VARONIS

REMEDIACIÓN

# EVALUACIÓN DE RIESGO SOBRE LOS DATOS

PREPARADA PARA UMBRELLA CORP

HALLAZGOS CRÍTICOS

0 10 20 30 40 50 60 70

FECHA DE CREACIÓN : 3.1.24

# ÍNDICE



**“Me sorprendió la rapidez con la que Varonis pudo clasificar los datos y descubrir posibles exposiciones de datos durante la evaluación gratuita. Fue realmente revelador”.**

Michael Smith, CISO, HKS

# ¿POR QUÉ UMBRELLA CORP INICIÓ UNA EVALUACIÓN DE RIESGO SOBRE LOS DATOS DE VARONIS?

Umbrella Corp tiene un requisito a nivel de la junta directiva para descubrir, clasificar y etiquetar toda la PII para garantizar el cumplimiento y la eficacia de DLP posterior.| El reciente incidente de ransomware de Umbrella Corp destaca la necesidad de monitorear los datos. Sin acción, la empresa enfrenta multas regulatorias y niveles de exposición con los que el liderazgo no se siente cómodo.

## Desafíos

**Clasificar datos confidenciales y corregir exposiciones es un desafío.**

**Cuantificar la postura de seguridad de datos y mostrar el progreso a la junta directiva es imprescindible.**

**Los esfuerzos de remediación de datos son difíciles de llevar a cabo con un equipo pequeño.**

**Es necesario monitorear el uso de datos y emitir alertas sobre actividad anormal.**

**Las subunidades operan de forma independiente: necesitan crear un programa unificado de seguridad de datos.**

**Las auditorías de cumplimiento son manuales e incompletas.**

# DESCRIPCIÓN GENERAL DE LA EVALUACIÓN DE RIESGOS DE UMBRELLA CORP

## Fuentes de datos conectadas y cronograma de evaluación

Varonis puede conectarse a decenas de fuentes de datos adicionales. La configuración demora unos minutos.


Microsoft 365 | Active Directory + Azure AD | Salesforce | Archivos compartidos de Windows | Google Workspace

**Instalación de la plataforma**
1 de junio de 2023

**Evaluación**

**Prueba de valor**
21 de junio de 2023

**5,6 millones** de recursos (archivos/objetos)

**12 000** Identidades

**805 000** eventos (promedio diario)

**2,4 millones** de registros confidenciales clasificados (PHI, PCI, secretos)

Nota: Solo se conectó una parte del entorno general de Umbrella Corp para el POC.

# HALLAZGOS CRÍTICOS

## Riesgos que podrían dar lugar a una brecha de datos

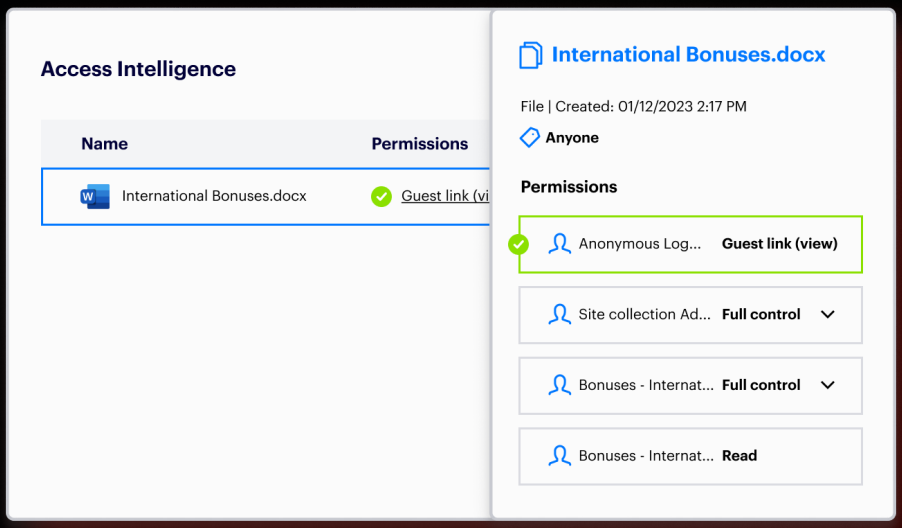
A continuación, se presentan los cuatro hallazgos principales que Varonis considera un riesgo crítico para la seguridad de los datos.

1. Reportes de compensación de RR. HH. compartidos públicamente a través de enlaces a los que puede acceder cualquier persona.
2. 332 usuarios de Salesforce pueden exportar datos de producción.
3. Un usuario externo es un super administrador en Google Workspace.
4. El asistente de marketing activó una alerta de acceso anormal a datos.

HALLAZGO CRÍTICO N.° 1

# Reportes de compensación de RR. HH. compartidos públicamente a través de enlaces a los que puede acceder “cualquier persona”.

Melissa Donovan expuso por error la información adicional de la empresa a Internet.




**Tipo de riesgo:**
Exposición de datos públicos

**Control del NIST:**
AC-3(9): liberación controlada

**Sistema afectado:**
Microsoft 365

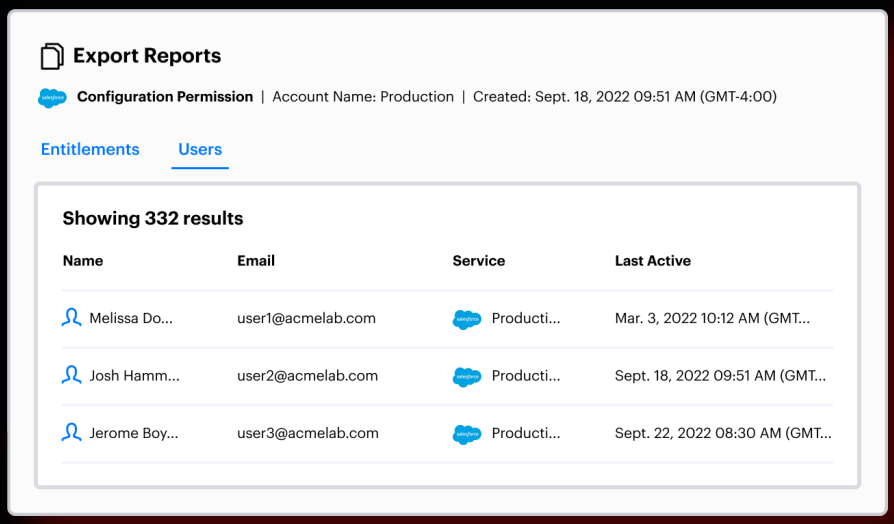
**Observación:**
Melissa Donovan, una socia de negocios de RR. HH., subió el documento International Bonsuses.docx al sitio de su equipo de RR. HH. el 12 de enero. El escaneo de clasificación de Varonis identificó 231 instancias de PII dentro del archivo y nuestros registros muestran que ella creó el enlace al que puede acceder “Cualquier persona” el 13 de febrero, y expuso el archivo a Internet. Usuarios anónimos accedieron al enlace desde 27 diferentes direcciones IP en todo el mundo.

**Recomendación:**
Revoque de inmediato el acceso de “Cualquier persona” a este archivo desactivando el enlace. Desactive la capacidad de compartir públicamente. Use la automatización de Varonis para revocar todo enlace público a archivos que contengan información confidencial.

HALLAZGO CRÍTICO N.° 2

# 332 usuarios de Salesforce pueden exportar datos de producción.

El perfil regular de “Ventas” otorga acceso de exportación. Esto es demasiado amplio y debería corregirse.




**Tipo de riesgo:**
Exposición de datos confidenciales

**Control del NIST:**
AC-2 (7): esquemas basados en roles

**Sistema afectado:**
Salesforce (producción, entornos de prueba, desarrollo)

**Observación:**
Los escaneos de Varonis identificaron una combinación tóxica de permisos que crea un grave riesgo de exfiltración de datos: 332 vendedores, a través de su perfil de “Ventas”, pueden exportar todos los datos de clientes potenciales, contactos, oportunidades y cuentas de la instancia de producción de Salesforce de Umbrella Corp.

**Recomendación:**
Elimine el permiso de reportes de exportación del perfil “Ventas” y de cualquier otro rol que no sea de administrador. Revise todos los perfiles y conjuntos de permisos que otorgan acciones altamente privilegiadas, como exportar reportes, modificar todos los datos y leer todos los datos.

HALLAZGOS CRÍTICOS N.° 3

# Un usuario externo es un superadministrador en Google Workspace.

Guy Incognito es un superadministrador sin MFA. Su actividad aumentó de manera considerable el 4 de julio, lo que activó una alerta.


**Tipo de riesgo:**
Cuenta de administrador insegura

**Control del NIST:**
AC-2(7): cuentas de usuario con privilegios

**Sistema afectado:**
Google Workspace

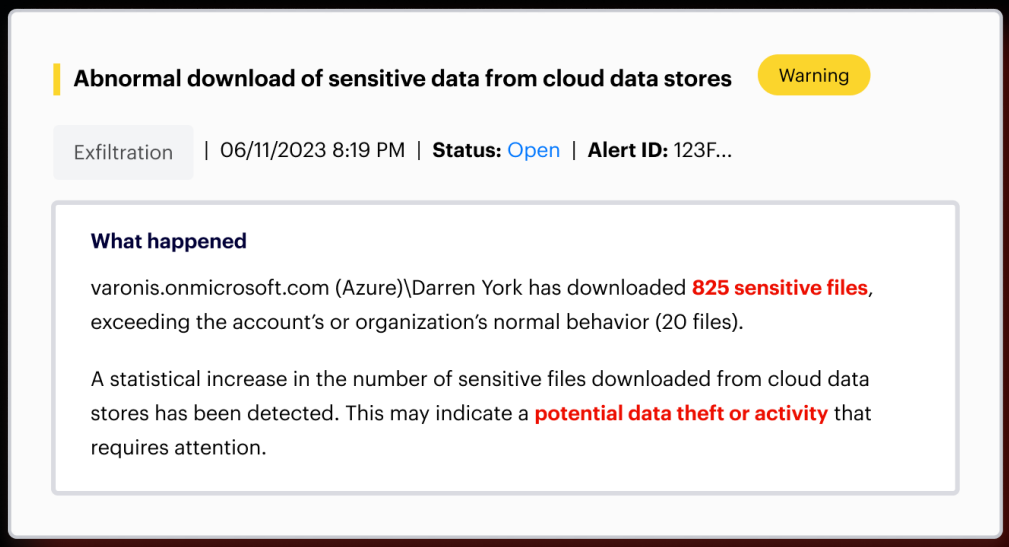
**Observación:**
Guy Incognito es un contratista externo que utiliza una cuenta personal de Gmail para acceder a la cuenta de Google Workspace de Umbrella. Este usuario tiene derechos de superadministrador y no tiene habilitada la MFA. Esta cuenta se considera de riesgo extremadamente alto.

**Recomendación:**
Implemente de inmediato la MFA en la cuenta de Guy Incognito y agréguela a una lista de observación en Varonis. Revise los últimos 30 días de actividad del usuario, sus derechos e identidades relacionadas. Decida si este usuario externo realmente necesita derechos de superadministrador.

HALLAZGOS CRÍTICOS N.° 4

# El asistente de marketing activó una alerta de acceso anormal a datos.

Darren York no debería tener acceso a datos financieros. UEBA de Varonis detectó un acceso anómalo.




**Tipo de riesgo:**
Comportamiento anormal del usuario

**Control del NIST:**
AC-2(12): monitoreo de cuentas para uso atípico

**Sistema afectado :**
Microsoft 365

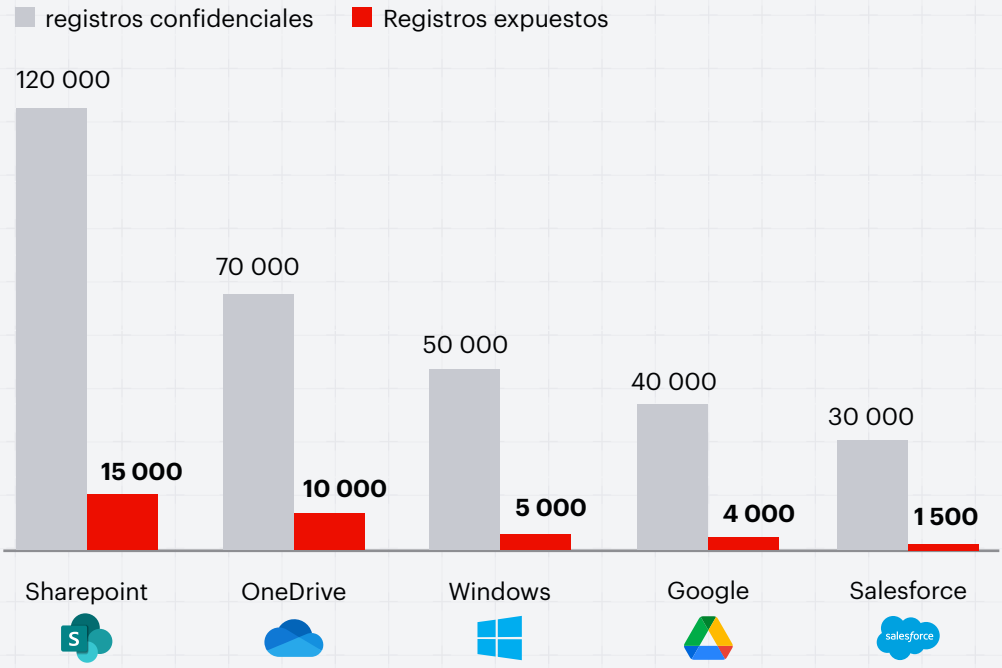
**Observación:**
El asistente de marketing Darren York activó una alerta basada en el comportamiento al desviarse de su referencia normal de actividad de acceso a datos. Varonis detectó que estaba accediendo a archivos con datos financieros, algo atípico para su función.

**Recomendación:**
Use Varonis para ejecutar una consulta para ver toda la actividad de Darren en los últimos 30 días. Asegúrese de que los permisos para acceder a los datos que contienen registros financieros solo estén disponibles para los empleados que necesitan acceso.

# POSTURA DE SEGURIDAD DE DATOS

Los datos confidenciales de Umbrella Corp están distribuidos entre múltiples servicios en la nube y el repositorio de datos en premisas. Para minimizar el riesgo de una brecha de datos, es fundamental que la empresa tenga visibilidad y control en tiempo real sobre su patrimonio de datos que cambia rápidamente, con clasificación unificada, detección de amenazas y aplicación de políticas.

### ¿Dónde están los datos más confidenciales de Umbrella Corp y cuántos corren riesgo?




### Indicadores clave de riesgo:

| | |
|---|---|
| **310 000**<br>registros confidenciales | **27 000**<br>eventos sobre datos confidenciales por día |
| **24 500**<br>Registros confidenciales expuestos en toda la organización | **11 000**<br>Registros confidenciales expuestos externamente |

# Descubrimiento y clasificación de datos

## Políticas de clasificación habilitadas

Habilitamos 85 reglas integradas y creamos tres reglas personalizadas durante esta evaluación de riesgos. Los cuatro tipos de datos principales por volumen se muestran a continuación.

### PCI-DSS

**Contenedores:** 1 160
**Objetos:** 12 421
**Registros:** 89 924

### Contraseñas

**Contenedores :** 160
**Objetos:** 421
**Registros:** 923

### PII de EE. UU.

**Contenedores :** 2 620
**Objetos:** 72 245
**Registros:** 199 104

### Números de asunto

**Contenedores:** 1 002
**Objetos:** 92 420
**Registros:** 799 922

## Biblioteca de políticas incorporada

| PII | GDPR | Credenciales | Financiero | FEDERAL |
|---|---|---|---|---|
| HIPAA PHI 2.0 | GDPR Alemania | Contraseñas | PCI-DSS 2.0 | ITAR |
| Ley de Privacidad de Colorado | GDPR Francia | Claves privadas | SOX | altamente secretos |
| Ley SHIELD de Nueva York | GDPR Austria | Certificaciones | GLBA | CUI |

*Además de cientos de reglas, patrones y diccionarios más*

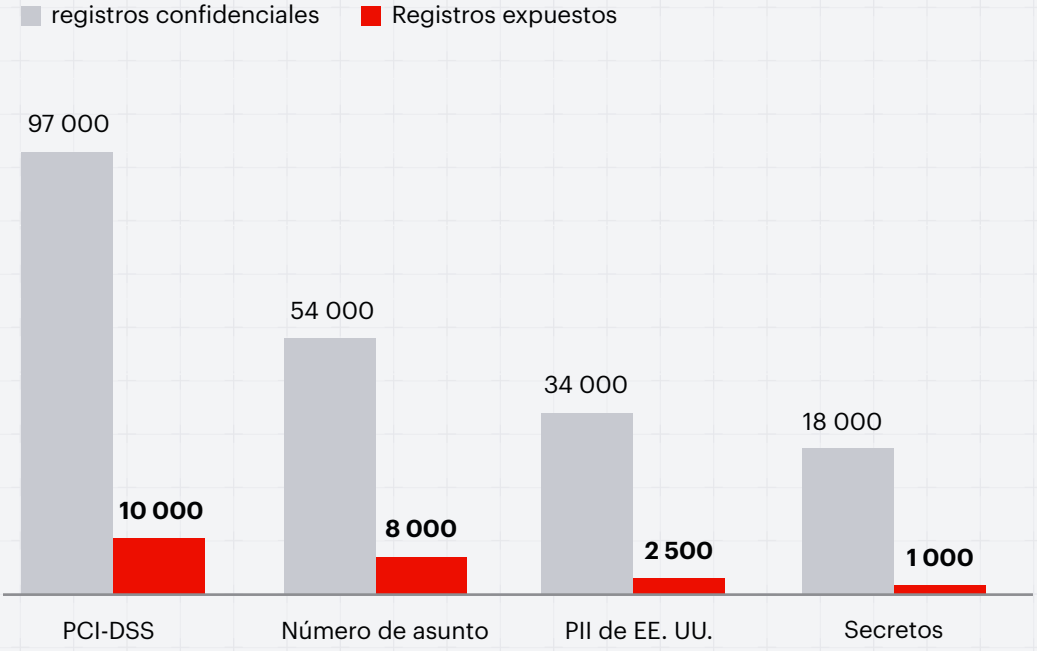
## El poder de la clasificación de datos de Varonis

+ Escaneado incremental real para un descubrimiento eficaz y escalable en
+ conjuntos de datos masivos
+ Políticas de clasificación unificadas en todos los repositorios de datos compatibles
+ Verificado en batalla en entornos de múltiples petabytes
+ Más de 400 reglas probadas y creadas por
+ expertos disponibles (y en crecimiento)
+ listas para usar
+ Ámbitos de escaneo y muestreo personalizables

# Exposición de datos de Microsoft 365

La exposición de datos en M365 no es exclusiva de Umbrella Corp. La empresa promedio tiene más de 40 millones de permisos únicos en sus datos en múltiples nubes y, según Microsoft, más del 50 % de los permisos son de alto riesgo y son capaces de causar daños catastróficos si están mal configurados.

### ¿Qué tipo de datos se encuentran en M365 y cuál es la exposición de Umbrella Corp?




### Indicadores clave de riesgo:

**203 000**
registros confidenciales

**20 000**
Registros confidenciales expuestos en toda la organización

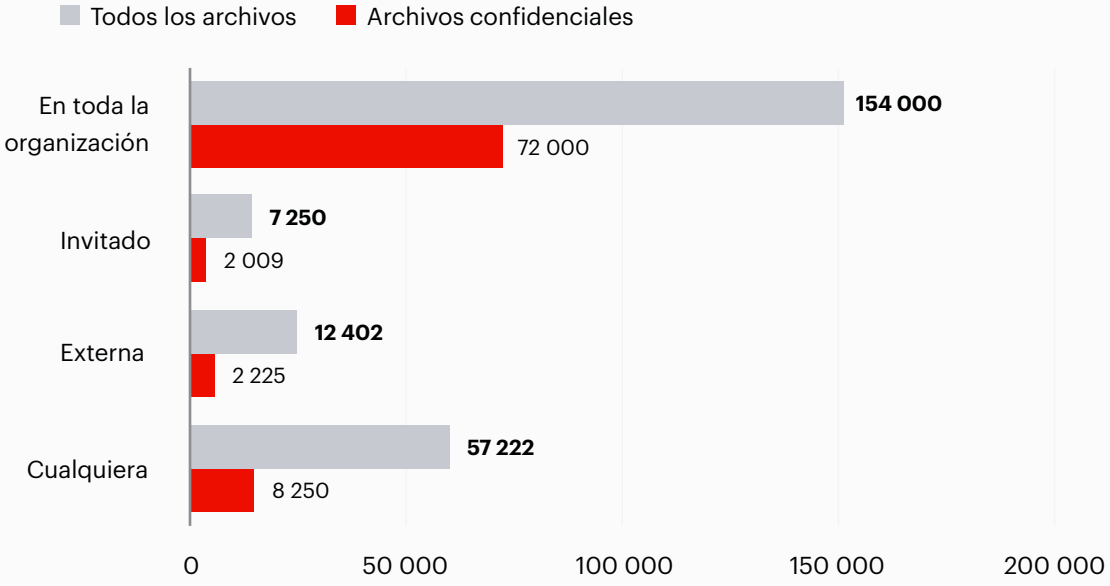
**1 500**
Registros confidenciales expuestos externamente

# Riesgo de colaboración

## Niveles de exposición

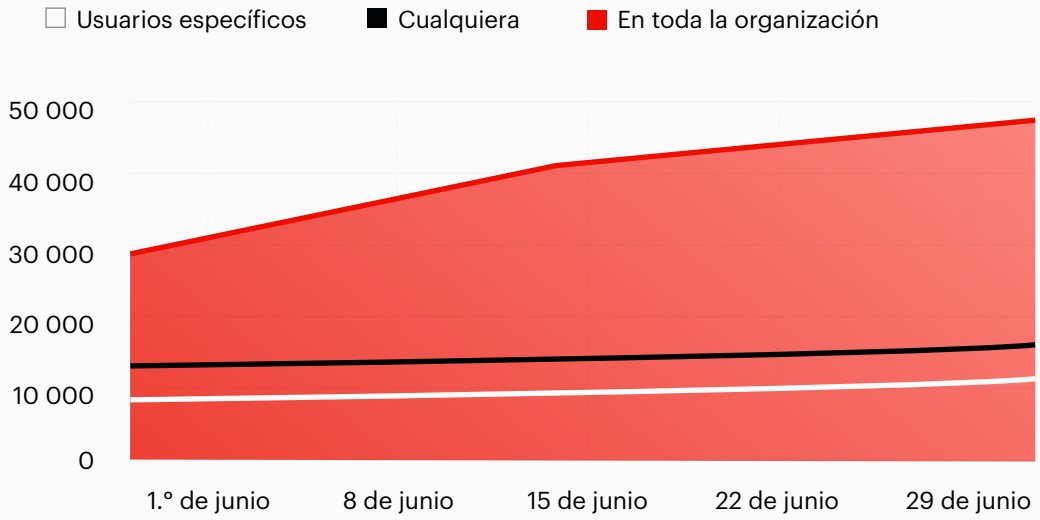
Los enlaces compartidos son útiles para la colaboración, pero pueden exponer esos datos a todos los miembros de la organización, a usuarios invitados o a Internet. Umbrella Corp tiene una cantidad significativa de exposición de datos confidenciales debido a los enlaces en SharePoint y OneDrive.

### SharePoint Online y OneDrive




## Aumento de los enlaces compartidos

El radio de ataque potencial de Umbrella Corp está creciendo rápido semana tras semana. A continuación, se muestra un gráfico del crecimiento de enlaces por tipo durante el período de evaluación de riesgos.



# Datos expuestos públicamente

## Datos expuestos públicamente a través de enlaces a los que puede acceder “cualquier persona”

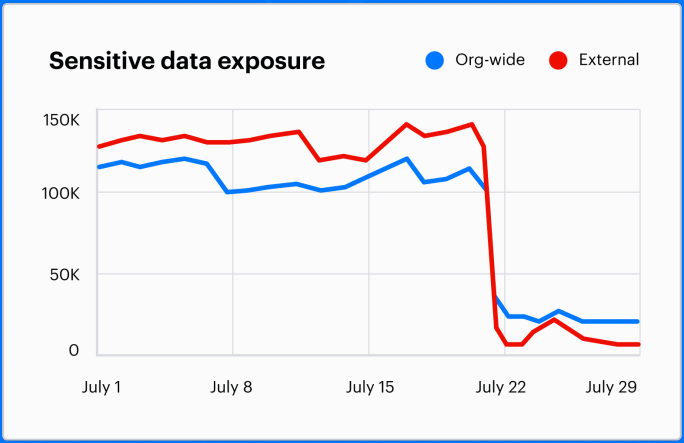
A continuación, se muestra una pequeña muestra de archivos confidenciales a los que puede acceder cualquier persona en Internet. La trazabilidad de auditoría de Varonis muestra el tipo de datos dentro del archivo (PCI, PHI, etc.), quién compartió el enlace, cuándo y si se ha accedido al archivo a través del enlace.

| | File type | Name (resource) | Classification category | Total record |
|---|---|---|---|---|
| ☐ | | JV costs for Feb-Apr.xls | *Credentials (6) | 28 |
| ☐ | | JV costs for Feb-Apr.xls | *Credentials (4) | 22 |
| ☐ | | Transaction-English-06.xsl | *Credentials (4) | 22 |
| ☐ | | GL Entry.ppt | *Credentials (4) | 22 |
| ☐ | | Employee Agreement.docx | *Financial (3) | 21 |
| ☐ | | Employee Agreement.docx | *Financial (3) | 21 |
| ☐ | | Employee Agreement.docx | *Financial (3) | 21 |
| ☐ | | Employee Agreement.docx | *Financial (3) | 21 |

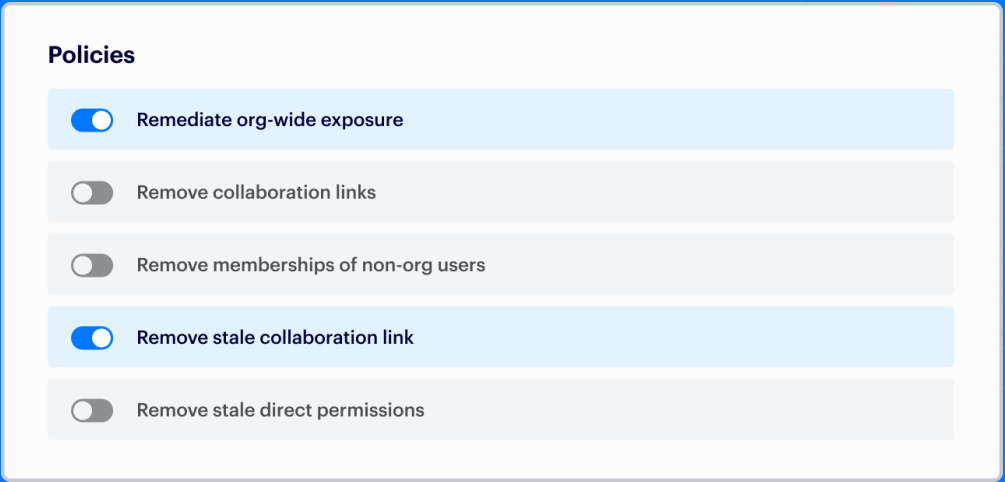
1. Hojas de cálculo con credenciales e información de tarjeta de crédito
2. Acuerdos de empleo con PII e información de cuenta bancaria

# ¿Qué tan rápido podemos solucionar el riesgo de los vínculos compartidos?

Un cliente típico de Varonis puede eliminar la exposición rápidamente con la automatización. A continuación, se muestran los resultados de una institución financiera grande que habilitó la automatización de privilegios mínimos. Casi el 100 % de la exposición de datos externos y de toda la organización se eliminó en menos de 30 días.




Las políticas de automatización mantienen bajo el riesgo frente al crecimiento de datos y a la colaboración continua. Con las políticas configuradas para aplicarse automáticamente, los nuevos riesgos se corrigen a medida que aparecen y el privilegio mínimo se aplica continuamente.



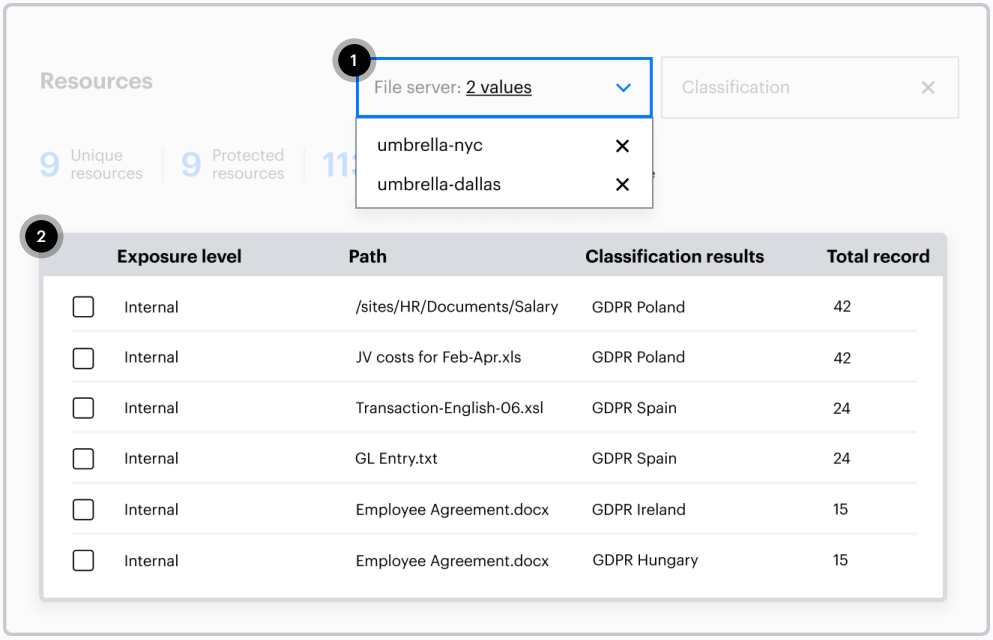

# Datos mal colocados y mal etiquetados

## Datos alojados en lugares inadecuados: riesgo de cumplimiento del GDPR

Varonis descubrió registros de PII de ciudadanos de la UE en un tenant de M365 alojado en Estados Unidos. Los archivos fueron cargados el 15 de julio por una cuenta de servicio llamada “ExportJob” que parece estar conectada a una tarea automatizada de Workato. Recomendamos migrar estos datos al tenant con base en Umbrella Corp y ajustar la tarea automatizada.

1 Tenants de M365 con base en EE. UU.

2 Archivos que contienen PII de ciudadanos de la UE




| Exposure level | Path | Classification results | Total record |
|---|---|---|---|
| Internal | /sites/HR/Documents/Salary | GDPR Poland | 42 |
| Internal | JV costs for Feb-Apr.xls | GDPR Poland | 42 |
| Internal | Transaction-English-06.xsl | GDPR Spain | 24 |
| Internal | GL Entry.txt | GDPR Spain | 24 |
| Internal | Employee Agreement.docx | GDPR Ireland | 15 |
| Internal | Employee Agreement.docx | GDPR Hungary | 15 |

## Archivos mal etiquetados: deficiencias en lo que respecta a la aplicación de DLP

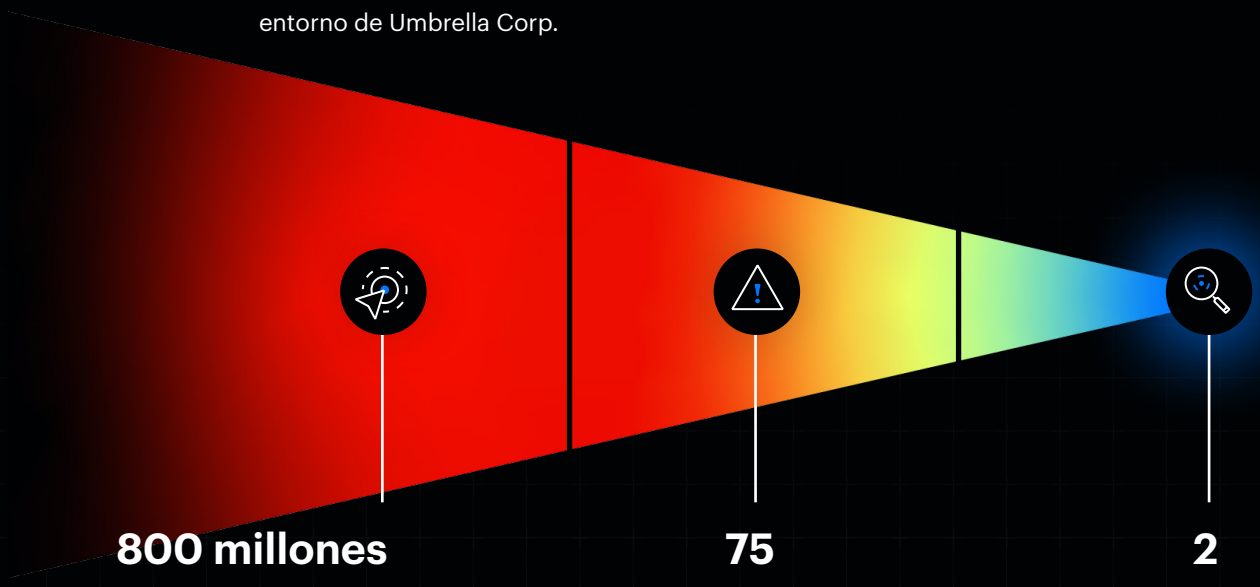
A muchos archivos les faltan etiquetas de MIP o tienen etiquetas desactualizadas y mal aplicadas. Como resultado, la aplicación de DLP posterior podría fallar, lo que provocaría una fuga de datos confidenciales o lo contrario: se impide a los usuarios compartir datos no confidenciales que están mal etiquetados.

Encontramos más de 27 000 archivos confidenciales sin etiqueta.

| Path | Classification results | Classification labels | Name |
|---|---|---|---|
| C:\Share\Finance | US PII, HIPAA PHI Data | GDPR Regulated Data (0/1) | Finance |
| C\Share\Finance\Controllers | US PII, HIPAA PHI Data | | Controllers |
| C\Share\Finance\Controllers | US PII, HIPAA PHI Data | | Q1 2006 |
| C\Share\Finance\Controllers | US PII, HIPAA PHI Data | | Inventory |
| C\Share\Finance\Controllers | US PII, HIPAA PHI Data | | Revenues |
| C\Share\Finance\Controllers | US PII, HIPAA PHI Data | | SEC |

# Detección y respuesta a amenazas

El monitoreo en tiempo real y la detección de amenazas basadas en el comportamiento de Varonis se habilitaron en cada sistema dentro del alcance. Durante el período de evaluación, nuestros modelos de IA fueron entrenados en más de 800 millones de eventos para que aprendan el comportamiento único de los usuarios y dispositivos en el entorno de Umbrella Corp.



**800 millones**

**cientos de millones de eventos recopilados**

*Cada evento se enriquece y normaliza automáticamente*

**75**

**Decenas de alertas activadas**

*Promedio de aproximadamente 3 por día*

**2**

**Se investigaron algunos incidentes**

*El equipo de respuesta proactiva a incidentes de Varonis detectó y escaló dos incidentes.*

## UEBA centrado en datos

Los eventos se enriquecen con contexto de datos, usuarios y dispositivos. Los analistas de seguridad pueden ejecutar consultas como: “Enumerar todos los eventos de acceso a datos confidenciales por cuentas con privilegios desde dispositivos conectados desde Alemania”.

**Identificación de la cuenta**

**Resolución de IP a dispositivo**

| Operación por | Tipo de cuenta | Objeto | ¿Es confidencial? | Dirección IP del dispositivo | Nombre del dispositivo | Dirección IP externa | Geolocalización |
|---|---|---|---|---|---|---|---|
| Amy Johnson | Ejecutiva | customer.xlsx | sí | 173.17.33.3 | aj-03154 | 54.239.13.2 | Canadá |

**Confidencialidad de archivos**

**Geolocalización**

# ANÁLISIS DE AMENAZAS

## Reporte de incidentes: cuenta de servicio vulnerada

**Observación:**
El equipo de Respuesta a incidentes de Varonis descubrió que se vulneró una cuenta de servicio de copia de seguridad y se comenzó a acceder a los datos de los usuarios.

**Abnormal service behavior: access to atypical folders containing GDPR data**

Exfiltration | 06/11/2023 8:19 PM | **Status:** Open | **Alert ID:** 123F...

**What happened**

BackupService File opened shared folder C:\Share\Finance\Controllers\Financereports.

A service account accessed folders containing GDPR data it has not accessed previously. Service accounts can be expected to perform the same actions repeatedly; therefore, a behavioral change is suspicious. Attackers may impersonate a service account and exploit its privileges.

**Mitigación:**
El equipo de Respuesta a incidentes de Varonis calificó y remedió el incidente en cuestión de minutos. La cuenta UC\BackupService se deshabilitó de inmediato, se eliminaron las sesiones activas y se restableció la contraseña. Varonis entregó un reporte completo de investigación al equipo de Umbrella Corp con un análisis de la causa raíz y recomendaciones.

**Desglose:**
La cuenta vulnerada accedió a 142 archivos. 82 de esos archivos fueron clasificados como confidenciales por Varonis.

| Event time (event) | Event type... | Account name | Path (affected resource) |
|---|---|---|---|
| 06/11/2023 3:19 PM | File renamed | BackupService | C:\Share\apps\Backoffice... |
| 06/11/2023 3:19 PM | File renamed | BackupService | C:\Share\apps\Backoffice... |
| 06/11/2023 3:19 PM | File renamed | BackupService | C:\Share\apps\Backoffice... |
| 06/11/2023 3:19 PM | File renamed | BackupService | C:\Share\apps\Backoffice... |
| 06/11/2023 3:19 PM | File renamed | BackupService | C:\Share\apps\Backoffice... |

# RIESGO DE CONFIGURACIÓN

Varonis escanea todo el tiempo las configuraciones de los sistemas en las plataformas SaaS e IaaS de Umbrella Corp para determinar si alguna configuración es riesgosa o si alguna configuración se ha desviado de su estado deseado.

## Se detectaron 21 configuraciones erróneas

Salesforce tiene la mayor cantidad de configuraciones erróneas (8).

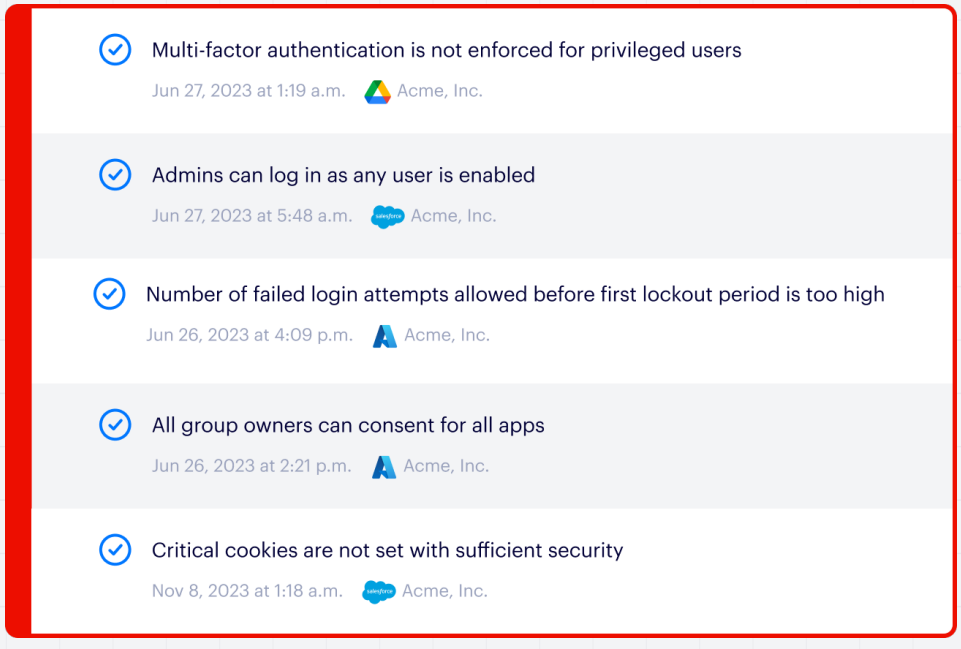
## 5 configuraciones erróneas de gravedad alta

M365 y Salesforce tienen 2 configuraciones erróneas críticas cada uno.

## 4 configuraciones establecidas para aplicar automáticamente

Varonis puede aplicar automáticamente configuraciones seguras.

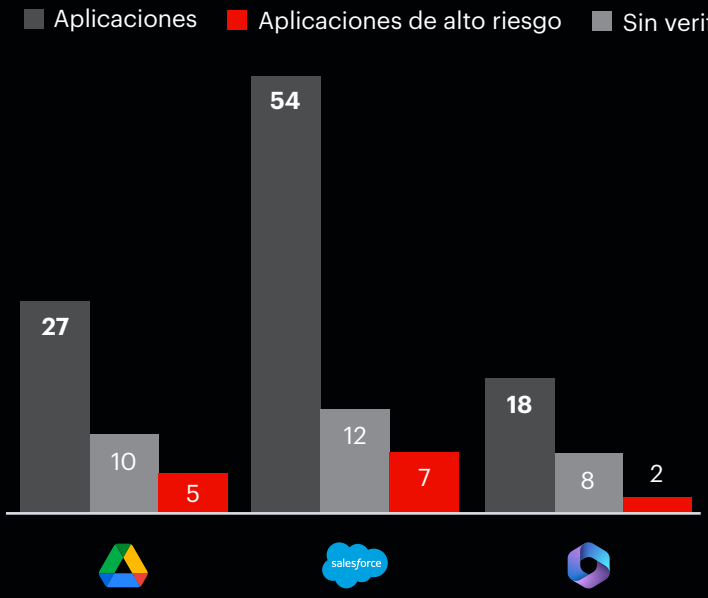
A continuación, encontrará un resumen de las **cinco configuraciones erróneas de gravedad alta** que se descubrieron durante la evaluación. Los detalles completos y las recomendaciones para cada uno de ellos se pueden encontrar en la interfaz de usuario de Varonis.




**Haga clic aquí** para ver más configuraciones de SaaS y IaaS de muestra que Varonis puede monitorear.

# RIESGO DE APLICACIONES DE TERCEROS

**Identificamos 36 aplicaciones de terceros riesgosas, inactivas o no verificadas.**




**99**
Aplicaciones de terceros instaladas

**14**
de alto riesgo con amplio acceso a los datos

**22**
Aplicaciones inactivas

Aquí hay un desglose de las cuatro mejores aplicaciones de terceros, por número de usuarios, que están integradas con las plataformas SaaS que Varonis está monitoreando:

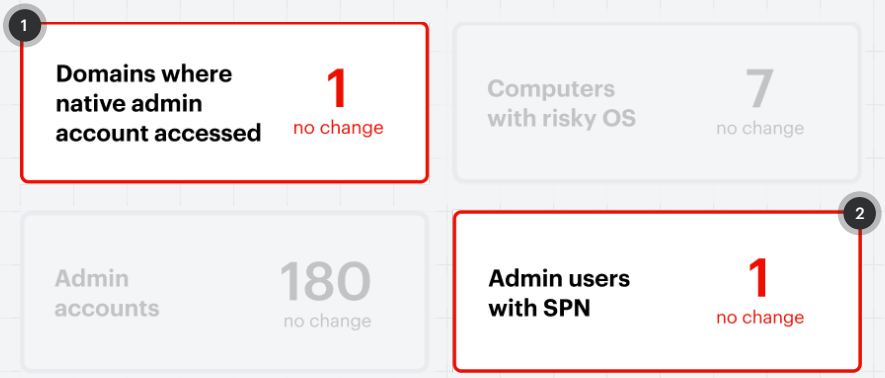
| Google | Salesforce | Microsoft 365 |
|---|---|---|
| miro | 6sense | |
| dialpad | HubSpot | slack |
| Signeasy | INCENT | Trello |
| SUPERMETRICS | Power BI | Evernote |

Además, descubrimos 111 usuarios inactivos cuyas asignaciones de aplicaciones pueden revocarse directamente desde la interfaz de usuario de Varonis.

# RIESGO DE IDENTIDAD

## Postura de seguridad de Active Directory

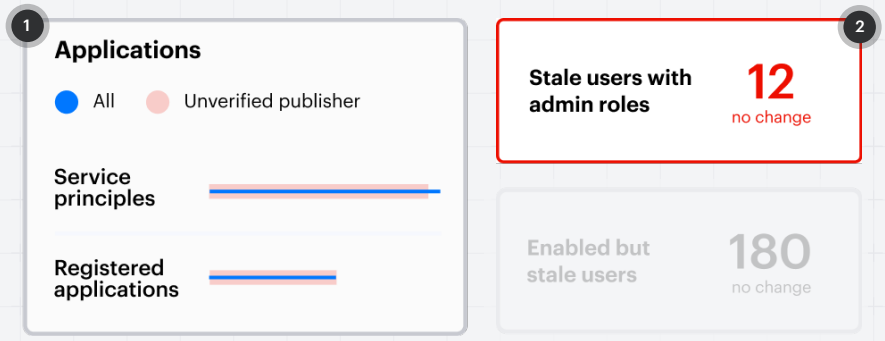
Varonis escanea los servicios de directorio en premisas y en la nube de Umbrella Corp y detecta configuraciones débiles que pueden proporcionar rutas de acceso para los atacantes. Estos riesgos se actualizan en tiempo real en los paneles de control de Varonis y ayudarán a priorizar los esfuerzos de fortalecimiento de AD.




1. Es raro que esta cuenta se use en circunstancias normales. Esto podría indicar un riesgo.
2. Vulnerable al descifrado de contraseñas de Office.

## Postura de seguridad de Entra ID (Azure AD)

Varonis monitorea y califica continuamente la postura de Entra ID. Las configuraciones riesgosas que ponen en peligro sus datos se destacan en sus paneles de riesgo y reportes.



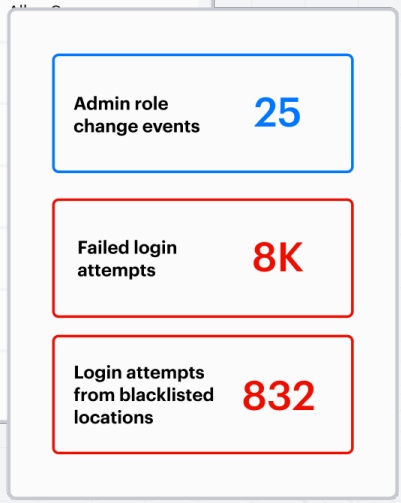

1. Revise el permiso de la aplicación y el acceso a los datos no verificados.
2. Estas cuentas deben desactivarse de inmediato.

## Monitoreo del Directorio Activo

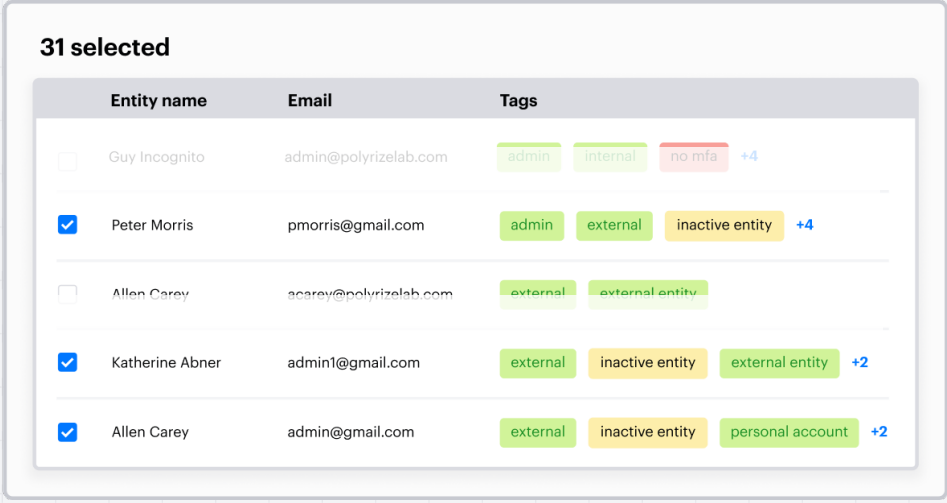
Varonis monitorea los eventos en los servicios de directorio de Umbrella Corp y correlaciona esas acciones con los eventos centrados en los datos recopilados de las plataformas de colaboración y los repositorios de datos.

Estos cambios se realizaron fuera de la ventana de control de cambios.

| Event type (event) | Event time (event) | Event description | Account Name |
|---|---|---|---|
| Access request | 06/29/2023 5:15 a.m. | abc1234.com\Demo | Allen Carey |
| Access authentication | 06/29/2023 5:15 a.m. | abc1234.com\Demo | |
| Access request | 06/29/2023 5:15 a.m. | abc1234.com\Demo | |
| Group member removed | 06/29/2023 5:15 a.m. | "DemoUser" was removed | |
| Group member removed | 06/29/2023 5:15 a.m. | "DemoUser" was removed | |
| Group member added | 06/29/2023 5:15 a.m. | "DemoUser" was added | |
| Group member added | 06/29/2023 5:15 a.m. | "DemoUser" was added | |
| User updated | 06/29/2023 5:15 a.m. | "DemoUser" was updated | |



# Cuentas personales y usuarios externos riesgosos




Las cuentas de usuario de Gmail están obsoletas, pero tienen acceso a datos confidenciales.

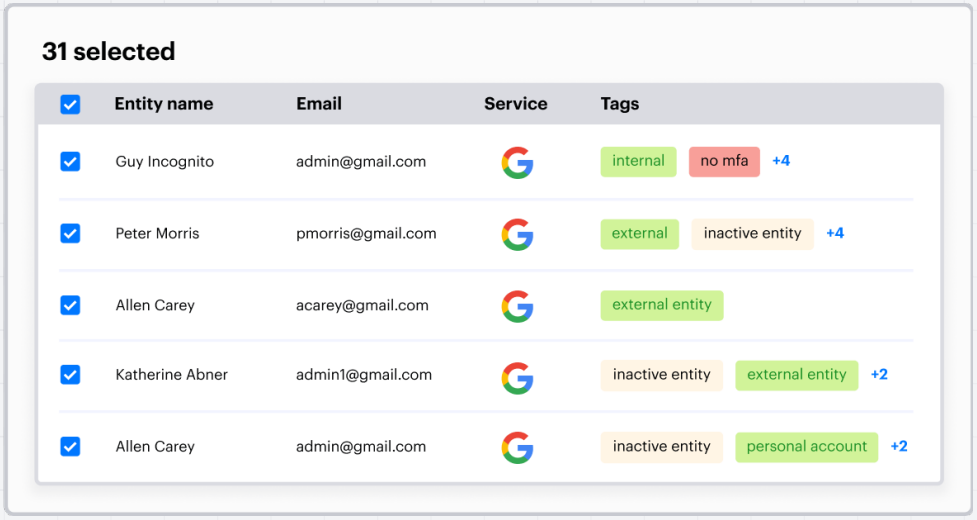
## Mapeo de identidades relacionadas

Varonis identifica automáticamente las cuentas relacionadas mediante un algoritmo patentado. Guy Incognito es un usuario administrador de Google Workspace que usa una cuenta personal de Gmail sin MFA. Está conectado a varias identidades en los entornos de Umbrella Corp.

Guy tiene varios alias, una combinación de cuentas corporativas y personales.

## Brechas de desvinculación: cuentas inactivas

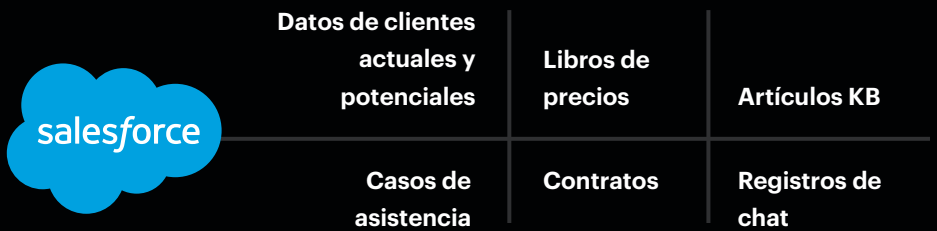
Varonis encontró más de 3000 identidades obsoletas en los servicios de directorio y repositorios de cuentas locales de Umbrella Corp.




Contratistas desvinculados que conservan el acceso desde sus cuentas personales de Google.

# RIESGO DE SALESFORCE

Salesforce almacena los datos más valiosos de una organización, pero sus estructuras de permisos complejas y la falta de visibilidad sobre quién puede acceder a esos datos lo exponen al riesgo de amenazas internas y ciberamenazas.

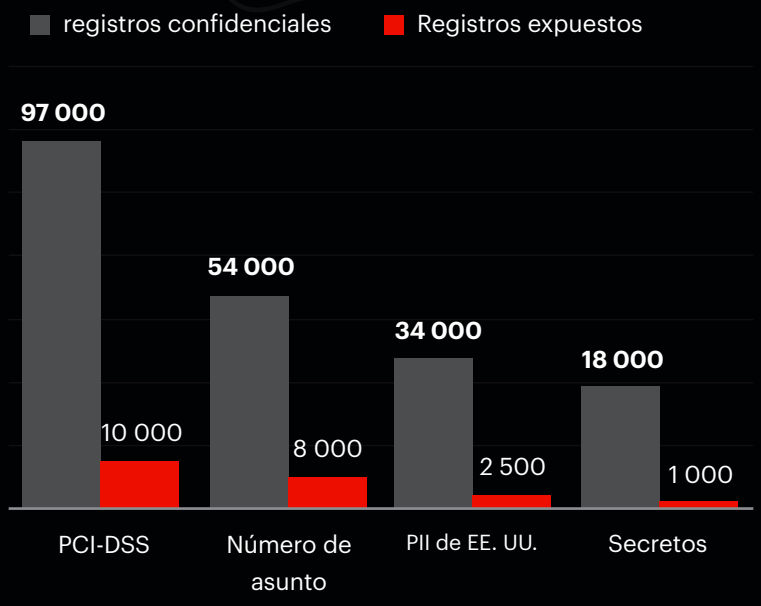



## Alcance de la evaluación

| | | |
|---|---|---|
| **Entornos** | + Producción<br>+ Entorno de prueba | + Desarrollo |
| **Datos** | + 234 240 registros<br>+ 8241 documentos<br>+ 520 campos<br>+ 9214 recursos confidenciales | + 203 registros compartidos externos/públicos<br>+ 22 aplicaciones de terceros monitoreadas |
| **Identidades** | + 2012 usuarios internos<br>+ 425 usuarios externos<br>+ 124 contratistas | + 212 usuarios invitados<br>+ 55 superadministradores |
| **Permisos** | + 89 perfiles<br>+ 52 perfiles privilegiados<br>+ 22 perfiles de la comunidad<br>+ 3 perfiles de invitados | + 55 conjuntos de permisos<br>+ 27 grupos de conjuntos de permisos<br>+ 33 roles |
| **Los 3 principales dominios externos** | Gmail.com | Hotmail.com<br>Proton Mail<br>Protonmail.com |

# EXPOSICIÓN DE DATOS DE SALESFORCE

**¿Qué tipo de datos se encuentran en Salesforce y cuál es su exposición?**




**203 000**
Objetos con al menos un registro confidencial

**1 500**
Registros confidenciales expuestos externamente

**20 000**
Registros confidenciales expuestos en toda la organización

## Riesgo de exfiltración de datos de Umbrella Corp

Hay un pequeño número de derechos, que se describen a continuación, que deben considerarse altamente privilegiados. Si se otorgan a un número demasiado grande de usuarios, estos derechos pueden crear un riesgo significativo de exfiltración y exposición de datos.

### 23235 permisos con la opción Exportar reporte habilitada

La opción Exportar reporte les permite a los usuarios exportar datos directamente desde Salesforce. Si es necesario, debe aplicarse a Conjuntos de permisos.

### 124 permisos con las opciones Ver todos los datos o Modificar todos los datos habilitadas

Los usuarios con este permiso pueden ver y modificar todos los datos dentro de la organización.

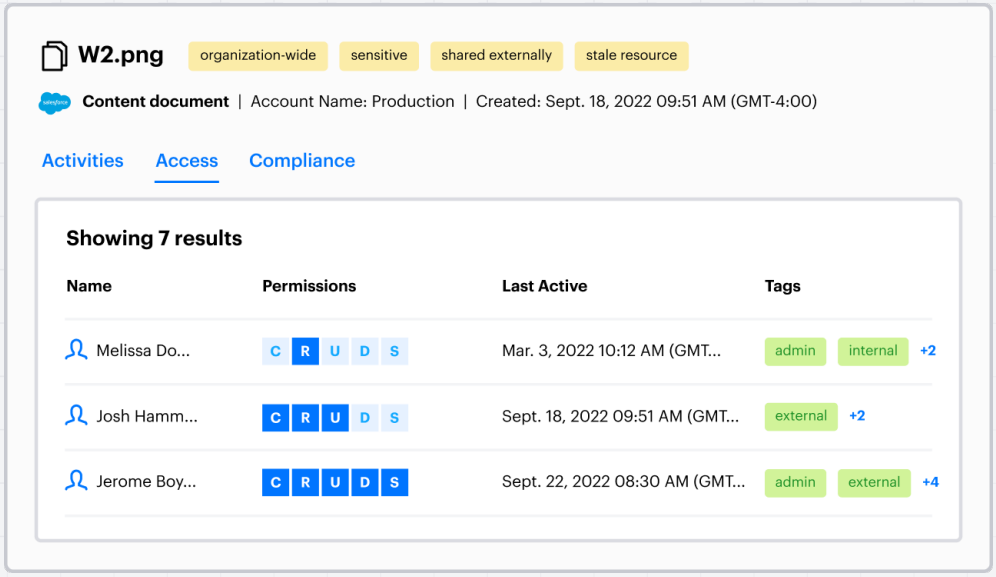
### 52 permisos con API habilitada

Permite a los usuarios comunicarse con todas las API de Salesforce, exfiltrar datos o realizar otras acciones.

Varonis le ofrece a Umbrella Corp una visión en tiempo real de los derechos críticos y la capacidad de ajustar rápidamente el acceso y aplicar privilegios mínimos. También recomendamos configurar las alertas de Varonis que se activan cuando cambian estos derechos con privilegios.

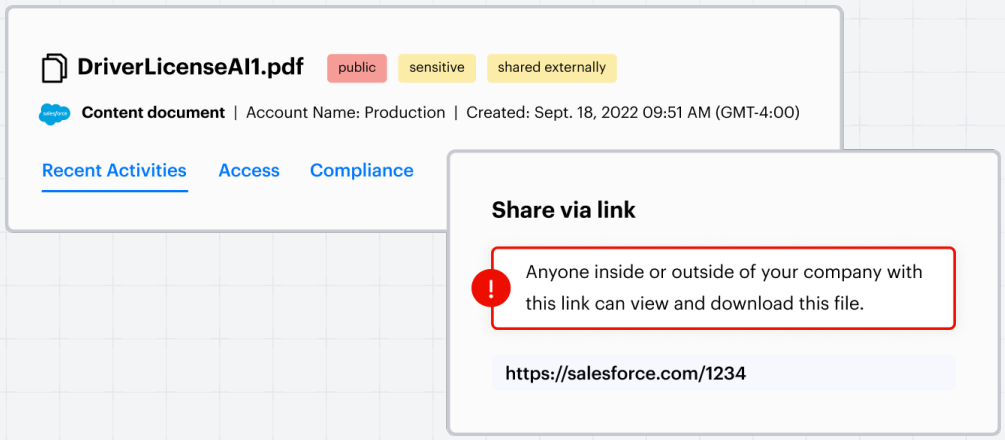
# DATOS CONFIDENCIALES COMPARTIDOS EXTERNAMENTE

Las instancias de Salesforce de Umbrella Corp permiten el acceso de usuarios invitados. También hay varias cuentas de usuario que actúan como cuentas de servicio para aplicaciones de terceros. Varonis detectó más de 1500 registros confidenciales expuestos externamente, como el archivo adjunto W2 a continuación.



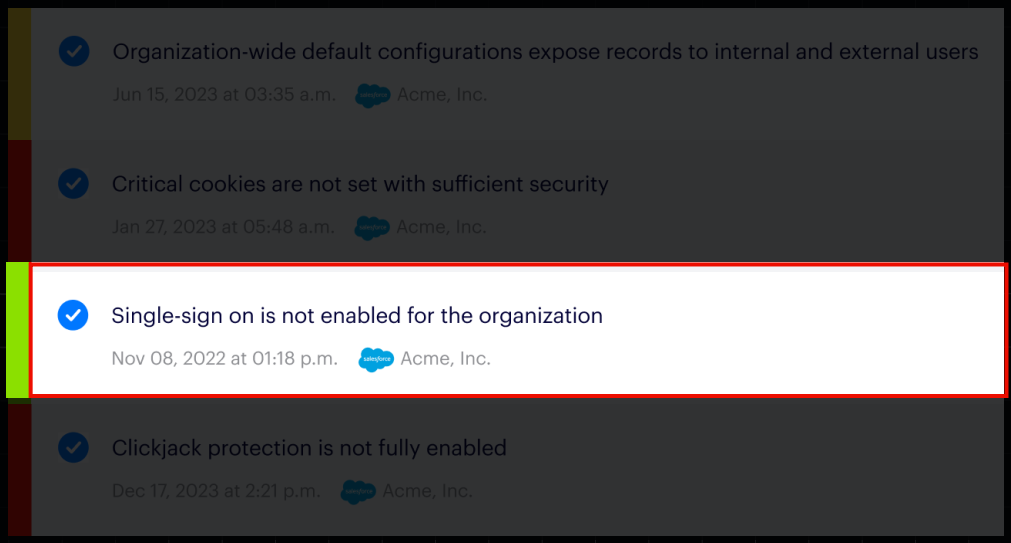

Los usuarios fuera de la empresa pueden acceder, actualizar o eliminar datos de PCI y PII en su instancia de Salesforce.

Además de exponer datos a usuarios invitados, contratistas y otros terceros autenticados, nuestra evaluación también reveló datos expuestos en Internet a través de enlaces públicos.



# CONFIGURACIONES ERRÓNEAS DE SALESFORCE

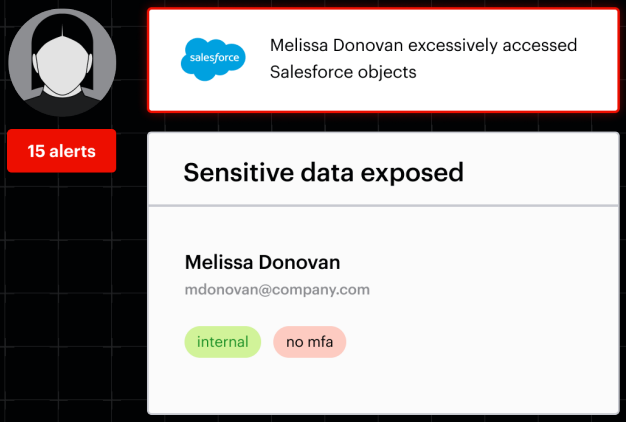
Varonis detectó y corrigió cuatro configuraciones erróneas o ajustes predeterminados inseguros en toda la organización que podrían proporcionar una ruta de ataque.




Los contratistas desvinculados accedieron a la cuenta del entorno de prueba a pesar de que las cuentas de Okta se habían dado de baja.

## Alertas de Salesforce

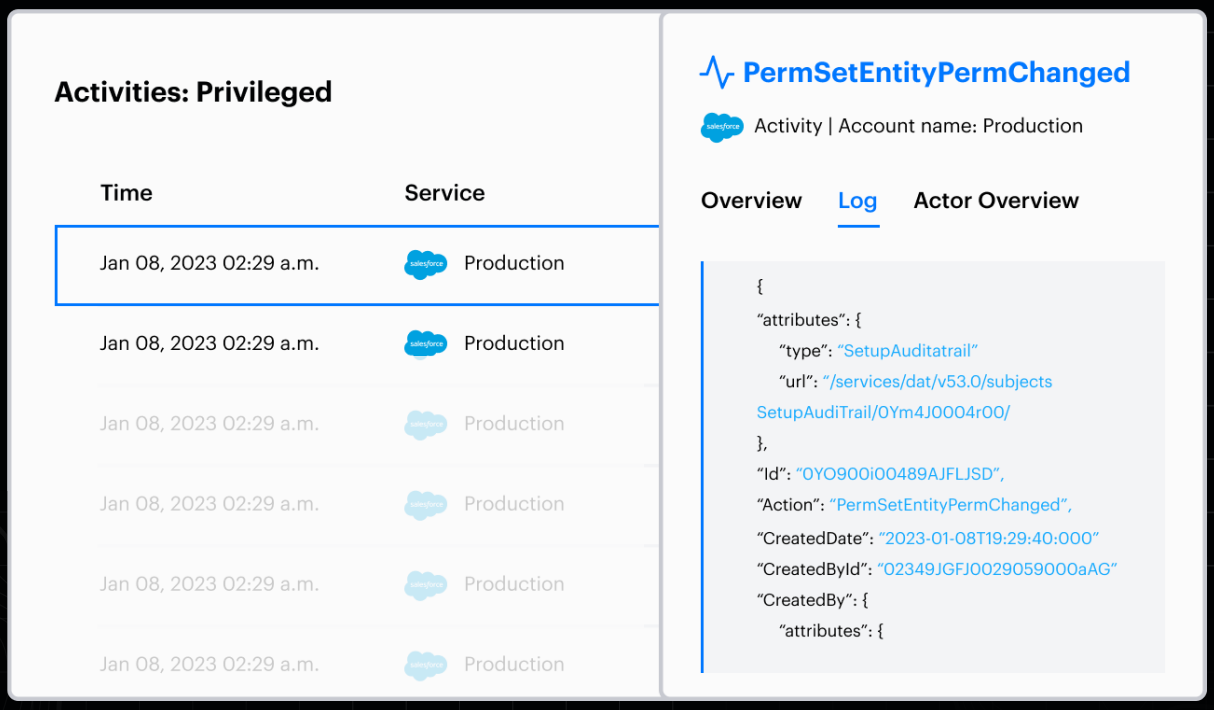
El equipo de Respuesta a incidentes de Varonis activó y resolvió 15 alertas, incluido un caso en el que la empleada interna Melissa Donovan estaba accediendo a una cantidad anormal de registros en comparación con su comportamiento habitual. Nuestra investigación mostró que Melissa había instalado una extensión de navegador que accedía rápidamente a las URL de los registros de Salesforce.




Melissa Donovan se desvió de su actividad normal y accedió a los registros que generalmente no toca.

## Monitorear los cambios de administrador

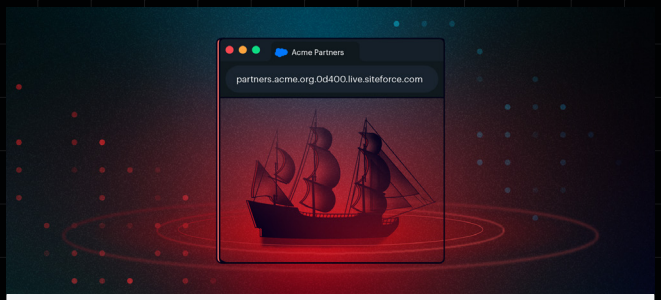
Josh Hammond hizo varios cambios de administrador en producción fuera de la ventana de control de cambios. A continuación, se muestra el registro de cambios detallado.



VARONIS
THREAT LABS

# INVESTIGACIÓN DE SALESFORCE

Nuestro equipo busca y divulga vulnerabilidades y configuraciones tóxicas en Salesforce.




**Sitios fantasma: robo de datos de comunidades de ventas inactivas**


**El agujero de gusano de Einstein: captura de calendarios de Outlook y Google a través del error de usuario invitado de Salesforce**

## Acerca del laboratorios de amenazas de Varonis

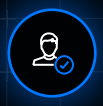
Los miembros de nuestro equipo de investigadores de seguridad y científicos de datos son algunas de las mentes más brillantes del mundo en términos de ciberseguridad. Con décadas de experiencia militar, de inteligencia y empresarial, el equipo del laboratorio de amenazas de Varonis busca proactivamente vulnerabilidades en las aplicaciones que nuestros clientes utilizan, para encontrar y cerrar las deficiencias antes de que los atacantes puedan hacerlo. Todos estos aprendizajes están programados en nuestra plataforma para ayudarlo a mantenerse a la vanguardia de los ataques cibernéticos.

Eche un vistazo a las últimas investigaciones: **www.varonis.com/blog/tag/threat-research**

# REDUZCA SU RIESGO SIN ASUMIR NINGÚN OTRO

Nuestra evaluación de riesgos gratuita se configura en cuestión de minutos y ofrece un valor inmediato. En menos de 24 horas, tendrá una visión clara y basada en el riesgo de los datos que más importan y un camino claro hacia la remediación automatizada.

**Acceso completo a la plataforma SaaS de Varonis**
Obtenga acceso completo a nuestra plataforma de seguridad de datos durante el tiempo de su evaluación y obtenga información útil para sus datos más críticos.



**Analista dedicado del equipo de respuesta a incidentes**
Estar conectado con la plataforma de seguridad de datos SaaS de Varonis significa que nuestros expertos están al tanto de sus alertas y que lo llamaremos si detectamos algo alarmante.

**Reporte de hallazgos clave**
Un resumen detallado de sus riesgos de seguridad de datos y una presentación ejecutiva para revisar los hallazgos y recomendaciones. Este reporte es suyo, incluso si no se convierte en cliente.

**Obtenga su evaluación gratuita**

**Con la confianza de miles de clientes**

ING · U.S. AIR FORCE · NASA · BlueCross BlueShield · Nasdaq · Coca-Cola · TOYOTA · U.S.ARMY · Penguin Random House · E*TRADE

LÍDER DE FORRESTER


# Varonis fue nombrado líder en plataformas de seguridad de datos.

**"Varonis es una de las principales opciones para las organizaciones que priorizan la visibilidad profunda de los datos, las capacidades de clasificación y la remediación automatizada para el acceso a los datos".**

Forrester Wave™ : Plateformes de sécurité des données, 1er trimestre 2023

LÍDER DE FORRESTER

0 10 20 30 40 50 60 70

VARONIS