

El Ministerio de Educación de Nueva Zelanda protege miles de centros educativos con Proofpoint



El desafío

- Proteger a alumnos y profesores frente a las amenazas por correo electrónico.
- Responder a las necesidades de cada centro con un enfoque estandarizado.
- Ofrecer a los centros una solución de protección del correo electrónico a un precio asequible.

La solución

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection

Los resultados

- Reducción de las amenazas avanzadas con una protección actualizada del correo electrónico
- Seguridad más proactiva gracias a una mayor visibilidad del correo electrónico
- Integración fluida con varios entornos

La organización

¿Cómo proteger un sistema educativo nacional compuesto por más de 900 000 alumnos y personal? Para el Ministerio de Educación de Nueva Zelanda, la respuesta empieza por proteger las comunicaciones de correo electrónico. La organización actúa como principal asesor del gobierno sobre el sistema educativo del país. Establece las directrices para que las agencias y los proveedores ayuden al gobierno a alcanzar sus objetivos educativos.

El desafío

Proteger las comunicaciones de alumnos y profesores en todo el país

En Nueva Zelanda, las escuelas de primaria y secundaria y las Kura Kaupapa Māori (escuelas públicas donde se enseñan las culturas y los valores maoríes) deben respetar en todo momento el equilibrio entre los estándares locales y los estándares nacionales. Las escuelas neozelandesas tienen su propio consejo escolar elegido a nivel local, que establece la mayoría de las normas y procedimientos de funcionamiento. Sin embargo, las amenazas modernas del correo electrónico pueden extenderse fácilmente más allá de las fronteras geográficas, y el Ministerio de Educación de Nueva Zelanda se dio cuenta de que necesitaba proporcionar una solución estandarizada para proteger a sus estudiantes, profesores y personal.

"Hace unos años, una de las juntas sanitarias de distrito de Nueva Zelanda sufrió un incidente de ciberseguridad bastante importante", explicó Andrew Hood, asesor principal de ciberseguridad del Ministerio de Educación de Nueva Zelanda. "Así que nos preguntaron qué podíamos hacer para mejorar la madurez en ciberseguridad de las escuelas neozelandesas".

En Nueva Zelanda, las escuelas tienen libertad para elegir sus herramientas de productividad ofimática y suelen optar por Google con Workspace Plus o Microsoft 365, o una combinación de ambas. El Ministerio de Educación paga las licencias, mientras que las escuelas configuran los inquilinos individuales.

"Hay unos 3500 inquilinos diferentes de Google y Microsoft en nuestros sitios", dice Hood. "Nos preocupaba que su configuración predeterminada no fuera suficiente para protegerles contra el tipo de amenazas de correo electrónico que pensábamos que les estaban atacando. No podíamos determinar qué amenazas se dirigían a nuestros inquilinos, pero sí nos dimos cuenta de que los usuarios se veían comprometidos. Por ejemplo, sabíamos que se estaban utilizando buzones de correo electrónico para lanzar ataques y campañas de phishing contra otros centros educativos y la comunidad en general. Así que estábamos convencidos de que algo pasaba, pero desconocíamos por completo cuáles eran las amenazas".

El Ministerio de Educación quería ofrecer una solución centralizada que permitiera a las escuelas filtrar sus mensajes de correo electrónico. Esta solución no solo eliminaría un riesgo importante para los centros, sino que también daría a la organización una mejor visibilidad de las amenazas.

"Queríamos poder visualizar estadísticamente lo que estaba ocurriendo y el volumen de ataques lanzados, para poder asesorar mejor a los centros sobre las defensas que debían establecer contra estas amenazas", añade Hood. "Necesitábamos una herramienta que pudiera funcionar de forma aislada pero colectiva, y que también pudiera gestionar miles de inquilinos diferentes".

"Proofpoint Email Protection es muy eficaz para bloquear correos electrónicos maliciosos. Nos permite ver los tipos de ataque y saber que nuestras escuelas están protegidas contra ellos".

Andrew Hood, asesor jefe de ciberseguridad, Ministerio de Educación de Nueva Zelanda

La solución

Una solución centralizada pero flexible para los centros educativos

En el marco de su procedimiento de adquisición, el Ministerio de Educación realizó un estudio en profundidad del mercado con el fin de elegir la mejor solución para sus centros. Tras tener en cuenta factores como el coste, el rendimiento y la compatibilidad con las herramientas de productividad de Google y Microsoft utilizadas por los centros, se decantó por Proofpoint Email Protection.

"Realizamos un estudio de mercado y Proofpoint salió vencedor", explica Hood. "Para desplegar la solución en las escuelas, trabajamos con Network for Learning (N4L), una empresa pública financiada por el Ministerio de Educación para prestar servicios digitales a los centros educativos del país. N4L despliega la solución en los centros educativos y es su contacto para la capacidad de servicio".

Proofpoint Email Protection ayuda a los centros educativos a proteger y controlar su correo electrónico entrante mediante técnicas de detección multicapa para identificar y bloquear el correo electrónico malicioso. Además, clasifica de forma dinámica las amenazas e incidentes más recientes. Implementar la solución a través de N4L fue un enfoque rentable y práctico para proteger un gran número de escuelas en un corto espacio de tiempo.

"Con casi 2500 centros que ya trabajan con N4L para servicios como redes y firewalls, vimos a Proofpoint como una extensión de este enfoque", explica Andrew Hood. "Los directores ya tienen suficientes problemas con los que lidiar. La protección del correo electrónico no debería ser uno de ellos. Les hacemos saber que podemos centralizar esta protección y ocuparnos de ella por ellos".

El despliegue en colaboración con Proofpoint y N4L fue increíblemente fluido, y el Ministerio de Educación trabajó estrechamente con la organización para que los centros pudieran dar soporte fácilmente a sus entornos y aplicaciones de productividad específicos. Los centros escolares pueden inscribirse en cualquier momento para utilizar Proofpoint Email Protection, que ofrece principalmente el clásico filtrado de correo electrónico, es decir, extraer y bloquear las amenazas de alto riesgo que llegan por correo electrónico.

Proofpoint Targeted Attack Protection (TAP) también desempeña un papel importante en la solución. Protege frente a los ataques Business Email Compromise (BEC), amenazas basadas en la nube y en archivos adjuntos, al tiempo que proporciona información y visibilidad sobre los objetivos para ayudar al Ministerio a planificar de forma más estratégica.

"Uno de los problemas era que, puesto que los centros pueden gestionar sus propios entornos, no sabíamos cuál era la configuración existente de Google y Microsoft para cada sitio concreto", afirma Hood. "Tuvimos que probar una serie de situaciones en función de lo que considerábamos que debían hacer los centros para garantizar un servicio fiable. N4L tuvo que probar diversas variaciones. Tardamos unos meses, tras los cuales empezamos a lanzar una versión piloto del servicio en determinados centros. A partir de ahí, el proceso se aceleró enormemente. En sólo nueve meses, el 60 % de los centros se habían inscrito en el servicio".

Los resultados

Mayor protección y visibilidad

A medida que aumenta el número de centros educativos que adoptan Proofpoint Email Protection, el Ministerio de Educación obtiene una visibilidad en profundidad del volumen y los tipos de amenazas a las que se enfrentan, y las bloquea de forma proactiva antes de que puedan llegar a los alumnos o al personal.

"Las cifras son la prueba del valor añadido que nos ofrece Proofpoint", afirma Andrew Hood. "Procesamos entre 80 y 100 millones de mensajes al mes a través de la plataforma. La mayoría se bloquean como spam de bajo nivel pero un número preocupante de mensajes (entre 80 000 y 100 000) son amenazas que extraemos de Proofpoint. Los contenidos y URL maliciosos detectados requieren un análisis más avanzado, y eso es exactamente lo que Proofpoint hace.

La principal ventaja es que podemos aportar pruebas en todo momento de que una amenaza ha sido bloqueada y de que no ha llegado a una bandeja de entrada de correo electrónico e incitado al usuario a hacer clic".

Proofpoint Email Protection protege los centros educativos de Nueva Zelanda con una protección del correo electrónico más eficaz. "Ni los profesores ni el personal nos han hablado de retrasos o problemas de rendimiento", afirma Hood.

Proofpoint no solo neutraliza las amenazas en cuanto aparecen, sino que también permite al Ministerio de Educación y a los centros bajo su responsabilidad adoptar un enfoque más proactivo en materia de seguridad.

"N4L se encarga de supervisar la plataforma y ha trabajado intensamente con Proofpoint en la integración de API. También puede integrar los registros de Proofpoint en su SOC", añade Hood. "Busca comportamientos y patrones inusuales, como picos repentinos en el volumen de ciertos tipos de ataques. Esta información también nos permite determinar si un centro ha interactuado con un correo electrónico potencialmente malicioso. De este modo, podemos informar al centro de que creemos que ha llevado a cabo una actividad de alto riesgo y que debe tomar ciertas medidas".

Gracias a su solución centralizada, el Ministerio de Educación permite a los equipos docentes y a los administradores centrarse más en el aprendizaje que en la ciberseguridad.

Proofpoint Attack Index, incluido en Proofpoint TAP, también ayuda a identificar a los VAP (Very Attacked People™, o personas muy atacadas) para ayudar al Ministerio a identificar objetivos clave y mantenerlos fuera de peligro.

"La capacidad de revisar la lista de VAP y correlacionar a las personas atacadas con las fuentes públicas de direcciones de correo electrónico de los centros escolares nos da una idea del comportamiento de los ciberdelincuentes", afirma Hood.

"Proofpoint nos ofrece una solución de filtrado de correo electrónico más rentable, al tiempo que libera al centro educativo de esta responsabilidad", explica Hood. "Los centros no tienen que preocuparse de configurar y mantener actualizada la solución, ni de las últimas amenazas. Saben que existe una solución, que les protege y que es extremadamente eficaz".

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.

©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.