druva

Druvaが提案する新しいバックアップの形

～セキュリティの最後の砦～

2023年9月6日

Druva Japan Y. Sakama

Druva: 業界初 & 大規模な データ回復向け SaaS プラットフォーム

25億回+
バックアップ / 年

50%
管理データ量
の年間伸び率

89
NPSスコア

60社+
Fortune 500

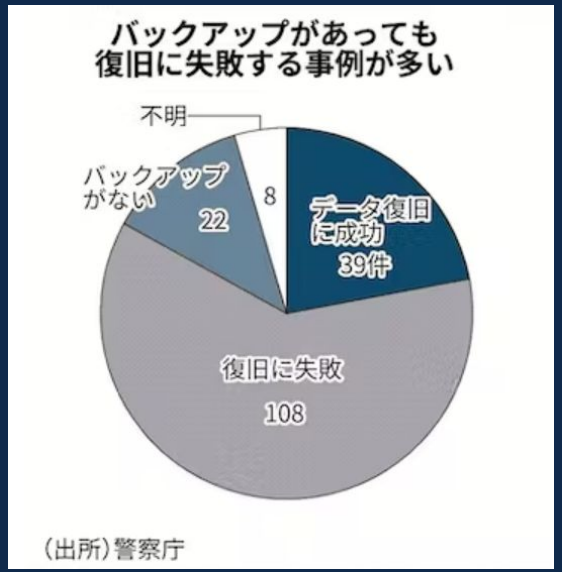
16
リージョン数

200 PB+
管理するデータ量

A.C. MOORE ARTS & CRAFTS
AMOREPACIFIC
ANDRITZ
ANGLO-EASTERN
APPTUS
BECKMAN COULTER
BROWN-FORMAN
CLEVELAND BROWNS
DHL
DHS HUMAN SERVICES
EGAN
FOREVER 21
Gap International Partners In Exceptional Growth
HITACHI Inspire the Next
IMMEDIATE MEDIA Co
jamf
NASA
OHEL
REGENERON
SAMSUNG SEMICONDUCTORS
Spirent
STARZ
UMBRAGROUP

druva

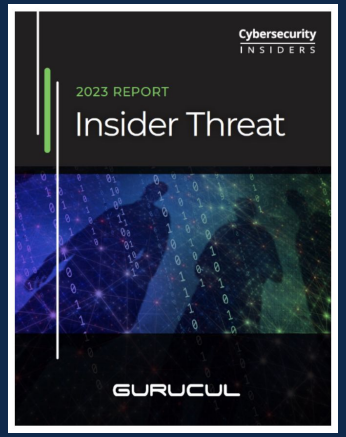
身代金ウイルス攻撃、「データ復旧できず」7割 バックアップ機能せず



保存したデータもウイルスで暗号化されていた

3-2-1ルールに則ってデータを別の地域の拠点で保管していても、元のデータと同じネットワークにつながっていれば、地震ではデータを守れても、サイバー攻撃では同様の被害を受けてしまうリスクがある

出典: 警察庁: サイバー空間をめぐる脅威の情勢等 (R3, R4上半期)



74%

管理者権限乗っ取りや、悪意ある内部犯行のリスクの高まりを認識し、脆弱性を認めている

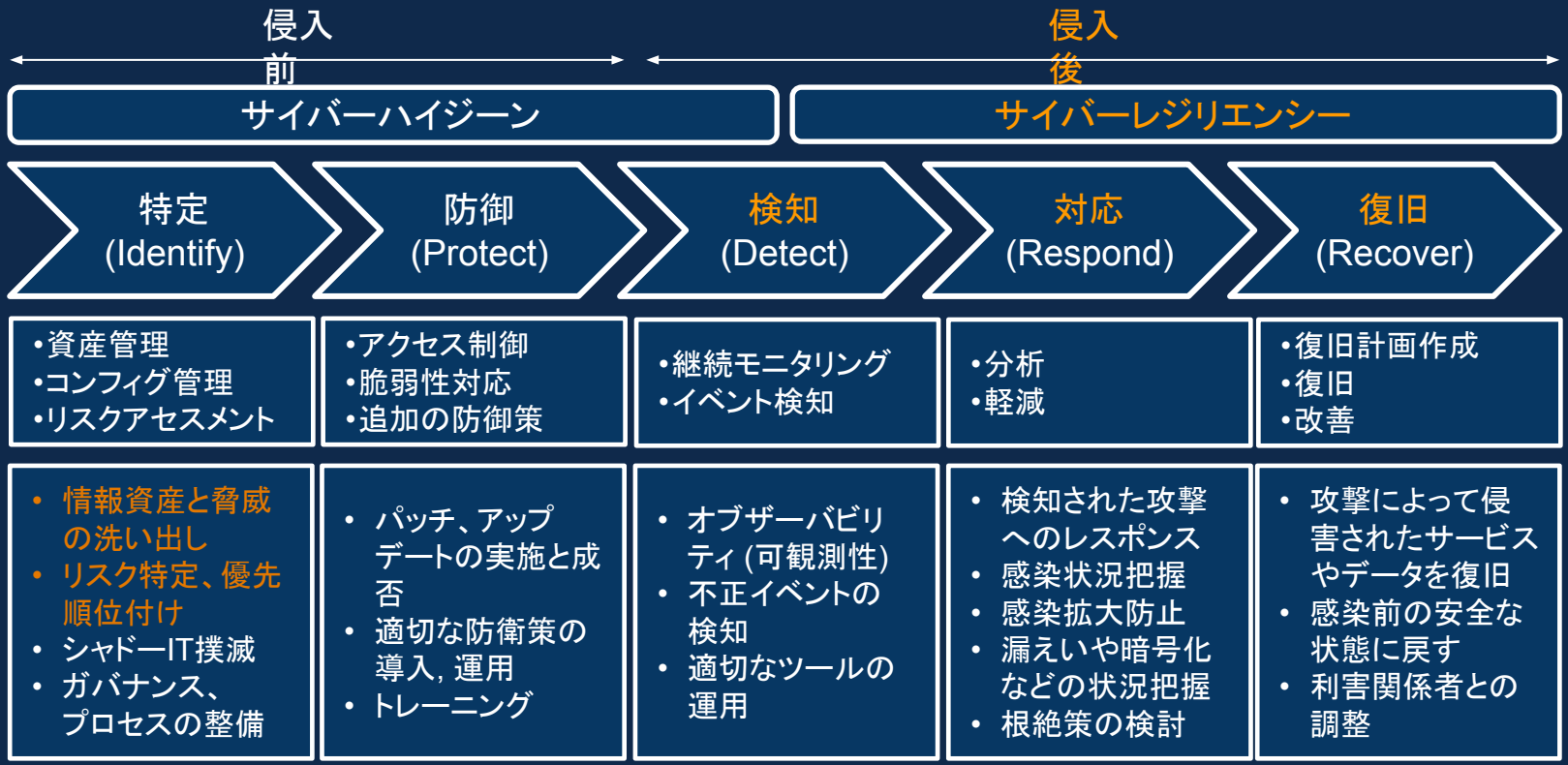
82%

データ漏洩/侵害がソーシャル攻撃や過失、誤操作などの人的要因に起因

出典: 2023 Insider Threat Report Cybersecurity Insiders Report
Verizon’s 2022 Data Breach Investigations Report

druva

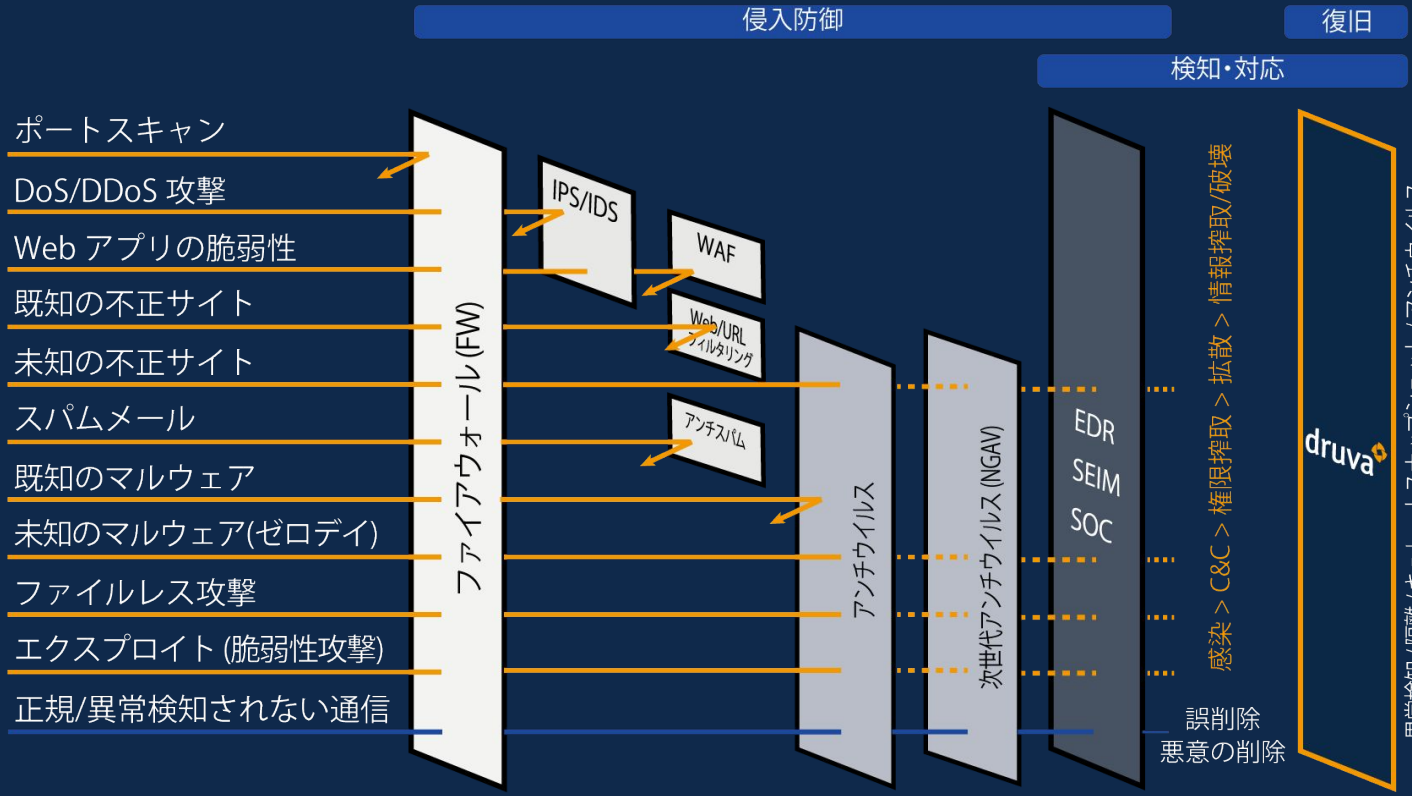
（自信が持てる）サイバーレジリエンシーが重要に！



バックアップはやっているがいざとなったら確実に復旧できるか自信がない

セキュリティの最後の砦

侵入防御や検知で対応しきれないマルウェアからの確実なデータ復旧



医療情報システムの安全管理に関するガイドライン (第5.2版; 厚労省)

サイバー攻撃等の非常時の対応

- ウイルス等感染時、バックアップから重要ファイルを復元
- 重要ファイルはバックアップ数世代を複数方式で実施
  - 追記可能と不可能な媒体の組み合わせ
  - ネットワークから切り離したバックアップデータ保管

見識性の確保

- 定期的なバックアップで、バックアップから患者情報を確認できるようにする
- 大規模火災等の災害対策として遠隔地に電子保存記録をバックアップ
- バックアップデータを汎用ブラウザ等により見読できるようにする

保存性の確保

- 情報損失時に備えて定期的に情報のバックアップを作成
- バックアップを履歴とともに管理し復元できる仕組みを備える

個人情報の保護

- バックアップ情報における個人情報の取り扱いも商用環境と同様の運用体制が求められる
- 外部保存を受託する事業者における医療情報へのアクセスの禁止

druva

ベストプラクティスの変化 – ランサムウェアの特徴と対策

（特徴）

長期間潜伏して ファイルを 徐々に暗号化

- どのスナップショットで復元すればよいか わからなくなる

脆弱なバックアップ インフラが攻撃 ポイントとなる

- バックアップ環境から ランサムウェアが侵入する
- 汚染されたバックアップ データによる再感染

バックアップ インフラを破壊する

- バックアップ環境が 攻撃に遭い使えなくなる

（対策）

「侵入防御」から「侵入される前提」の対策へ

- ファイルが暗号化されたことを検知できること
- 復旧に使える安全なバックアップデータを常時持つこと
- 再感染を阻止し、クリーンなデータで迅速に復旧できること

ベストプラクティスの変化 – バックアップルール

3-2-1 ルール

- 3つのデータコピー
- 2つの異なるメディア
- 1つのオフサイトコピー (遠隔地/クラウド)

3-2-1-1-(0) ルール

- 3つのデータコピー
- 2つの異なるメディア
- 1つのオフサイトコピー
- 1つはエアギャップのあるイミュータブルなオフラインバックアップ
- バックアップのリカバリテストを行ったときにエラーが発生しない (0)

druva

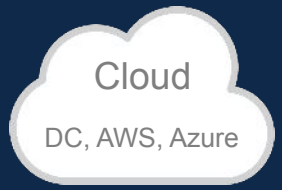
Druva: データレジリエンシークラウド

ランサムウェアに破壊されないアーキテクチャ

従来型ソリューション

- 多数の攻撃面 (attack surface)
- 汎用OS/ファイルシステムによるゼロデイ攻撃リスク
- ユーザー側でセキュリティ運用
  - 脆弱性チェック
  - パッチあて、アップグレード
  - 各種ポリシー定義、設定

- 物理的な消耗リスク
- 規格変更に伴うアップグレード



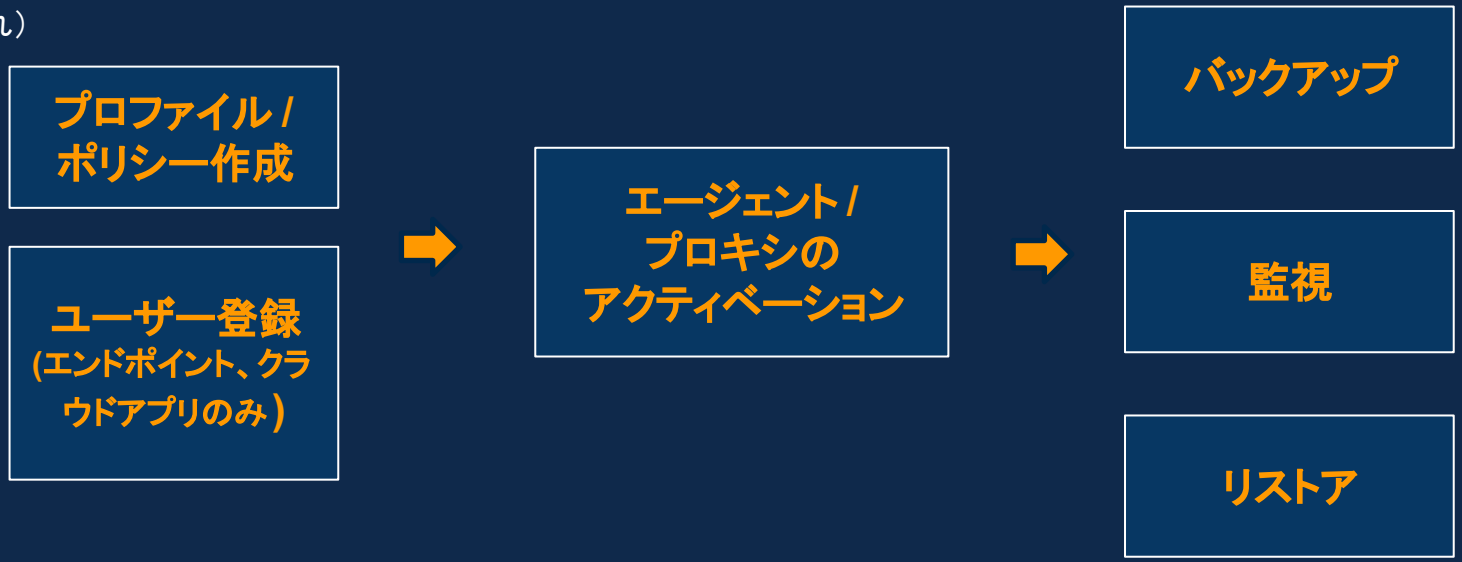
Druva

- 最小限の攻撃面、ゼロトラスト
- エアギャップ、イミュータブル
- ベンダー側でセキュリティ運用
  - 脆弱性チェック
  - パッチあて、アップグレード
  - 各種ポリシー定義、設定

druva

Druva - 15分で設定完了

（設定の流れ）



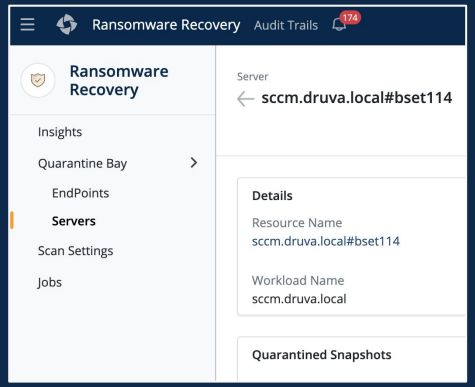
（不要になるもの）

- バックアップインフラの調達、構築、設定
- サイジング

- バックアップインフラのアップデート、パッチ適用
- ストレージ等リソース追加

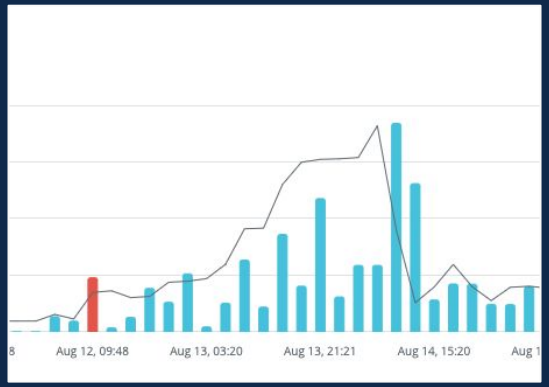
ランサムウェアリカバリの迅速化

封じ込め



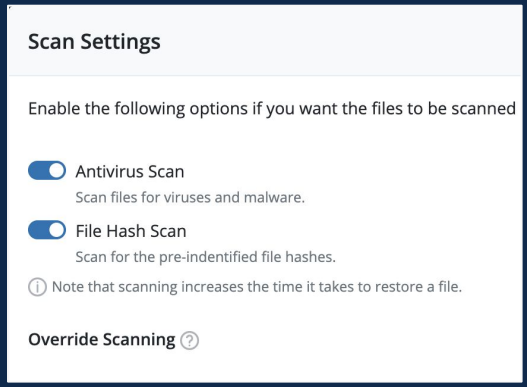
隔離
マルウェア拡散を防止

識別



異常データ操作
異常なデータセットを識別

復旧



リカバリ時のスキャンと
キュレートスナップショット
クリーンかつ感染していないデータで自動リカバリ

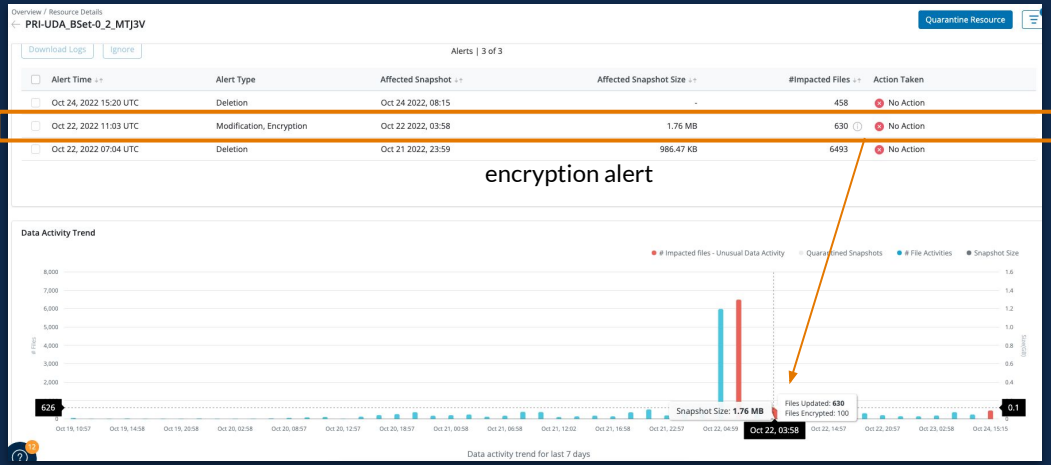
druva

セキュリティイベント　Security Events
MLを活用した異常なデータの振る舞いや、アクセスへのアラート機能

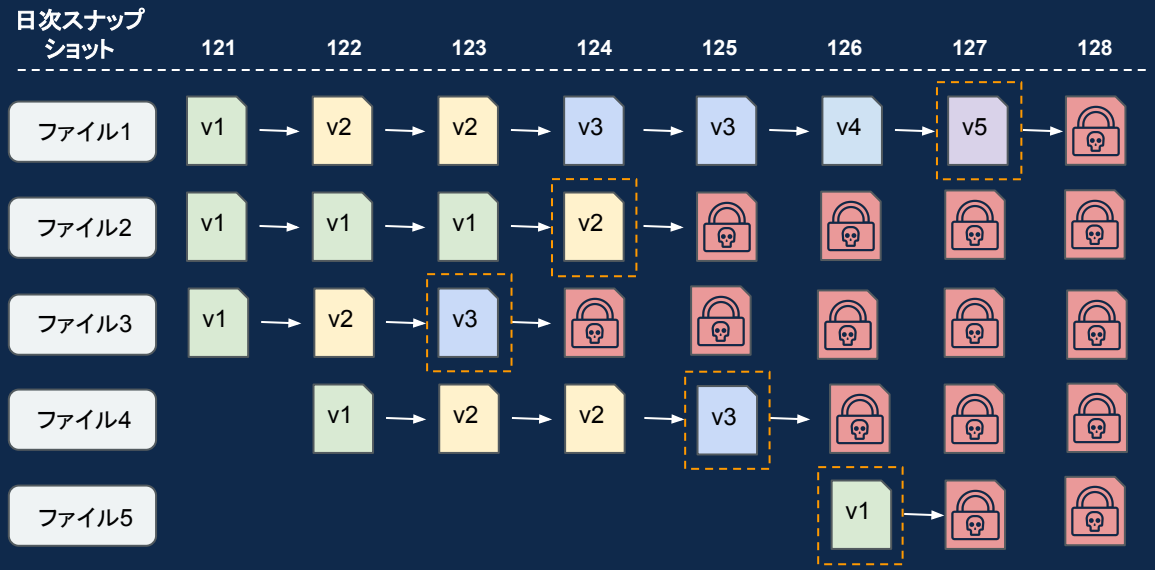
異常なデータの振る舞いや、アクセスを常に監視し一時間以内に管理者にアラートを送付

30日以上のスナップショットを 元に普段と逸脱した大量データ 操作が発生すると
検知してアラート

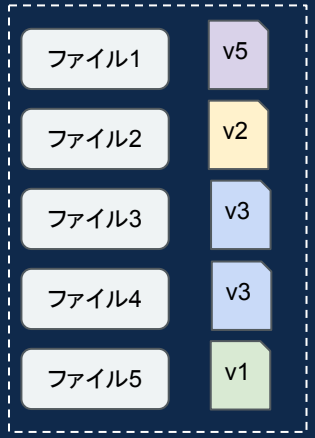
☑️ 追加、削除、変更、暗号化



キュレートリカバリ - 自動化により時間削減とデータ損失回避



キュレートリカバリ:
時間短縮とデータ保全



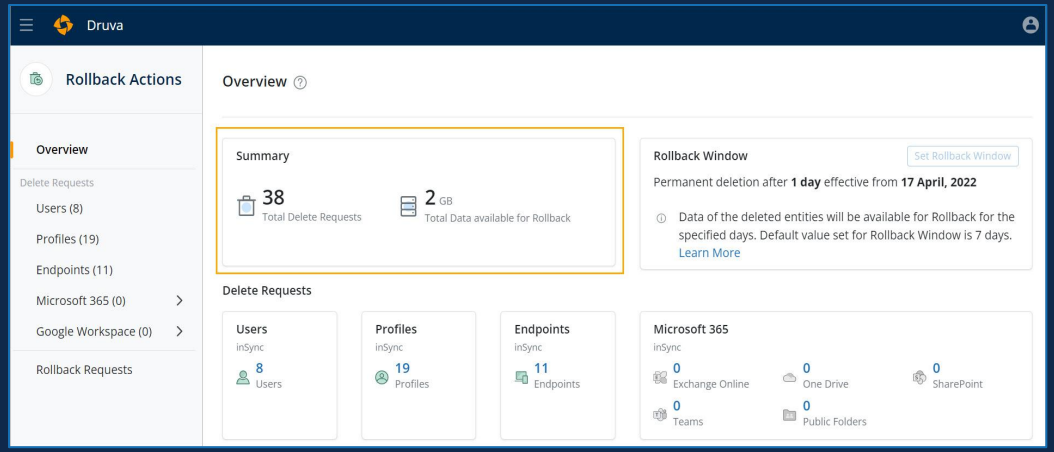
各ファイルの最新クリーンバージョンを自動的に検索し、単一の「ゴールデンスナップショット」に追加

ロールバック　Rollback Actions
「バックアップインフラの破壊を試みる」ランサムウェア等に対抗する機能

エンドポイント、クラウドアプリ、ハイブリッドワークロードが対象
デフォルトで7日間、ウインドウ (永久削除までの期間) を設定可能

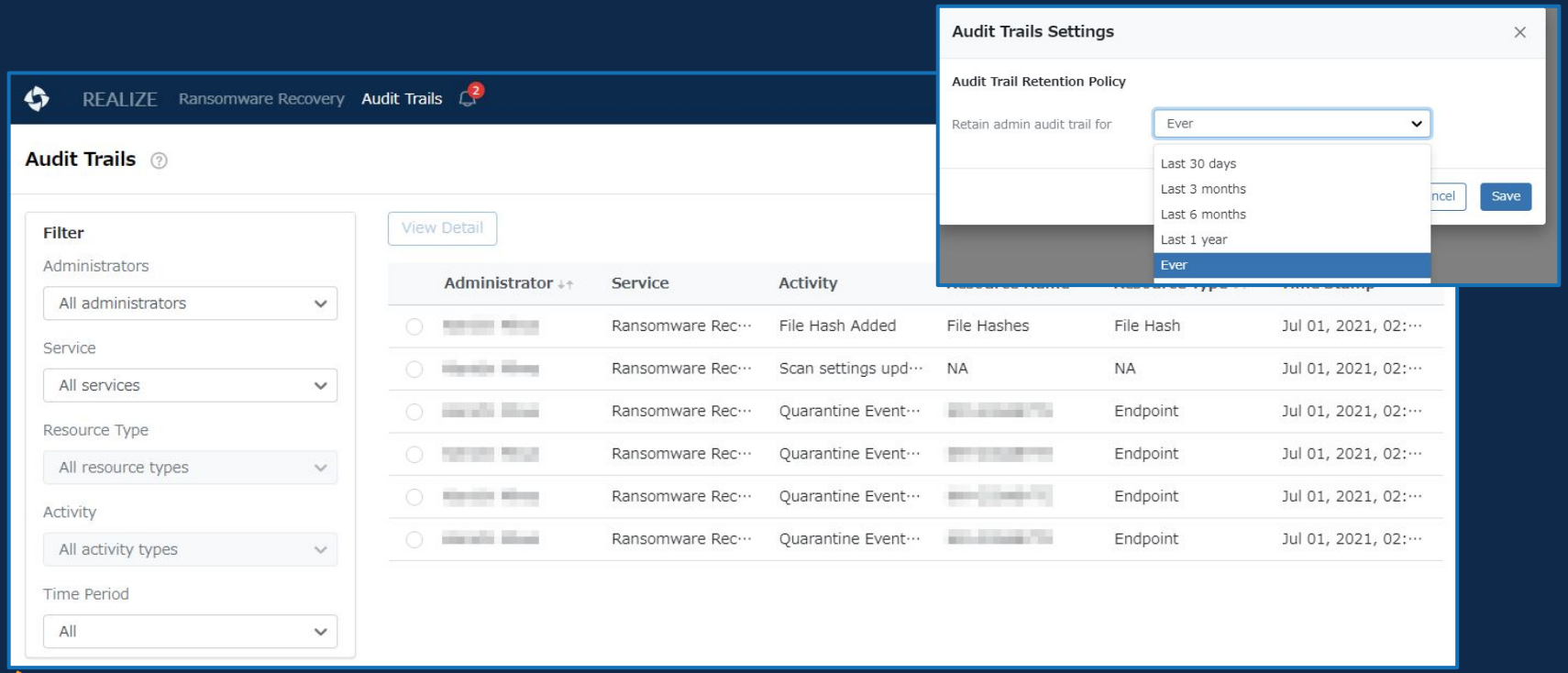
ユーザー、プロファイル、ワークロードの削除操作ごとにロールバック可能

設定したウインドウの期間内において、
悪意ある管理者によるもの、
または意図しない削除操作があった際、
その削除操作を「取消」できる



ランサムウェアリカバリ: 管理者操作の監査証跡　Audit Trail

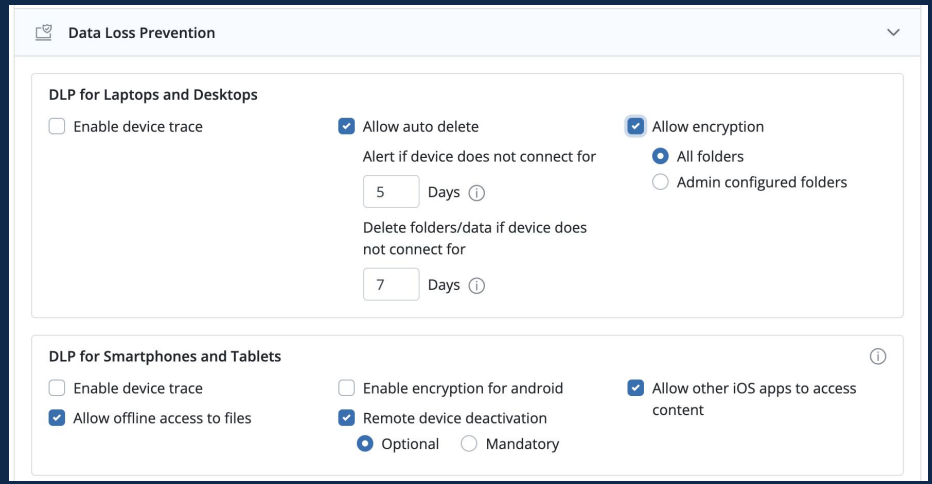
管理者が設定変更や削除などの操作を行うと変更不可能な監査証跡に記録



バックアップ以上の価値: ファット端末のデータ保護 (DLP)

- 課題: VDIからファット端末への移行、リモートワーク、持ち出し PC上に置かれた重要データ、個人情報、クラウドに上げる前の一時ファイルの保護

- 位置情報追跡
  - 最終バックアップ時の場所をGoogle Map上に表示
- 紛失や盗難されたデバイスから重要データをリモートワイプ / 自動削除
  - 失くしたファイルの詳細を追跡可能
  - 端末再取得時に容易に復元可能
- デバイス上でのファイル強制暗号化
  - Windows EFS
  - 抜き取ったディスクからのデータ盗難防止



druva

バックアップのベストプラクティス

- オフサイトストレージを使用する：クラウドまたは別サイトのサーバー（災害対策）
- 3-2-1ルールに従う（データを確実にバックアップする）
- データを定期的にバックアップする（少なくとも週1回、1日1回を推奨）
- バックアップを暗号化する（確実な復元、セキュリティ強化）
- エンドポイントについて考える（故障、紛失、盗難対策。ランサムウェア対策）
- BYODを考慮に入れる
- 定期的なテストの実施（年に1, 2回、バックアップとリカバリのテストを実施。除外できるコンテンツ、バックアップウインドウなど欠点の気づきと修正に役立つ）
- 保存期間の決定（業界規制やコンプライアンス要件への適合。
  月次、半年ごとのバックアップを可能な限り長く保持）
- 最低週1回、バックアップレポートを確認する
  （復元ポイント数、ストレージ使用容量、ジョブステータス、アラートの確認）

druva

Druva Cloud Platform: 一元プラットフォーム

inSync

エンドポイント & SaaSアプリ

Windows, Mac, Linux, Android, iOS
Microsoft 365, Google Workspace, Salesforce, Slack

Phoenix

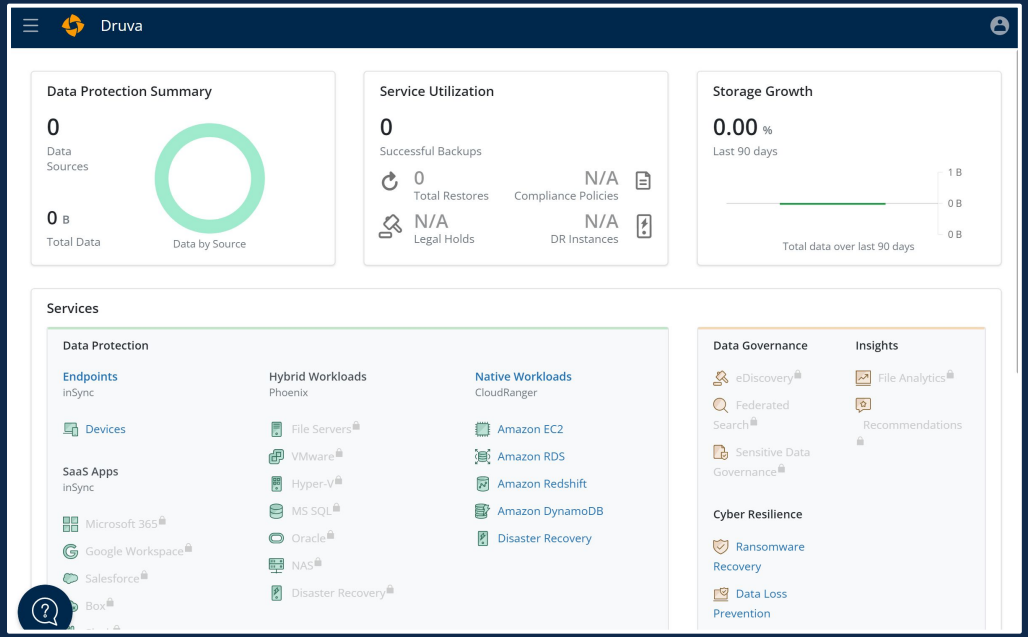
データセンター & リモートオフィス

Windows Server, Linux, MS-SQL, Oracle, VMware, Hyper-V, NAS, EC2

CloudRanger

AWS クラウドワークロード

EC2, EBS, RDS, Redshift



druva

Druvaは2023 Gartner® Magic Quadrant™ for Enterprise Backup and Recovery Software Solutionsにて、3年連続でVisionaryと評価されました

Druva のメリット:

- SaaS 配信モデルと透明な「従量課金」価格モデル
- データセンター、パブリッククラウド、エッジにまたがる分散環境のバックアップ、リストア、DR
- 15以上のリージョンにわたる地理的網羅と可用性
- eDiscovery, ランサムウェア検出とリカバリ, ストレージ最適化など、幅広いデータ管理のユースケースをサポート

Gartner

Figure 1: Magic Quadrant for Enterprise Backup and Recovery Software Solutions

druva

コストと複雑さを削減、TCOを最大50%削減

- 不要になるもの：
  - バックアップ向け H/W, S/W, コンピューティング, ストレージ
  - 保存 & オフサイト: テープやクラウド
  - サービス: MSP, プロフェッショナル サービス
  - 電源, 冷房, ホスティング
  - アップグレード, メンテナンス, データ送信コスト
  - インフラを管理するオンサイトの IT人員
- 得られるもの：
  - 透明な従量課金モデル
  - セキュリティ向上
  - 一元化された可視性

Druva TCO Calculator (tco.druva.com)

Druvaデータレジリエンシー保証

druva

$10M
(1000万ドル)

Druvaデータレジリエンシー保証

全体に適用、漏れがない

リスク

- サイバーリスク
  (ランサムウェア, 未知の攻撃)
- 人的リスク
- アプリケーションリスク
- 運用リスク
- 環境リスク

SLA

- **100% 機密性 (Confidentiality).** セキュリティインシデントによって顧客データが侵害されないことを保証
- **100% 不変性 (Immutability).** ランサムウェアインシデントが発生した場合、顧客データの最新バックアップデータが回復可能 (変更されない) であることを保証
- **99% 信頼性 (Reliability).** 顧客ポリシーに従ってバックアップが正常に完了することを保証
- **99.999% 耐久性 (Durability).** バックアップされた顧客データが回復可能である (破損していない) ことを保証
- **99.5% 可用性 (Availability).** 最低99.5%のアップタイムを保証

druva

データレジリエンシーの確保に向けて

Druva 無償トライアル

操作性/要件適合を確認

druva.com/free-trial

ハイブリッド
ワークロード向け
TCO試算

tco.druva.com

Druvaに問い合わせ

druva.com/ja

druva

Thank You!