VARONIS

修正

データリスク アセスメント

Umbrella Corp御中

重要な所見

0 10 20 30 40 50 60 70

作成日: 2023年8月7日

TOC

目次

「無償のアセスメントでは、Varonisがデータを分類してデータ露出の可能性を発見するまでの早さに驚かされました。」それは本当に目を見張るものでした。」

Michael Smith氏、最高情報セキュリティ責任者（CISO）、HKS

UMBRELLA CORPがVARONISデータリスクアセスメントを始めた理由

Umbrella Corpには、コンプライアンスと下流のDLPの有効性を確保するために、すべての個人情報（PII：Personally Identifiable Information）を発見、分類、ラベル付けするという取締役会レベルの要件があります。Umbrella Corpの最近のランサムウェアインシデントは、データ監視の必要性を浮き彫りにしました。アクションを起こさなければ、規制当局による罰金や、首脳陣が納得できないレベルのデータ露出に直面することになります。

課題

機密性の高いデータを分類と露出の修正は困難な作業です。

データセキュリティ態勢を数値化し、取締役会に進捗状況を示すことは必須です。

データ修復作業は小規模なチームでは困難です。

データ使用量を監視し、異常なアクティビティについて警告する必要があります。

サブユニットは独立して運営されています — 統一されたデータセキュリティプログラムが必要です。

コンプライアンス監査は手作業で実施されており、不完全です。

UMBRELLA CORPリスクアセスメント概要

接続されたデータソースとアセスメントスケジュール

Varonisはさらに多くのデータソースに接続することができます。セットアップは数分で完了します。

プラットフォームのインストール
2023年6月1日

アセスメント

価値の証明
2023年6月21日

5.6M
リソース（ファイル/オブジェクト）

12K
IDの数

805K
イベント（日次平均）

2.4M
分類された機密性の高いレコード（PHI、PCI、シークレット）

注：概念検証 (POC) のために接続されたのは、Unbrella Corpの環境全体の一部のみ。

重要な所見

情報漏洩事故を引き起こす可能性のあるリスク

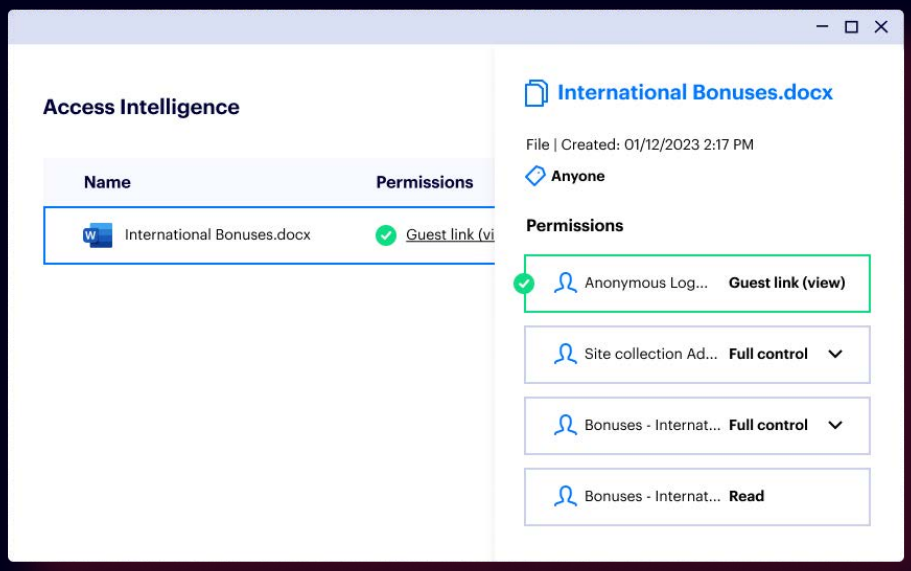
以下は、Varonisが重大なデータセキュリティリスクと考える4つの所見です。

1. 人事報酬レポートが「すべてのユーザー」リンクを通じて一般公開共有されています。
2. 332名のSalesforceユーザーが本番データをエクスポートできます。
3. 外部ユーザー1名が、Google Workspaceの特権管理者です。
4. マーケティングアシスタントが異常なデータアクセスのアラートをトリガーしました。

重要な所見 #1

人事報酬レポートは「すべてのユーザー」リンクを通じて一般公開共有されています。

Melissa Donovan氏は、会社の賞与情報を誤ってインターネットに公開してしまいました。



リスク種別:一般公開データ露出

NISTコントロール:
AC-3(9):管理されたリリース

影響を受けるシステム:
Microsoft 365

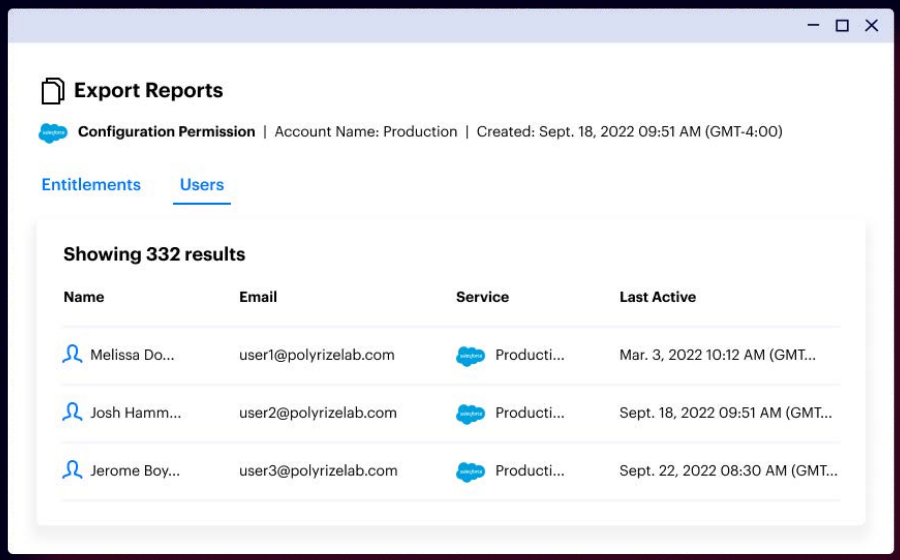
所見:
HRビジネスパートナーのMelissa Donovan氏は、1月12日に、自分の人事Teamsサイトに International Bonuses.docxをアップロードしました。Varonisの分類スキャンにより、ファイル内の231件のPIIがあることが確認され、Varonisのログによると、彼女は2月13日に「すべてのユーザー」リンクを作成し、ファイルをインターネットに公開していました。このリンクは、世界中の27種類のIPアドレスから匿名のユーザーによってアクセスされています。

推奨事項:
リンクを無効にして、このファイルの「すべてのユーザー」アクセス権を直ちに取り消します。一般公開共有を無効にします。Varonisの自動化を使用して、機密性の高い情報を含むファイルへの一般公開リンクを取り消します。

重要な所見 #2

332名のSalesforceユーザーが本番データをエクスポートできます。

通常の「Sales」プロファイルが、エクスポートアクセス権が付与しています。これは範囲が広過ぎるため、修正する必要があります。



リスク種別：機密性の高いデータの露出

NIST管理策：
AC-2(7)：役割ベースのスキーム

影響を受けるシステム：
Salesforce（本番環境、サンドボックス、開発環境）

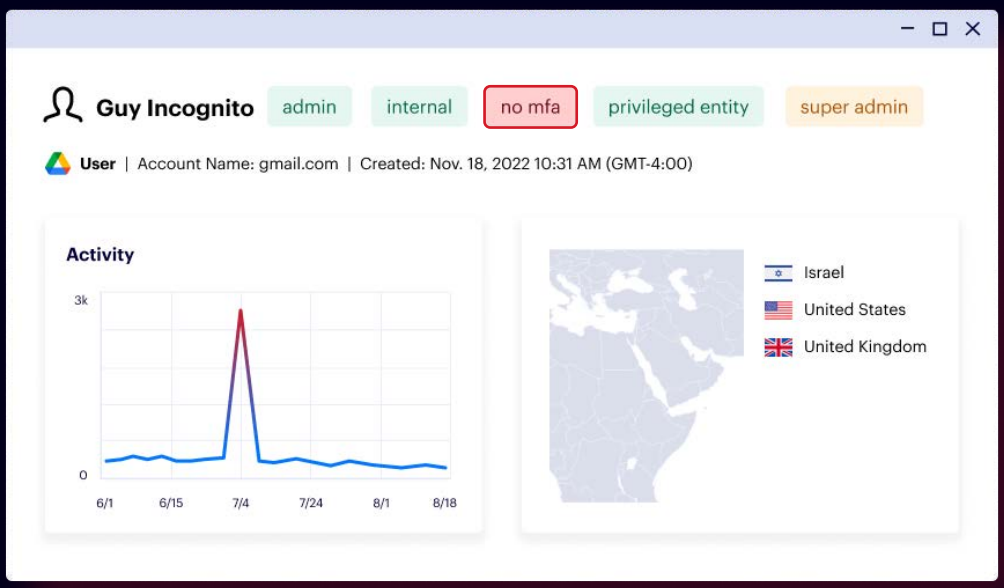
所見：
Varonisのスキャンでは、重大なデータ持ち出しリスクを引き起こす有害な権限の組み合わせが特定されました — 332人の営業担当者が、「Sales」プロファイルを介して、Umbrella Corpの本番Salesforceインスタンスからすべてのリード、連絡先、商談、およびアカウントデータをエクスポートできます。

推奨事項：
「Sales」プロファイルおよびその他の管理者以外のロールからレポートのエクスポート権限を削除してください。高度な特権アクションを付与するすべてのプロファイルと権限セットを見直します — レポートのエクスポート、すべてのデータの変更、すべてのデータの読み取りなど。

重要な所見 #3

外部ユーザー1名が、Google Workspaceの特権管理者です。

Guy Incognito氏は多要素認証 (MFA) が設定されていない特権管理者です。
彼のアクティビティは7月4日に急増し、アラートがトリガーされました。



リスク種別:
安全でない管理者アカウント

NIST管理策:
AC-2(7):特権ユーザアカウント

影響を受けるシステム:
Google Workspace

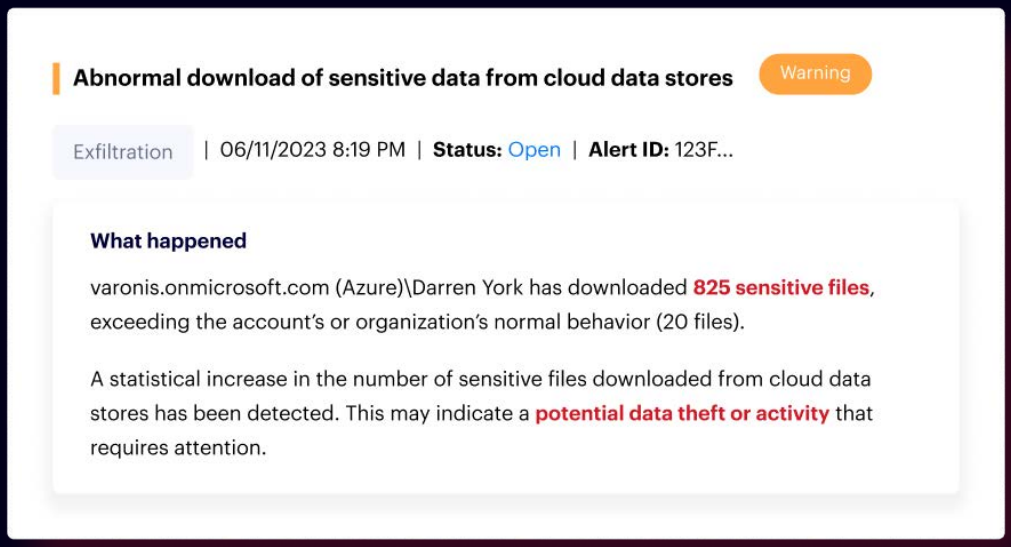
所見:
Guy Incognito氏は、個人のGmailアカウントを使用してUmbrella CorpのGoogle Workspaceアカウントにアクセスしている協力会社の従業員です。このユーザーはスーパー管理者権限を持っており、MFAが有効化されていません。このアカウントは極めてリスクが高いと考えられます。

推奨事項:
Guy Incognito氏のアカウントにMFAを直ちに適用し、Varonisのウォッチリストに追加します。このユーザーの過去30日間のアクティビティ、エンタイトルメント、および関連するIDを確認します。この外部ユーザーが本当にスーパー管理者権限を必要としているかどうかを判断します。

重要な所見 #4

マーケティングアシスタントが異常なデータアクセスアラートをトリガーしました。

Darren York氏は財務データにアクセス権を持つべきではありません。VaronisのUEBAが異常なアクセスを検出しました。



リスク種別:
ユーザーの異常な振る舞い

NIST管理策:
AC-2(12):非定型的な使用のアカウントの監視

影響を受けるシステム:
Microsoft 365

所見:
マーケティングアシスタントのDarren York氏は、通常のデータアクセスアクティビティのベースラインから逸脱したため、振る舞いベースのアラートをトリガーしました。Varonisは、彼が財務データを含むファイルにアクセスしていることを検出しましたが、これは彼の役割からは異常なことです。

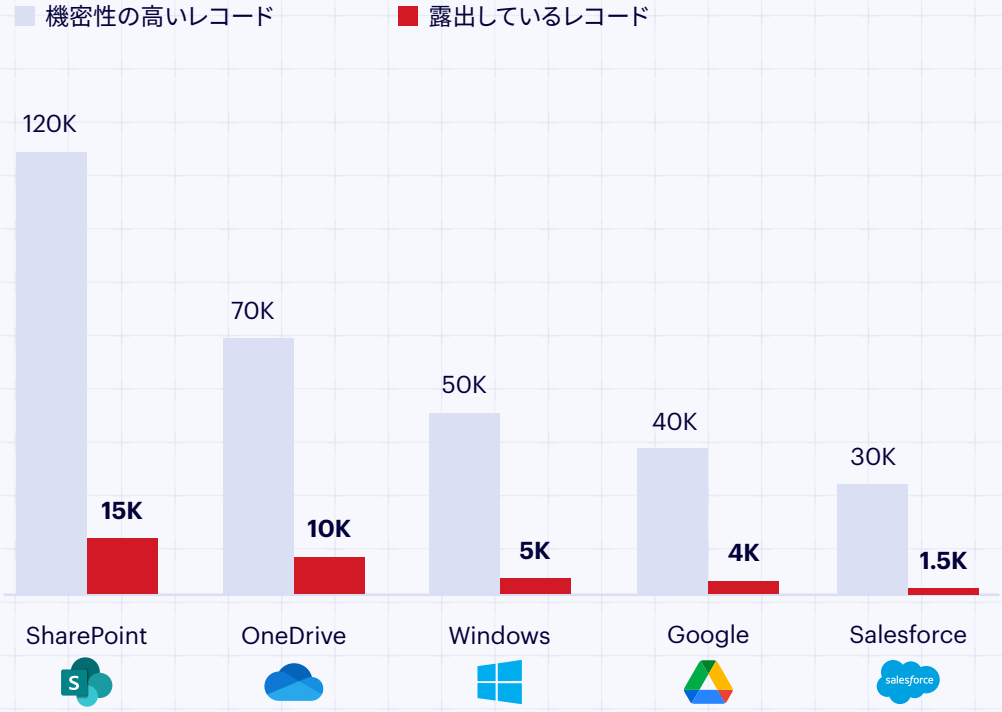
推奨事項:
Varonisを使用してクエリを実行し、Darrenの過去30日間のすべてのアクティビティを確認します。財務情報を含むデータへのアクセス許可を、アクセス権を必要とする従業員のみが使用することを確実にします。

詳細な調査結果

データセキュリティ態勢

Umbrella Corpの機密性の高いデータは、複数のクラウドサービスとオンプレミスのデータストアに散在しています。データ侵害のリスクを最小限に抑えるには、急速に変化するデータ資産をリアルタイムで可視化し、管理することが極めて重要です — 統一的な分類、脅威の検出、ポリシーの強制を活用します。

Umbrella Corpの最も機密性の高いデータはどこにあり、どの程度が危険に晒されていますか?



主要リスク管理指標:

310K 件の機密性の高いレコード	**27K** 機密データに関するイベント数/日
24.5K 組織全体に露出している機密性の高いレコードの数	**11K** 外部に露出している機密性の高いレコードの数

データのディスカバリーと分類

有効になっている分類ポリシー

今回のリスクアセスメントでは、85の組み込みルールを有効にし、3つのカスタムルールを作成しました。データ量別の上位4つのデータ種別を以下に示します。

PCI-DSS

コンテナ数:1,160
オブジェクト数:12,421
レコード数:89,924

パスワード

コンテナ数:160
オブジェクト数:421
レコード数:923

米国の個人識別情報 (PII)

コンテナ数:2,620
オブジェクト数: 72,245
レコード数:199,104

案件番号

コンテナ数:1,002
オブジェクト数:92,420
レコード数:799,922

組み込みポリシーライブラリ

PII	GDPR (EUデータ保護規則)	証明	財務情報	連邦政府
HIPAA PHI 2.0	GDPRドイツ	パスワード	PCI-DSS 2.0	国際武器取引規則 (ITAR)
コロラド州プライバシー法	GDPR France	秘密鍵	SOX法	トップシークレット
ニューヨーク州SHIELD法	GDPRオーストリア	証明書	GLBA (米国金融サービス近代化法)	管理された非機密情報 (CUI)

さらに何百ものルール、パターン、辞書

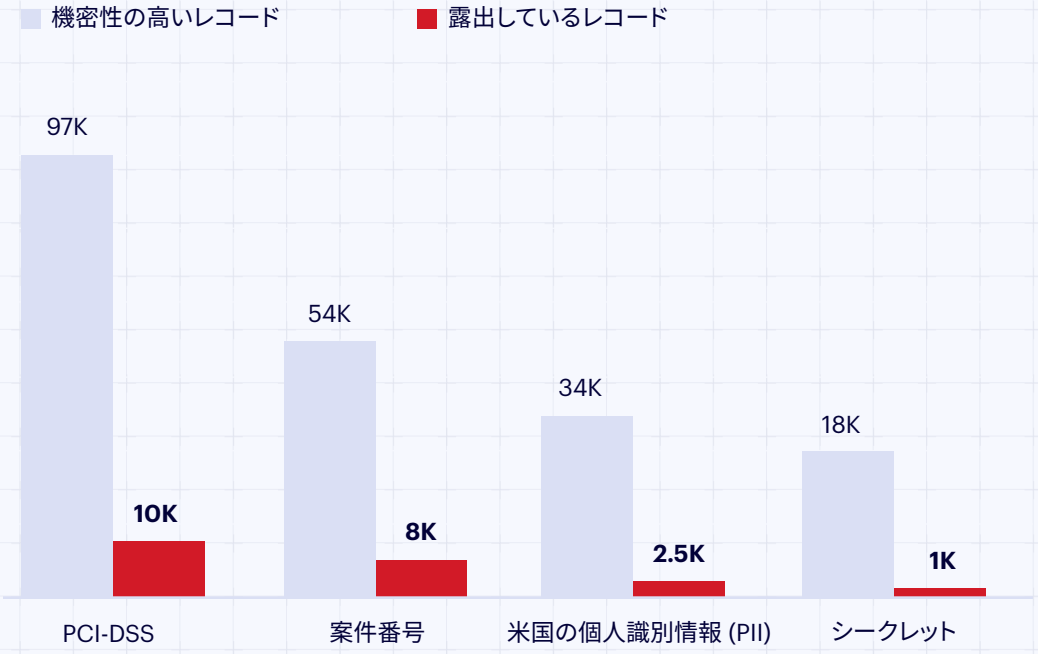
Varonisのデータ分類の威力

- 大量のデータセットから効率的でスケーラブルに検出する、本物の増分スキャン機能
- サポート対象のすべてのデータストアで共通の分類ポリシー
- マルチペタバイト環境で実証済み
- 専門家が作成してテストしたルール400種類以上 (さらに増加中) をすぐに利用可能
- カスタマイズ可能なスキャンスコープとサンプリング

Microsoft 365のデータの露出

M365のデータの露出は、Umbrella Corpに限ったことではありません。平均的な企業ではマルチクラウド環境のデータ全体で4,000万以上の一意のアクセス許可を抱えており、Microsoftによると、アクセス許可の50%超が高リスクで、設定を誤ると壊滅的な損害を引き起こす可能性があります。

M365にはどのようなデータが存在していて、Umbrella Corpの露出はどのような状況ですか？



主要リスク管理指標：

203K
件の機密性の高いレコード

20K
組織全体に露出している機密性の高いレコードの数

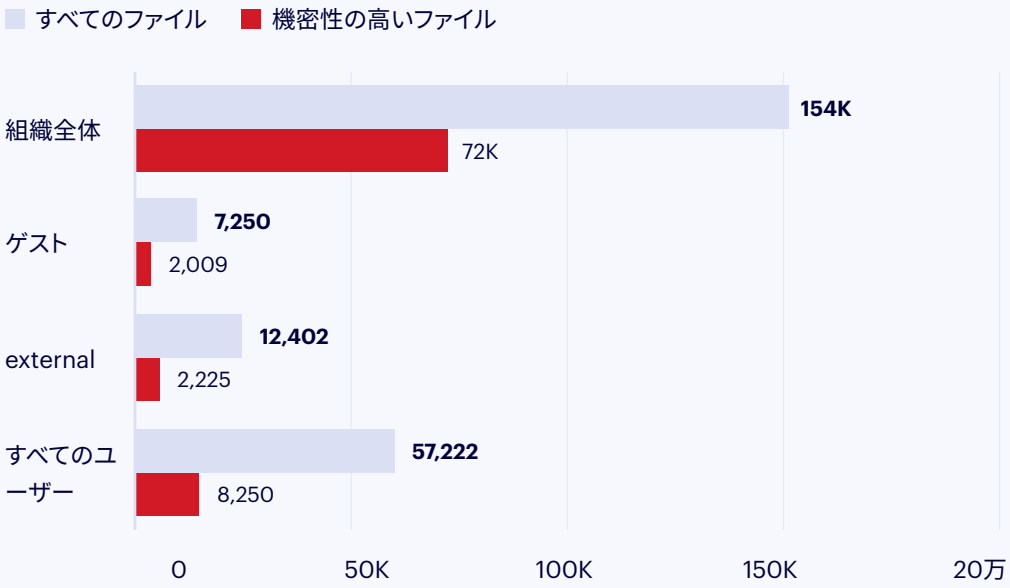
1.5K
外部に露出している機密性の高いレコードの数

コラボレーションのリスク

露出レベル

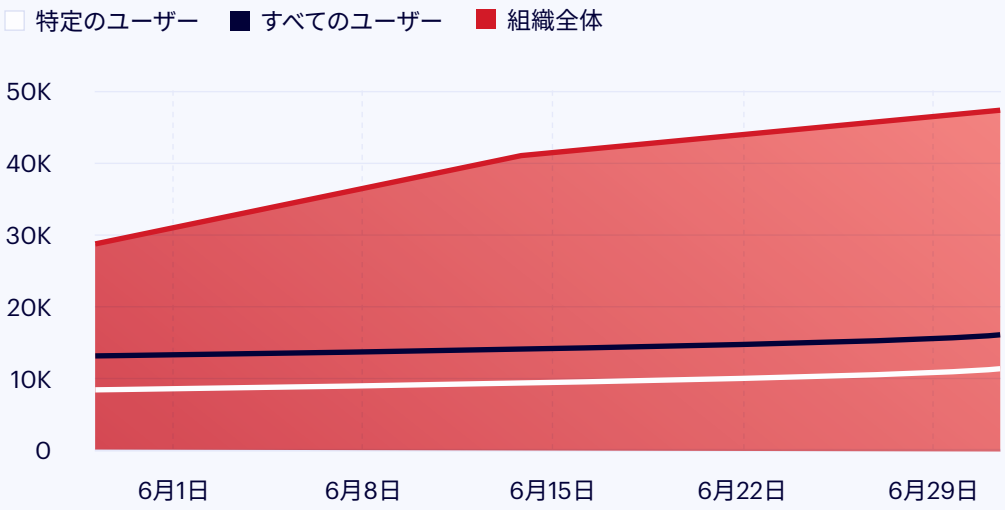
共有リンクはコラボレーションに役立ちますが、そのデータは組織内のすべてのユーザー、ゲストユーザー、インターネットに公開される可能性があります。Umbrella Corpでは、SharePointとOneDriveのリンクが原因で、大量の機密性の高いデータが露出しています。

SharePoint OnlineとOneDrive



共有リンクの増加

Umbrella Corpの爆発範囲は週を追うごとに急速に拡大しています。以下は、リスクアセスメント期間中のリンクの増加を種類別に示すグラフです。



一般公開露出しているデータ

「すべてのユーザー」リンクを介して一般公開露出しているデータ

以下は、インターネット上で誰でもアクセスできる機密性の高いファイルのごく一部です。Varonisの監査証跡では、ファイル内のデータの種類（PCI、PHIなど）、誰がいつリンクを共有したか、そのリンク経由でファイルにアクセスしたかどうかが示されています。

	File type	Name (resource)	Classification category	Total record
1		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
2		Employee Agreement.docx	*Financial (3)	21
		Employee Agreement.docx	*Financial (3)	21
		Employee Agreement.docx	*Financial (3)	21
		Employee Agreement.docx	*Financial (3)	21

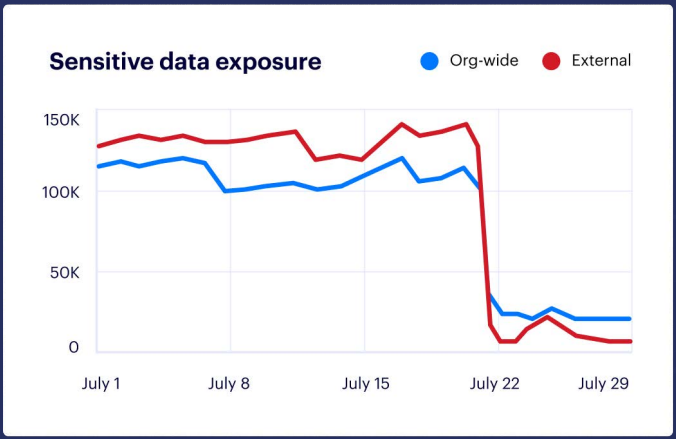
1 資格情報とクレジットカード情報を含むスプレッドシート

2 PIIと銀行口座情報を含む雇用契約

修正

共有リンクのリスクをどれくらい迅速に修正できるでしょうか？

Varonisの一般的なお客様は、自動化によって露出を迅速に解消することができます。以下は、最小特権の自動化を有効にした大手金融機関での結果です。最初の30日も掛からずに、外部および組織全体のデータ露出をほぼ100%解消しました。



自動化ポリシーによって、データの増大や継続的なコラボレーションに直面してもリスクを低く抑えられます。ポリシーを自動強制するように設定すると、新たなリスクは発生した時に修正され、最小権限が継続的に強制されます。

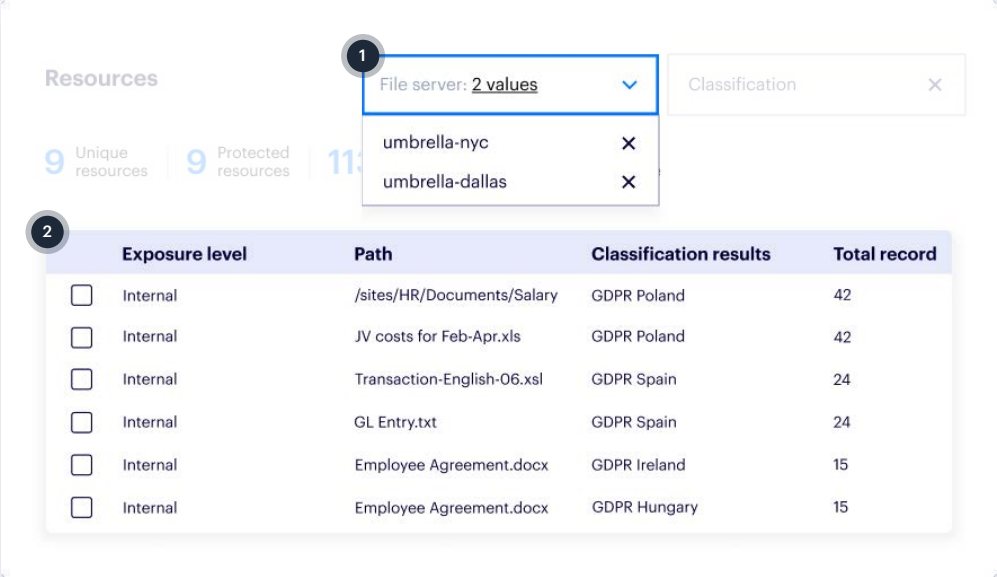
誤った場所に置かれたデータと誤ったラベル付けがされたデータ

誤った場所に置かれたデータ：GDPRコンプライアンスのリスク

Varonisは、米国でホストされているMicrosoft 365テナントでEU市民のPIIレコードを発見しました。ファイルは7月15日に「ExportJob」という名前のサービスアカウントによってアップロードされ、自動化されたWorkatoタスクに接続されているようです。このデータをUmbrella CorpのEU拠点のテナントに移行し、この自動タスクの設定を修正することをお勧めします。

1 米国ベースのM365テナント

2 EU市民のPIIを含むファイル



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

ラベルが間違っているファイル：DLP強制のギャップ

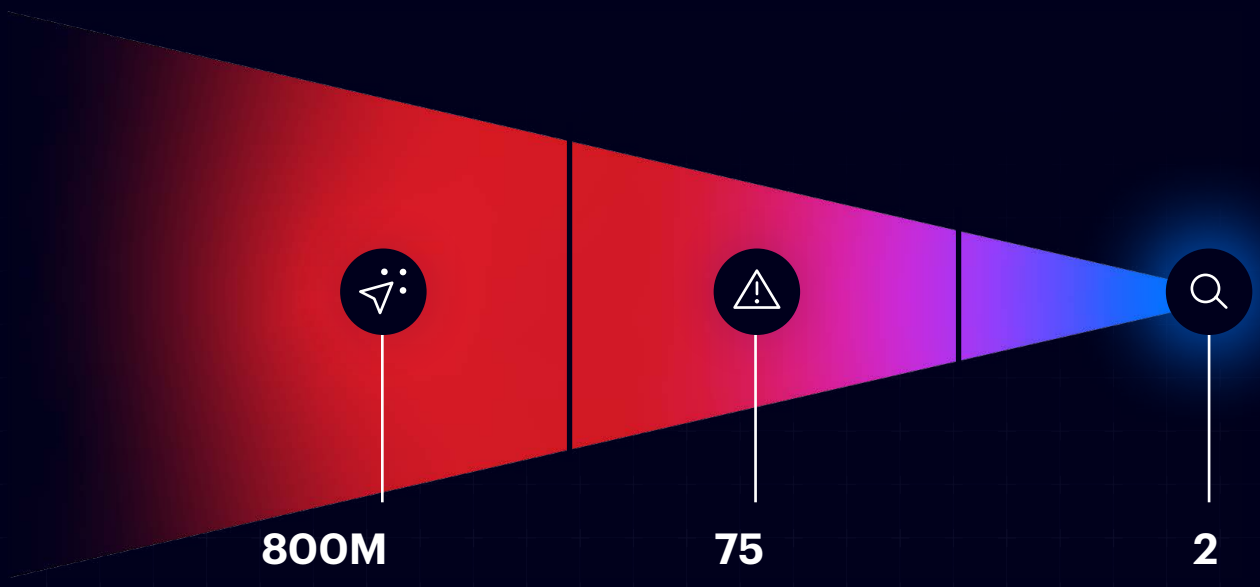
多くのファイルでMIPラベルが無かったり、古い、誤ったラベルが適用されています。その結果、下流でのDLP強制が失敗する可能性があり、機密性の高いデータが漏洩したり、その反対に— ユーザーが誤って適用したラベルが貼られた機密性の低いデータの共有がブロックされる可能性があります。

ラベルが適用されていない27,000以上の機密性の高いファイルが見つかりました。

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

脅威の検出と脅威への対応

Varonisのリアルタイム監視と振る舞いベースの脅威検出は、対象システム全体で有効化されました。アセスメント期間を通じて、VaronisのAIモデルは8億件以上のイベントで訓練され、Umbrella Corp社の環境におけるユーザーやデバイス固有の振る舞いを学習しました。



800M

何億件ものイベントを収集

各イベントは自動的に強化され、正規化されます。

75

数十件のアラートがトリガーされました

1 日あたり平均約3件

2

いくつかの調査対象となったインシデント

Varonisの積極的なIRが発見し、エスカレーションしたインシデントは2件でした。

データ中心のUEBA

イベントは、データ、ユーザー、デバイスの文脈で強化されます。セキュリティ分析担当者は次のようなクエリーを実行できます：「ドイツから接続されたデバイスで特権アカウントによって行われた機密性の高いデータのアクセスイベントをすべてリスト化せよ。」

アカウントの識別

IPアドレスからデバイスへの解決

実行者	アカウント種別	オブジェクト	機密性が高い?	デバイスのIP アドレス	デバイス名	外部IP アドレス	地理位置情報
Amy Johnson	Executive	Customer.xlsx	はい	173.17.33.3	aj-03154	54.239.13.2	カナダ

ファイルの機密性

地理位置情報

脅威分析

インシデントレポート：侵害されたサービスアカウント

所見：
VaronisのIRチームは、バックアップサービスのアカウントが侵害され、ユーザーデータにアクセスし始めたことを発見しました。

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 assessed 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.

軽減策：
Varonis IRは、数分以内にインシデントをトリアージし、修正しました。UC\BackupServiceアカウントを直ちに無効化し、アクティブなセッションを強制終了し、パスワードをリセットしました。Varonisは、根本原因の分析と推奨事項を含む完全な調査報告書をUmbrella Corpのチームに提供しました。

ドリルダウン：
142個のファイルが侵害されたアカウントによってアクセスされました。そのうち82個のファイルは、Varonisによって機密ファイルとして分類されていました。

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...

構成リスク

Varonisは、Umbrella CorpのSaaSおよびIaaSプラットフォームのシステム構成を継続的にスキャンして、リスクの高い設定がないか、または本来あるべき状態から逸脱した構成がないかどうかを判断しています。

21件の設定不備を発見

Salesforceの設定不備が最も多い (8件)。

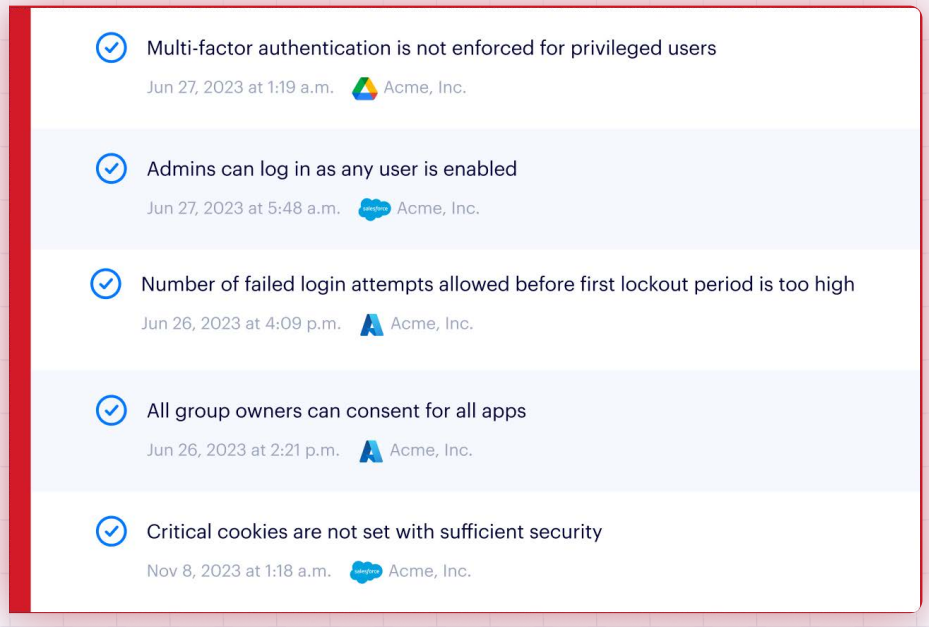
5件の重大度の高い設定不備

Microsoft 365とSalesforceには、それぞれ2件の致命的な設定不備があります。

4つの設定を自動強制に設定

Varonisは、安全な設定を自動的に強制することができます。

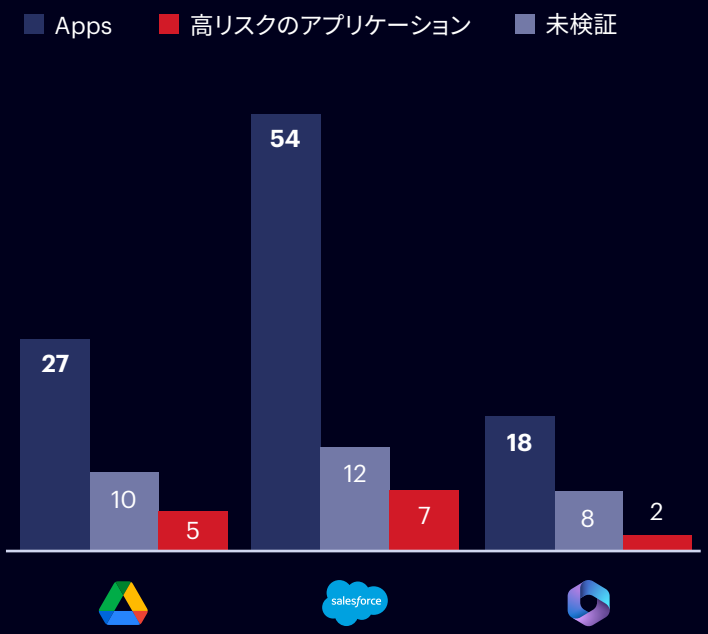
以下は、アセスメントで発見された**重大性の高い5つの設定不備**の概要です。それぞれの詳細と推奨事項は、Varonis UIでご覧いただけます。



こちらをクリックすると、Varonisで監視可能なSaaSおよびIaaS構成のサンプルをご覧いただけます。

サードパーティ製アプリケーションのリスク

36個のサードパーティ製アプリケーションが、リスクが高い、使用されていない、または未検証であることを特定しました。



99
インストールされているサードパーティ製アプリケーションの数

14
広範なデータアクセス権を持つ高リスクなもの

22
非アクティブなアプリケーションの数

以下は、Varonisが監視しているSaaSプラットフォームと統合されているサードパーティ製アプリケーションのユーザー数別の上位4つの内訳です：

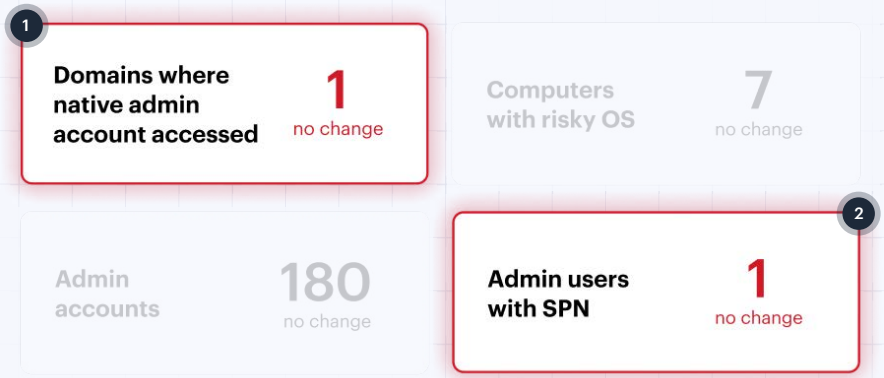
Google	Salesforce	Microsoft 365
miro	6sense	
dialpad	HubSpot	slack
Signeasy	INCENT	Trello
SUPERMETRICS	Power BI	Evernote

加えて、Varonis UIから直接アプリケーションの割り当てを取り消すことができる111人の非アクティブユーザーを発見しました。

IDリスク

Active Directoryのセキュリティ態勢

Varonisは、Umbrella Corpのクラウドとオンプレミスのディレクトリサービスをスキャンし、攻撃者に経路を提供する可能性のある脆弱な構成を検出します。これらのリスクはVaronisのダッシュボードでリアルタイムに更新され、ADのセキュリティ強化作業の優先順位付けに役立ちます。

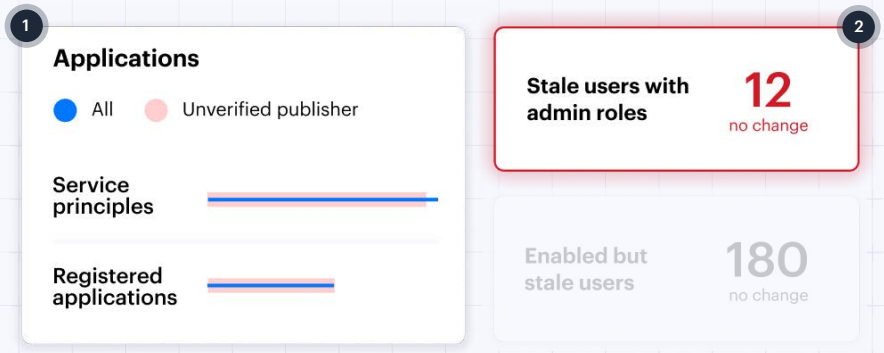


1 このアカウントが通常の状況で使用されることは滅多にありません。これは侵害を示している可能性があります。

2 オフィスのパスワードクラッキングに対して脆弱

Entra ID（Azure AD）のセキュリティ態勢

Entra IDの態勢は、Varonisによって継続的に監視され、採点されます。データを危険に晒すリスクの高い設定ミスは、リスクダッシュボードとレポートに表示されます。



1 未検証のアプリケーションの権限とデータアクセスを確認します。

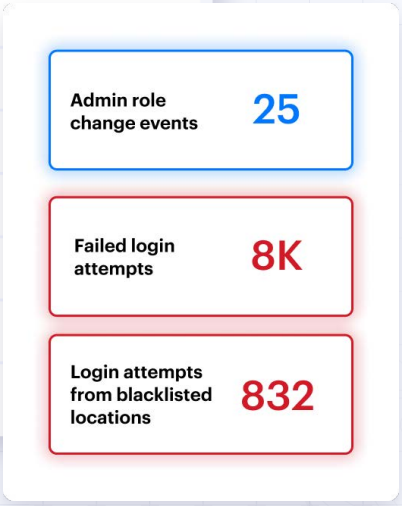
2 これらのアカウントは直ちに無効化すべきです。

Active Directory監視

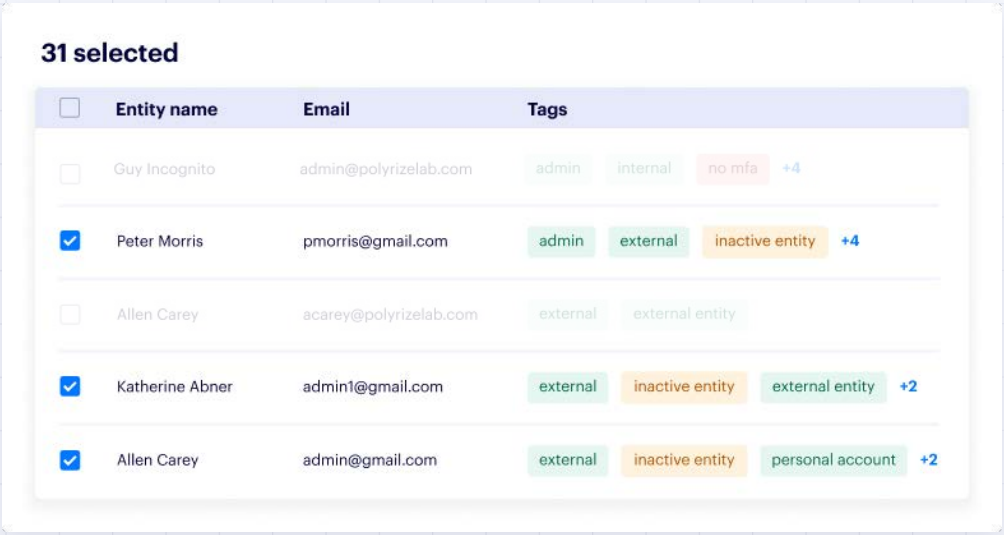
Varonisは、Umbrella Corpのディレクトリサービスのイベントを監視し、それらのアクションをコラボレーションプラットフォームやデータストアから収集したデータ中心のイベントと関連付けています。

これらの変更は、変更作業時間外に行われました。

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	



リスクの高い外部ユーザーと個人アカウント



古いGmailユーザーアカウントが、機密性の高いデータへのアクセス権を持っています。

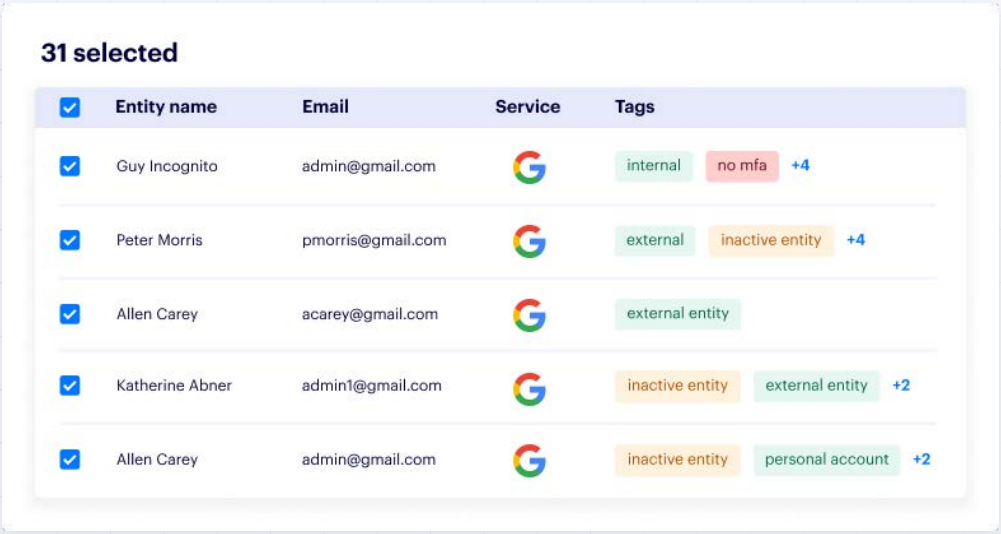
関連するIDのマッピング

Varonisは、独自のアルゴリズムを使用して関連するアカウントを自動的に識別します。Guy IncognitoはGoogle Workspaceの管理者ユーザーで、MFAを設定していない個人のGmailアカウントを使用しています。彼は、Umbrella Corpの環境全体で複数のIDに接続されています。

Guyはいくつかのエイリアスを持っています — 企業アカウントと個人アカウントを混在しています。

離職対応の漏れ：非アクティブなアカウント

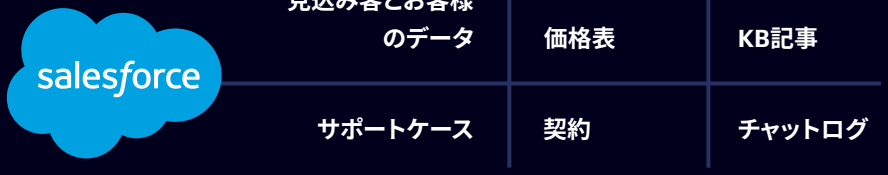
Varonisは、Umbrella Corpのディレクトリサービスとローカルアカウントリポジトリ全体で3,000以上の古いIDを発見しました。



契約が終了した契約社員が個人のGoogleアカウントからのアクセス権を保持しています。

SALESFORCEのリスク

Salesforceには組織の最も貴重なデータが格納されていますが、その複雑なアクセス許可構造と、誰がアクセスできるかについての可視性が欠如していることから、データが内部者脅威にサイバー脅威のリスクに晒されています。

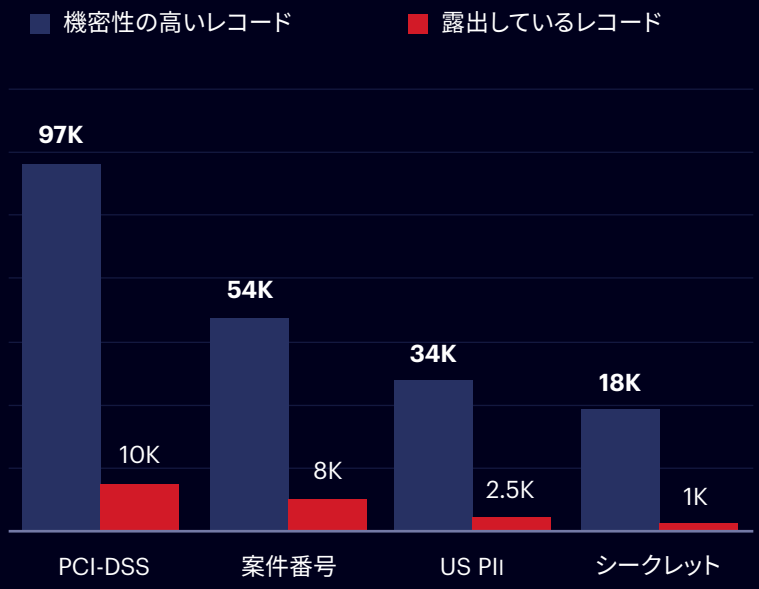


アセスメントのスコープ

環境	• Production • サンドボックス	• 開発
データ	• 234,240件のレコード • 8,241件のドキュメント • 520個ののフィールド • 9,214件の機密性の高いリソース	• 203件の外部/一般公開共有レコード • 22個の監視対象のサードパーティ製アプリケーション
IDの数	• 2,012人の内部ユーザー • 425人のの外部ユーザー • 124人の契約社員	• 212人のゲストユーザー • 55人の特権管理者
エンタイトルメント	• 89のプロファイル • 52の特権プロファイル • 22のコミュニティプロファイル • 3つのゲストプロファイル	• 55個の権限セット • 27個の権限セットグループ • 33のロール
上位3つの外部ドメイン	Gmail.com	Hotmail.com Proton Mail Protonmail.com

SALESFORCEのデータの漏洩

Salesforceにはどのようなデータが存在していて、その露出はどのような状況ですか？



203K
少なくとも１つの機密レコードを含むオブジェクトの数

1.5K
外部に露出している機密性の高いレコードの数

20K
組織全体に露出している機密性の高いレコードの数

Umbrella Corpのデータ持ち出しリスク

高い特権と見做す必要があるエンタイトルメントがいくつかありますので、以下でご説明します。これらのエンタイトルメントの付与対象ユーザーが多過ぎると、重大なデータの露出や持ち出しのリスクが生じる可能性があります。

235のエンタイトルメントで[レポートのエクスポート] が有効

[レポートのエクスポート] を使用すると、ユーザーはSalesforceから直接データをエクスポートできます。
必要であれば、権限セットに適用すべきです。

124のエンタイトルメントで[すべてのデータの参照] または [すべてのデータを変更] が有効

この権限を持つユーザーは、組織内のすべてのデータを表示および変更できます。

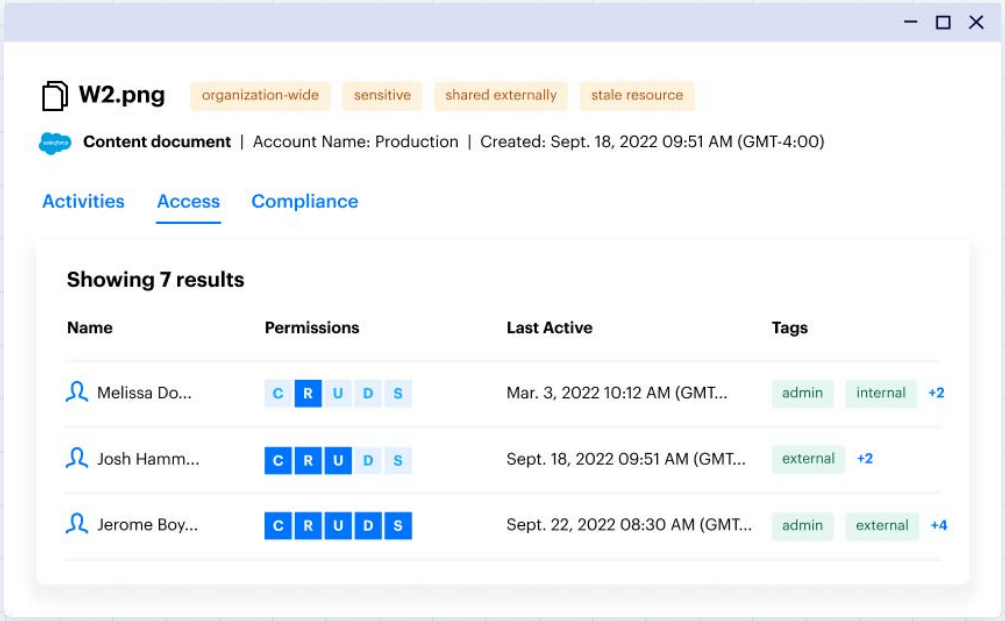
52のエンタイトルメントでAPIが有効

この権限を持つユーザーは、すべてのSalesforce APIと通信したり、データを持ち出したり、その他のアクションを実行できます。

Varonisは、重要なエンタイトルメントのリアルタイムビューと、アクセス権を迅速に適正化する能力と、最小権限の強制機能をUmbrella Corpに提供します。また、特権エンタイトルメントが変更されるとトリガーされるVaronisアラートを設定することを推奨します。

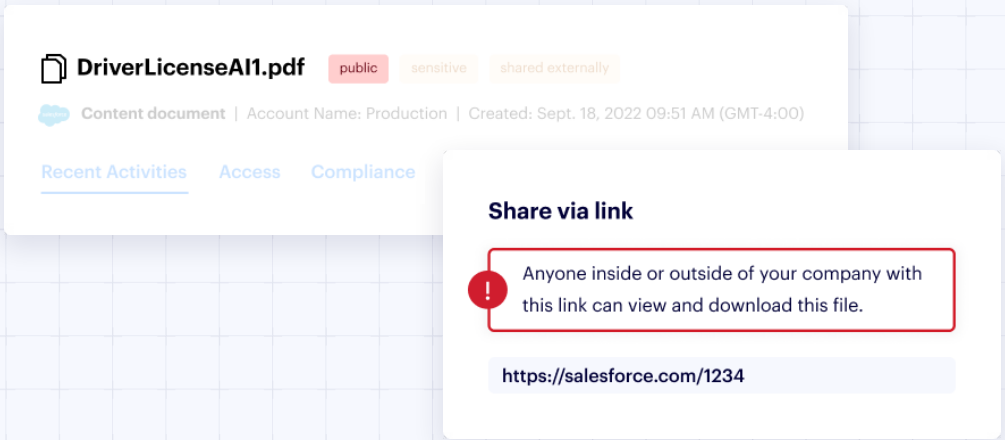
外部と共有されている機密性の高いデータ

Umbrella CorpのSalesforceインスタンスでは、ゲストユーザーのアクセスが許可されています。サードパーティ製アプリケーションのサービスアカウントとして機能するユーザーアカウントもいくつかあります。Varonisは、下記のW2添付ファイルなど、外部に露出している機密性の高いレコードを1,500件以上、検出しました。



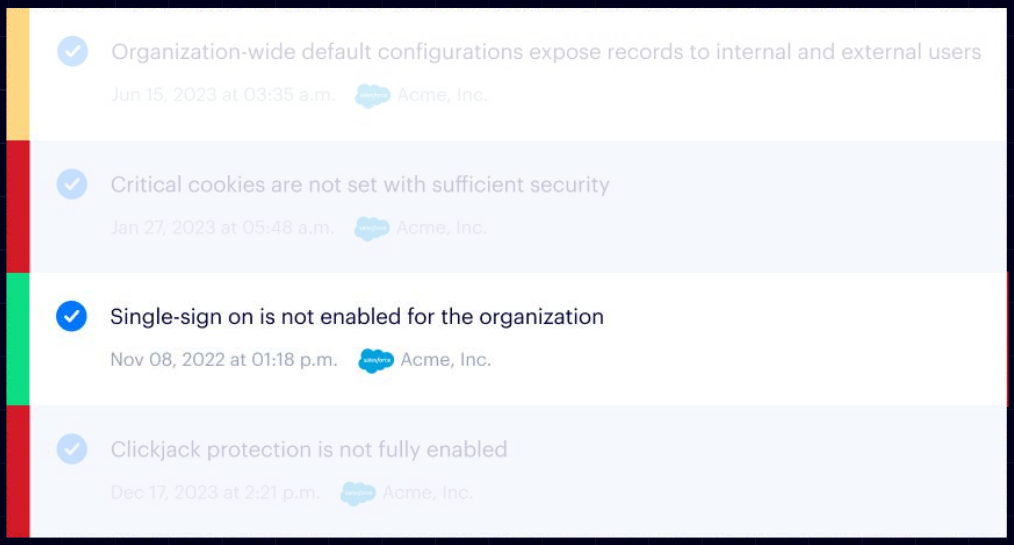
社外のユーザーが、SalesforceインスタンスのPCIデータとPIIデータをアクセス、更新、削除できてしまいます。

ゲストユーザー、契約社員、その他認証された第三者にデータが露出していることに加え、今回のアセスメントでは一般公開リンクを通じてインターネットに露出しているデータがあることも明らかになりました。



SALESFORCEの設定不備

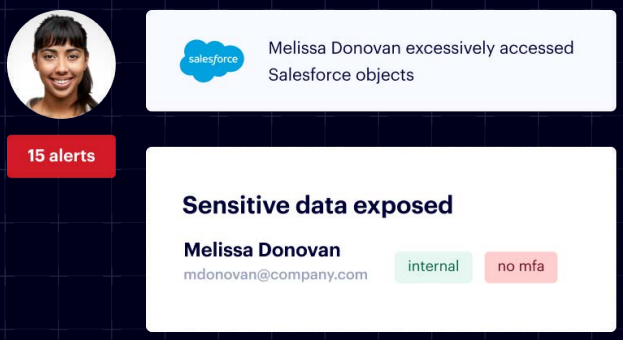
Varonisは、攻撃経路となり得る4つの設定不備や、安全でない組織全体のデフォルト設定を検出して修正しました。



Oktaアカウントがプロビジョニング解除されていたにも拘らず、契約が終了した契約社員がサンドボックス環境のアカウントにアクセスしていました。

Salesforceのアラート

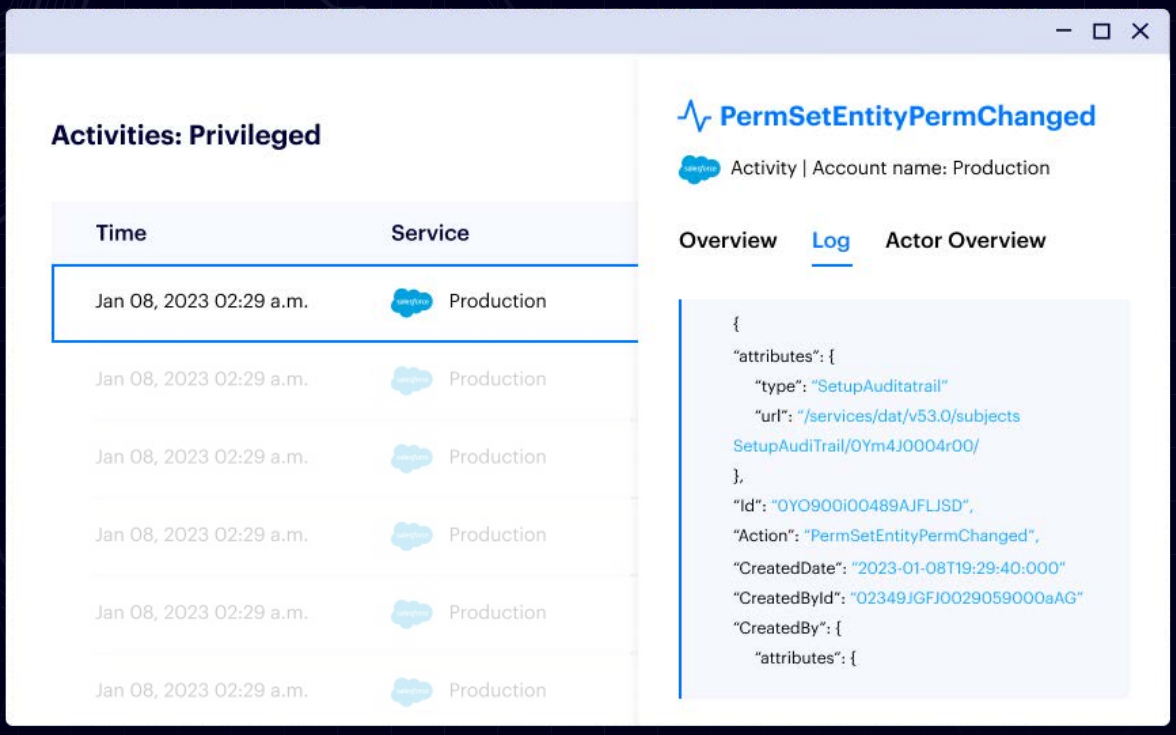
内部者のMelissa Donovanが振る舞いのベースラインと比較して異常な数のレコードにアクセスしていたケースを含め、15件のアラートがトリガーされ、Varonis IRにより解決されました。調査の結果、MelissaがSalesforceレコードのURLに高速でアクセスするブラウザ拡張機能をインストールしていたことが判明しました。



Melissa Donovanは普段のアクティビティから逸脱していました — 普段は触れないレコードにアクセスしていました。

管理者の変更の監視

Josh Hammondは、変更作業時間外に、本番環境に対して管理者による変更をいくつか加えました。以下に詳細な変更ログを示します。

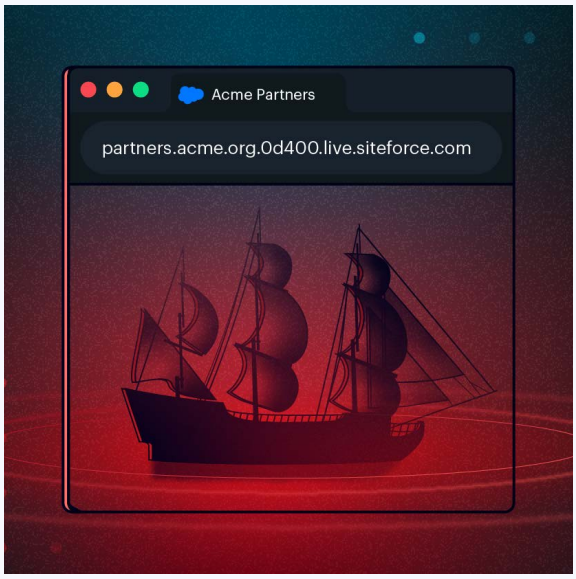


VARONIS
THREAT LABS

SALESFORCEの調査

Varonisのチームは、Salesforceの脆弱性や有害な設定を探し出し、公開しています。

ゴーストサイト：非アクティブ化されたSalesコミュニティからデータを盗む



アインシュタインのワームホール：SalesforceゲストユーザーによるOutlookとGoogleカレンダーの取得バグ

Varonis Threat Labsについて

セキュリティ研究者とデータサイエンティストで構成されるVaronisのチームは、世界で最も優れたサイバーセキュリティ人材を集めたグループです。軍隊、諜報機関、企業で何十年もの経験を持つVaronis Threat Labsチームは、お客様が使用するアプリケーションの脆弱性を積極的に探し、攻撃者が発見する前に隙間を見つけて対処します。これらの学習はすべてVaronisのプラットフォームにプログラムされており、サイバー攻撃への先手を打つのに役立ちます。

最新の調査をご覧ください：**www.varonis.com/blog/tag/threat-research**

リスクを取らずにリスクを軽減しましょう。

Varonisの無償のリスクアセスメントは数分で設定でき、すぐに価値をもたらします。24時間以内に、最も重要なデータを明確にリスクベースで把握し、修正の自動化のための明確な道筋を把握できます。

Varonis SaaSプラットフォームのすべての機能にアクセス

アセスメント期間中、Varonis Data Security Platformのすべての機能にアクセスして、最も重要なデータに関する対応可能な洞察を得ましょう。

専任のIR分析担当者

Varonis SaaS Data Security Platformに接続するということは、Varonisの専門家がアラートに目を光らせ、危険に気付き次第、お客様に通知するということです。

調査結果概要レポート

データセキュリティリスクの詳細な概要と、調査結果および推奨事項をレビューするためのエグゼクティブプレゼンテーション。
このレポートは、Varonisを購入しなくてもお客様のお手元に残ります。

無償のアセスメントを受ける

何千社ものお客様が信頼

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

FORRESTER LEADER

Varonisはデータセキュリティプラットフォームのリーダーに選出されました。

「Varonisは、データに対する深い可視性、分類機能、データに対する自動的な修正を優先したい組織にとって最良の選択肢です。」

Forrester Wave™: データセキュリティプラットフォーム、2023年第1四半期

FORRESTER LEADER

0 10 20 30 40 50 60 70

VARONIS