VARONIS

REMEDIAÇÃO

AVALIAÇÃO DE RISCO DE DADOS

Preparado para a Umbrella Corp

RESULTADOS CRÍTICOS

0 10 20 30 40 50 60 70

DATA DE CRIAÇÃO: 07/08/2023

TOC

SUMÁRIO

“Fiquei impressionado com a rapidez com que a Varonis conseguiu classificar os dados e descobrir a potencial exposição durante a avaliação gratuita. Foi realmente revelador.”

Michael Smith, CISO, HKS

POR QUE A UMBRELLA CORP SOLICITOU O RELATÓRIO DE RISCO DE DADOS COM A VARONIS?

A Umbrella Corp possui exigências a nível de diretoria para descobrir, classificar e rotular todas as PII para garantir a conformidade e a eficácia do DLP. O incidente recente de ransomware da Umbrella Corporation destaca a necessidade do monitoramento de dados. Sem ações preventivas, eles enfrentam multas regulatórias e níveis de exposição de dados com os quais a liderança não se sente confortável.

Contestações

A classificação dos dados sensíveis e a correção das exposições é uma tarefa difícil.

Quantificar a postura de segurança dos dados e mostrar o progresso à direção é uma obrigação.

Esforços de remediação de dados são difíceis com uma equipe pequena.

É necessário monitorar o uso de dados e alertar sobre atividades anormais.

As subunidades operam de forma independente - é necessário um programa de segurança de dados unificado.zero-width

As auditorias de conformidade são manuais e incompletas.

VISÃO GERAL DA AVALIAÇÃO DE RISCO DA UMBRELLA CORP

Fontes de dados conectadas e cronograma de avaliação

A Varonis pode se conectar à dezenas de fontes de dados adicionais. A configuração leva alguns minutos.

Microsoft 365 | Active Directory + Azure AD | Salesforce | Compartilhamento de arquivos do Windows | Google Workspace

Instalação da plataforma
1 de junho de 2023

Relatório

Prova de valor
21 de junho de 2023

5,6M recursos (arquivos/objetos)

12 mil identidades

805 mil eventos (média diária)

2,4M registros sensíveis classificados (PHI, PCI, segredos)

Observação: apenas uma parte do ambiente geral da Umbrella Corp estava conectada à POC.

RESULTADOS CRÍTICOS

Riscos que podem resultar em um vazamento de dados

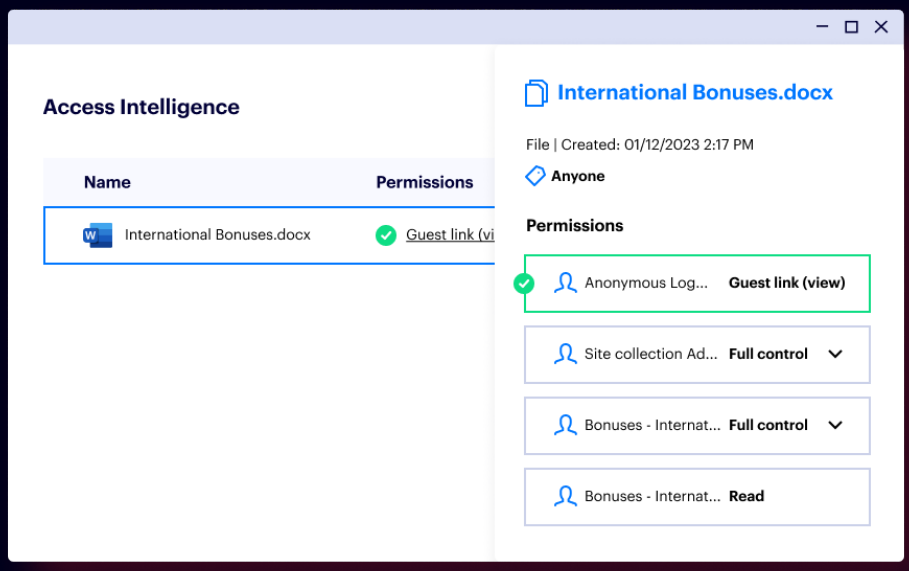
Abaixo estão os quatro principais resultados que a Varonis considera um risco crítico à segurança de dados.

1. Relatórios de remuneração do RH compartilhados publicamente por meio de links de "qualquer pessoa".
2. 332 usuários do Salesforce podem exportar dados de produção.
3. Um usuário externo é um superadministrador no Google Workspace.
4. Um assistente de marketing acionou um alerta anormal de acesso aos dados.

Resultado crítico nº 1

Relatórios de remuneração do RH compartilhados publicamente por meio de links de "qualquer pessoa".

Melissa Donovan expôs acidentalmente as informações de bônus da empresa na internet.



Tipo de risco:
exposição pública de dados

Controle NIST:
AC-3(9): versão controlada

Sistema afetado:
Microsoft 365

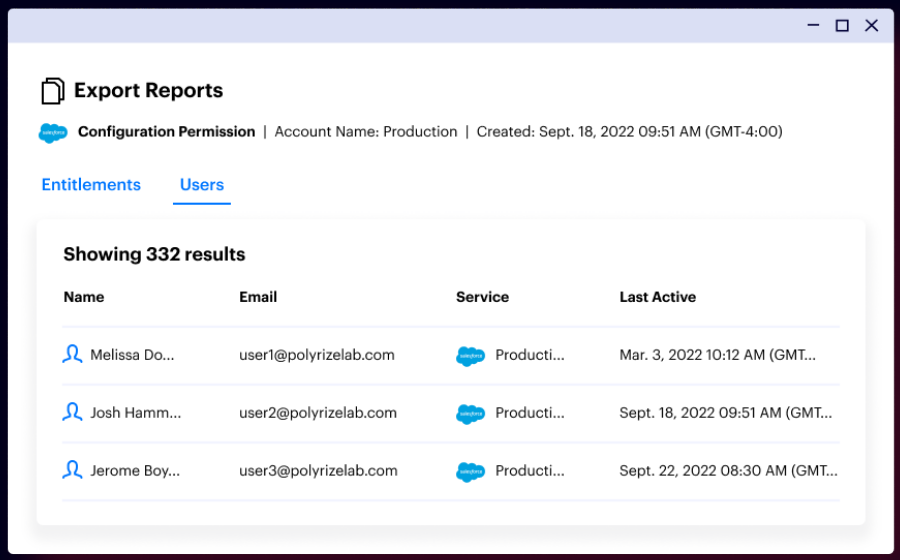
Observação:
Melissa Donovan, uma parceira de negócios do RH, enviou o International Bonsuses.docx para o Teams da equipe de RH em 12 de janeiro. A verificação de classificação da Varonis identificou 231 instâncias de PII dentro do arquivo e nossos logs mostram que ela criou o link "Qualquer pessoa" em 13 de fevereiro, expondo o arquivo à internet. O link foi acessado por usuários anônimos de 27 endereços IP diversos em todo o mundo.

Recomendação:
revogar o acesso de "Qualquer pessoa" a este arquivo imediatamente, desativando o link. Desative a capacidade de compartilhar publicamente. Use a automação da Varonis para revogar qualquer link público para arquivos que contenham informações confidenciais.

Resultado crítico nº 2

332 usuários do Salesforce podem exportar dados de produção.

O perfil regular "Vendas" concede acesso à exportação. Ele é muito amplo e deve ser corrigido.



Tipo de risco:
Exposição a dados confidenciais

Controle NIST:
AC-2(7): Estratégias baseadas em Funções

Sistema afetado:
Salesforce (produção, sandbox, desenvolvimento)

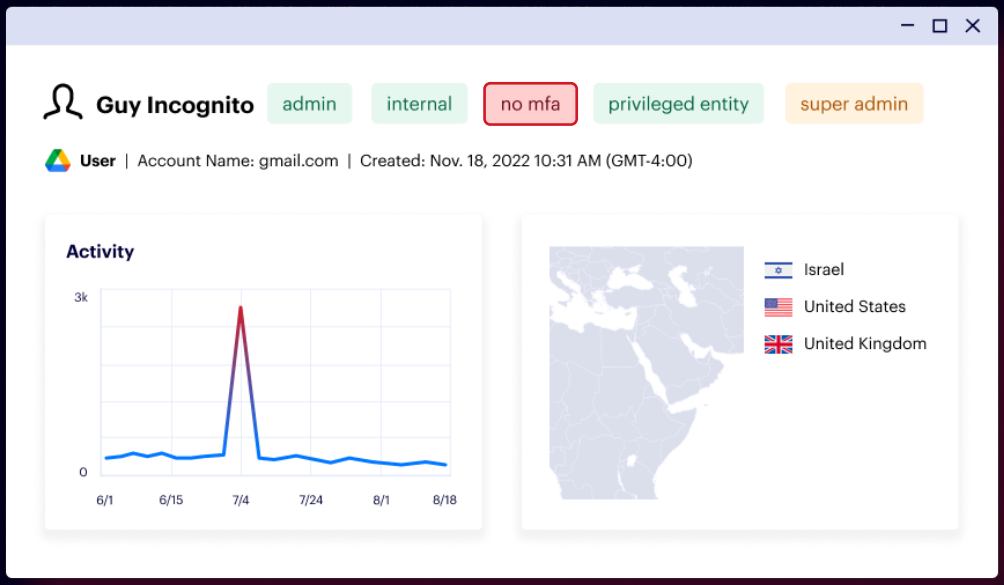
Observação:
as varreduras da Varonis identificaram uma combinação tóxica de permissões que cria um risco sério de exfiltração de dados - 332 vendedores, por meio de seu perfil "Vendas", podem exportar todos os dados de leads, contatos, oportunidades e contas da instância de produção do Salesforce da Umbrella Corp.

Recomendação:
remova a permissão de exportação do relatório do perfil "Vendas" e qualquer outra função não-administrativa. Revise todos os perfis e conjuntos de permissões que concedem ações altamente privilegiadas, como exportar relatórios, modificar todos os dados e ler todos os dados.

Resultado crítico nº 3

Um usuário externo é um super administrador no Google Workspace.

Guy Incognito é um super administrador sem MFA. A atividade desse usuário aumentou em 4 de julho, o que desencadeou um alerta.



Tipo de risco:
Conta de administrador insegura

Controle NIST:
AC-2(7): contas de usuário privilegiadas

Sistema afetado:
Google Workspace

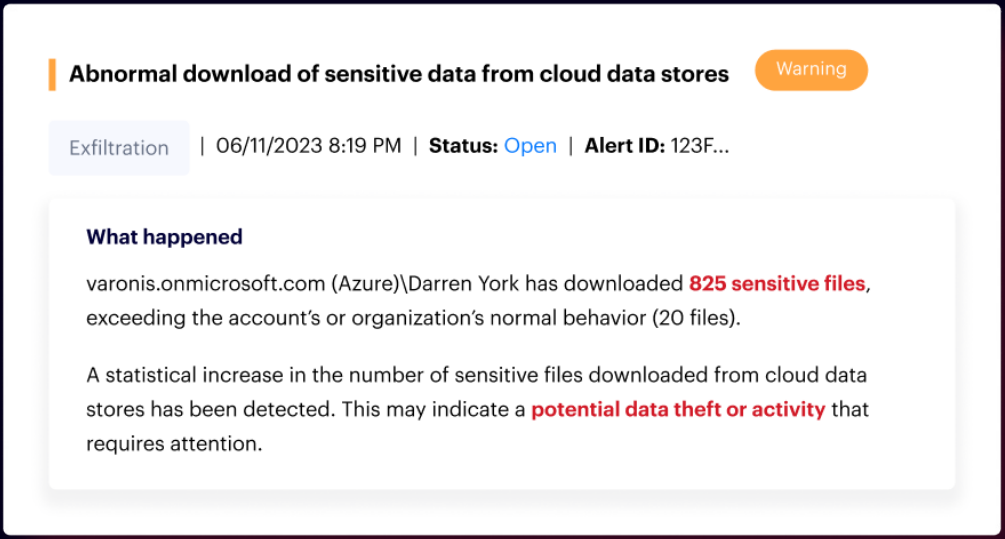
Observação:
o Guy Incognito é um prestador de serviços que usa uma conta pessoal do Gmail para acessar a conta do Google Workspace da Umbrella Corp. Esse usuário tem direitos de super administrador e não tem MFA habilitado. Essa conta é considerada de risco extremamente alto.

Recomendação:
implemente imediatamente o MFA na conta do Guy Incognito e adicione a uma lista de observação da Varonis. Analise os últimos 30 dias de atividade, direitos e identidades relacionadas ao usuário. Decida se esse usuário externo realmente precisa dos direitos de super administrador.

Resultado crítico nº 4

Um assistente de marketing acionou um alerta anormal de acesso aos dados.

Darren York não deve ter acesso a dados financeiros. A Varonis UEBA detectou acesso anômalo.



Tipo de risco:
comportamento anormal do usuário

Controle NIST:
AC-2(12): monitoramento de conta para uso atípico

Sistema afetado:
Microsoft 365

Observação:
o assistente de marketing Darren York acionou um alerta baseado em comportamento ao sair do seu padrão normal de atividade de acesso à dados. A Varonis detectou que ele estava acessando arquivos com dados financeiros, o que é atípico para sua função.

Recomendação:
use a Varonis para executar uma consulta e compilar todas as atividades do Darren nos últimos 30 dias. Certifique-se de que as permissões para dados que contêm registros financeiros estejam acessíveis apenas aos funcionários que precisam deste acesso.

POSTURA DE SEGURANÇA DE DADOS

Os dados confidenciais da Umbrella Corp estão espalhados em vários repositórios de dados de serviços em nuvem e on-premises. Para minimizar o risco de um vazamento de dados, é crucial que a empresa tenha visibilidade e controle em tempo real sobre seu patrimônio de dados em constantes mudanças - com classificação unificada, detecção de ameaças e aplicação de políticas.

Onde estão os dados mais confidenciais da Umbrella Corp e quantos estão em risco?

Principais indicadores de risco:

310 mil de registros confidenciais	**27 mil** eventos em dados confidenciais por dia
24,5 mil registros confidenciais expostos em toda a organização	**11 mil** registros confidenciais expostos externamente

Descoberta e classificação de dados

Políticas de classificação ativadas

Habilitamos 85 regras integradas e criamos três regras personalizadas durante esta avaliação de risco. Os quatro tipos principais de dados por volume são mostrados abaixo.

PCI-DSS

Contêineres: 1.160
Objetos: 12.421
Registros: 89.924

Senhas

Contêineres: 160
Objetos: 421
Registros: 923

PII dos EUA

Contêineres: 2.620
Objetos: 72.245
Registros: 199.104

Números do Processo

Contêineres: 1.002
Objetos: 92,420
Registros: 799.922

Biblioteca de políticas integrada

PII	GDPR	Credenciais	Financeiro	Federal
HIPAA PHI 2.0	LGPD Alemanha	Senhas	PCI-DSS 2.0	ITAR
Lei de Privacidade do Colorado	LGPD França	Chaves privadas	SOX	Ultrassecreto
Lei NY SHIELD	LGPD Áustria	Certificados	GLBA	CUI

Mais centenas de regras, padrões e dicionários

O poder da classificação de dados da Varonis

- Verdadeira varredura incremental para descoberta escalável e eficiente em grandes conjuntos de dados
- Políticas de classificação unificadas em todos os repositórios de dados compatíveis
- Testada na prática em ambientes de vários petabytes
- 400+ regras testadas e criadas por especialistas disponíveis (com ainda mais por vir) e prontas para uso
- Amostragem e escopos de verificação personalizáveis

Exposição de dados do Microsoft 365

A exposição de dados no M365 não é exclusiva da Umbrella Corp. Em média, a empresa tem mais de 40 milhões de permissões exclusivas em seus dados multinuvem e, de acordo com a Microsoft, mais de 50% das permissões são de alto risco e capazes de causar danos catastróficos se configuradas incorretamente.

Que tipo de dados residem no M365 e qual é a exposição da Umbrella Corp?

Principais indicadores de risco:

203 mil
de registros confidenciais

20 mil
registros confidenciais expostos em toda a organização

1,5 mil
registros confidenciais expostos externamente

Risco no modelo de colaboração

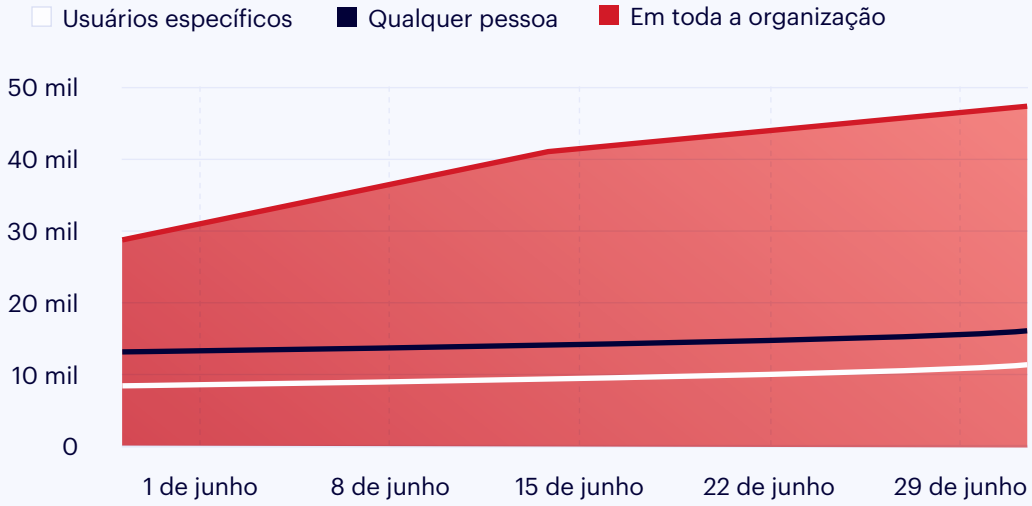
Níveis de exposição

Compartilhar links é útil para a colaboração, mas eles podem expor os dados associados à todos na organização, usuários convidados ou internet. A Umbrella Corp tem uma quantidade significativa de exposição de dados confidenciais devido a links do SharePoint e do OneDrive.

SharePoint Online e OneDrive

Aumento de links compartilhados

O raio de exposição da Umbrella Corp está crescendo rapidamente, semana após semana. Abaixo temos um gráfico de crescimento por tipo de links durante o período da avaliação de risco.



Dados expostos publicamente

Dados expostos publicamente por meio de links para “qualquer pessoa”

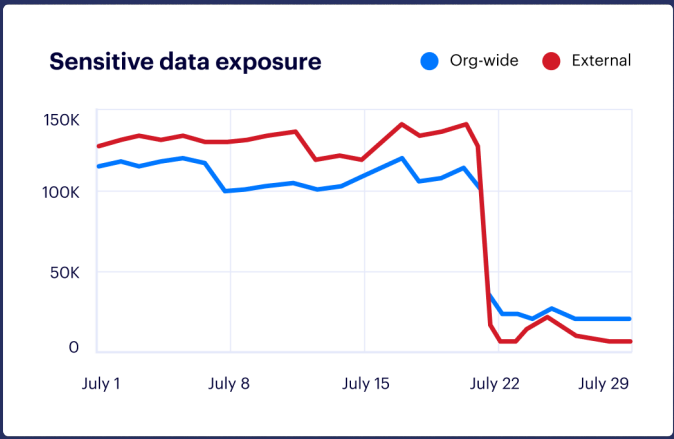
Veja abaixo uma pequena amostra de arquivos confidenciais que podem ser acessados por qualquer pessoa na internet. A trilha de auditoria da Varonis mostra o tipo de dados dentro do arquivo (PCI, PHI, etc.), quando o link foi compartilhado, quem compartilhou e se o arquivo foi acessado por meio do link.

	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. Planilhas com credenciais e informações de cartão de crédito
2. Contratos de trabalho com PII e informações de contas bancárias

Com que rapidez podemos corrigir o risco de links compartilhados?

Um cliente em potencial da Varonis pode eliminar a exposição rapidamente com a automação. Abaixo estão os resultados de uma grande instituição financeira que ativou a automação de privilégios mínimos. Quase 100% da exposição de dados ao ambiente externo e em toda a organização foi eliminada em menos de 30 dias.



As políticas de automação mantêm o risco baixo diante do crescimento dos dados e da colaboração contínua. Com as políticas definidas para serem aplicadas automaticamente, os novos riscos são corrigidos à medida que aparecem, e o privilégio mínimo é aplicado continuamente.

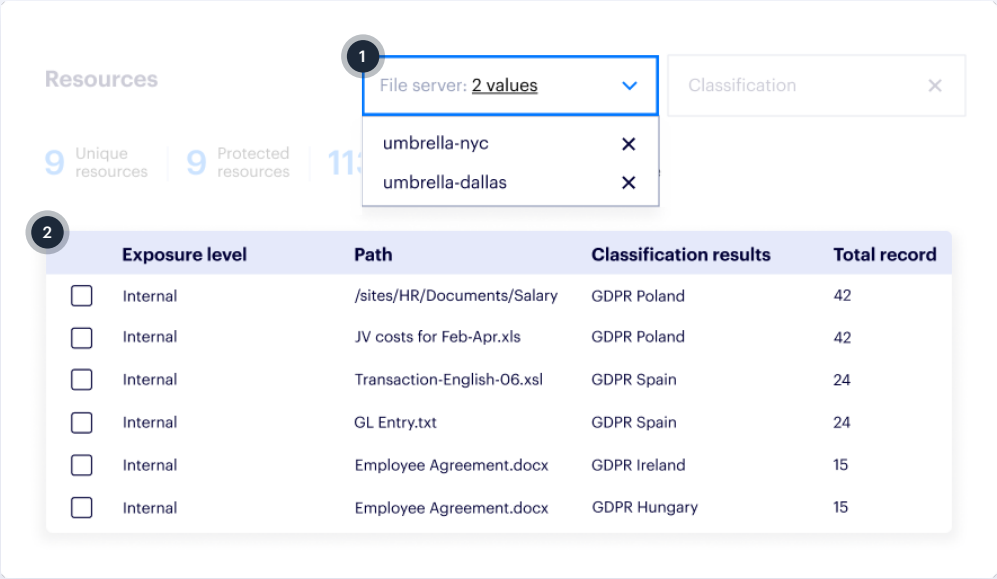
Dados extraviados e rotulados incorretamente

Dados extraviados: risco de conformidade com a LGPD

A Varonis descobriu registros de PII de cidadãos da União Européia em um tenant do M365 hospedado nos EUA. Os arquivos foram carregados em 15 de julho por uma conta de serviço chamada "ExportJob", que parece estar conectada a uma tarefa automatizada do Workato. Recomendamos a migração desses dados para o tenant da Umbrella Corp baseado na União Européia e o ajuste de tarefa automatizada.

1 Tenants do M365 baseado nos EUA

2 Arquivos contendo PII de cidadãos da 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

Arquivos com rótulos errados: lacuna na aplicação do DLP

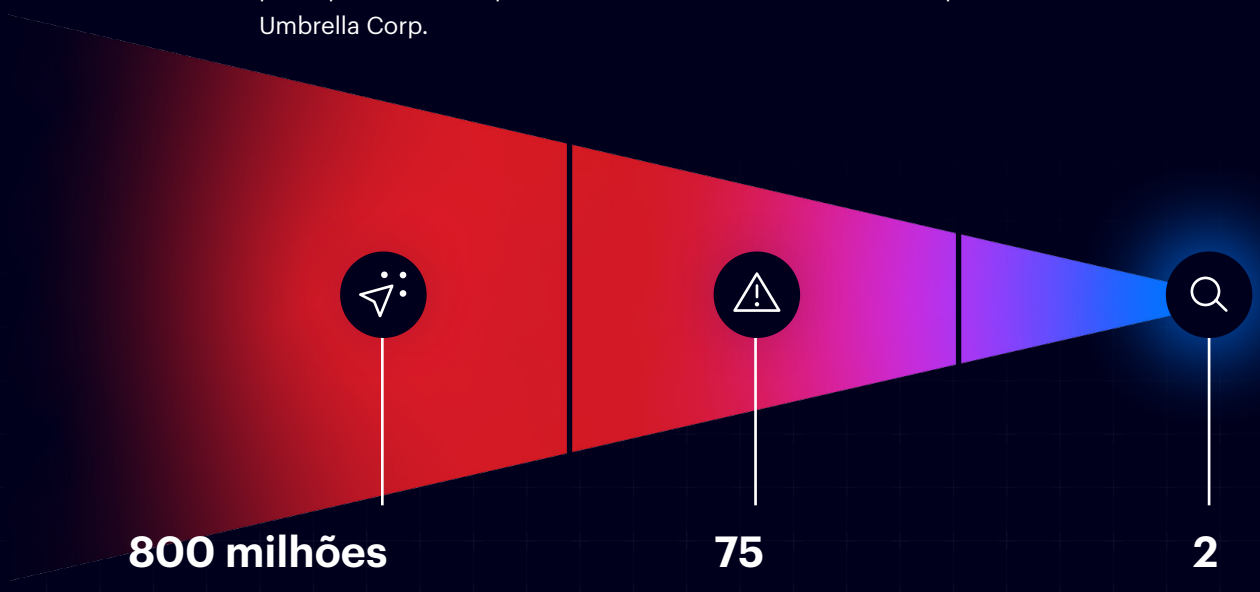
Muitos arquivos não possuem os rótulos MIP ou têm rótulos desatualizados e mal aplicados. Como consequência, a imposição de DLP downstream pode falhar, resultando em vazamento de dados confidenciais ou o inverso: os usuários ficam impedidos de compartilhar dados não confidenciais que estão rotulados incorretamente.

Encontramos mais de 27.000 arquivos confidenciais sem rótulo aplicado.

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

Detecção e resposta contra ameaças

O monitoramento em tempo real e a detecção de ameaças baseada em comportamento da Varonis foram ativados em todos os sistemas no escopo. Durante o período de avaliação, nossos modelos de IA foram treinados em mais de 800 milhões de eventos para aprender o comportamento exclusivo dos usuários e dispositivos no ambiente da Umbrella Corp.



800 milhões

Centenas de milhões de eventos coletados

Cada evento é automaticamente enriquecido e normalizado.

75

Dezenas de alertas acionados

Média de ~3 por dia

2

Vários incidentes investigados

A equipe proativa de resposta à incidentes da Varonis detectou e escalou dois incidentes.

UEBA centrada em dados

Os eventos são enriquecidos com dados, usuário e contexto do dispositivo. Os analistas de segurança podem executar consultas como: "Listar todos os eventos de acesso à dados confidenciais por contas privilegiadas de dispositivos conectados da Alemanha".

Identificação da conta

Resolução do IP para o dispositivo

Operação por	Tipo de conta	Objeto	Confidencial?	Endereço IP do dispositivo	Nome do dispositivo	Endereço IP externo	Geolocalização
Amy Johnson	Executivo	Customer.xlsx	Sim	173.17.33.3	aj-03154	54.239.13.2	Canadá

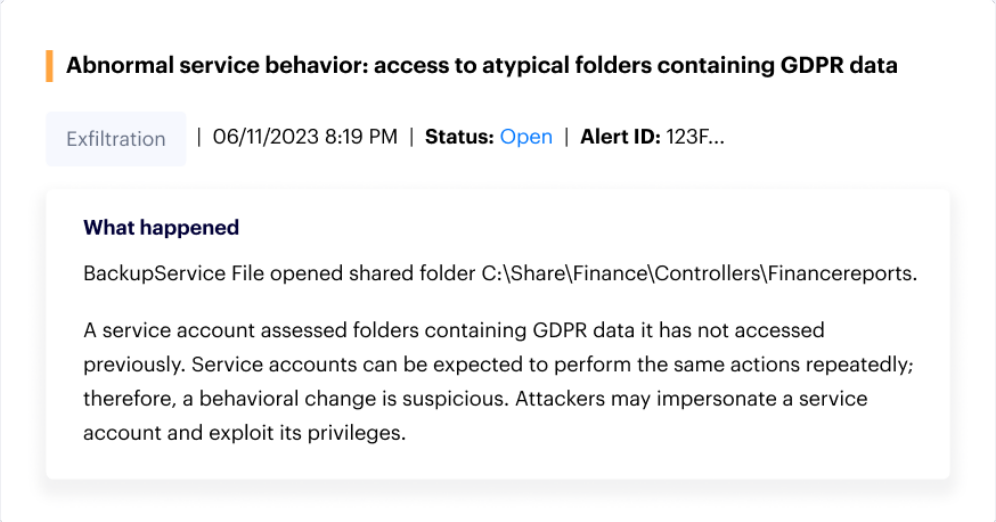
Confidencialidade dos arquivos

Geolocalização

ANÁLISE DE AMEAÇAS

Relatório de incidente: conta de serviço comprometida

Observação:
a equipe de resposta à incidentes da Varonis descobriu que uma conta de serviço de backup foi comprometida e começou a acessar os dados do usuário.



Mitigação:
a equipe de resposta à incidentes da Varonis analisou e remediou o incidente em minutos. A conta UC\BackupService foi imediatamente desabilitada, as sessões ativas foram encerradas e a senha foi redefinida. A Varonis forneceu um relatório de investigação completo à equipe da Umbrella Corp com análise e recomendações da causa raiz.

Detalhes:
142 arquivos foram acessados pela conta comprometida. 82 desses arquivos foram classificados como confidenciais pela 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...

RISCO DE CONFIGURAÇÃO

A Varonis está verificando continuamente as configurações do sistema nas plataformas SaaS e IaaS da Umbrella Corp para determinar se alguma configuração é arriscada ou se foi removida do estado desejado.

21 configurações incorretas descobertas

O Salesforce tem as configurações mais incorretas (8).

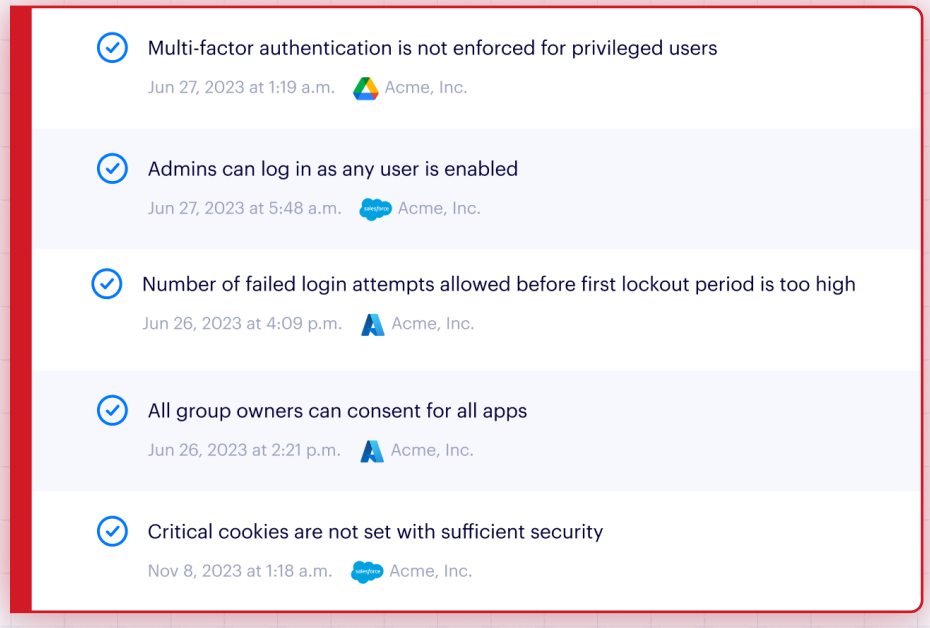
5 configurações incorretas de alta gravidade

O M365 e o Salesforce têm dois erros críticos de configuração.

4 configurações definidas para auto-aplicação

A Varonis pode aplicar automaticamente configurações seguras.

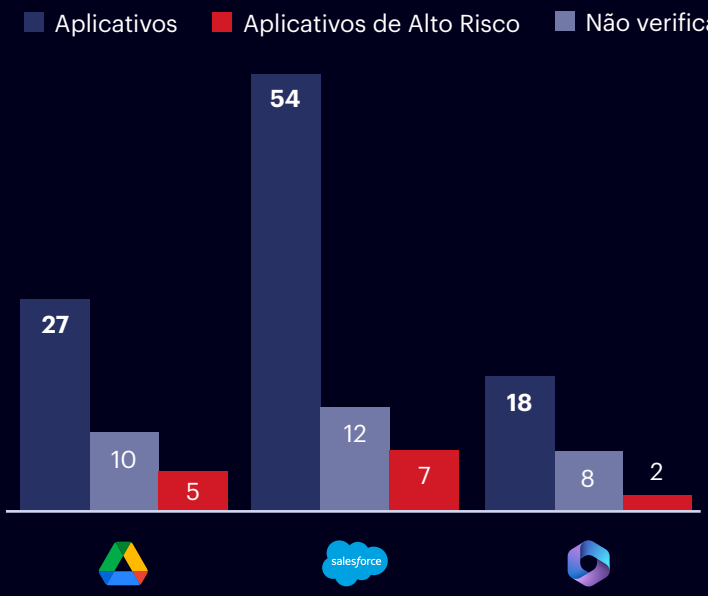
Veja abaixo um resumo dos **cinco erros de configuração de alta gravidade** descobertos durante a avaliação. Todos os detalhes e as recomendações para cada um deles podem ser encontrados na interface do usuário da Varonis.



Clique aqui para ver mais exemplos de configurações de SaaS e IaaS que a Varonis pode monitorar.

RISCO DE APLICATIVOS DE TERCEIROS

Identificamos 36 apps de terceiros que são arriscados, estão inativos ou não foram verificados.



99
Aplicativos de terceiros instalados

14
alto risco com amplo acesso à dados

22
Aplicativos inativos

Aqui está um detalhamento dos quatro principais aplicativos de terceiros, por contagem de usuários, que estão integrados às plataformas SaaS que a Varonis está monitorando:

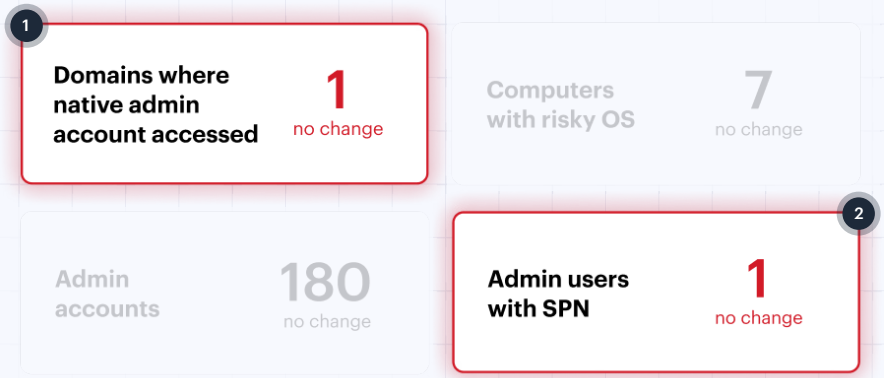
Google	Salesforce	Microsoft 365
miro	6sense	
dialpad	HubSpot	slack
Signeasy	INCENT	Trello
SUPERMETRICS	Power BI	Evernote

Além disso, descobrimos 111 usuários inativos cujas atribuições de aplicativos podem ser revogadas diretamente da interface do usuário da Varonis.

RISCO DE IDENTIDADE

Postura de segurança do Active Directory

A Varonis examina os serviços de diretório na nuvem e on-premises da Umbrella Corp e detecta configurações fracas que podem fornecer caminhos para os invasores. Esses riscos são atualizados em tempo real em seus painéis da Varonis e ajudarão a priorizar os esforços de fortalecimento do AD.

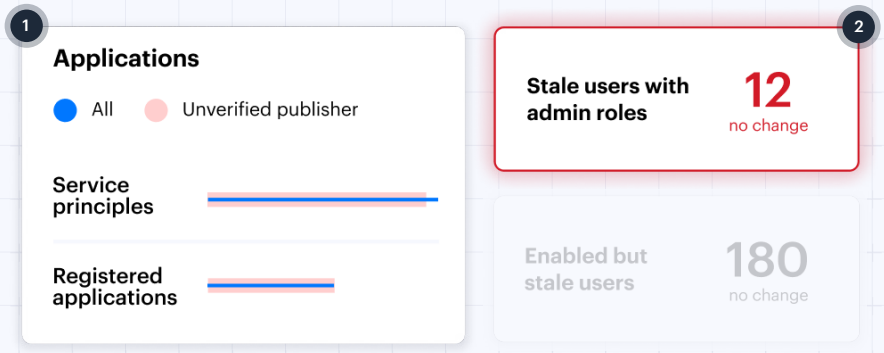


1 Raramente essa conta é usada em circunstâncias normais. Isso pode indicar comprometimento.

2 Vulnerável à quebra de senha do Office

Postura de segurança Entra ID (Azure AD)

A postura da Entra ID está sob monitoramento contínuo e recebe pontuação da Varonis. Configurações erradas e incertas que colocam seus dados em risco são exibidas em seus painéis e relatórios de risco.



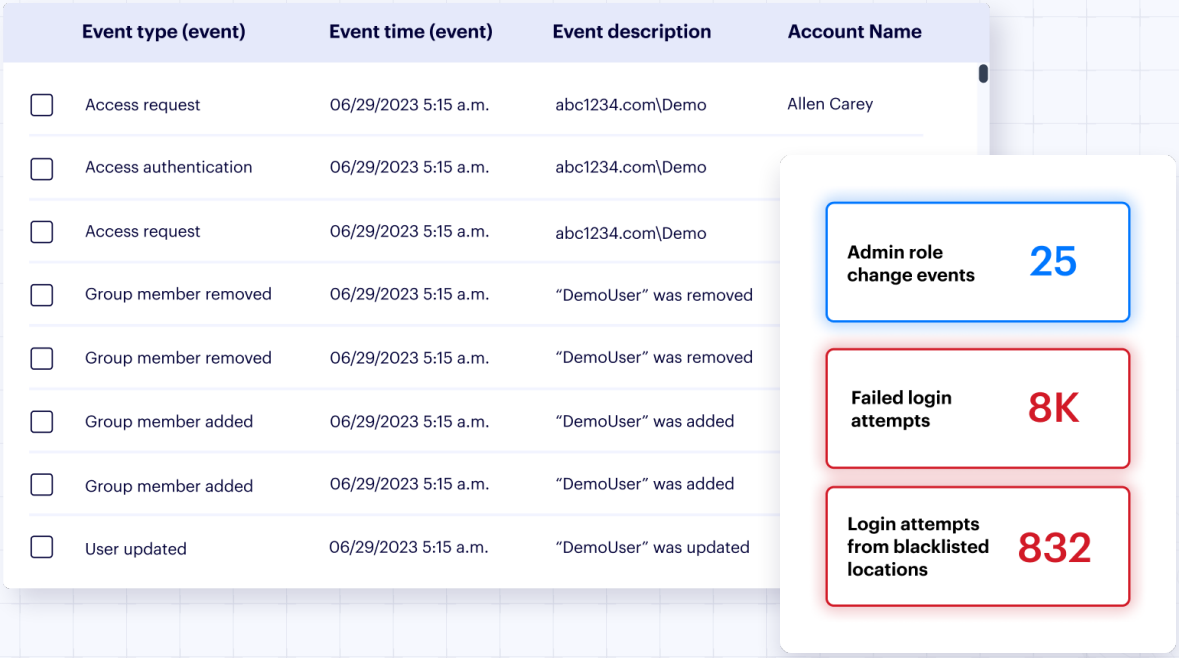
1 Revise a permissão de aplicativos não verificados e o acesso aos dados.

2 Essas contas devem ser desativadas imediatamente.

Monitoramento de Active Directory

A Varonis está monitorando eventos nos serviços de diretório da Umbrella Corp e correlacionando essas ações com os eventos centrados em dados coletados de plataformas de colaboração e repositórios de dados.

Essas mudanças foram realizadas fora da janela de controle de alterações.



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	

Usuários externos e contas pessoais de risco

As contas de usuário do Gmail estão obsoletas, mas têm acesso a dados confidenciais.

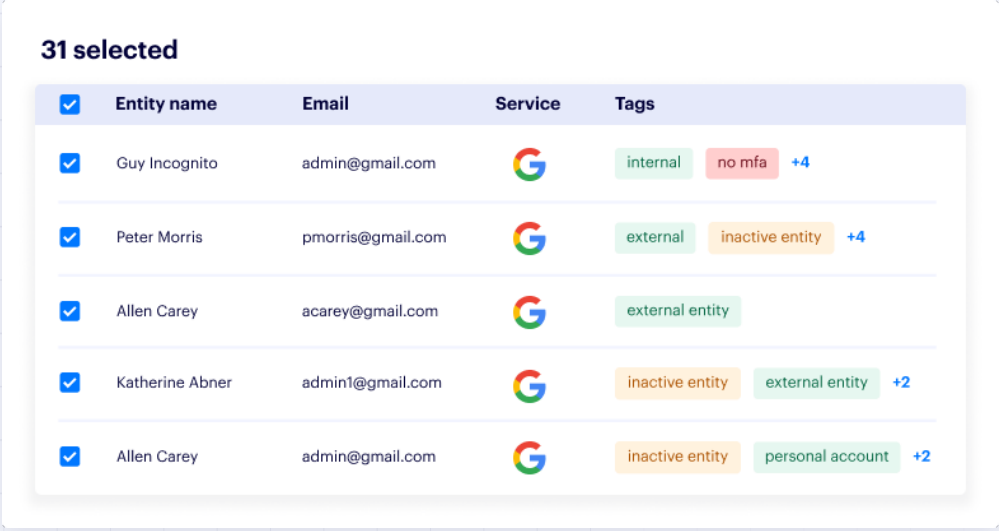
Mapeamento de identidade associada

A Varonis identifica automaticamente contas associadas usando um algoritmo reservado. Guy Incognito é um usuário administrador do Google Workspace usando uma conta pessoal do Gmail sem MFA. Ele está conectado a várias identidades em ambientes da Umbrella Corp.

Guy tem vários pseudônimos, uma combinação de contas corporativas e pessoais.

Lacunas de offboarding: contas inativas

A Varonis encontrou mais de 3.000 identidades obsoletas nos serviços de diretório e repositórios de contas locais da Umbrella Corp.



Contratantes demitidos mantêm o acesso de suas contas pessoais do Google.

RISCO DO SALESFORCE

O Salesforce abriga os dados mais valiosos de uma organização, mas suas complexas estruturas de permissão e a falta de visibilidade sobre quem pode acessar esses dados a colocam em risco de ameaças internas e ameaças cibernéticas.

Dados de clientes e de prospects	**Livros de preços**	**Artigos da base de conhecimento**
Casos de suporte	**Contratos**	**Logs de bate-papo**

Escopo do relatório

Ambientes	• Produção • Sandbox	• Dev
Dados	• 234.240 registros • 8.241 documentos • 520 campos • 9.214 recursos confidenciais	• 203 registros compartilhados externos/públicos • 22 aplicativos de terceiros monitorados
Identidades	• 2.012 usuários internos • 425 usuários externos • 124 prestadores de serviços	• 212 usuários convidados • 55 super administradores
Direitos	• 89 perfis • 52 perfis privilegiados • 22 perfis da comunidade • 3 perfis de convidados	• 55 conjuntos de permissões • 27 grupos de conjunto de permissões • 33 funções
3 domínios externos principais	Gmail.com	Hotmail.com Proton Mail Protonmail.com

EXPOSIÇÃO DE DADOS DO SALESFORCE

Que tipo de dados residem no Salesforce e qual é a exposição?

203 mil
objetos com pelo menos um registro confidencial

1,5 mil
registros confidenciais expostos externamente

20 mil
registros confidenciais expostos em toda a organização

Risco de exfiltração de dados da Umbrella Corp

Existem alguns direitos, descritos abaixo, que devem ser considerados altamente privilegiados. Se concedidos a muitos usuários, esses direitos podem criar um risco significativo de exposição e exfiltração de dados.

235 direitos com relatório de exportação ativado

O Relatório de Exportação permite que os usuários exportem dados diretamente do Salesforce. Se necessário, o relatório deve ser aplicado à Conjuntos de Permissões.

124 direitos com Visualizar Todos os Dados ou Modificar Todos os Dados Habilitados

Os usuários com essa permissão podem visualizar e modificar todos os dados dentro da organização.

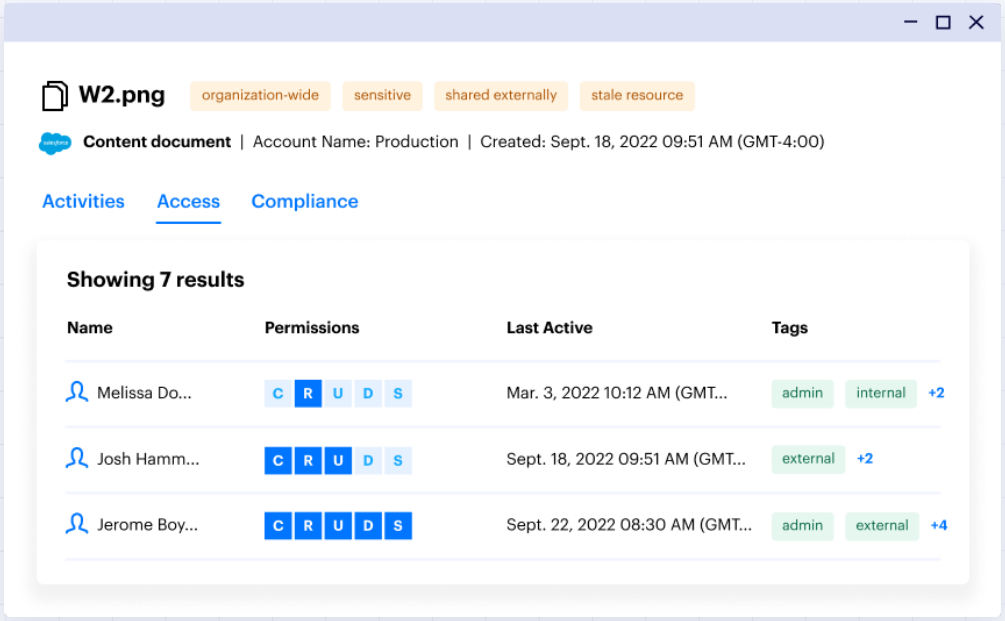
52 direitos com API habilitada

Permite que os usuários se comuniquem com todas as APIs do Salesforce, extraiam dados ou executem outras ações.

A Varonis fornece à Umbrella Corp uma visão em tempo real de direitos críticos e a capacidade de acessar rapidamente o tamanho correto e impor os mínimos privilégios. Recomendamos também configurar alertas da Varonis que são acionados quando esses direitos de privilégios mudam.

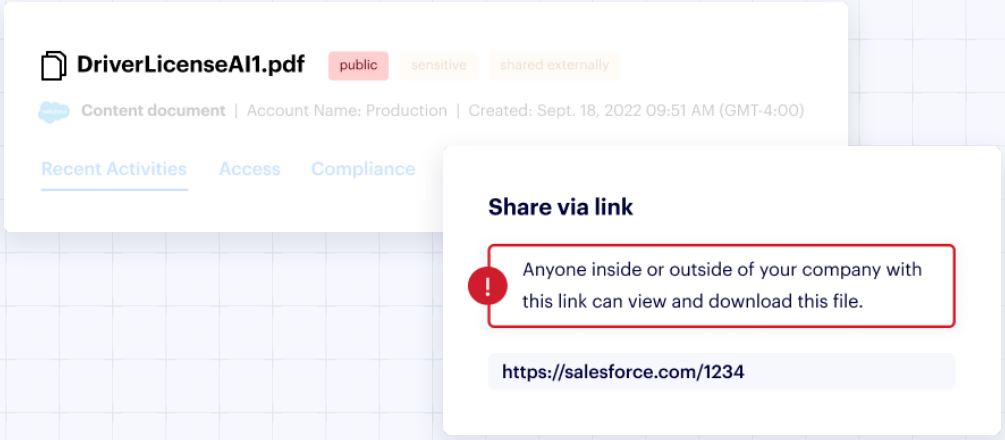
DADOS CONFIDENCIAIS COMPARTILHADOS EXTERNAMENTE

As instâncias do Salesforce da Umbrella Corp permitem acesso de usuário convidado. Há também várias contas de usuário que atuam como contas de serviço para aplicativos de terceiros. A Varonis detectou mais de 1.500 registros confidenciais que estão expostos externamente, como o anexo do arquivo W2 abaixo.



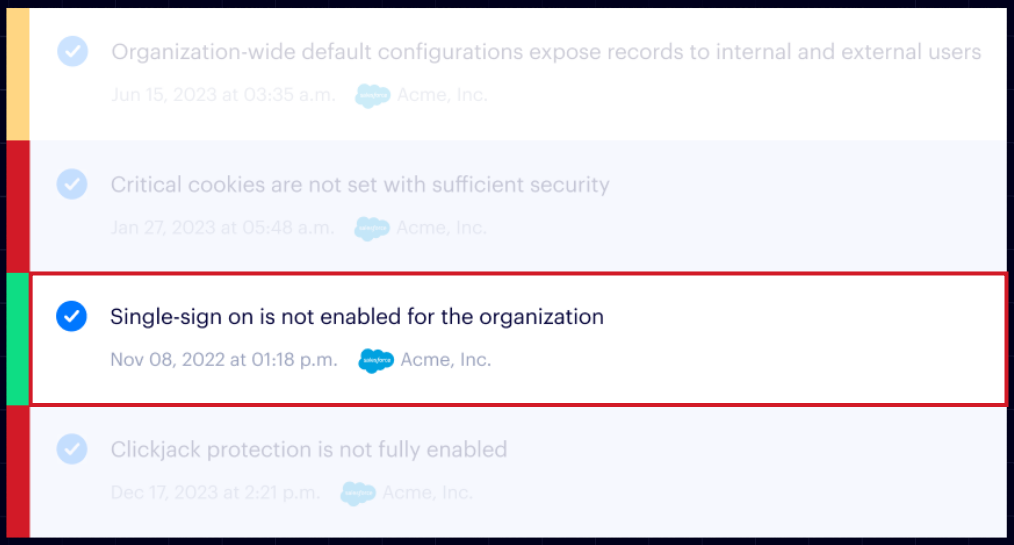
Os usuários fora da empresa podem acessar, atualizar ou excluir dados de PCI e PII em sua instância do Salesforce.

Além de expor dados a usuários convidados, contratados e outros terceiros autenticados, nossa avaliação também apresentou dados expostos à Internet por meio de links públicos.



CONFIGURAÇÕES INCORRETAS DO SALESFORCE

A Varonis detectou e corrigiu quatro configurações incorretas ou padrões inseguros em toda a organização que poderiam oferecer um caminho de ataque.



Os prestadores de serviços cujos contratos foram encerrados estavam acessando a conta sandbox mesmo que as contas do Okta tivessem sido desprovisionadas.

Alertas do Salesforce

Quinze alertas foram acionados e resolvidos pela equipe de resposta à incidentes da Varonis, incluindo um caso em que a colaboradora Melissa Donovan estava acessando um número anormal de registros em comparação com seu comportamento padrão. Nossa investigação mostrou que Melissa havia instalado uma extensão do navegador que estava acessando URLs de registro do Salesforce rapidamente.

15 alerts

Melissa Donovan excessively accessed Salesforce objects

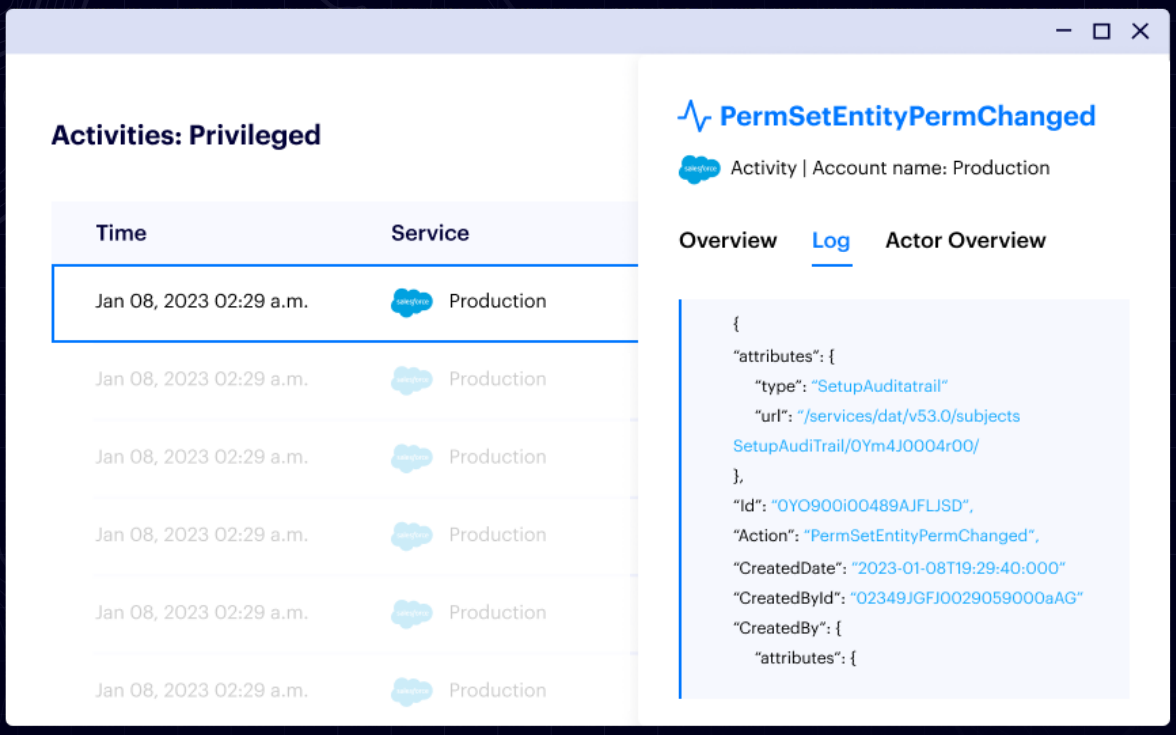
Sensitive data exposed

Melissa Donovan
mdonovan@company.com
internal
no mfa

Melissa Donovan saiu da sua atividade normal, acessando registros que ela geralmente não precisava.

Monitorando alterações de administradores

Josh Hammond fez várias alterações de administrador para produção fora da janela de controle de alterações. Abaixo está o log de alterações detalhado.



VARONIS
THREAT LABS

PESQUISA DO SALESFORCE

Nossa equipe procura e divulga vulnerabilidades e configurações tóxicas no Salesforce.

Sites Fantasmas: Roubando Dados de Comunidades de Vendas Desativadas

Einstein's Wormhole: O bug que busca informações do Outlook e do Google Agenda usando usuários convidados do Salesforce

Sobre Varonis Threat Labs

Nossa equipe de pesquisadores em segurança e cientistas de dados estão entre os principais especialistas em cibersegurança do mundo. Com décadas de experiência nos setores militar, corporativo e de inteligência, a equipe Varonis Threat Labs procura proativamente por vulnerabilidades em aplicações usadas por nossos clientes para encontrar e fechar lacunas antes que os invasores as detectem. Todo esse conhecimento está programado em nossa plataforma para ajudar você a ficar um passo à frente dos ataques cibernéticos.

Confira a pesquisa mais recente: **www.varonis.com/blog/tag/threat-research**

REDUZA OS RISCOS SEM SE ARRISCAR.

Nosso relatório de riscos gratuito leva alguns minutos para ser configurado e oferece valor imediato. Em menos de 24 horas, terá uma visão clara e baseada no risco dos dados mais importantes e um caminho assertivo para a correção automatizada.

Acesso total à plataforma Varonis SaaS

Obtenha acesso total à nossa Plataforma de Segurança de Dados durante a sua avaliação e obtenha insights acionáveis para seus dados mais críticos.

Analista de RI dedicado

Estar conectado à Plataforma de Segurança de Dados SaaS da Varonis significa que nossos especialistas estão de olho em seus alertas e que ligaremos para você se virmos algo alarmante.

Relatório de resultados importantes

Um resumo detalhado de seus riscos à segurança de dados e uma apresentação executiva para analisar os resultados e as recomendações. Esse relatório é seu, mesmo que você não se torne um cliente.

Obtenha sua avaliação gratuita

Com a confiança de milhares de clientes

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

A Varonis é nomeada Líder em Plataformas de Segurança de Dados.

"A Varonis é a melhor opção para organizações que priorizam a visibilidade profunda dos dados, capacidade de classificação e remediação automatizada para acesso aos dados."

Forrester Wave™: Plataformas de Segurança de Dados, 1.º trimestre de 2023

VARONIS