Rubrik Zero Labs

データセキュリティの現状

データ分散の危機

概要：

忍び寄る危機からの脱出

企業のIT環境がオンプレミスのみの状態からオンプレミス/クラウドの
ハイブリッド環境へと移行したことは、ビジネスにおけるコンピュータ活用の
歴史において、最も重要な出来事の1つです。

拡張性と柔軟性が増し、イノベーションを実現できる機会が増えました。

多くの場合、企業ワークフローや企業間協力にとって不可欠になっています。

当然のこととして

90%

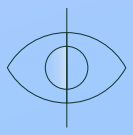
のITリーダーがハイブリッド環境に分散する
データを管理していると回答しています。

しかし、RubrikのテレメトリーとWakefield Researchによる次のデータが示すとおり、
ハイブリッド環境には、これまでになかった危険も生じています。

ITリーダーはシステム全体のデータの安全確保が難しく、全体的な可視性に欠け、一元的な管理を確立できないと回答しています。

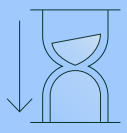
調査の回答者の90%がサイバー攻撃を受けたことがあると回答しています。ほぼ5人に1人が平均して2週間に1回の頻度で攻撃を受けていると回答しています。これは、攻撃を受けた側が把握している事案にすぎません。

悪意のある攻撃者はこのことを把握しており、ハイブリッドクラウドシステムの弱点を容赦なく利用して攻撃を行っています。



脅威アクターの手口がマルウェアから、ソーシャルエンジニアリングやアイデンティティを悪用した戦略へと変わりつつあります。アイデンティティ攻撃は、今や全攻撃の80%近くを占めている可能性があります。

攻撃者の侵入経路は10以上と、以前と比べてはるかに多くなっています。



理由は、その成功率の高さです。攻撃の成功率は上昇傾向にあり、侵入から機密データを支配下に置くまでの時間は急激に短縮してきています。

その結果

86%

の調査対象企業が、恐喝を受け身代金を支払ったと報告しています。

ほぼ4人に3人が、攻撃者は不正アクセスにより
データを侵害できたと回答しています。

このような危険は危機的状況になりつつありますが、誰もこれについて語ろうとしません

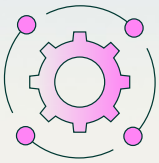
その理由は、おそらく、ほぼ誰も良い対策が思い付かないからでしょう。徐々にクラウドへの移行が進むなか、問題の解決はクラウドプロバイダー任せとなります。あるいは、単純に問題の解決は無視され、代わりにビジネスの代償と呼ばれることになります。

対策はあります。

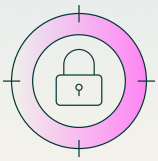
企業がすべきことは

攻撃者の視点で考えることです

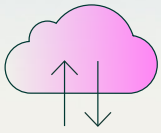
脅威アクターは事業を中断させるために、最重要データを探してコントロールしようと考えています。攻撃者にできるのなら、企業にもできて然るべきです。



まず、状況を把握しコントロールの回復に焦点を置きます。次いで、機密データの優先順位付けと継続的な運用を行えるよう保護、防御、復旧の計画を立てます。



機密データは特定して、個人情報、金融情報、技術情報などのカテゴリに分類することができます。脅威アクターより先に状況を明言してコントロールを確立し、標的を特定します。



継続的なバックアップと復元のプロセスがセキュリティプロセスの一部となるようにします。クラウドでもオンプレミスと同様に厳格に適用されるようにします。

データと調査手法

Rubrik Zero Labsは、組織でのデータセキュリティリスクの低減に役立つよう、実用的で偏りのないインテリジェンスの提供に取り組んでいます。この目的を達成するため、Rubrikでは3つの主要ソースからの情報を利用しています。

01

RUBRIKテレメトリー

標準的な組織のデータ環境と関連するリスクについての分析情報を取得するため、Rubrikのテレメトリーを採用しました

02

WAKEFIELD RESEARCH

Wakefield Researchを通じて得た1,600人以上のIT/セキュリティチームのリーダーによる視点を提供しています

03

組織に貢献

定評あるサイバーセキュリティ企業および機関による調査結果を提供しています

RUBRIKテレメトリー

標準的な組織のデータ環境と関連するリスクについての分析情報を取得するため、Rubrikのテレメトリーを採用しました

基になったソースは次の2つです。

バックアップデータ

お客様の環境からバックアップしているクラウド、SaaS、オンプレミスのデータです。

本番データ

Rubrikが積極的に監視しているクラウド、SaaS、本番のデータで、組織はこれに基づいて環境内でのリスク管理の方法を決定することができます。

保護されているクラウドファイルの数

データの対象期間：2024年1月1日～2024年12月31日

5.8 BILLION

クラウドとSaaSの本番環境全体でのファイルの総数

175+ MILLION

管理対象のクラウドおよびSaaS環境全体での
機密ファイルの数

WAKEFIELD RESEARCH

1,600人以上

IT/セキュリティのリーダー

10

か国

50%超

CIOまたはCISO

50%

CIOまたはCISO

1,625

10カ国に500人以上の従業員を抱える企業を調査対象としています（オーストラリア、フランス、ドイツ、インド、イタリア、日本、オランダ、シンガポール、英国、米国など、北米、南米、アジア太平洋、ヨーロッパ、中東、アフリカの各地域に及ぶ）

50%

ディレクターまたはVP

組織に貢献

より包括的で公平な視点が得られるように、Rubrikでは独自の視点を提供する多様な組織からの重要な情報も取り入れています。

使用した情報

CROWDSTRIKE

CrowdStrikeの侵入とブレイクアウトタイムに関するクラウドおよびアイデンティティベースの分析

Microsoft

Microsoftによるアイデンティティベースの分析と攻撃の頻度に関するデータ

Allied Market Research®

Allied Market Researchによるクラウド導入に関する情報

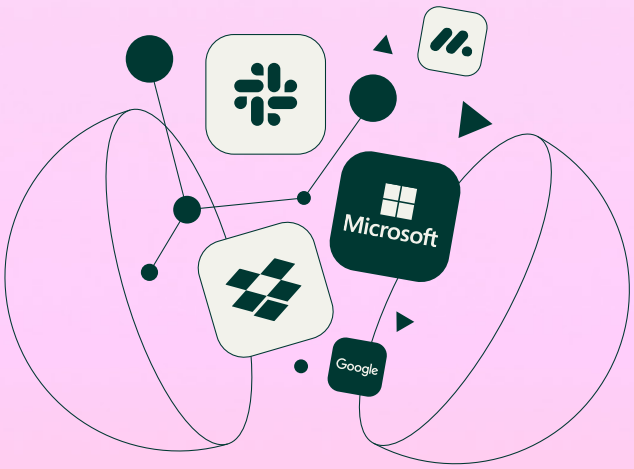
クラウド時代のデータスプロール

データを特定して保護することは、コンピュータがネットワーク化された当初からの課題でした。

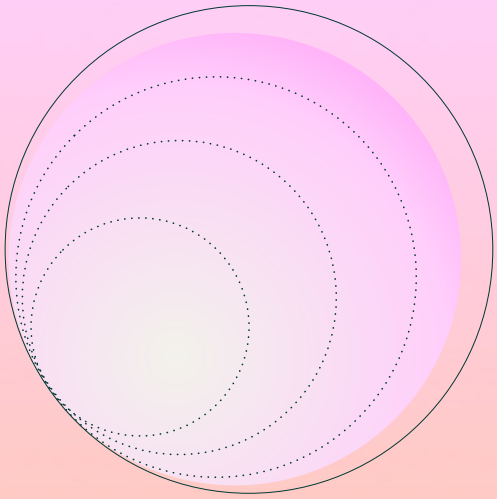
以前は、データは企業のデータセンターか社用コンピューターに存在し、デスクトップが主流だった時代から、やがてデスクトップとノートパソコンへと移り変わりましたが、単一のネットワークに接続されていました。現在では、データはさまざまな種類のデバイスに無秩序に広がっています。企業の貴重なデータにアクセスするのに多くのネットワークを使用しており、そのデータの場所も現在は、オンプレミスとクラウドになっています。

ある時点で、規模と複雑さにおける変化により、ITの専門家たちは新たな世界に踏み込むことになりました。

この20～30年間、企業はクラウドおよびSaaSサービスを利用することで得られるメリットを求めてきました。
それにはもっともな理由があります。



クラウドにより私たちの暮らしは多くの面でより快適になりました。



89%

組織のクラウドおよびSaaSサービスの利用は増加し続けており、ハイブリッドおよびマルチクラウド戦略が標準になりつつあります。Allied Market Researchによると、組織の89%が複数のクラウドプラットフォームを利用しています。[1]

さらに、RUBRIKの調査結果では次のことが明らかになりました。

89%

ハイブリッドクラウド環境を管理していると回答したIT/セキュリティリーダーの割合。
（Wakefield）

50%

オンプレミスのワークロードよりも、主にクラウドおよびSaaSベースのワークロードを管理していると回答したIT/セキュリティリーダーの割合。
（Wakefield）

92%

データの保存、アプリケーション、サービスに対して2～5種類のクラウドおよびSaaSプラットフォームを使用していると回答した調査対象のIT/セキュリティリーダーの割合。
（Wakefield）

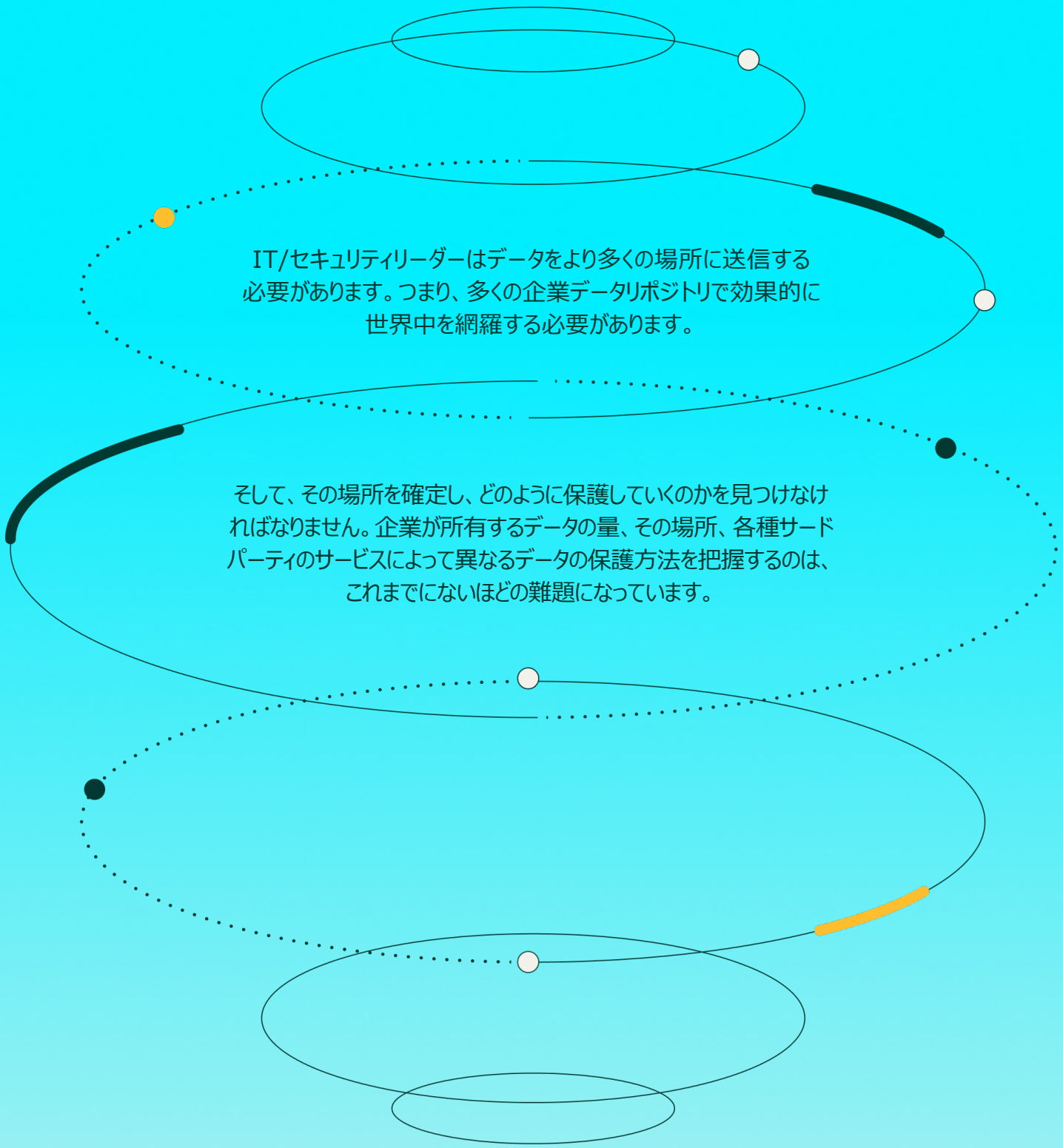
66%

1年以内にクラウドおよびSaaSベースのサービスの利用拡大を計画していると回答した調査対象のIT/セキュリティリーダーの割合。これに対し、31%はハイブリッドクラウド環境とオンプレミス環境の比率を維持する予定。
（Wakefield）

*https://www.alliedmarketresearch.com/cloud-native-applications-market-A210373

クラウド時代のデータの複雑性

新しいクラウドとSaaSのユースケースではどれも、
データ管理の制御性に若干の問題が生じています。

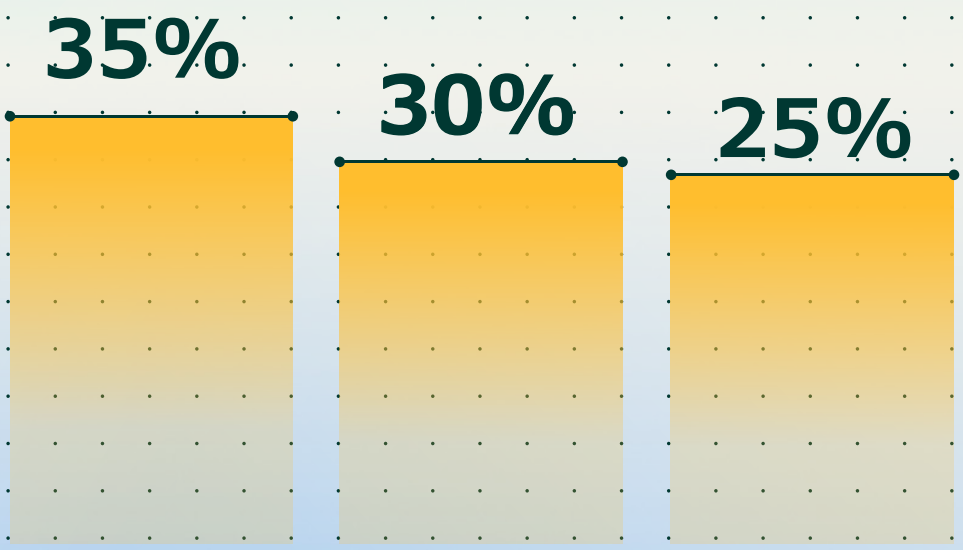


IT/セキュリティリーダーはデータをより多くの場所に送信する必要があります。つまり、多くの企業データリポジトリで効果的に世界中を網羅する必要があります。

そして、その場所を確定し、どのように保護していくのかを見つけなければなりません。企業が所有するデータの量、その場所、各種サードパーティのサービスによって異なるデータの保護方法を把握するのは、これまでにないほどの難題になっています。

ITリーダーが捉えている課題は主に次の3つのカテゴリに分けられます。

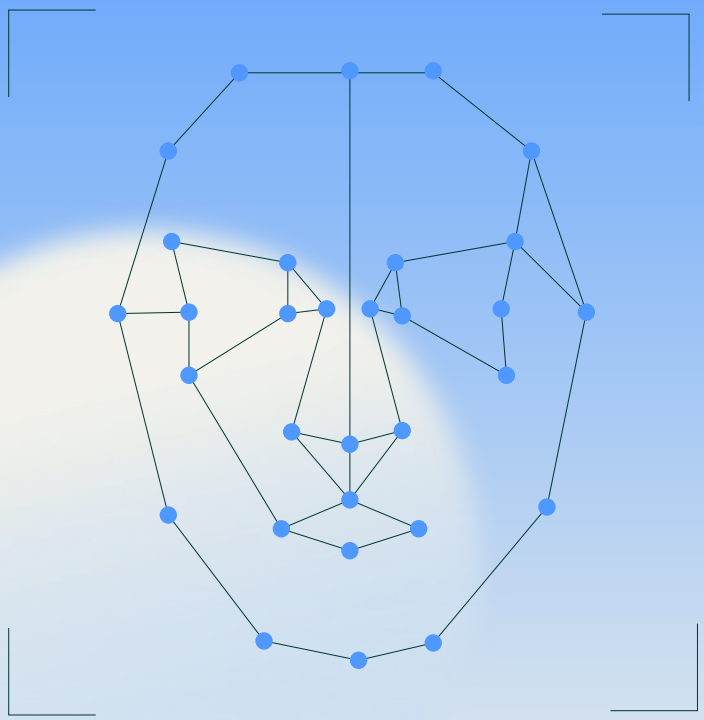
（Wakefield）

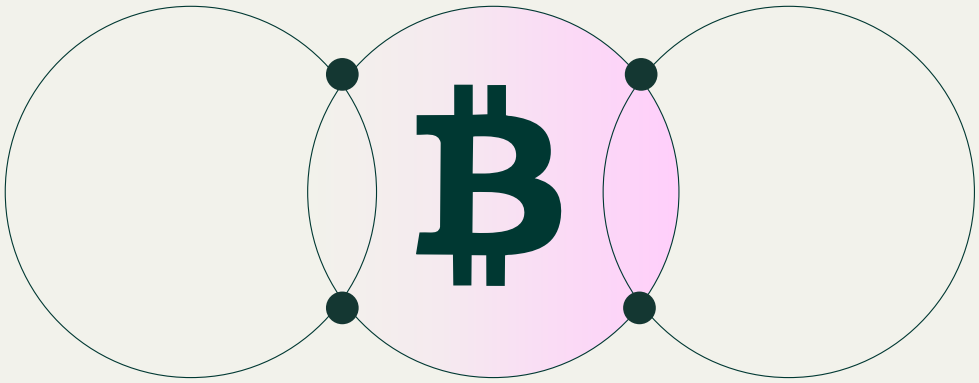


1. 複数の環境に存在する機密データの保護
2. 一元管理ができない
3. クラウドベースのデータに対する可視性がなく制御が困難

脅威アクターは時代とともに変化する

今日の攻撃者は目的意識を持ち、規律正しく、ビジネスのように正確な攻撃を行い、最新の企業環境の弱点を悪用しようと、その攻撃手法を絶えず適応させています。





多くの企業がクラウドインフラ、アイデンティティを利用したアクセス、分散型従業員という環境に移行したことで、必然的に脅威アクターもその作戦を実施し拡大するための新たな手法を模索することになりました。

脅威アクターは進化しており、正当な認証情報の悪用、ハンズオンキーボード攻撃、ソーシャルエンジニアリングなどの手法が多くなり、従来のマルウェアによる攻撃をまったく用いない傾向にあります。その手法にはイノベーション、業務効率、技術的スキルを重視する起業家的マインドセットが反映されています。

CrowdStrikeの『2025年版グローバル脅威レポート』
によると、「2024年、新規および原因不明の

クラウド侵入は前年と比較して

26%

増加しており、クラウドサービスを標的とする攻撃者が増えていることを示しています。CrowdStrikeの調査により、攻撃者が正当なアカウントによって最初のアクセスを行い、クラウド環境の管理ツールを活用して横展開を行い、クラウドプロバイダーのコマンドラインツールを悪用する攻撃が増加していることが明らかになっています」[1]

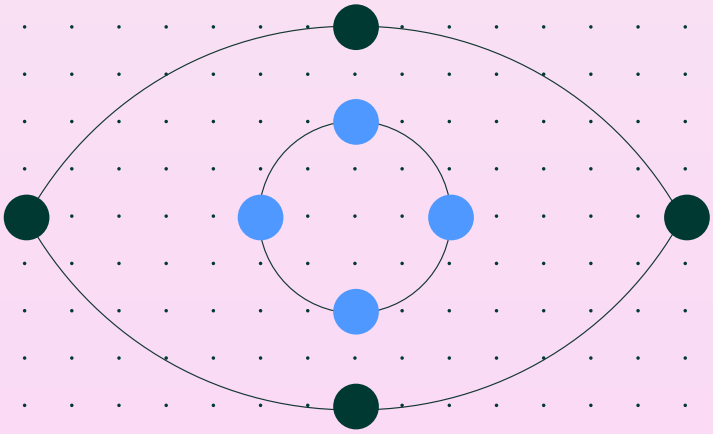
（CrowdStrike）

「2024年、アクセスブローカーの活動は急増しており、宣伝されたアクセスは2023年と比較して約50%増加しています。同時に、正当なアカウントの悪用はクラウド関連インシデントの35%を占めていました。より多くの企業環境への侵入手段として、攻撃者がますますアイデンティティ侵害に重点を置くようになっていることが示されています」[1]

（CrowdStrike）

Microsoftは『Microsoft デジタル防衛レポート（MDDR）』でアイデンティティを悪用した膨大な件数の攻撃に言及し、1日あたり6億件を超えるアイデンティティベースの攻撃をブロックしていると述べています。[2]

（Microsoft）



「2024年は、検知された活動のうちマルウェアを使用していないものが79%を占め、2019年の40%から大幅に増加しています」[1]

（CrowdStrike）

最後に、この報告では、脅威アクターが最初に侵害したエリアから他のシステムに移動するまでにかかる時間（ブレイクアウトタイム）の短縮が急激に進んでいることも明らかにされています。

「サイバー犯罪（eCrime）の対話型侵入の2024年の平均ブレイクアウトタイムは、2023年の62分から48分にまで短縮されました。

驚くべきことに、ブレイクアウトタイムの
最速記録はわずか

00:51

— つまり、攻撃者が確固としたコントロールを確立する前に、防御側が検知して対応する時間は1分もないかもしれないということです」[1]

（CrowdStrike）

このような統計情報は、クラウドやSaaS環境にデータを所有している
すべての組織に対する警告です。

誰が持つ

データ

でも標的となる
可能性があります。

また、アイデンティティベースの攻撃の増加に伴い、侵入ではなく、ログインによる攻撃が行われるようになっています。これはどの環境においても検知と防止が非常に困難です。その最初の足掛かりによって、ITシステム間のすばやい移動も非常に容易になります。

このような状況が最前線に及ぼしている影響について、IT/セキュリティリーダーの声を次にご紹介します。

90%

昨年、自組織がサイバー攻撃を経験したと答えたIT/セキュリティリーダーの割合。

（Wakefield）

18%

この1年で、25回を超えるサイバー攻撃を受けたと答えたIT/セキュリティリーダーの割合。これは、平均して1週間おきに少なくとも1回の攻撃を受けていることになります。

（Wakefield）

86%

2024年にランサムウェア攻撃を受けたIT/セキュリティリーダーのうち、86%がデータの復元や攻撃の停止のために身代金を支払ったと回答しています。前年に比べて7%の低下となっています。

（Wakefield）

74%

ランサムウェア攻撃を受けたIT/セキュリティリーダーの割合。74%がバックアップおよび復元オプションへの脅威アクターによる侵害が少なくとも部分的に可能だったと回答しました。

（Wakefield）

35%

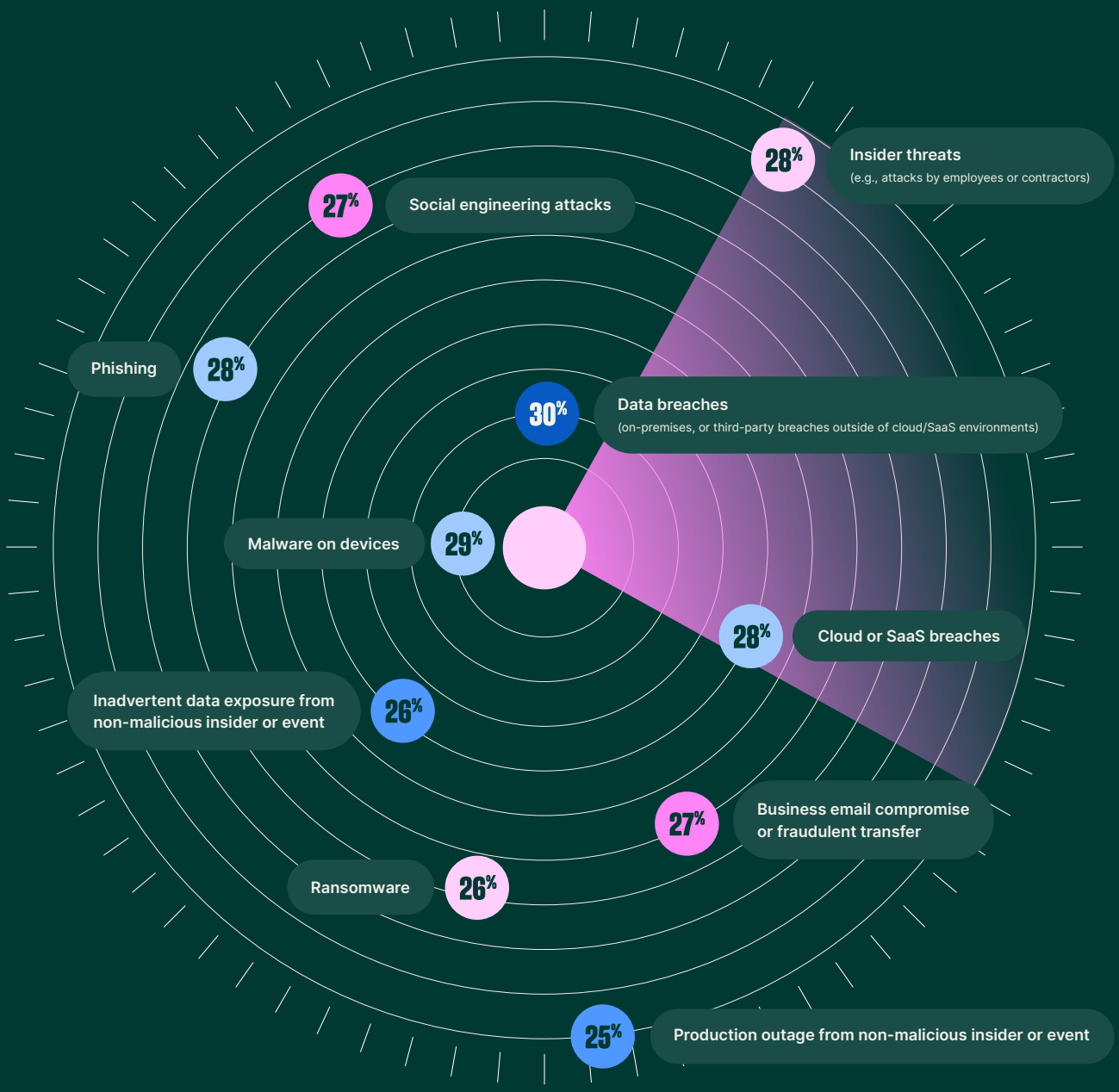
脅威アクターによりバックアップおよび復元オプションが全面的に損害を受けたという回答の割合。

（Wakefield）

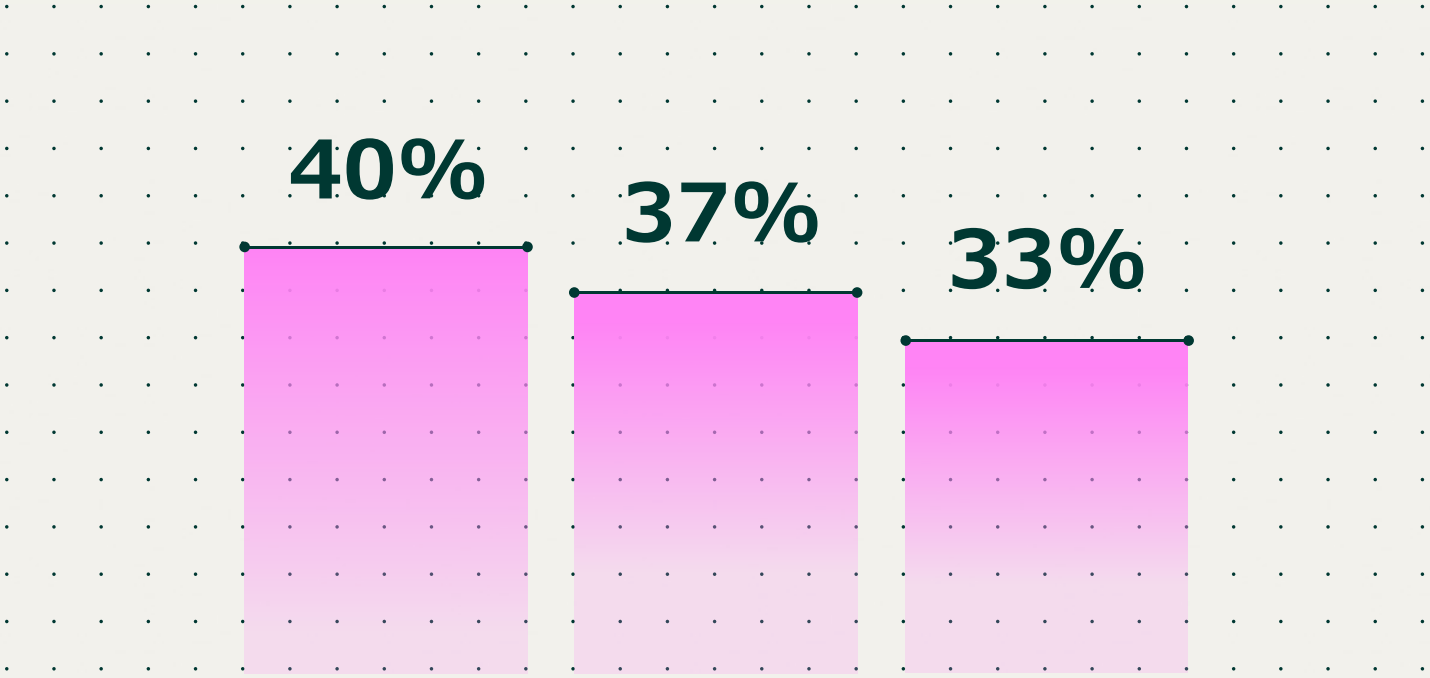
IT/セキュリティリーダーによると、彼らが経験した種類の
サイバー攻撃は、

あらゆる方向から来ている。

（Wakefield）



このような状況が最前線に及ぼしている影響について、IT/セキュリティリーダーの声を次にご紹介します。



1. セキュリティ対策を強化しコストが増加した
2. 会社の評判を損ない、顧客の信頼を失った
3. リーダーの交代を余儀なくされた

ただし全体として注目すべきは、その経験がセキュリティ対策強化とコストの増加から復元不可能なデータ損失まで、あらゆる範囲に及んでいることです。

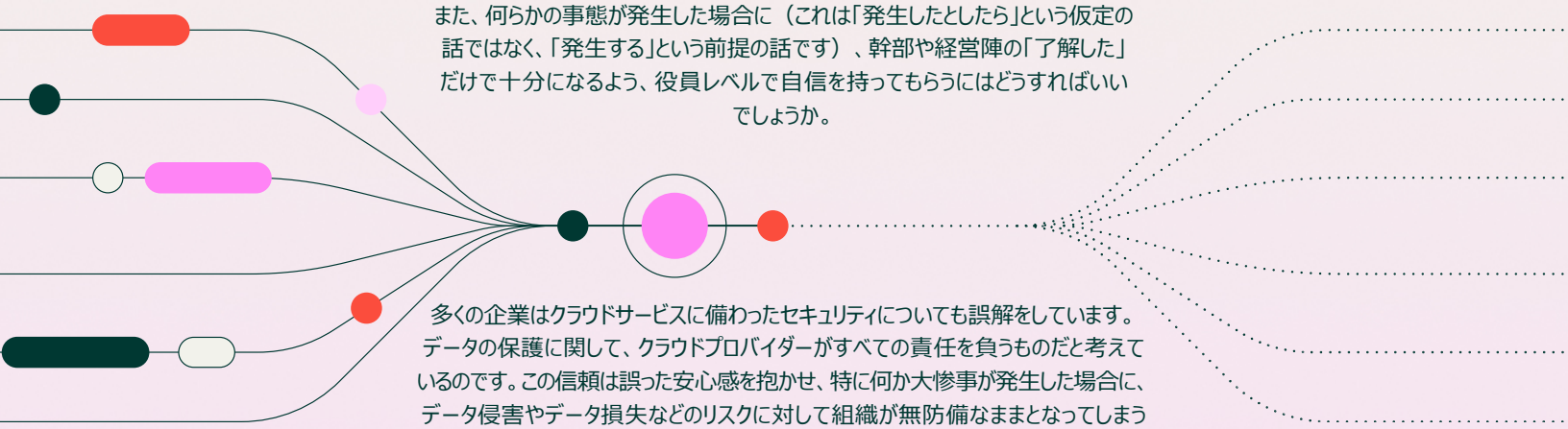
[1] CrowdStrike - 『2025年版グローバル脅威レポート』

[2] Microsoft - 『Microsoft デジタル防衛レポート』

混乱 から 自信へ 行動計画

新しく出現したこの複雑性と、それを受けて生じた新しい脅威を踏まえて、IT/セキュリティリーダーがデータセキュリティ対策に自信を持つにはどうすればいいでしょうか。

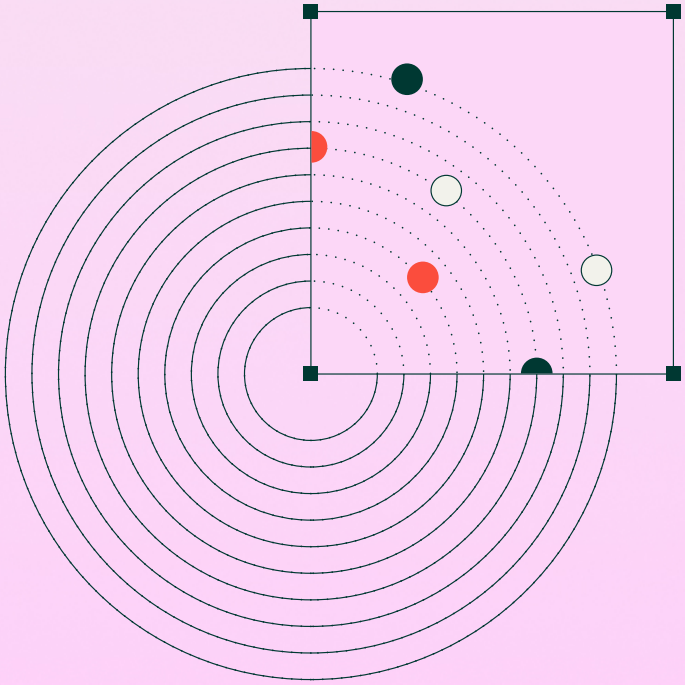
また、何らかの事態が発生した場合に（これは「発生したとしたら」という仮定の話ではなく、「発生する」という前提の話です）、幹部や経営陣の「了解した」だけで十分になるよう、役員レベルで自信を持ってもらうにはどうすればいいでしょうか。



多くの企業はクラウドサービスに備わったセキュリティについても誤解をしています。データの保護に関して、クラウドプロバイダーがすべての責任を負うものだと考えているのです。この信頼は誤った安心感を抱かせ、特に何か大惨事が発生した場合に、データ侵害やデータ損失などのリスクに対して組織が無防備なままとなってしまうおそれがあります。

クラウドの導入は現代のビジネス慣行の基本となっていますが、完全な移行には積極的ではない組織もあります。アプリケーションの依存関係の理解、オンプレミスとクラウドのコストの比較、技術的な実現可能性の評価などの課題が、多くの場合、移行の大きな障害となっています。

ゼロトラストセキュリティモデル



一方、ゼロトラストセキュリティモデルを取り入れようとしている組織もあります。このモデルでは場所に関係なく、どのユーザーやデバイスも本質的に信頼できないことが前提となっています。

このアプローチの場合、セキュリティは強化できますが、多大な労力を要するもので、組織内のすべてのデバイス、アプリケーション、ユーザーの評価を含む綿密な計画が必要となります。ゼロトラストモデルはその厳格な性質により文化的にも運用的にも大幅な変更が求められます。それによりコストが増加し、複雑さが増し、業務に混乱が生じます。そのため、ビジネスの速度を落とさずに実装することが難しくなっており、セキュリティと業務効率のいずれかを犠牲にすることが余儀なくされています。

別の方法があります。グローバルに分散したハイブリッドのデータの管理は、データの場所を把握することから始まります。企業が標的となりうる機密情報をできるだけ早く特定し保護できるよう、機密データの場所を突き止め、分類しておきます。

たとえば、本番データのRubrikテレメトリーによって、
お客様の機密の構造化データが次の環境にあることがわかっています。

[Rubrikテレメトリー - 本番データ]

DYNAMODB
35.51%

Amazon DynamoDB（**キーバリュードキュメントストア**）
- ソーシャルメディアのユーザープロファイル
- IoT/デバイスのセンサーデータまたはテレメトリー
- 製品カタログ（Eコマース）

リレーショナルデータベースサービス
6.81%

Amazon RDS（**Relational Database Service**）
- 人事部門の従業員データベース
- 受注管理（Eコマース）
- 医療分野における患者の記録

SNOWFLAKE
19.09%

Snowflakeはクラウド型のデータウェアハウスを提供しています
- 顧客データ（小売/Eコマース）
- 金融取引（銀行）
- 販売取引
- 分析の集約（総収益、顧客の生涯価値）
- セキュリティログ（SIEMの連携）

仮想マシン
4.53%

仮想マシン（**EC2、AzureVM**）
- データベースのホスティング
- アプリケーションのホスティング
- レガシーなワークロード
- 設定データ
- 分析用のログデータ

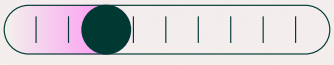
機密の非構造化データが格納されている主な場所は次の環境にあると
推定されます。

（Rubrikテレメトリー - 本番データ）

56.67%

のOneDriveファイルは機密ファイル

25.56%



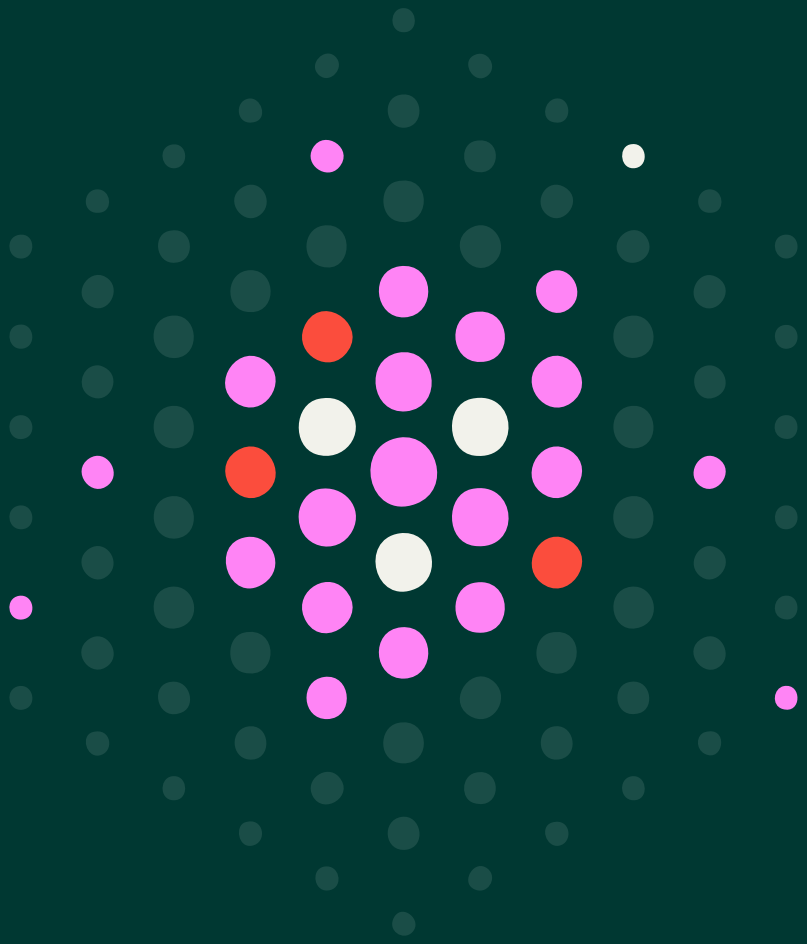
のSharePointファイルは機密ファイル

14.27%

のS3ファイルは機密ファイル

機密データの保護

IT/セキュリティリーダーとして、これだけの量の
情報からでも何らかの意思決定を開始できます。
最終的にはすべてのデータに気を配ることになるとはいえ、
本当に注意が必要なのは機密データです。

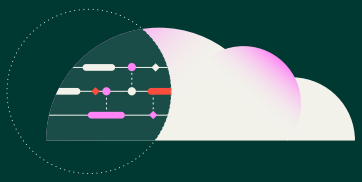


保有しているデータ量とその保存場所を把握することは、
その安全を適切に確保するための最初の一歩です。

そこから、クラウドやSaaSにあるデータの機密性の度合いを
分析し始めることができます。スタート地点となる例を示します。

クラウド | SaaS環境 | クラウドとSaaSの合計

クラウド内：



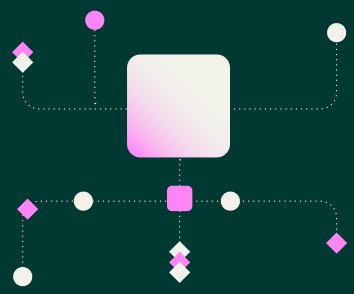
36.29%
機密ファイル（構造化/非構造化ファイルを含む）全体のうち、
高として分類されるファイルの割合

14.66%
すべての非構造化データのうち、**高として分類されるデータの割合**

45.49%
機密ファイル（構造化/非構造化ファイルを含む）全体のうち、
中として分類されるファイルの割合

クラウド | SaaS環境 | クラウドとSaaSの合計

SaaS環境内：



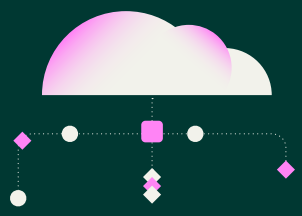
5.78%
機密ファイル（構造化/非構造化ファイルを含む）全体のうち、
高として分類されるファイルの割合

79.23%
すべての非構造化データのうち、**高として分類されるデータの割合**

0.85%
機密ファイル（構造化/非構造化ファイルを含む）全体のうち、
中として分類されるファイルの割合

クラウド | SaaS環境 | クラウドとSaaSの合計

SaaSとクラウドの合計：



42.07%
機密ファイル（構造化/非構造化ファイルを含む）全体のうち、
高として分類されるファイルの割合

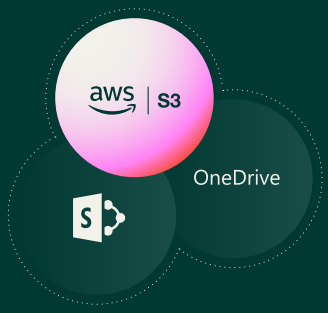
93.89%
すべての非構造化データのうち、**高として分類されるデータの割合**

46.34%
機密ファイル（構造化/非構造化ファイルを含む）全体のうち、
中として分類されるファイルの割合

次に、機密性の高いデータの具体的な保存場所を特定していきます。

クラウドS3 | SaaS OneDrive | SaaS SharePoint

クラウドS3



34.70%

S3内に存在するすべての機密ファイルのうち、**高として分類されるファイルの割合**

41.68%

S3内に存在するすべての機密ファイルのうち、**中として分類されるファイルの割合**

13.58%

すべての機密ファイルのうち、非構造化ファイルで**高として分類されるファイルの割合**

0.51%

すべての機密ファイルのうち、非構造化ファイルで**中として分類されるファイルの割合**

クラウドS3 | SaaS OneDrive | SaaS SharePoint

SAAS ONEDRIVE

3.89%

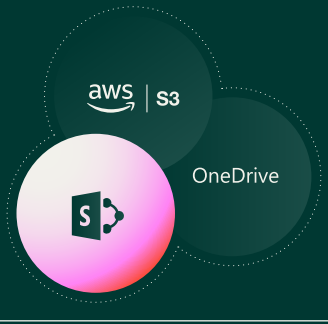
OneDrive内に存在するすべての機密ファイルのうち、**高として分類されるファイルの割合**

54.41%

すべての機密ファイルのうち、非構造化ファイルで**高として分類されるファイルの割合**

クラウドS3 | SaaS OneDrive | SaaS SharePoint

SAAS SHAREPOINT



1.81%

SharePoint内に存在するすべての機密ファイルのうち、**高として分類されるファイルの割合**

24.04%

すべての機密ファイルのうち、非構造化ファイルで**高として分類されるファイルの割合**

ここから、機密データに含まれている可能性がある内容をより明確にしていきます。

個人情報

PII（Personally Identifiable Information - 個人の特定が可能な情報）：社会保障番号、生年月日、住所、電話番号など。

64.51%

すべての機密データのうちPIIデータの割合。

93.84%

すべての機密の非構造化データのうちPIIデータの割合。

デジタル

APIキー、ユーザー名、アカウント番号、IPアドレス、モバイルデバイスIDなど。

26.96%

すべての機密データのうちデジタルデータの割合。

1.89%

すべての機密の非構造化データのうち1.89%がデジタルデータです。

ビジネス

知的財産：製品設計、ソースコード、研究開発のインサイト、戦略計画、サプライチェーンのロジスティクス、在庫情報など。

24.25%

すべての機密データのうちビジネスデータの割合。

3.79%

すべての機密の非構造化データのうちビジネスデータの割合。

金融

PCIデータ（支払いカード業界のデータ）：取引レコード、銀行情報、クレジットカード/デビットカード情報、納税申告、内部監査報告書など。

13.97%

すべての機密データのうち金融データの割合。

7.82%

すべての機密の非構造化データのうち金融データの割合。

次に、状況を明言してコントロールを確立するための第一歩に進みます。
セキュリティ戦略に役員レベルでのサポートを得る上でも有効な方法になります。

セキュリティ戦略の概要を示すメッセージ

“WE HAVE SENSITIVE DATA SPREAD ACROSS SEVERAL UNKNOWN POINTS, WITH VARYING SECURITY,” TO “HERE IS A LIST OF HOW OUR SENSITIVE DATA IS BEING USED AND HOW WE ARE PROTECTING IT.”

明確で包括的なポリシーの策定

ハイブリッドシステム内のデータの場所とデータの種類を十分に把握したら、明確で包括的なポリシーを策定することが重要です。残念なことに、現在、多くの企業が場当たり的なアプローチをとっています。

顧客の本番環境でモニタリングしているデータと顧客の環境で行っているバックアップデータとを比較したところ、Rubrikでは組織によるオンプレミスデータの保護方法とクラウドやSaaSデータの保護方法とのあいだに大きな差があることを確認しました。

データのバックアップの扱い方の違いは特に明らかです。オンプレミスデータは厳格な保持ポリシーのもとで、完全に隔離されたコピーとして定期的にバックアップされます。また、障害復旧計画は長期にわたって改訂されています。

一方、クラウドとSaaSのデータはバックアップされたとしても、場当たり的なバックアップになっている傾向があります。クラウドを標的としたランサムウェア攻撃が目覚ましいことと無縁ではないでしょう。

この情報から、組織はクラウドプロバイダーのネイティブバックアップツールに依存し、データの安全を確保しようとしていると考えられます。残念ながら、ネイティブバックアップツールは多くの場合、限界があり、実行頻度が低く、プロバイダーのインフラストラクチャに縛られるため組織の復元のニーズには合わない可能性があります。仮にすべてのクラウド/SaaSプロバイダーのパフォーマンスが最高水準であるとしても、状況の把握とコントロールを怠れば、それは問題のあるセキュリティアプローチだと言えるでしょう。

すべてが最高水準であるという仮定に基づくリスク管理は堅実なアプローチとは言えません。オンプレミスデータと比較して、クラウドアプリケーションやSaaSプラットフォームに保存されている重要ビジネスデータが偶発的な削除、ランサムウェア攻撃、ポリシーの設定ミスなどに対してより脆弱であることは事実です。

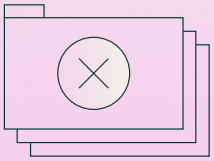
バックアップ機能を、オンプレミスと同様にオフプレミスでもコントロールすることは企業セキュリティ管理の重要な一部です。

これは単に技術的な問題ではなく 戦略的な盲点です。

IT/セキュリティのリーダーが自問すべき問い

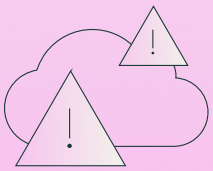
自社のクラウドとSaaSのバックアップ戦略は、オンプレミスのバックアップ戦略と同程度によく練られた堅牢なものか？

実際に起きた事例を見ていきましょう。2017年1月31日にGITLABのデータベースに発生したインシデントです。



1.

エンジニアが誤って本番データベースを削除し、作業時間にして6時間分の重要データを失ってしまいました。ここには、イシュー、マージリクエスト、コメントが含まれていました。



2.

エンジニアが誤って本番データベースを削除し、6時間分の重要データを失ってしまいました。ここには、イシュー、マージリクエスト、コメントが含まれていました。

3.

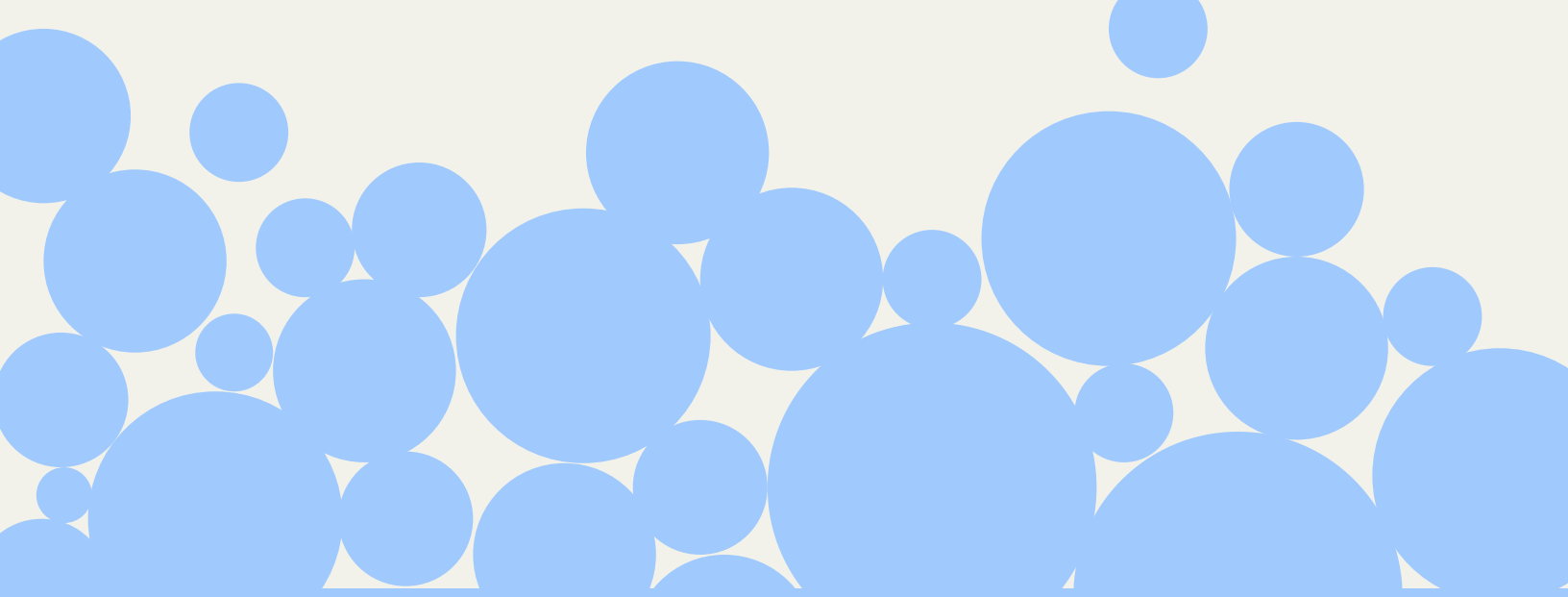
このインシデントにより、クラウドネイティブ環境なら本質的に堅牢なバックアップ保護を期待できるという思い込みによるリスクが露呈しました。GitLabの事後分析により、そのバックアップ戦略が従来のオンプレミスで実施していたバックアップと比べて不十分であることが明らかになりました。[1]

https://about.gitlab.com/blog/gitlab-dot-com-database-incident/

この問題に対処するには、バックアップや復元のポリシーの範囲を、オンプレミスのシステムという枠を超えてクラウドネイティブの世界にまで広げる、データ保護に対する統一されたアプローチが必要です。

提案

ここでは、IT/セキュリティリーダーがクラウド、SaaS、オンプレミス環境
全体でデータを保護する能力と自信を高めるための方法を提案します。

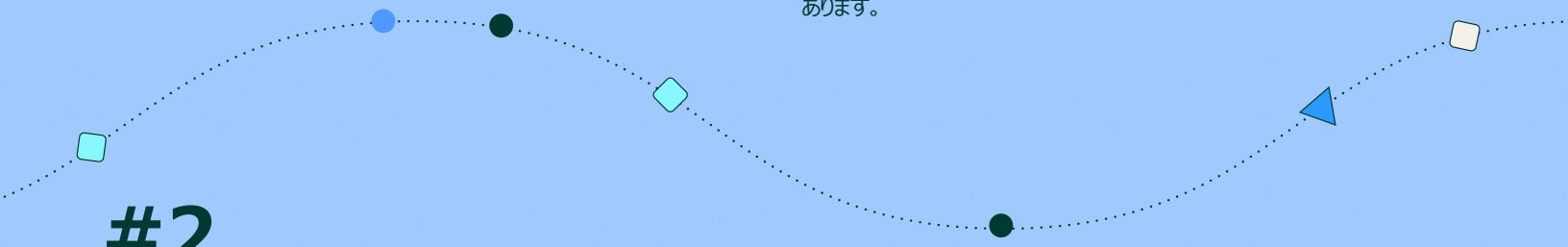


#1

まず、転送中のデータ、保存データを含め、データ（特に機密データ）の場所を把握します。

誰でもリソースには限りがあるため、優先順位付けが重要です。組織の最も貴重な知的財産に求められる保護と同じレベルで、5年前のマーケティング動画のフォルダを保護するようなことはしないでください。

場所の特定は考えているよりも大変な仕事になる可能性があるため留意しておいてください。どのデータもそうですが、機密データは時間とともに変化します。たとえば、1人の社員の単なる思い付きだったアイデアが、数週間後には組織戦略の重要な構成要素の1つになることもあり得るのです。いずれにせよ、すべてのデータの場所を把握し、状況に沿って適切に保護する必要があります。



#2

データの理解と優先順位付けに基づくポリシー、プロセス、手順を共有します。

ポリシー

適切なポリシーを設定します。たとえば、機密ファイルをダウンロードするための条件を管理します。

たとえば、公衆Wi-Fiネットワークでの組織のソースコードへの編集アクセスを制限するポリシーなど（VPNを使用していない場合）が該当します。そんなことは当たり前の発想だと思うかもしれませんが、驚くべきことに、いつもの作業習慣でつい忘れてしまう人は結構多いのです。

プロセスと手順

ポリシーを施行するための方法を定義します。たとえば、ユーザーが特定の状況下で特定のファイルをダウンロードすることを許可されていない場合、

- ポリシーの施行方法は？
- 違反があった時の追跡方法は？
- その違反の副次的影響への対処方法は？
- ポリシーの施行に関する責任者は？

企業はデータの安全を確保するために、これらすべての質問に答える必要があります。さらに、すべての機密データの場所を把握し、それを保護するための計画を策定しているという安心感を役員や幹部に与える必要があります。

#3

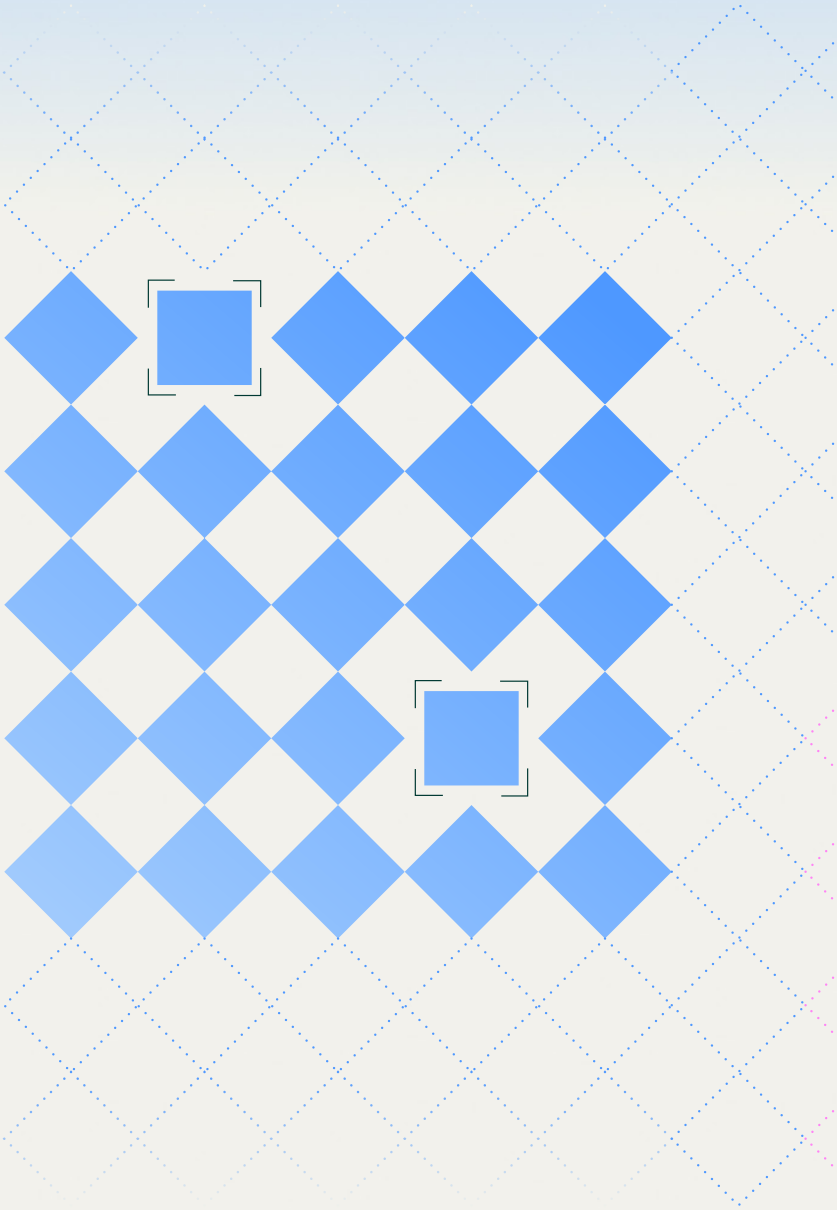
自動化を利用して、セキュリティ/ITチームの効率性を改善します。

よほどの支援がなければ、セキュリティ/ITチームは組織で生成される膨大な量のデータに何が起きているかを把握することはできません。
監視・集計ツールを使用したとしても、多くの場合、人手不足のチームが受け取るアラートは相当の量であり、どんなに優秀で鍛えあげられたIT/セキュリティ担当者であっても、現実逃避したくなるほどのものです。

確実にポリシーが施行され、プロセスと手順が遵守されるようにする唯一の効果的な方法は、自動化を活用することです。

一例として、セキュリティインシデントが発生すると、根本原因分析が必要となります。自動化なしでは、セキュリティアナリストは手作業で膨大な量のデータをしらみつぶしに調べる必要があります。これは大変面倒で時間のかかるプロセスです。ご存じのとおり、繰り返しタスクではヒューマンエラーの発生確率が高くなります。よくある例としては、正しく検知されたものをSOCのアナリストが誤って誤検知としてマークしてしまうことが挙げられます。これにより、脅威に対処しないまま残してしまう可能性があります。

定期的な繰り返しタスクを自動化することで、組織でエラーの発生を減らせるだけでなく、優秀な担当者を解放して、より戦略的で価値の高いセキュリティに関する取り組みに専念させられるようになります。



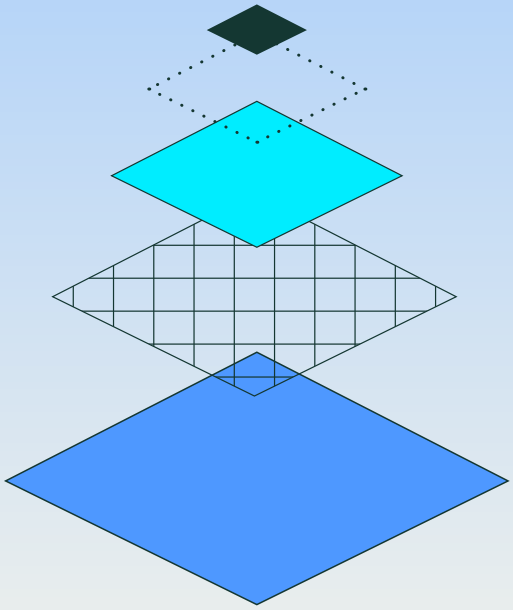
データのバックアップと復元

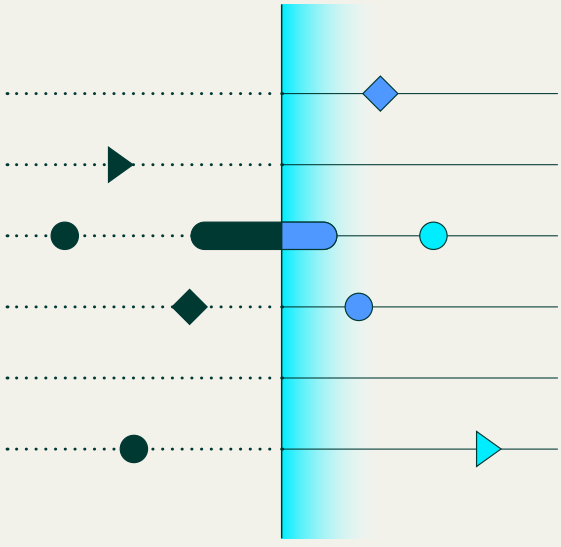
自動化なし

ITチームは手動でバックアップを管理します。スケジュールを監視したり、データの完全性を検証したり、インシデントの発生時には復元プロセスを実施する必要があります。このアプローチでは時間がかかるだけでなく、バックアップの欠落や復元の失敗などのエラーが発生しやすくなり、重大な局面で組織が脆弱な状態になります。

自動化あり

バックアップと復元の自動化ソリューションを利用すると、手動での介入なしに、継続的に安全にデータのバックアップを確実に取ることができます。ランサムウェア攻撃やシステム障害の発生時には、これらのソリューションにより、バックアップは完全に書き換え不可の状態で利用でき、迅速なデータ復元が可能となり、ダウンタイムが大幅に短縮され、データの損失も最小限に抑えられます。これらのプロセスを自動化することにより、ITチームは複雑な復旧ワークフローを管理する代わりに先を見越したセキュリティ対策に集中することができ、事業継続を確保しながらサイバー脅威に対する防衛を強化することができます。





脅威検知とアラートトリアージ

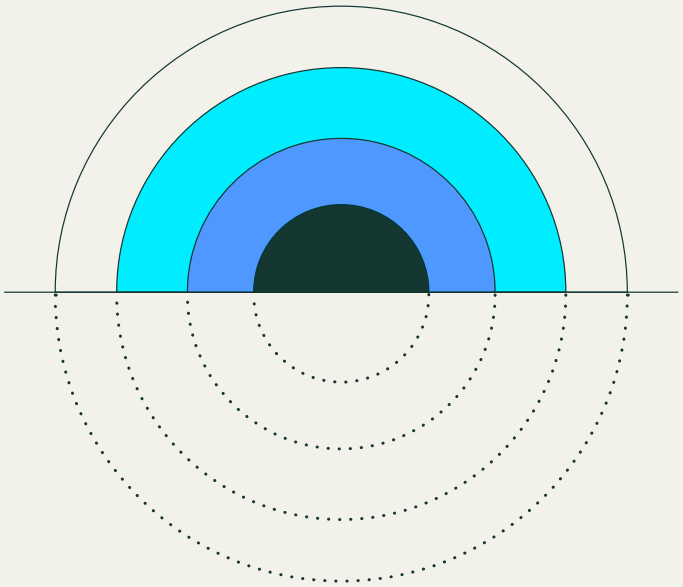
自動化なし

セキュリティアナリストが膨大なセキュリティアラートを手動で取捨選択するため、アラート疲れにつながり、脅威を見逃す可能性があります。

自動化あり

自動化された脅威検知・対応ツールでは、特定のアラートの分類、優先順位付け、さらには修正もできるため、アナリストは新しい脅威や高度な脅威の調査に集中することができます。

インシデント対応と根本原因分析

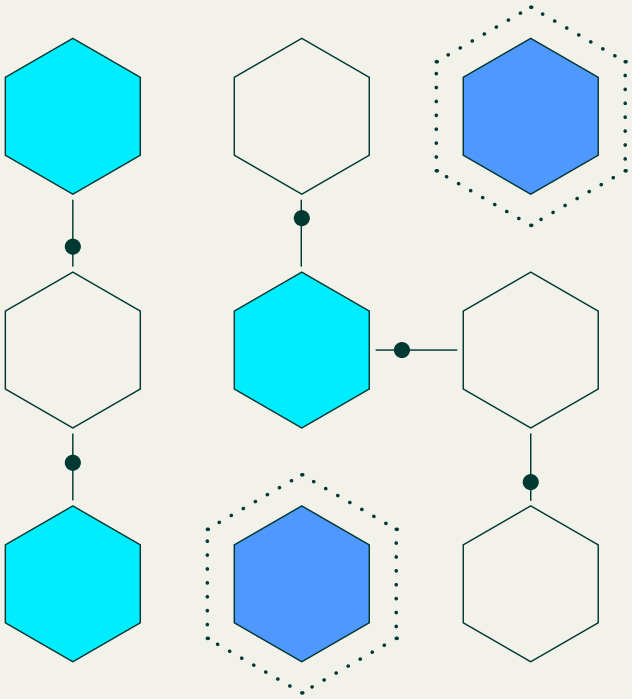


自動化なし

セキュリティチームが、各種ソースのログ（ファイアウォール、SIEM、エンドポイント保護システム）を手動で関連付けて、インシデントの根本原因を特定する必要があります。

自動化あり

SOAR（セキュリティオーケストレーション、自動化、レスポンス）プラットフォームにより自動でログデータの収集と分析が行われるため、調査時間が大幅に短縮されます。



脆弱性管理とパッチ適用

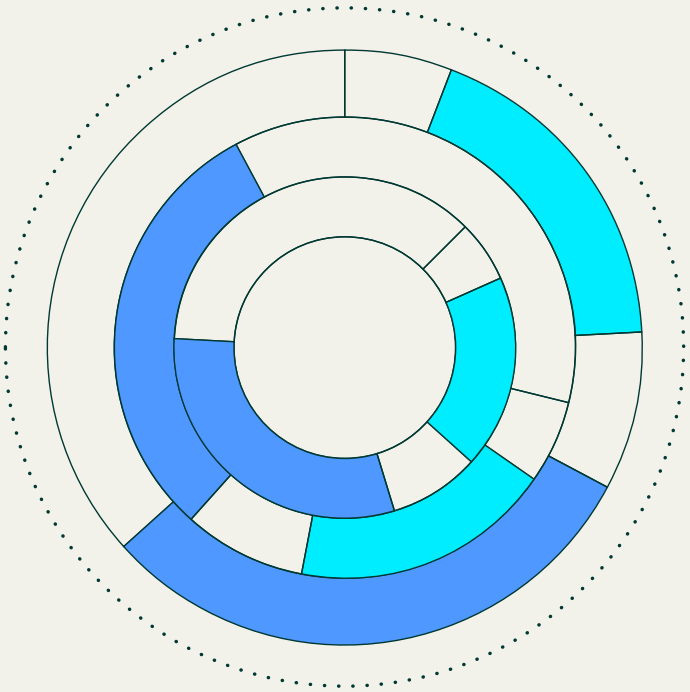
自動化なし

ITチームが手動で脆弱性を追跡し、リスクを評価し、パッチを適用するため、時間がかかり、ミスが発生しやすくなります。

自動化あり

自動化された脆弱性スキャンおよびパッチ管理ソリューションにより、継続的な手動による介入を必要とせずに事前にリスクを特定して修正することができます。

アクセス制御とアイデンティティ管理

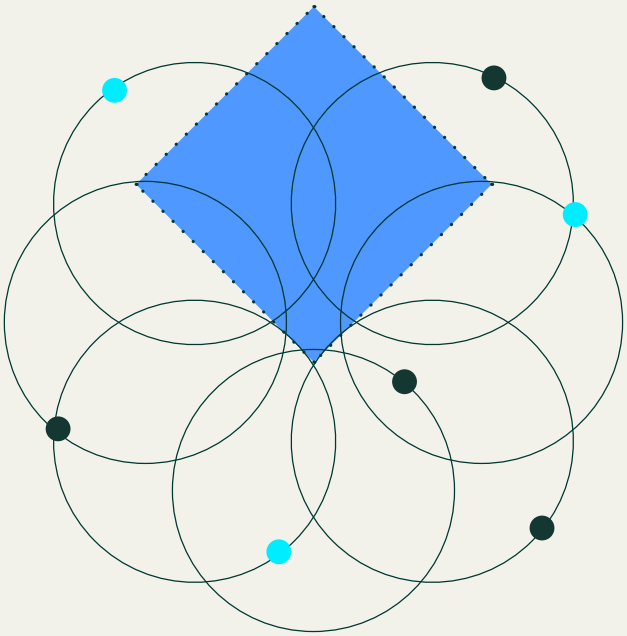


自動化なし

IT管理者がユーザーのアクセス権を手動で付与したり取り消したりするため、特権アカウントが残存するリスクが高まります。

自動化あり

アイデンティティおよびアクセス管理（IAM）ソリューションにより、ロールの変更に基づいて動的に権限が調整されるため、内部脅威のリスクが低減します。



動作異常検知

自動化なし

セキュリティチームが静的なルールに従って疑わしいアクティビティを警告するため、過剰な誤検知が発生する可能性があります。

自動化あり

AIを利用したセキュリティツールが継続的にユーザーの行動を学習し、それに合わせてより効果的に新しい攻撃パターンを検知します。

まとめ

マルチクラウドハイブリッド環境への移行は、ビジネスにおけるコンピュータ活用の歴史において特に重要な節目の1つに数えられます。

企業ワークフローや企業間協力にとって不可欠なものとなっています。ただし、今回の分析で示されたように、そのメリットにはセキュリティリスクの面で大きな犠牲が伴います。ハイブリッド環境では、これまでに例のない危険が生じています。ITリーダーからはシステム全体のデータセキュリティに関する課題、可視性の欠如、一元管理を確立できないなどの問題が報告されています。脅威アクターはこのような弱点を容赦なく利用し、現在では攻撃の大部分を占めるアイデンティティベースの攻撃のような進化した手法を用いています。

憂慮すべき結果

約90%

調査対象の組織のうち、攻撃を受けたことがある（多くは何度も攻撃された）と回答した組織の割合

86%

金銭の要求を受けた企業のうち、実際に支払いに応じたと回答した企業の割合

3/4

攻撃者による不正アクセスおよびデータ侵害が可能だったと回答した割合

謝意

多大な労力をかけて収集・分析されたデータ知見を本調査に提供していただいたすべての外部組織に対し、Rubrikとしてさらなる感謝を伝えたく思います。

Rubrik Zero Labsの研究は、多くの人々の協力によって成り立っています。Wakefield Researchには、この研究を可能な限り客観的なものとするための外部データを提供していただきました。Shaped Byには、データを意味づけするためのすばらしい方法を見つけていただきました。最後に、多くのRubrik関係者が多大な労力により、能力、コンテキスト、ガイダンスを提供してくれました。Amanda O'Callaghan、Linda Nguyen、Lynda Hall、Ben Long、Peter Chang、Ajay Kumar Gaddam、Dan Eldad、Gunakar Goswami、Prasath Mani、Ethan Hagan、Kevin Nguyen、Caleb Tolin、Sindhu Nagendra、Trinetra Reddy、Heather Webb、Meghan Fintland、Görkem Otman、Fareed Fityanの各氏に対し、格別の感謝を申し上げます。