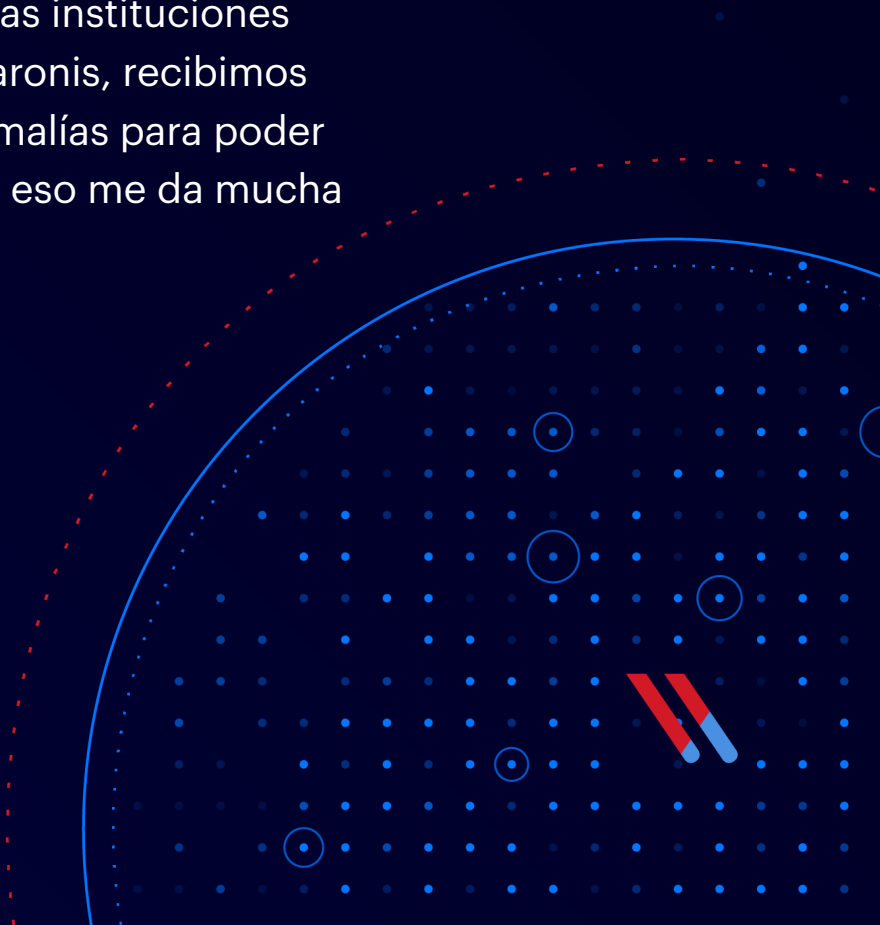
Cómo Varonis ayuda a una institución cultural de EE. UU. a protegerse contra los ciberataques

> Nuestro factor de amenaza es 25 veces mayor al de la mayoría de las instituciones de nuestro tamaño. Con Varonis, recibimos alertas anticipadas de anomalías para poder corregirlas de inmediato, y eso me da mucha tranquilidad.



Acerca de este estudio de caso:

Nuestro cliente es una institución cultural de EE. UU. Con gusto, accedimos a su pedido de anonimizar todos los nombres y lugares.

Aspectos destacados

Desafíos

- Protección contra las amenazas cibernéticas constantes
- Mejorar un proceso de auditoría que demanda mucho tiempo
- Encontrar una plataforma de seguridad para proteger los datos en la nube

Solución

La **plataforma de seguridad de datos Varonis:**

- Ofrece visibilidad y control completos sobre los datos críticos en Google Drive, Zoom y Box
- Encuentra y clasifica datos confidenciales automáticamente
- Repara y mantiene los permisos del sistema de archivos
- Supervisa y detecta comportamientos anormales en los sistemas críticos

Resultados

- Reducción del 72 % en permisos dañados
- Mayor protección contra ciberataques
- Más visibilidad del ecosistema SaaS

Desafíos

Amenazas de alto nivel por parte de actores externos

Una institución cultural de EE. UU. vive bajo la amenaza constante de ataques externos. Con ese riesgo en mente, proteger la privacidad de los donantes es la misión primordial del equipo de seguridad.

Su equipo de seguridad creó un proceso de auditoría para ayudar a identificar y defender los datos confidenciales. Pero la situación se complicó porque el proceso era riguroso y poco productivo. Una auditoría completa habría demorado semanas, un tiempo que no disponía el equipo de seguridad.

Hablamos con Michael Trofi, de Trofi Security, que tiene más de 30 años en el ámbito de la seguridad y que ofrece servicios de vCISO, SOC, auditoría y evaluación.

> **Nunca contamos con el tiempo suficiente para hacer la auditoría de manera correcta, por lo que siempre tuvimos miedo de pasar por alto algunas cosas.**

Una filtración de datos era el peor escenario posible. Si la PII de los donantes quedara expuesta, ellos podrían convertirse en el objetivo de los atacantes.

> **Lo peor que podía pasar es que se filtrara una hoja de cálculo con información de un donante.**

La institución necesitaba saber: ¿cuán grande fue el riesgo? Para responder a esa pregunta y obtener un informe real de la vulnerabilidad de los datos, contrataron a Varonis para que llevara a cabo una evaluación gratuita de riesgos de los datos.

VARONIS

Los resultados fueron aleccionadores: el cliente tenía una enorme cantidad de datos obsoletos en la nube y en premisas y una cantidad alarmante de acceso abierto. Los problemas eran más de los que podía manejar por sí solo el reducido equipo de seguridad.

> **Los escaneos de detección durante una auditoría mostraron que teníamos mucha información que se compartió. Sabía que había un problema, pero era mucho peor de lo que pensaba.**

Por suerte, Varonis aporta seguridad de datos automatizada a repositorios en la nube, aplicaciones SaaS y almacenes de datos en premisas, lo que libera a los equipos de seguridad para que puedan anticiparse a los datos y al uso compartido en constante crecimiento.

> **Tengo una carpeta de alertas de Varonis en mi Outlook y la reviso todos los días para comprender lo que sucede en mi entorno.**

“Siempre estamos bajo amenaza. Recibimos amenazas que están a la par de las agencias gubernamentales de tres letras”.

Solución

Proteger la información de los donantes

La **plataforma de seguridad de datos Varonis** conforma la base de la plataforma de seguridad de datos Varonis. Con estos productos, el equipo de seguridad de la institución puede ver el verdadero alcance de la exposición de los datos y obtener más control sobre los datos críticos en la nube y en premisas.

Según el CISO:

> **Tendemos a mantener las cosas para siempre. Pero esto nos empujó a crear nuevas políticas en torno al archivo de datos para reducir el riesgo de fuga de datos y minimizar la huella de las amenazas.**

La institución cultural también implementó la clasificación de datos para Windows y SharePoint a fin de encontrar y clasificar los datos confidenciales que podían poner en riesgo a los donantes.

Con Varonis, la remediación de riesgos es un proceso más rápido y eficiente. Varonis le permitió a la institución agilizar sus esfuerzos de reducción de riesgos al analizar quién realmente necesitaba acceso a los datos y eliminar el acceso de todos los demás. Esto ayuda a controlar el acceso a datos confidenciales y reduce de forma radical el daño potencial que podría causar un actor malicioso.

Ampliación de la protección para la nube

A continuación, el equipo de seguridad lanzó **Varonis para Google Drive**. En tan solo 15 minutos, pudieron ver qué información confidencial se había guardado en Google Drive y cómo se compartía.

Esto le brindó al equipo de seguridad mayor visibilidad de la que tenían antes. Pero con esa visibilidad llegaron nuevas sorpresas, según el CISO:

> **Descubrimos que un buen porcentaje del personal estaba compartiendo carpetas personales en sus correos electrónicos personales. Cuando un empleado se va, deshabilitamos sus cuentas, pero aun así tiene acceso a sus datos. Fue esclarecedor.**

Era un problema radical del que el equipo de TI no estaba al tanto antes. Tomaron medidas, creando nuevas políticas de retención de datos y configurando unidades compartidas con mucha más seguridad. También reorientaron al personal de TI con las prácticas recomendadas.

Además de **Varonis para Google Drive**, la institución cultural también adoptó **Varonis para Box** y **Zoom**. Estas incorporaciones ayudarán a proteger la confidencialidad de los datos, eliminar la exposición y acelerar las investigaciones entre nubes.

Alertas en tiempo real sobre todos los datos, en todo momento

Con el acceso bloqueado a los datos, aún quedaba una cosa por abordar: la detección de amenazas externas.

La institución cultural necesitaba saber cuándo el comportamiento de los usuarios ponía en riesgo a los datos. Y necesitaba la capacidad de detener los ataques maliciosos en curso. Aquí es donde entra en juego Varonis.

> **La pérdida de datos es algo que solía desvelarme. Los usuarios tienden a hacer clic en muchos correos electrónicos y cosas peligrosas. Pero Varonis detecta firmas de ransomware y las reduce de manera automática.**

“No teníamos información sobre quién estaba compartiendo qué en Google. Varonis clasificó nuestros datos y nos dio la visibilidad que no teníamos antes”.

Resultados

Una institución cultural es libre de continuar su importante trabajo

Hoy en día, los archivos compartidos de la institución cultural son más seguros y requieren mucho menos mantenimiento manual. Las auditorías que solían demorar semanas ahora se completan con un solo clic, y limpiar los permisos es igual de fácil.

Varonis ayudó al CISO y a su equipo de seguridad a identificar el riesgo de forma proactiva y, luego, a tomar medidas para capacitar a otros empleados para que sean más seguros en su comunicación en línea y en el uso compartido de archivos. Sus iniciativas fueron recompensadas con una importante reducción en las alertas, según el CISO:

> **Ahora identificamos datos en la nube y en premisas para ver dónde fluyen o se almacenan los datos de la PII para que podamos seguir las prácticas recomendadas en torno a la privacidad de los datos.**

Cuando el CISO hizo una prueba de penetración, el Blue Team (simulando un equipo de seguridad defensivo) usó Varonis para atrapar y detener todo lo que el Red Team (simulando piratas informáticos malintencionados) pudiera arrojarles.

> **Hicimos una prueba de penetración y detectamos todo lo que probamos. Se confirmó que nuestras ciberdefensas funcionan.**

Incluso en el peor de los casos, la buena higiene de los datos de la institución cultural ha minimizado de manera eficaz el radio de explosión de cualquier ataque. Disminuyeron la cantidad de carpetas con datos obsoletos en un 54 % y la cantidad de usuarios obsoletos en un 44 % en solo siete meses.

También redujeron la cantidad de carpetas con permisos dañados en un 72 % en el mismo plazo.

Hoy el CISO está satisfecho con el trabajo que se hizo para proteger a esta importante institución cultural.

> **La mayoría de los directores de seguridad asumen que si no han sido vulnerados o no han perdido datos, todo debe estar bien. Pero en realidad, no es así.**

“Varonis le muestra debilidades de seguridad que no creía que tenía. Y no puede reparar lo que no sabe que tiene”.

Encuentre y corrija las debilidades de seguridad de los datos.

Solicitar una demostración