Cómo Varonis ayuda a un equipo de seguridad compuesto por una persona a ahorrar más de 400 horas al año

ESTUDIO DE CASO

“Cuando se trata de análisis forense de datos y análisis intensivo, un equipo pequeño simplemente no tiene suficiente tiempo para dedicarle. Varonis es invaluable en ese aspecto: es necesario para aumentar las capacidades de una sola persona”.

ACERCA DE ESTE ESTUDIO DE CASO:

Nuestro cliente es un hospital de EE. UU. Con mucho gusto, hemos atendido su solicitud de ocultar todos los nombres y lugares.

ASPECTOS DESTACADOS

DESAFÍOS

- Mitigar la amenaza del ransomware que podría convertirse en un problema de seguridad para los pacientes.
- Proteger la PHI y la información de la HIPAA de amenazas internas y externas.
- Reparar las áreas en riesgo con un equipo de seguridad compuesto por una sola persona.

SOLUCIÓN

La plataforma de seguridad de datos más sólida:

- **DatAdvantage** para descubrir en qué punto los usuarios tienen demasiado acceso y hacer cumplir de forma segura las políticas de privilegios mínimos de acceso.
- **DatAlert Suite** para monitoreo y alerta continuos de datos y sistemas.

RESULTADOS

- Ahorro de más de 400 horas al año
- Visibilidad de servidores locales que permiten a un equipo compuesto por una sola persona adelantarse al ransomware.
- Tranquilidad desde 2009, gracias a una solución de seguridad que crece con las necesidades del hospital.

Desafíos

La protección de los sistemas críticos podría salvar vidas

Para los hospitales y las organizaciones de atención médica, detener los ataques de ransomware es literalmente una cuestión de vida o muerte.

En septiembre de 2020, los servicios de emergencia se vieron obligados a llevar a un paciente con lesiones potencialmente mortales a otro centro de atención, a 20 millas de distancia, después de que el hospital más cercano sufriera una vulneración. El paciente murió, y se cree que ese retraso de una hora fue un factor que contribuyó a su muerte.

Al comprender el riesgo, un proveedor de atención médica de los EE. UU. (anónimo por solicitud) se asoció con Varonis en 2009.

> “Una de nuestras principales preocupaciones es el ransomware”, explica el gerente de Seguridad. “El ransomware podría dejarnos fuera del negocio... o peor. Como hospital, un ataque podría convertirse en un problema de seguridad para los pacientes. Si el ransomware nos hace cerrar durante una o dos semanas, sería un gran problema para nuestros pacientes”.
>
> “No solo se trata del ransomware. Si no nos adelantamos a las amenazas internas y la exfiltración de datos, la información de identificación personal (PII) y la información médica protegida (PHI) pueden sufrir un ataque de ransomware y permanecer secuestradas, además del daño que los archivos cifrados causarían”.

Los equipos de seguridad hospitalaria son notoriamente pequeños. En este caso, un equipo compuesto por una sola persona es responsable de mantener los datos a salvo de los ataques de ransomware y de garantizar el cumplimiento con la HIPAA y la PHI.

> “Muchos de nuestros archivos contienen PHI y están bajo la protección de las reglas de seguridad de la HIPAA. Tenemos que asegurarnos de que solo las personas que necesitan revisarlos tengan acceso a ellos. Sin una solución como la de Varonis, no hay forma de que podamos saber quién accede y quién debería acceder a esos archivos”.

Incluso para un equipo grande, sería un gran trabajo. Para una persona es un desafío imposible, por eso recurrieron a Varonis.

> “No tendría suficientes horas en el día para proteger nuestra red sin Varonis. Una sola persona no puede hacer ese trabajo”.

> “El ransomware podría dejarnos fuera del negocio... o peor. Como hospital, un ataque podría convertirse en un problema de seguridad para los pacientes”.

Solución

Visibilidad y alerta en todos los archivos y sistemas críticos

DatAdvantage para Windows ayuda al equipo de seguridad compuesto por una sola persona a evaluar, priorizar y mitigar los mayores riesgos de seguridad en los servidores locales del hospital. Si un archivo está sobreexpuesto (es decir, abierto a todos) o un usuario comienza a acceder, mover o eliminar datos que normalmente no se tocan, Varonis advierte al gerente de Seguridad en tiempo real.

Más tarde, el hospital agregó **DatAdvantage para Servicios de directorio**, compatible con el Directorio Activo, a su línea de seguridad. Ahora tienen una vista panorámica del acceso a los datos en sus sistemas más críticos, y DatAdvantage ayuda detectando y resolviendo de forma segura los problemas con los permisos, los grupos anidados y la herencia.

> “Comenzamos con DatAdvantage y agregamos soporte para Servicios de directorio, lo que permite monitorear el Directorio Activo para detectar cambios. Definitivamente lo necesitábamos porque hasta ese momento no sabíamos los detalles sobre quién, qué, dónde o cómo se producían los cambios”.

El hospital también agregó **DatAlert Suite** a su pila de seguridad. Gracias al descubrimiento de posibles amenazas a lo largo de la cadena de eliminación antes de que puedan escalar, DatAlert es fundamental en su lucha contra el ransomware.

> “DatAlert se mantiene al tanto de todo lo que ocurre en nuestros servidores de archivos y en el Directorio Activo. Sabríamos de inmediato si detectara ransomware o si se produjera una vulneración real”.

Sin embargo, incluso con todas estas soluciones, un equipo de seguridad compuesto por una sola persona tendría dificultades para detener un ataque concentrado. Ahí es cuando llega el momento de solicitar refuerzos: **el equipo de Respuesta a incidentes de Varonis**.

> “El producto de un vendedor sufrió una vulneración. El equipo de Respuesta a incidentes nos ayudó a confirmar que el pirata informático no había llegado más allá de ese dispositivo. Sin Varonis, habría sido una tarea mucho más difícil, que requeriría mucho más tiempo y trabajo”.

“DatAlert se mantiene al tanto de todo lo que ocurre en nuestros servidores de archivos y en el Directorio Activo. Sabríamos de inmediato si detectara ransomware o si se produjera una vulneración real”.

Resultados

Ahorro de más de 400 horas al año

Según el gerente de Seguridad, el valor práctico de Varonis para un equipo compuesto por una sola persona es el ahorro de tiempo: **al menos un día de trabajo completo cada semana o más de 400 horas al año.**

> “Cuando se trata de análisis forense de datos y análisis intensivo, un equipo pequeño simplemente no tiene suficiente tiempo para dedicarle. Varonis es invaluable en ese aspecto: es necesario para aumentar las capacidades de una sola persona”.
>
> “El ahorro de tiempo me permite concentrarme en otros problemas y revisar alertas que de otro modo no tendría tiempo para investigar”.

Pero si bien el ahorro de tiempo es excelente, la tranquilidad es aún mejor. Saber que ahora son capaces de bloquear los datos y que el equipo de Respuesta a incidentes está a solo una llamada de distancia llena de confianza al gerente de Seguridad y a los directivos.

> “En el entorno de seguridad actual, la tranquilidad es difícil de conseguir. Casi todos los días, hay noticias sobre otro hospital que ha sido víctima de un ataque informático o infectado por ransomware. Tener las herramientas para evitar que una mala situación se intensifique me ayuda a dormir por la noche”.

A medida que el hospital evalúa los próximos pasos, se compromete a tomar precauciones adicionales para proteger los datos y las vidas de sus pacientes. Para lograr ese objetivo, el gerente de Seguridad espera agregar más soluciones de Varonis a su línea de seguridad en un futuro próximo.

“Varonis ya ha encontrado cosas como cuentas obsoletas, permisos incorrectos y otras áreas en riesgo. Estamos analizando cómo conseguir el siguiente Automation Engine, seguido de cerca por el Data Classification Engine”.

“El ahorro de tiempo me permite concentrarme en otros problemas y revisar alertas que de otro modo no tendría tiempo para investigar”.

Varonis ayuda a los equipos pequeños a llevar la delantera.

Gane visibilidad, seguridad de datos y la tranquilidad de tener un equipo experimentado a su lado.

SOLICITAR UNA DEMOSTRACIÓN