

# Una empresa líder en dispositivos médicos se alía con Proofpoint para proteger las operaciones y ahorrar tiempo

## El desafío

- Obtener protección frente al phishing y otras amenazas.
- Minimizar los procesos manuales para mejorar la eficiencia del equipo de TI.
- Reforzar las mejores prácticas de seguridad en la empresa.

## La solución

- Proofpoint Email Protection
- Proofpoint Email Fraud Defense
- Proofpoint Targeted Attack Protection
- Proofpoint Domain Discover
- Proofpoint Threat Response Auto-Pull
- Proofpoint Closed-Loop Email Analysis and Response
- Proofpoint Security Awareness

## Los resultados

- Disminución del phishing y otras amenazas, gracias a la actualización de la seguridad del correo electrónico.
- Reducción de los procesos manuales, gracias a la automatización de la seguridad del correo electrónico.
- Mejora de la seguridad global mediante la formación para concienciar en materia de seguridad.

## La organización

Con más de 20 sedes en todo el mundo y cerca de 8000 empleados, este líder en el sector de los dispositivos médicos es consciente de la importancia de poder confiar en las comunicaciones digitales. Este proveedor de servicios a nivel mundial goza de una excelente reputación en el desarrollo de dispositivos médicos de vanguardia que mejoran la vida de las personas, y mantiene un fuerte compromiso con la protección de sus clientes, sus empleados y su marca. Destaca también por su excelente combinación del servicio y la atención al cliente propios de una pequeña empresa, junto con la disponibilidad de recursos de una gran empresa.

## El desafío

### Protección de los clientes y empleados en el sector sanitario

Esta empresa especializada en dispositivos médicos mantiene su clara ventaja competitiva gracias a diversos factores, como la integración total, una competencia técnica avanzada, un compromiso absoluto con los clientes y la excelencia operativa. Como toda organización empresarial internacional, se apoya en una infraestructura de red segura para el funcionamiento de todos sus procesos operativos.

Sin embargo, ante la evolución del panorama de las amenazas, el equipo de seguridad de la empresa consideró que dedicaba demasiado tiempo a proteger las comunicaciones de la empresa. El sistema de seguridad del correo electrónico que utilizaba era difícil de configurar y adaptar a sus necesidades. Y, además, era ineficaz a la hora de bloquear las últimas amenazas.

"La seguridad de nuestro correo electrónico no satisfacía nuestras necesidades", explica el responsable de seguridad de esta empresa de dispositivos médicos. "Recibíamos muchas amenazas, como phishing y recopilación de credenciales. No confiábamos en la solución que teníamos para cubrir nuestras necesidades, por lo que dedicábamos mucho tiempo y recursos a bloquear manualmente los ataques. Para colmo, nos dimos cuenta de que nuestra formación para concienciar en seguridad no estaba a la altura de las circunstancias".

La empresa decidió actualizar su sistema para ofrecer una protección más completa contra las amenazas avanzadas, incluido el phishing, la detección de estafas por correo electrónico y los dominios maliciosos que hacían un uso indebido de su marca. No solo quería implementar un sistema eficaz de seguridad del correo electrónico, sino también obtener análisis e informes que le ayudaran a tomar decisiones más inteligentes y estratégicas.

## La solución

### Hacia un enfoque de la seguridad centrado en las personas

La empresa analizó varios productos de seguridad del correo electrónico para encontrar el más adecuado para sus necesidades. Eligió Proofpoint, que ofrecía la solución más completa y con mejor servicio de soporte.

"Efectuamos evaluaciones personalizadas de productos competidores, y fueron decisivos los niveles de soporte y atención que podíamos obtener con Proofpoint", afirmó el responsable de seguridad. "Proofpoint nos ofreció una visión de la seguridad centrada en las personas".

"Proofpoint facilita un verdadero ahorro de tiempo y de recursos. La solución permite a nuestro equipo ser más proactivo en el ámbito de la seguridad, en lugar de reactivo como ocurría hasta ahora. En cierto modo, consideramos a Proofpoint otro miembro de nuestro equipo".

Responsable de seguridad, empresa de dispositivos médicos

El responsable de seguridad y su equipo desplegaron varias soluciones que funcionan de forma coordinada para bloquear el malware, el phishing y los fraudes, a la vez que automatizan las operaciones de seguridad y la respuesta a amenazas.

"Proofpoint Email Protection, junto con Proofpoint Targeted Attack Protection (TAP), Proofpoint Threat Response Auto-Pull (TRAP) y Proofpoint Closed-Loop Email Analysis and Response (CLEAR) funcionan de manera conjunta para ofrecer una respuesta automatizada integral", añadió el responsable de seguridad. "Estas herramientas eliminan una buena parte del trabajo manual que requería la investigación de amenazas".

El responsable de seguridad y su equipo aprovecharon la formación de Proofpoint para conseguir una transición fluida y una migración sin complicaciones.

"Sin duda, la experiencia marcó la diferencia", explica el responsable de seguridad. "Proofpoint aplica un enfoque sistemático; si se sigue, todo encaja. Podemos avanzar exactamente al ritmo que necesitamos".

El proceso de migración también ayudó a la empresa a reforzar sus políticas DMARC (Domain-based Message Authentication, Reporting, and Conformance) para aumentar la protección frente a los ataques de suplantación de identidad y estafas por correo electrónico.

"Nuestras políticas DMARC eran básicamente de cuarentena, ya que carecíamos de una buena visibilidad de todos los remitentes", explica el responsable de seguridad. "Esto mejoró durante el proceso de migración. Obtuvimos visibilidad de todos los mensajes de correo electrónico enviados utilizando nuestro dominio.

Y esto fue de gran ayuda en la implementación de Proofpoint Email Fraud Defense".

Además, esta solución también permite a la empresa detectar los dominios parecidos (o "lookalike domains") que podría utilizarse en sitios web de phishing y ataques por correo electrónico. Para proteger aún más la reputación de la organización, el responsable de seguridad ha añadido recientemente Proofpoint Virtual Takedown. Se trata de un servicio adicional que ayuda a la empresa a gestionar los procesos que permiten bloquear y desmantelar dominios maliciosos.

El equipo también descubrió el papel fundamental que desempeñan los empleados en la defensa de la organización. Para reforzar esta idea, el responsable de seguridad adquirió Proofpoint Security Awareness, que aplica un enfoque de la formación basado en los datos, para promover una cultura de mejores prácticas de seguridad.

"Llevamos a cabo un programa de formación trimestral para todos nuestros colaboradores y exigimos un 100 % de participación", manifestó el responsable de seguridad. "Somos muy estrictos en este aspecto".

## Los resultados

### Reducción de los riesgos y mejora del conocimiento

La cartera completa de soluciones de Proofpoint para la seguridad y protección del correo electrónico ha permitido a la empresa mejorar y automatizar sus procedimientos de análisis, protección y corrección de las amenazas por correo electrónico, como el phishing y el malware. La solución ayuda a las organizaciones y a sus clientes a estar protegidos y, además, reduce la carga de trabajo para sus equipos de seguridad.

"Cada vez que sufrimos algún tipo de incidente de seguridad, hay que registrar y clasificar toda la información en nuestro sistema", declaró el responsable de seguridad. "Pasamos de tener entre 800 y 1000 incidencias al mes a reducirlas a menos de 150. Esta importante disminución nos permitió liberar recursos ocupados en tareas manuales".

Además, Proofpoint TAP ha ofrecido al responsable de seguridad y a su equipo visibilidad en tiempo real e información sobre las amenazas y sus objetivos, todo ello centralizado en un panel. La solución es particularmente eficaz para proteger a empleados en puestos de responsabilidad que gestionan información confidencial, que son los más expuestos a amenazas. El análisis que proporciona Proofpoint permite a la empresa conocer los patrones de amenazas, las tendencias y los ataques contra las personas más atacadas o Very Attacked People (VAP)™.

"Sobre la base de esa información, hemos generado políticas de acceso condicional de Microsoft para garantizar la máxima protección posible", manifestó el responsable de seguridad.

Asimismo, destacó las funcionalidades de generación de informes de la solución, que ahorran tiempo al equipo de seguridad y permiten tener a los directivos al corriente del estado general de la seguridad en la empresa.

"Una de las principales ventajas para nosotros es el nivel de soporte que ofrece Proofpoint", afirmó el responsable de seguridad. "Los informes nos permiten ahorrar tiempo y nos ofrecen una visión general de todos los datos. Con esta visión podemos cambiar nuestros comportamientos y adoptar una estrategia de seguridad más proactiva. Además, los incluimos en las distintas presentaciones que usamos en las reuniones con los directivos, para mostrarles las amenazas por correo electrónico y cómo las gestionamos. También usamos los informes de Proofpoint Security Awareness para mejorar la concienciación y la formación sobre seguridad".

Con los productos, servicios y formación de Proofpoint, esta empresa líder en dispositivos médicos pasa de limitarse a responder a las nuevas amenazas a adoptar un enfoque de la seguridad más estratégico, que optimiza el personal y la tecnología.

## MÁS INFORMACIÓN

Para obtener más información, visite [proofpoint.com/es](https://www.proofpoint.com/es).

### ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 85 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en [www.proofpoint.com/es](https://www.proofpoint.com/es).

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.