registros MX a la solución de Proofpoint para obtener el máximo control y una protección completa del correo electrónico antes de la entrega.

Paso 4: Planificar la migración y lanzar un proyecto piloto

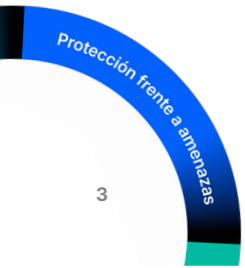
Valide los resultados antes del despliegue completo. Un proyecto piloto controlado le permite probar Proofpoint en paralelo con su gateway de correo electrónico actual, confirmar las ventajas en términos de una detección más eficaz y una respuesta más rápida, y reforzar la confianza de la dirección gracias a datos concluyentes.

- Defina sus criterios de éxito desde el principio. ¿Qué resultados desea obtener? Por ejemplo: detección mejorada de amenazas, reducción de falsos positivos, corrección más rápida y prevención de la usurpación de cuentas (ATO).
- Observe las posibles mejoras en la detección ejecutando la protección de correo electrónico de Proofpoint en modo silencioso.
- Determine si su proyecto piloto ofrece los siguientes resultados:
    - Una comparación clara que muestra las amenazas que Proofpoint ha detectado y que su gateway de correo electrónico tradicional no ha detectado.
    - Un resumen claro de los fallos identificados en la protección que ofrece el gateway.
    - Un informe sobre el valor añadido que cuantifica, en euros, el ahorro de tiempo para su equipo y la reducción de riesgos para la organización.

Paso 5: Establecer su calendario

Planifique una transición gradual teniendo en cuenta los ciclos de renovación, su dotación de personal y su tolerancia al riesgo. Con el soporte para migración de Proofpoint, puede modernizar la protección sin interrumpir el servicio.

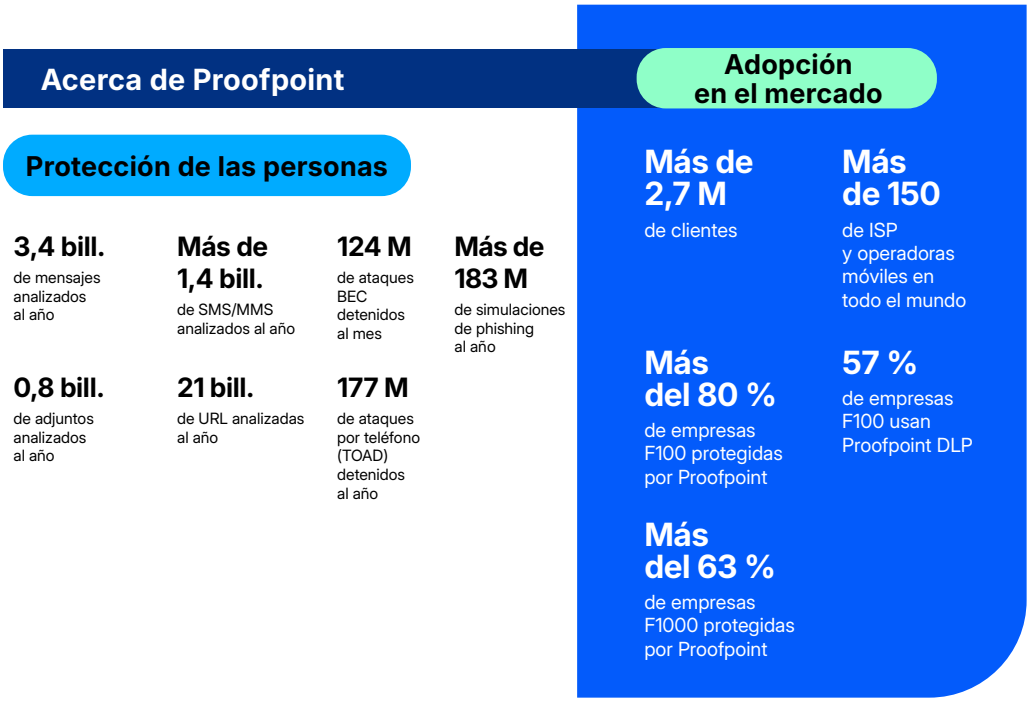
- Cree un plan en tres fases:
    1. Proyecto piloto
    2. Ejecución paralela
    3. Cambio definitivo
- Revise su calendario de renovación de licencias y sus ciclos presupuestarios. Si es necesario, busque oportunidades para adquirir contratos.
- Ejecute su antiguo sistema en paralelo como medida de seguridad adicional hasta que la nueva implementación haya recibido la aprobación de la dirección.
- Utilice los Servicios Premium de Proofpoint para disfrutar de una experiencia de migración de alta calidad. Nuestros equipos de Proofpoint Advisory y Applied Services proporcionan conocimientos prácticos para optimizar las configuraciones, acelerar el despliegue y garantizar una protección continua durante la transición.



Conclusión

Cuando adopta Proofpoint, le apoyamos durante la fase de transición. Proporcionamos guías de migración, plantillas de proyectos piloto e historias de éxito de clientes reales para acompañarle en su proceso. Tanto si ha optado por un despliegue inicial de API, una transición gradual o una sustitución completa de su gateway de correo electrónico tradicional, le ayudamos a migrar con confianza y a obtener rápidamente resultados medibles.

¿Por qué Proofpoint?



proofpoint.

Proofpoint, Inc. es un líder mundial en ciberseguridad centrada en las personas y los agentes, que protege cómo las personas, los datos y los agentes de IA se conectan a través del correo electrónico, la nube y las herramientas de colaboración. Proofpoint es un partner de confianza para más de 80 de las empresas Fortune 100, más de 10 000 grandes empresas y millones de pequeñas organizaciones. Les ayuda a bloquear las amenazas, prevenir la pérdida de datos y reforzar la resiliencia de las personas y los flujos de trabajo de IA. La plataforma de colaboración y seguridad de datos de Proofpoint ayuda a organizaciones de todos los tamaños a proteger y capacitar a sus empleados para que utilicen la inteligencia artificial con seguridad y confianza. Más información en www.proofpoint.com/es.

Conecte con Proofpoint: LinkedIn

DESCUBRA LA PLATAFORMA DE PROOFPOINT →