



Cómo Exela Pharma Sciences remedió el 100 % de sus datos de I+D en premisas y en la nube con Varonis



Están sucediendo cosas que simplemente no sé. Varonis me ayuda a investigar qué está sucediendo, quién está haciendo qué y a tomar medidas proactivas.



Aspectos destacados

Desafíos

- Limitar el radio de ataque potencial de Microsoft 365 de la empresa
- Mantener un modelo de privilegios mínimos
- Descubrimiento y clasificación de datos

Solución

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

- Proporciona visibilidad y control completos de los datos críticos
- Repara y mantiene los permisos del sistema de archivos
- Hace que los datos se puedan buscar fácilmente
- Detecta y bloquea datos confidenciales automáticamente
- Encuentra datos regulados
- Detecta comportamientos anormales en sistemas críticos

Resultados

- Se remedió el 100 % de los datos de I+D
- Se minimizó el radio de ataque potencial eliminando el acceso a los datos
- Se cumplieron regulaciones complejas de la industria farmacéutica

Desafíos

Identificar y proteger los datos patentados

Proteger los datos patentados de I+D es fundamental para las empresas farmacéuticas, y Exela Pharma Sciences no es una excepción.

John Kearney, director de TI de Exela, siempre había dado prioridad a la protección de la propiedad intelectual de la empresa, pero le preocupaba lo que podía estar perdiéndose.



Sabía que había problemas de permisos y archivos huérfanos. No tenía idea de cuántos. Se puede verificar una carpeta, se puede verificar una unidad, se puede verificar un sistema, pero hasta que no haya algo que realmente supervise todo, no se sabrá.

En particular, le preocupaba la exposición que pudo haber ocurrido cuando Exela migró a Microsoft 365.



Cuando lanzamos por primera vez Microsoft 365, estábamos aprendiendo. Y durante un tiempo, fue todo muy desprolijo. La gente colocaba archivos en Microsoft 365 en Teams, OneDrive, SharePoint, etc. Podían hacer cosas malas sin darse cuenta.

John quería reducir el radio de ataque potencial de Exela eliminando el acceso a la información confidencial de los usuarios donde no era necesario. Al igual que otras empresas en el espacio, la empresa está sujeta a regulaciones complejas.

Exela necesitaba implementar medidas de privacidad sin abrumar a su pequeño equipo de TI.



Somos un fabricante farmacéutico, por lo que hay una gran cantidad de datos patentados. También estamos en una industria altamente regulada. La FDA, la DEA, el Departamento de Agricultura, el Departamento de Defensa. Respondemos a muchos organismos.

“Cuando lanzamos por primera vez Microsoft 365, estábamos aprendiendo. Y durante un tiempo, fue todo muy desprolijo”.

Solución

Visibilidad y control de los datos de I+D

John y su equipo implementaron Varonis para obtener visibilidad y control sobre la propiedad intelectual de Exela. Exela eligió usar Varonis para descubrir y bloquear datos dentro de estas soluciones de Microsoft:

- **Windows**
- **Directorio Activo**
- **SharePoint Online**
- **OneDrive**
- **Azure**

Tal como sospechaba John, el cambio a la nube provocó una sobre exposición inadvertida. Descubrió que algunos archivos confidenciales tenían enlaces a los que cualquiera podía acceder, no solo usuarios y grupos autorizados. Al actuar de forma proactiva, pudo cerrar esa funcionalidad y proteger esos archivos de una posible vulneración de seguridad.



La nube facilita que los empleados compartan datos. Con Varonis, pudimos acceder a Microsoft 365 y asegurarnos de que el uso compartido no expusiera información confidencial.

Con esta nueva visibilidad, John y su equipo utilizaron la remediación automatizada de Varonis para reparar de manera inteligente los permisos del sistema de archivos dañados y bloquear los datos expuestos.

Minimizar el radio de ataque potencial

John y su equipo también utilizaron Varonis para minimizar el radio de ataque potencial de Exela al identificar, y eliminar silenciosamente, el acceso a información confidencial que no se estaba utilizando.



Usamos Varonis para encontrar aquellas situaciones en las que le dimos acceso a alguien a la unidad de I+D hace seis meses porque lo necesitaba. Pero tenemos un reporte que dice que nunca abrió la unidad de I+D. Así que podemos quitarle el acceso.

Con este enfoque, el equipo de TI no tiene que desempeñar el papel mal visto del “hombre malo”.



No digo: “No pueden tener acceso”. Digo: “Les di acceso y nunca lo usaron”.

Cumplir con regulaciones farmacéuticas complejas

El equipo de Exela Pharma también aprovechó la clasificación de datos de Varonis para encontrar y clasificar datos confidenciales automáticamente para fines de cumplimiento normativo. La tarea compleja se hizo fácil con el conjunto de cientos de políticas de actualización automática creadas por expertos de Varonis.

Varonis ayuda además a descubrir información confidencial, facilitando la búsqueda de datos confidenciales y protegidos.



Si la FDA dice: “Ese lote de Pharma X que hizo hace 10 años, ¿qué es esto en la página dos?” Varonis me ayuda a encontrar esos detalles a través de búsquedas por palabras clave.

Alertas de comportamiento anormal

John y su equipo también utilizan Varonis para monitorear y detectar cualquier comportamiento anormal en los sistemas críticos. Además, usan Varonis para detectar y ayudar a prevenir los intentos de exfiltración de DNS.

Por ejemplo, John recibe alertas cada vez que un miembro del personal se conecta desde un lugar inesperado. Por lo tanto, si un empleado vive en Maine y se conecta desde Inglaterra, John recibe una alerta. Si alguien restablece una contraseña para una cuenta de administrador o para un miembro del equipo de administración, también recibe una alerta.



Confío implícitamente en todos los miembros de mi equipo. Lo más probable es que yo ya lo sepa. Pero si no lo hago, puedo preguntarles al respecto.

Este tipo de alertas son particularmente importantes con una fuerza laboral remota donde los archivos se comparten en la nube.



Es diferente de tener una red regular en un servidor interno. La gente puede hacer cosas malas sin darse cuenta.

“Varonis nos brinda la capacidad de garantizar que estemos tan seguros como sea posible”.

Resultados

Se bloqueó el 100 % de los datos de I+D patentados

Con Varonis, Exela descubrió y bloqueó el 100 % de sus datos patentados de I+D en premisas y en la nube.



No solo encontramos y solucionamos estos problemas, sino que también hicimos cambios para evitar que vuelvan a suceder.

En la actualidad, John puede supervisar y proteger todos los datos confidenciales de Exela en un solo lugar, tanto si están ubicados en premisas como en la nube.



Varonis es una solución integral. Lo hace todo y lo resume en reportes básicos o detallados, según a quién le presente la información. No tengo que pasar horas buscando en seis fuentes diferentes para averiguar qué está pasando en la red. Está todo allí.

El control de los datos es tan completo que si la alta gerencia le preguntara a John a qué datos tiene acceso un empleado en particular, puede obtener esa información rápidamente.



Puedo mostrárselos en detalle con un reporte fácil de leer. Lo hace mucho más fácil.

John también confía en que los empleados de Exela solo tienen acceso a la información que realmente necesitan para hacer sus tareas.



Con Varonis, la gente no tiene acceso a lo que no debe. Y cuando no tienen acceso, no pueden hacer daño.



“Solicitar una demostración de Varonis es como revisar su auto antes de un largo viaje por carretera. Todos pensamos que sabemos dónde están todos los datos, pero no es así. Ocurren demasiadas cosas”.



Proteja sus datos regulados y su propiedad intelectual.

Encuentre y bloquee datos confidenciales con tan solo unos clics.

[Solicitar una demostración](#)