クラウド時代のデータ保護基盤のあり方とその活用

Druva製品紹介

2021年8月

Druva 合同会社 三輪 賢一

自己紹介:

- 三輪 賢一 (みわ けんいち)
  - Druva合同会社 システムエンジニアリング本部長
- 経歴: ネットワークセキュリティベンダーのSE
  - シスコシステムズ (Cisco; 20年ほど前)
  - ジュニパーネットワークス (Juniper; 15年ほど前)
  - パロアルトネットワークス (PANW; 10年ほど前)
- インフラはクラウドへ、守るべきものはデータへ
  - 2015年3月より現職
- 著書
  - TCP/IPネットワークステップアップラーニング
  - かんたんネットワーク入門
  - プロのための [図解] ネットワーク機器入門

4000+

企業ユーザー数

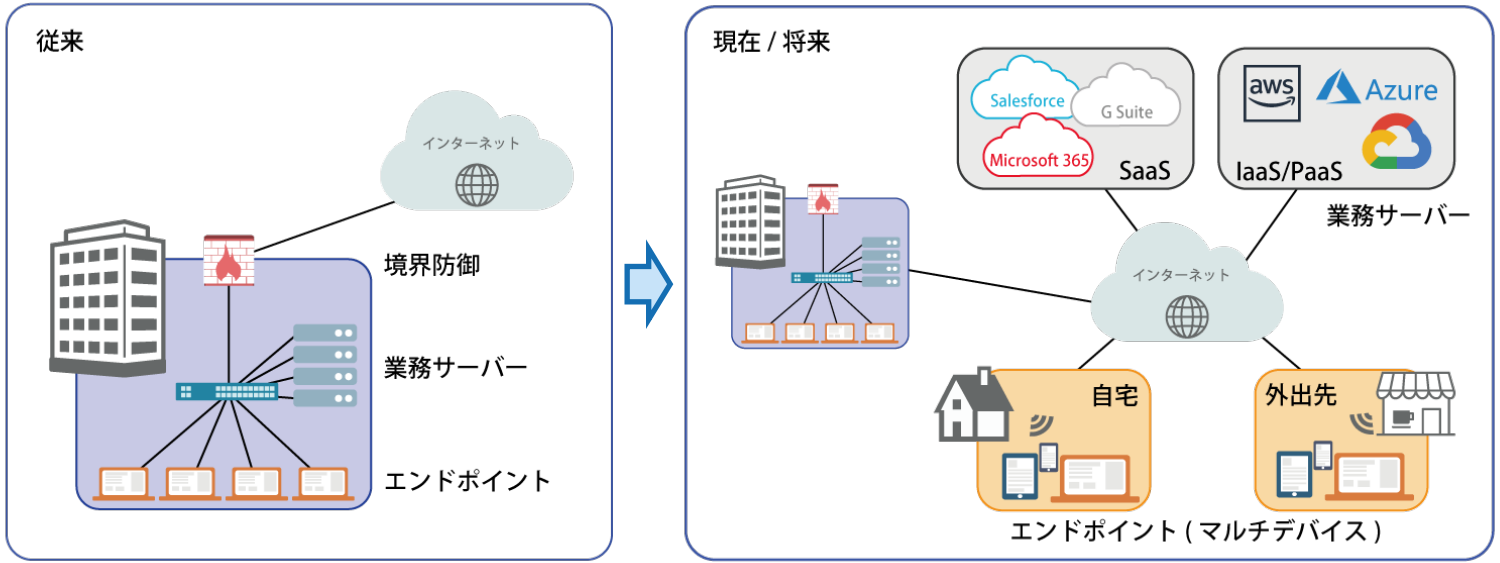
AWS上でネイティブに構築

200PB+

管理データ総量

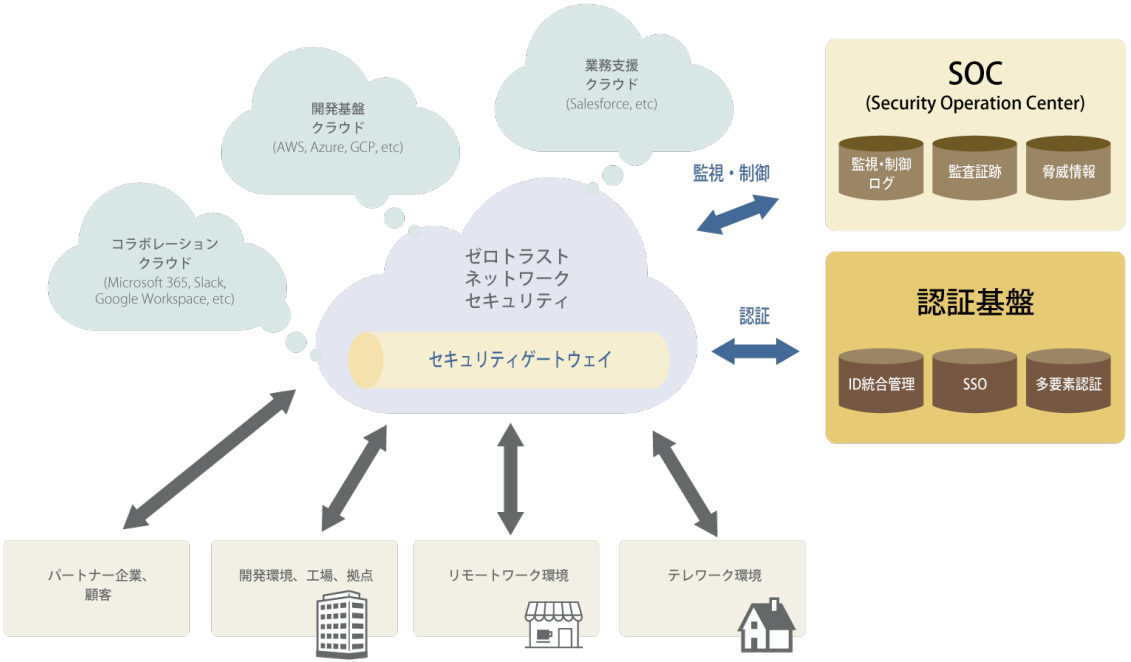
ITインフラの変化

- COVID-19によりテレワークが増加
- クラウドファースト戦略、複数SaaSの導入、ハイブリッドクラウド環境
- マルチデバイスによるリモートワークフォース



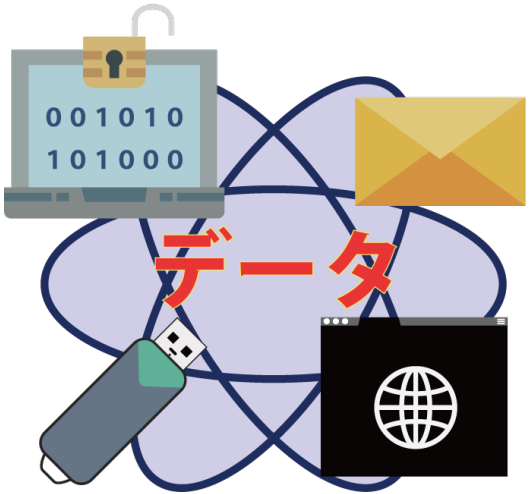
ゼロトラストアーキテクチャの実装

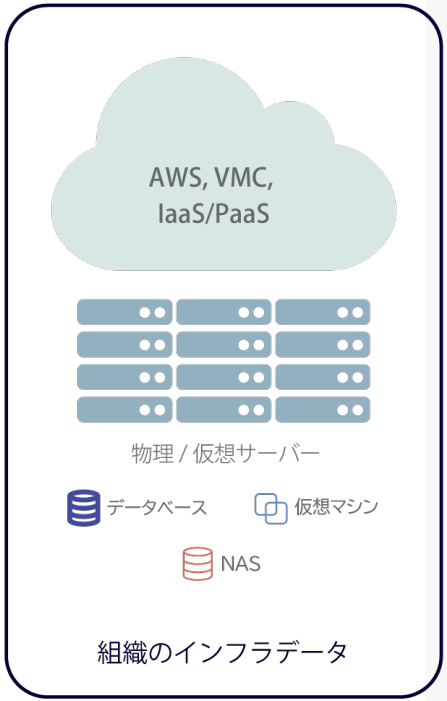
- 組織内部・外部ネットワークの概念をなくす
- すべてのデバイス・人が同じリスクを持つものとして認証・アクセス制御



守るべきものはデータ

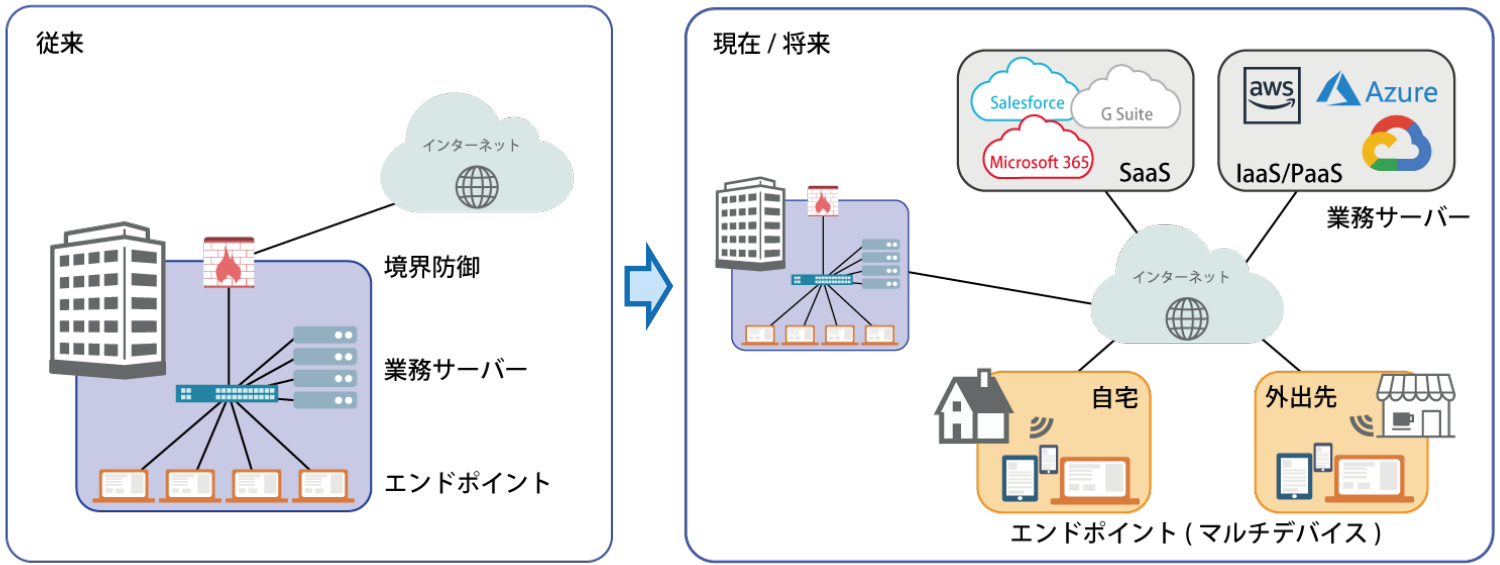
- クラウドと端末（マシン）上のデータ
  - 多くのデータがクラウドへ
  - IoTによりエンドポイント数も急増
- さまざまなリソース上のデータ保護が必須



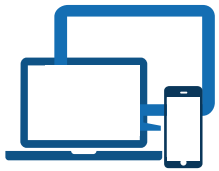


インフラの変化に合わせたデータ保護・統制が必要

- 従来はファイルサーバーや業務サーバーのデータのみバックアップ
- 今後はクラウド上を含めた全リソース上のデータを対象に



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

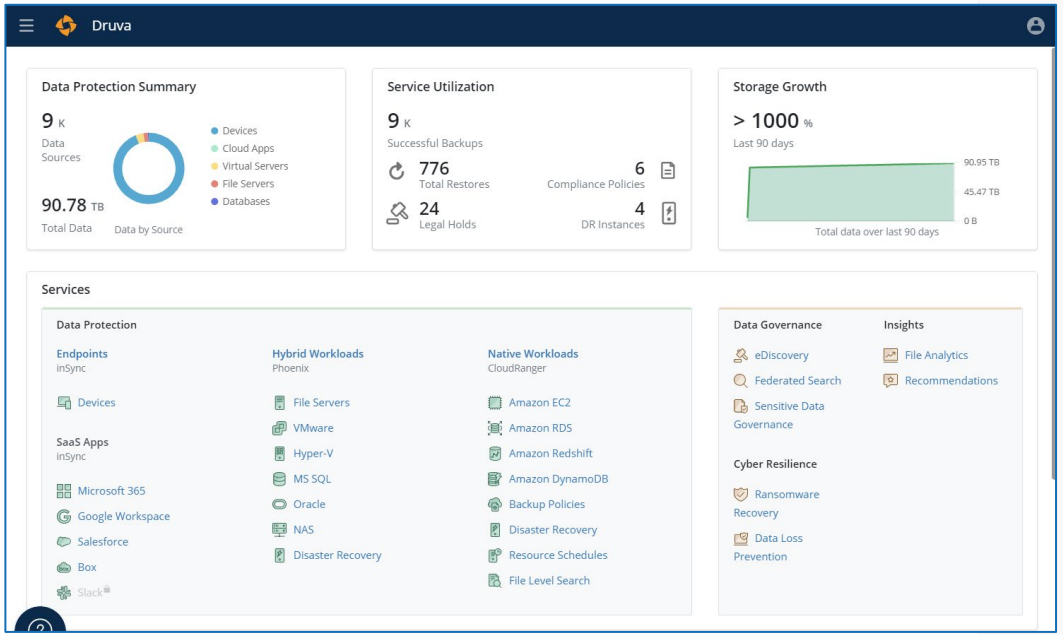
データセンター & リモートオフィス

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

CloudRanger

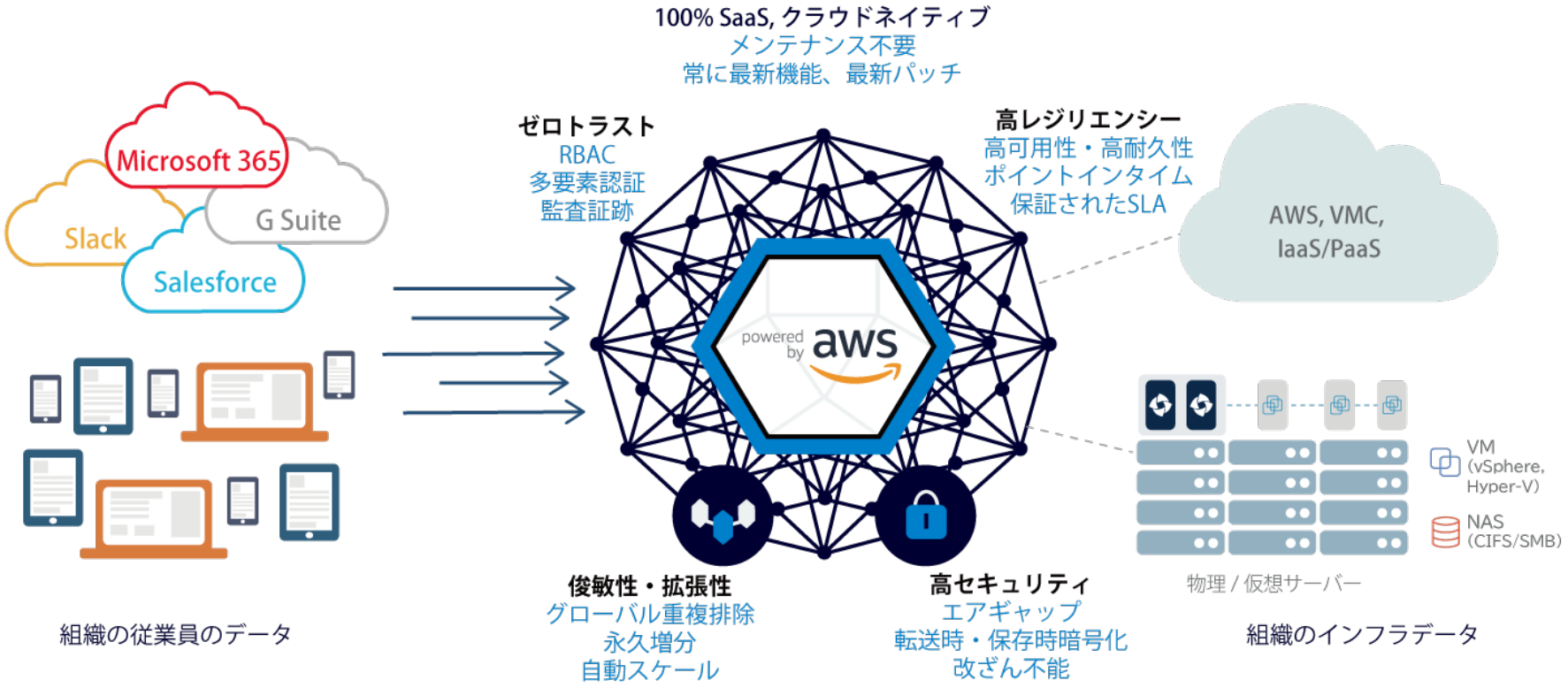
AWS クラウドワークロード

EC2, EBS, RDS, Redshift

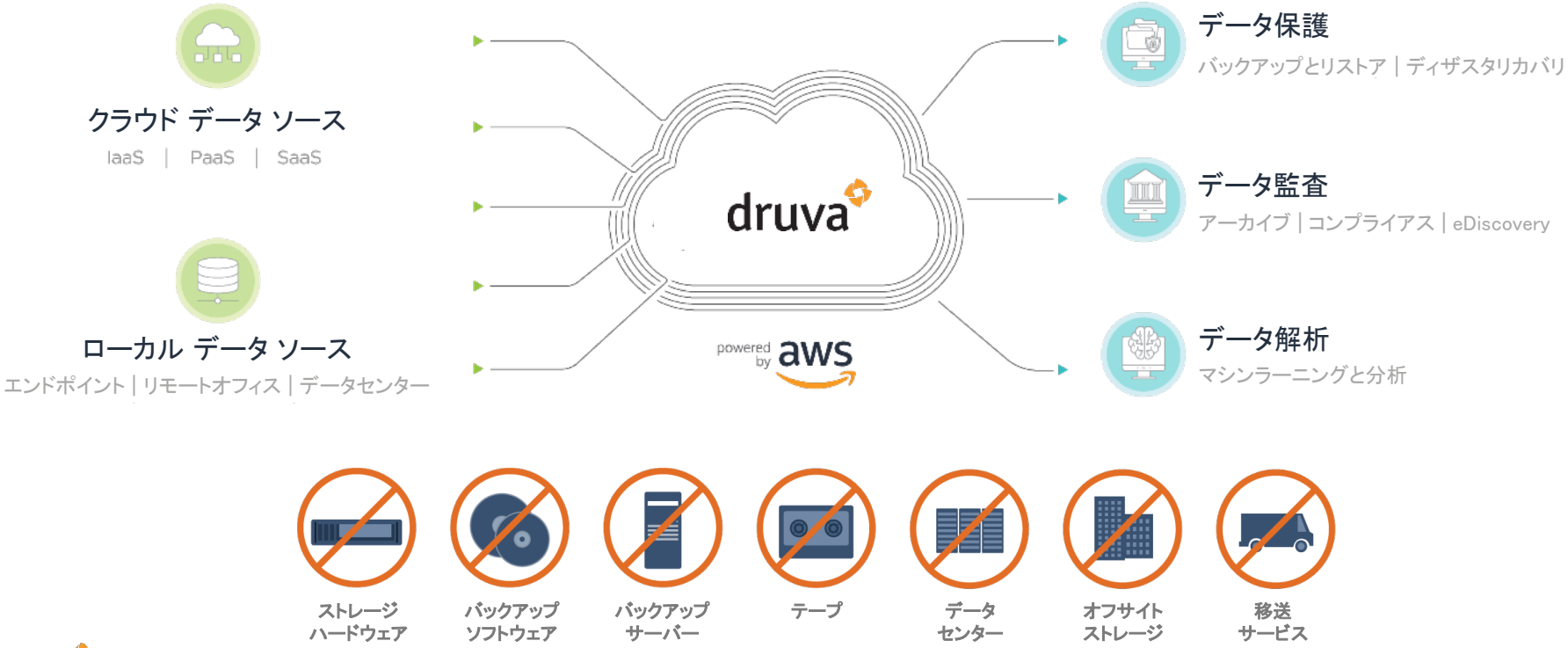


druva

Druvaデータ保護ソリューション

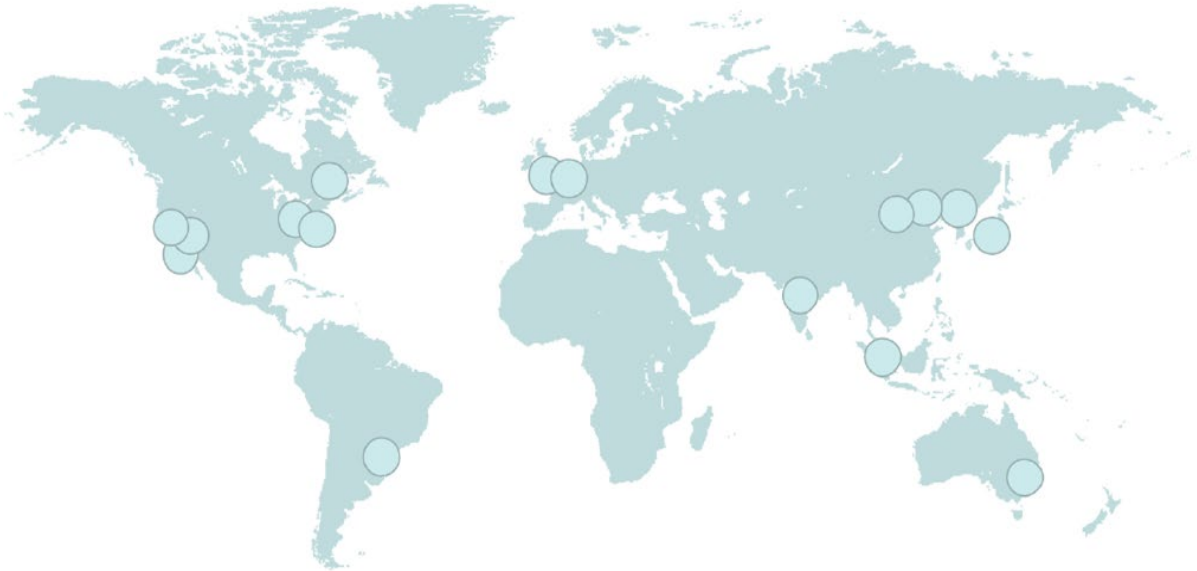


DMaaS – サービスとしてのデータ保護



ユーザーごとにAWSリージョンを指定可能

US East (N. Virginia)
US West (N. California)
US West (Oregon)
Asia Pacific (Mumbai)
Asia Pacific (Singapore)
Asia Pacific (Sydney)
Asia Pacific (Tokyo)
Canada (Central)
Europe (Frankfurt)
Europe (Ireland)
Europe (London)
Europe (Paris)
South America (Sao Paulo)
AWS GovCloud (US-West)



スナップショットの作られ方

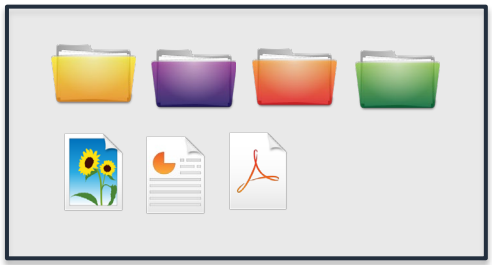
（1日1回の例）

inSyncクラウド

バックアップポリシー
（プロファイル）

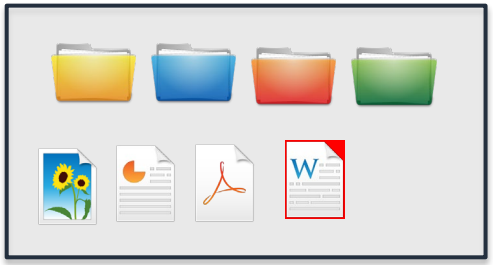
inSyncクライアント

2020/7/1



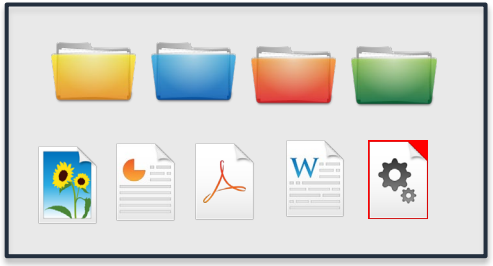
1日目:
初期バックアップ
（フルバックアップ）

2020/7/2



2日目:
差分バックアップ

2020/7/3

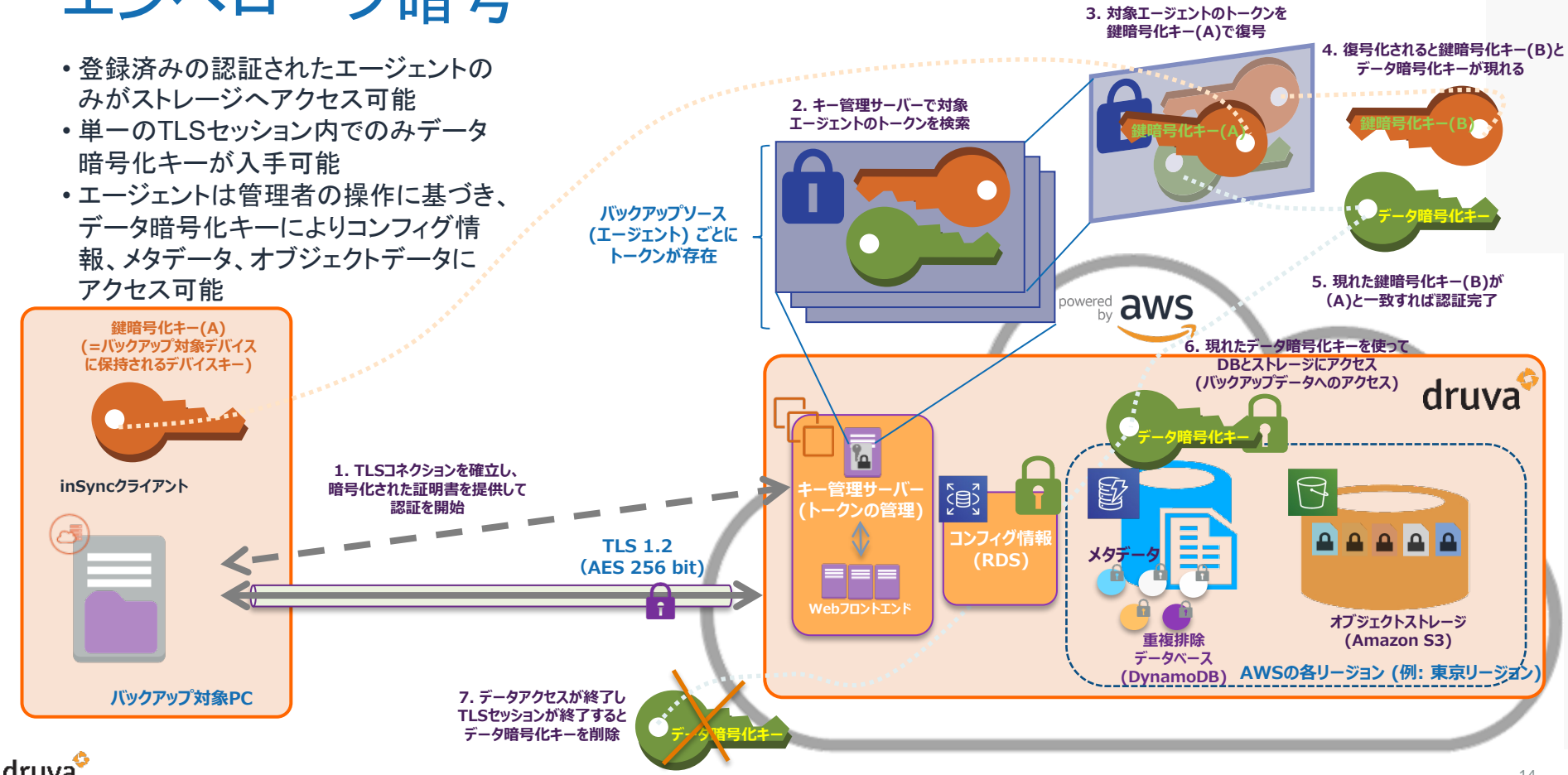


3日目:
差分バックアップ

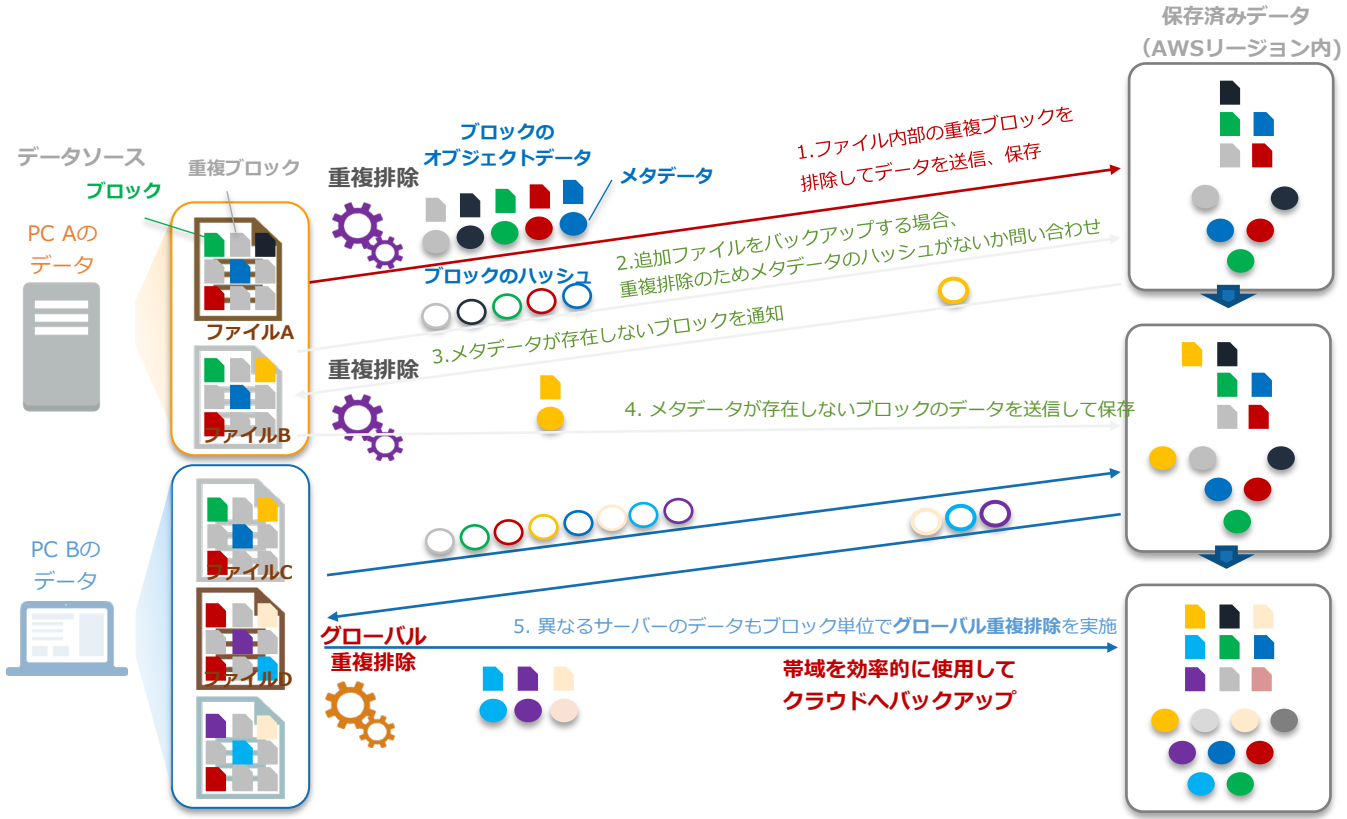
druva

エンベロープ暗号

- 登録済みの認証されたエージェントのみがストレージへアクセス可能
- 単一のTLSセッション内でのみデータ暗号化キーが入手可能
- エージェントは管理者の操作に基づき、データ暗号化キーによりコンフィグ情報、メタデータ、オブジェクトデータにアクセス可能



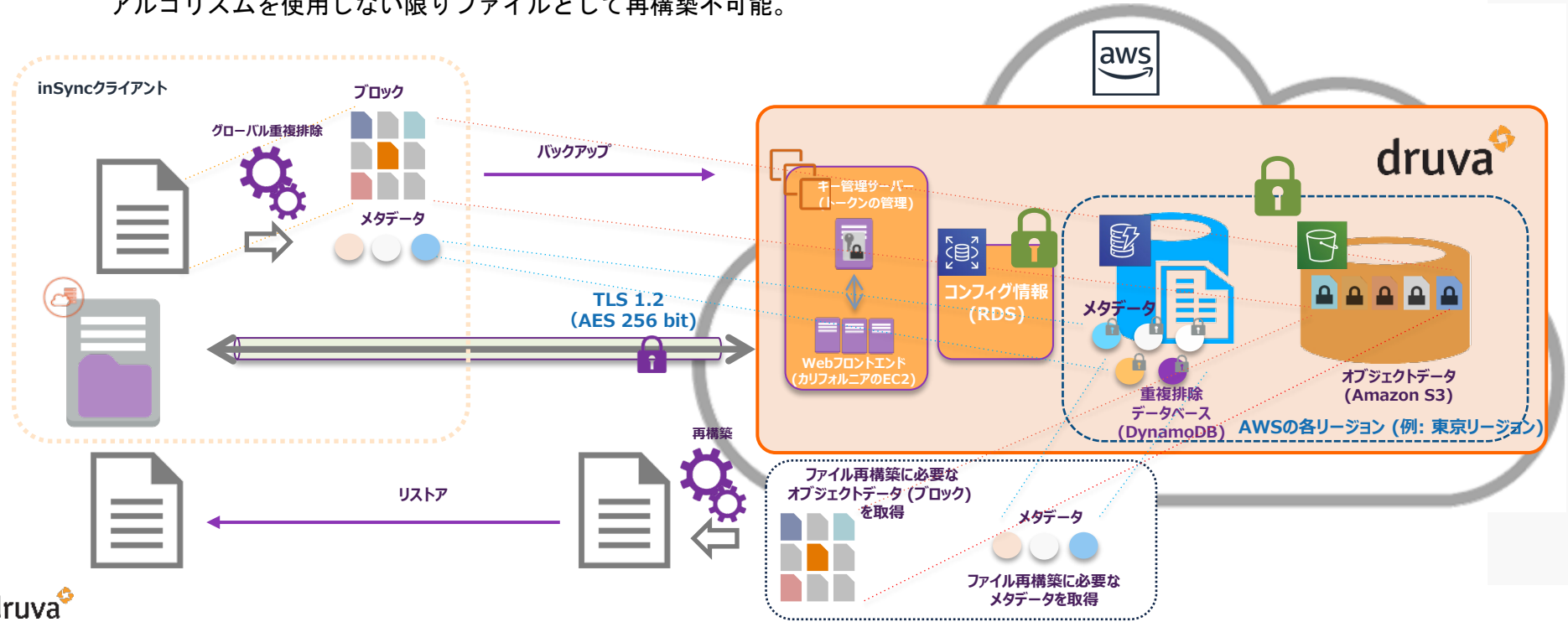
グローバル重複排除の流れ



1. 最初にファイルAがバックアップされるとする。Aはユニークなブロックのハッシュ値をエージェント内のローカルDBに記録し、その後Phoenixクラウドへデータを転送(オブジェクトデータはS3に、メタデータはDynamo DBに)
2. 次にファイルBがバックアップされるとする。まずB内の各ブロックのハッシュ値をエージェント内のローカルDBにないか参照。なければクラウドにハッシュを送る。
3. クラウド側でハッシュをチェック、保存されていないブロックのハッシュをエージェントへ返す
4. 保存されていないブロックのオブジェクトデータとメタデータをクラウドへ転送
5. 同様に、以降のバックアップでも最初にブロック単位のハッシュのやり取りが行われ、クラウドに保存されてないブロックのデータのみが転送される

ファイルデータの難読化

- バックアップされるファイルはブロック化され、ブロック単位で重複排除が行われ、クラウドに存在しないブロックのみがクラウドへ転送、保存される
- 登録済みの認証された管理者からの要求に基づき、登録されたエージェントのみへデータ暗号化キーを使ってリストア（ファイルとして取得）可能。またメタデータとオブジェクトデータが完全に分離（難読化）されており、Druvaのアルゴリズムを使用しない限りファイルとして再構築不可能。



最も厳しいプライバシーとセキュリティ認定

- 転送中の暗号化
- デジタルエンベロープ暗号
- DruvaもAWSもお客様の暗号キーやデータにアクセスできない
- Gov Cloud と FedRamp 認定

druva

inSyncのご紹介

inSync - 機能とソリューション

組織の従業員のデータ

エラスティックなクラウドプラットフォーム

拡張性 グローバル重複排除

主要技術

セキュリティ エンベロープ暗号化

機能

- バックアップと復元
- DLP (情報漏えい対策)
- ファイル/メールのメタデータ検索
- 訴訟ホールド/eDiscovery対応
- 自動コンプライアンス監視
- 振舞検知 / 指定ファイル削除

ITソリューション

- デバイス更改 / OS移行
- ランサムウェア対策

可視化と制御

inSync - 対処できる課題

		失われるリスク	inSync対応機能
1	データの誤削除/破損 デバイス紛失	知的財産 / 生産性	バックアップ、リストア、 情報漏えい防御
2	ランサムウェア	収益 / 風評 / 知財 / 生産性	リストア、振舞検知
3	訴訟とeDiscovery	法務とコンプ ライアンスの コスト	訴訟ホールド、 eDiscovery
4	コンプライアンス	罰金 / 風評 / コスト	横断検索、監査証跡、 自動コンプライアンス追跡 指定ファイル削除
5	デバイスとOS更改	コスト / 作業中断	リストア、 ペルソナバックアップ

Microsoft 365 のバックアップ

- Microsoft 365 の責任共有モデル
  - Microsoft: Microsoft 365のパフォーマンスと可用性の管理責任
  - 顧客: Microsoft 365データの保護と長期保存に責任
- M365障害時、一括リカバリ必要時への対応
- 「ごみ箱」はデータ保護ではない
  - 期間制限、簡単に削除可能、リカバリが複雑、サポートされないコンテンツ
- 3-2-1ルールに非対応 (分離/不変でない)
  - 3つのコピー、2つを別メディア、1つをリモートに:データ保護のベストプラクティス
- 悪意ある削除、リストアによるデータ喪失に対処できない
- マルウェアや破損ファイルの同期による伝播
- 退職社員データの保全、訴訟ホールド/eDiscovery対応
- Microsoft 365 (OneDrive等) はバックアップツールではない

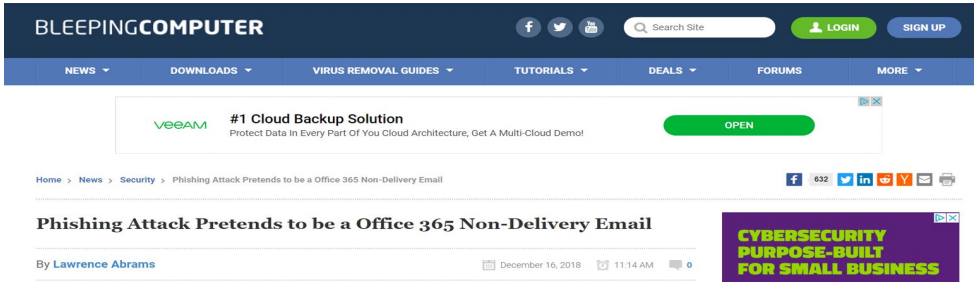
Microsoft 365はランサムウェアの攻撃対象になるか?


June 27, 2016

Microsoft Office 365 hit with massive Cerber ransomware attack, report

Updated: Millions of Microsoft Office 365 users were potentially exposed to a massive zero-day Cerber ransomware attack last week that not only included a ransom note, but an audio warning

Microsoft Office 365


BLEEPINGCOMPUTER

Search Site LOGIN SIGN UP

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS FORUMS MORE

veeam #1 Cloud Backup Solution
Protect Data In Every Part Of You Cloud Architecture, Get A Multi-Cloud Demo! OPEN

Home > News > Security > Phishing Attack Pretends to be a Office 365 Non-Delivery Email

Phishing Attack Pretends to be a Office 365 Non-Delivery Email

By Lawrence Abrams December 16, 2018 11:14 AM

CYBERSECURITY PURPOSE-BUILT FOR SMALL BUSINESS

- **Microsoft 365は、バックアップベンダーを使用してデータを保存することを推奨**

  *“一部のランサムウェアはバックアップ バージョンを暗号化または削除します。そのため、ファイルの履歴やシステム保護を使用してファイルを復元することはできません。その場合は、次のセクションで説明するように、ランサムウェアやマルウェアの影響を受けOneDriveデバイスでバックアップを使用する必要があります。”**

- **Gartnerは、ランサムウェア攻撃から復旧するためにSaaSアプリのバックアップソリューション要件を強調**

  *“現在および将来のOffice365の顧客は、包括的なバックアップおよび復元プロセスがOffice365サブスクリプションに含まれていると考えがちです。この仮説は正しくありません。Gartnerのクライアントは、ランサムウェアによるリカバリの試行の失敗とデータの損失を報告しています...”***

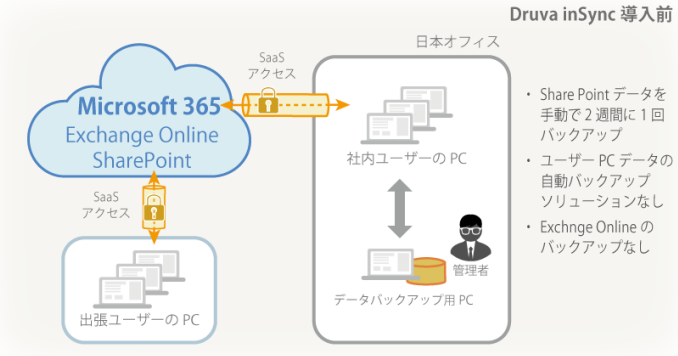
- **英国の国家サイバーセキュリティセンター（NCSC）のような政府のセキュリティ機関は、データの保存にOne Driveのみを使うことに対して警告しています。**

  *“NCSCは、クラウド同期サービス（Dropbox、OneDrive、SharePoint、Googleドライブなど）を唯一のバックアップとして使用すべきではないと警告しました。ファイルが「ランサムウェア被害」に遭った直後に自動的に同期する場合、その時点で同期されたコピーも失われます。"***

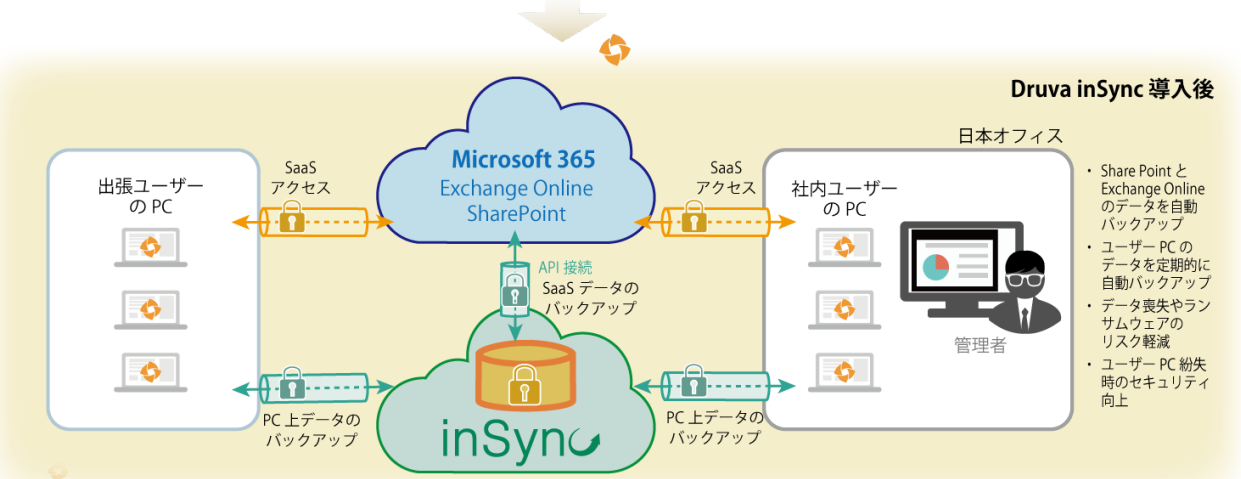
*ユーザーのランサムウェア攻撃から回復Microsoft 365
**When to Leverage Third-Party Solutions to Back Up Office 365 - Gartner
***Ransomware victims thought their backups were safe. They were wrong

druva

事例: ネオファーマ ジャパン様



ネオファーマジャパン株式会社 医薬開発部
左から、富岡氏、児玉氏、中園氏

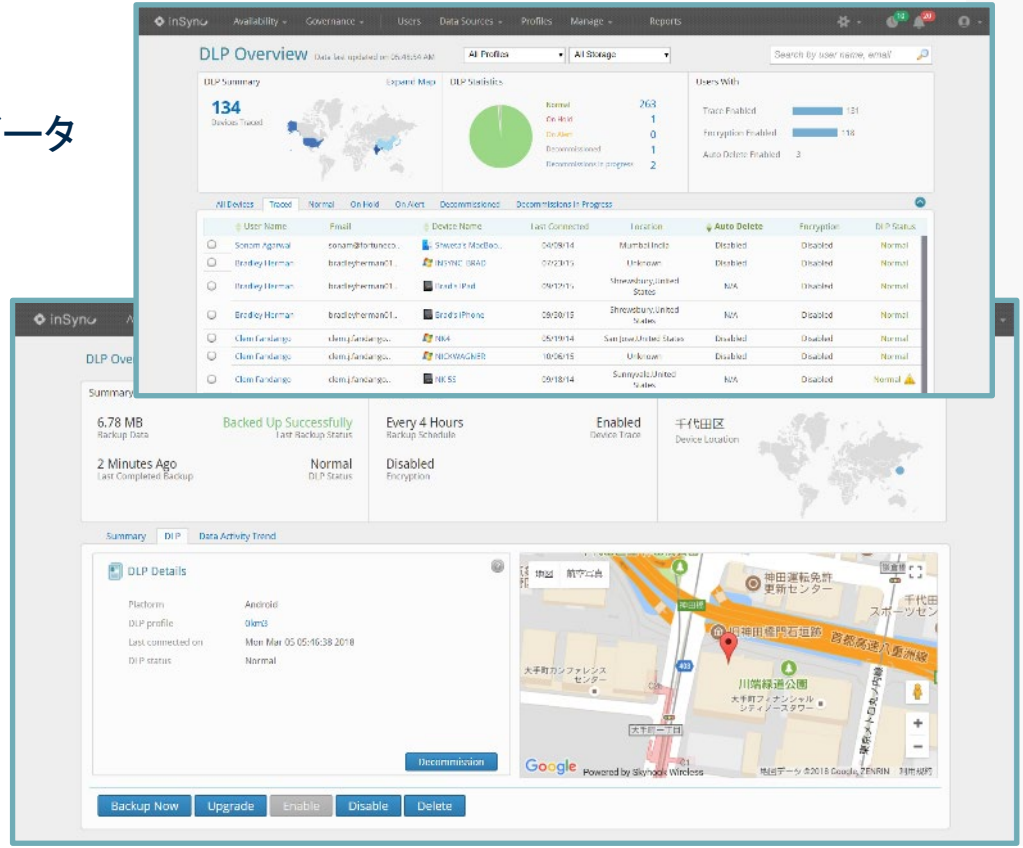


- オンプレサーバーは持たずOffice 365を活用
- 従来SharePointデータを手動でバックアップ
- 製薬業界ではさまざまなデータ規制が存在
- 全PC、Exchange Onlineを含め自動バックアップが可能に
- 退職社員向けにも長期間データ保全が可能
- デバイス紛失時の情報漏えい対策も可能に

druva

エンドポイント向け情報漏えい対策 (DLP)

- 正確な位置情報追跡
- 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内訳がわかる
  - 再取得時に容易に復元
- デバイス上でのファイル強制暗号化
  - Windows EFS
- モバイルデバイスのコンテナ制御



druva

事例: ファイザー製薬

課題

- エンドポイントバックアップの不足に対処
- システム移行
- 法務データの取り扱い

結果

- 110,000人の従業員を保護
- セルフサービスのリストア
- 自動化されたシステム移行
- ワンステップの訴訟ホールド

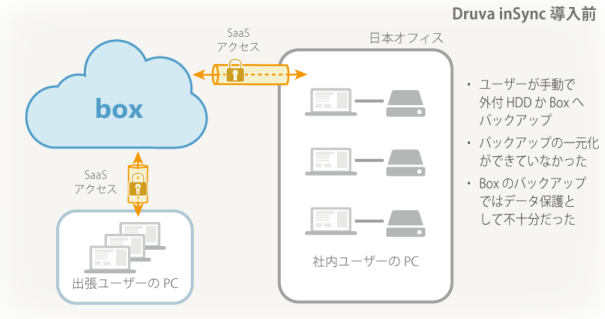
データ監査: 個人情報保護法 令和2年改正案対応

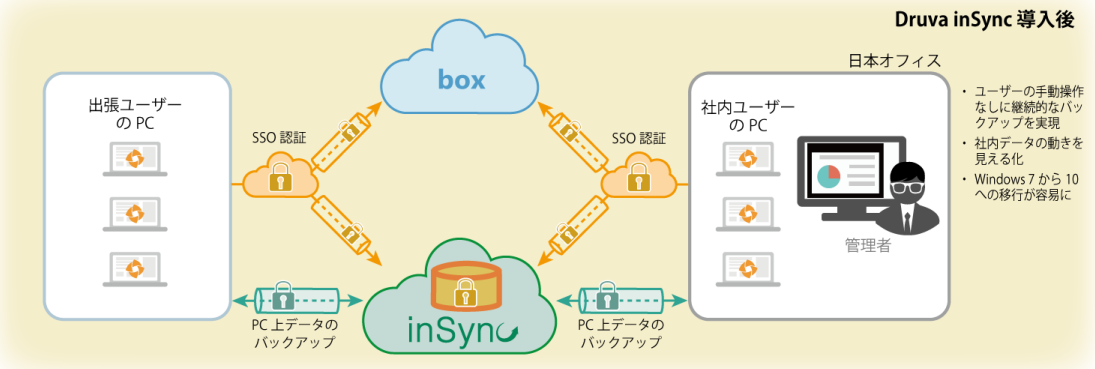
- 個人情報の不適正な方法による利用禁止
- 一定以上の漏えい等が起きた場合、国への報告と本人への通知が義務化
- 本人からの開示請求可能範囲が拡大
  - 利用停止、消去、第三者提供停止
- 命令違反や不正提供の罰金は最大1億円

Druvaによる個人情報保護法対応

- データの可視化
  - データが存在する場所の可視化
- 情報ガバナンス
  - 組織内に分散したデータを一か所に集約して捕捉
- データモニタリング
  - 横断検索とプロアクティブコンプライアンス
- セキュアな転送
  - TLS 1.2 / AES 256 を使った暗号化
- 忘れられる権利への対応
  - 個人情報の削除要求に応じられる機能

事例: ADK ONE (旧ADKアーツ) 様





- PC内のローカルデータ保護 (ISMSの要求事項)
- PCでSSDが壊れるケースや初期ロット不良があった
  - 復旧サービスが高価、代替マシンが必要
- 個人情報不正取扱や不正会計処理発生時、過去を含めて改ざんのない形で追跡できるように
- 導入後、Win7からWin10への移行プロジェクト
  - ディスクコピーだと3時間かかる、外注が高価、トラブルリスク

druva

inSync導入の流れ

プロファイル作成

- バックアップコンテンツ
- バックアップスケジュール
- 保存期間
- ユーザー認証方法
- リソース制御 (CPU, 帯域)
- DLP
- ユーザー操作の制御

ユーザー作成

- プロファイル割り当て
- リージョン割り当て
- ローカル認証、AD/LDAP認証、シングルサインオン
- 個別登録、CSV一括登録
- AD/LDAPインポート
- SCIM連携

クライアントインストール

- 実行ファイルのダウンロードとインストール
- アクティベーション

バックアップ

- スケジュールバックアップ
- ユーザーによる即時実行
- 管理者による即時実行

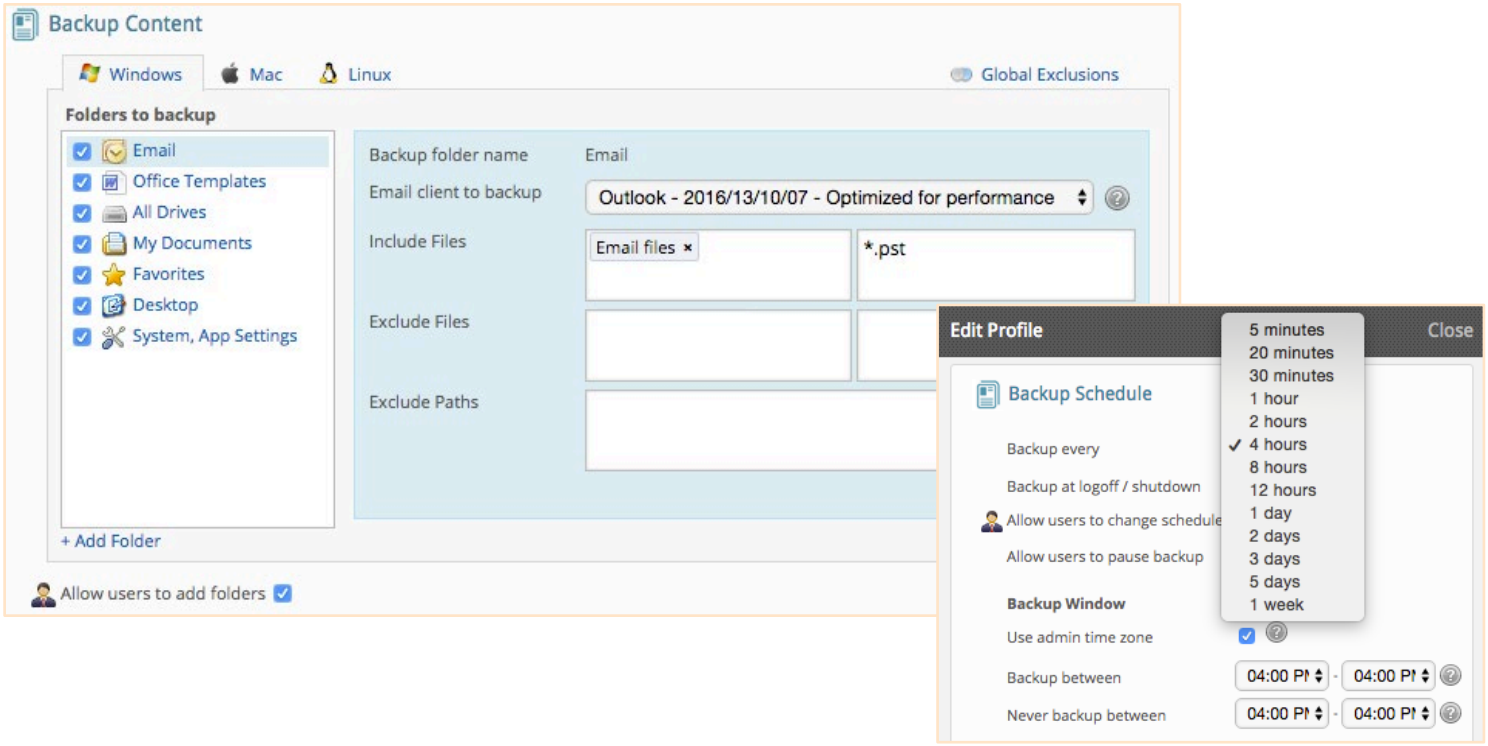
監視

- ダッシュボード、レポート
- 監査証跡
- 横断検索
- 振舞検知、防衛的削除

リストア

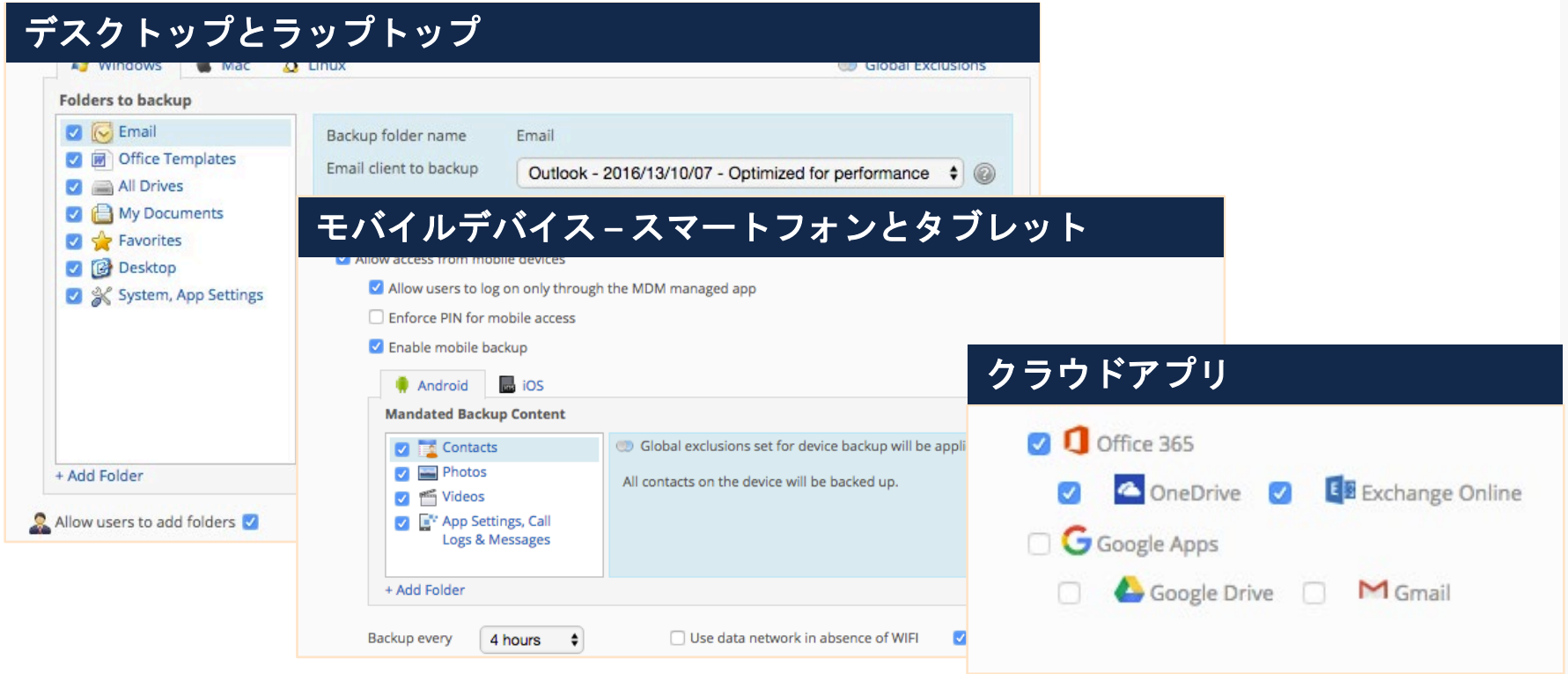
- ユーザーがクライアントソフトから復元
- ユーザーがブラウザから復元 / ダウンロード
- 管理者が復元代行 / ダウンロード

制御可能なタイムインデックス化されたバックアップ



druva

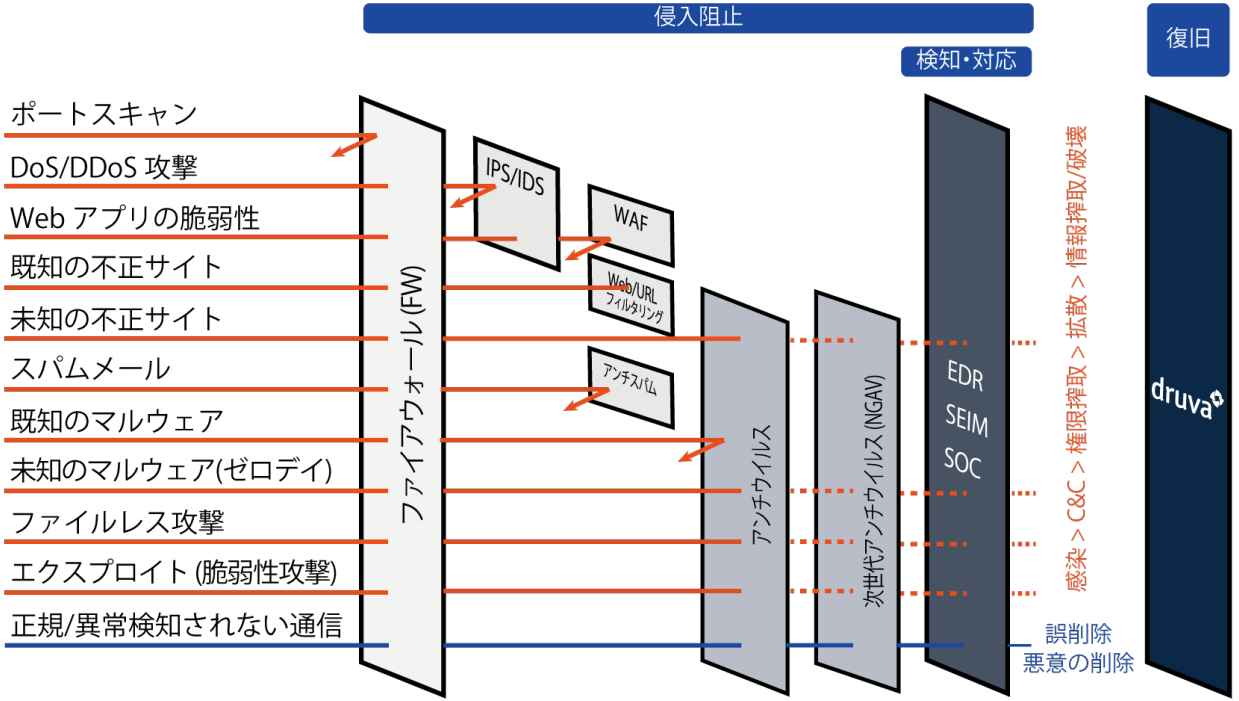
全範囲をバックアップ



druva

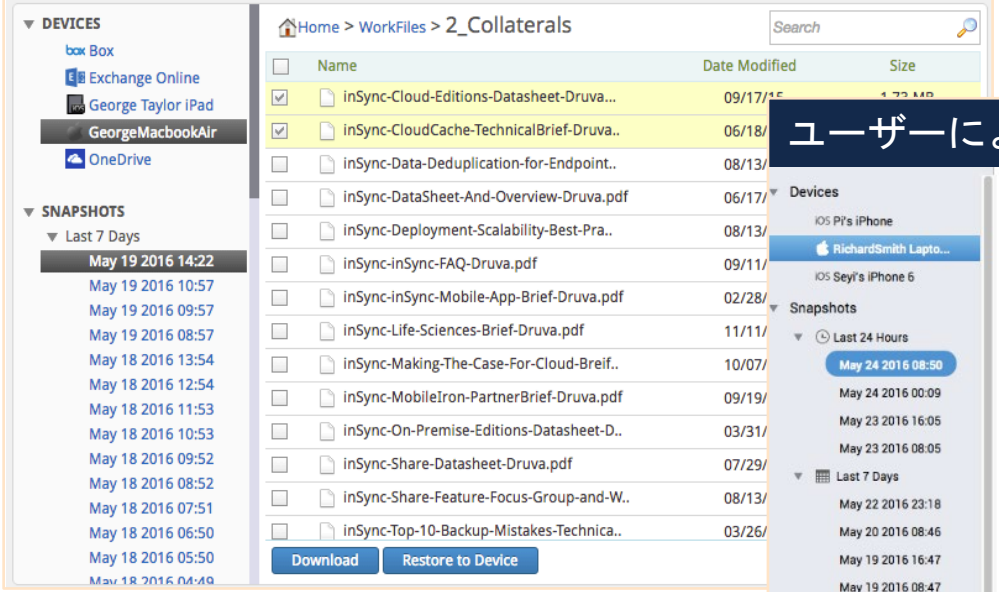
セキュリティの最後の砦

- 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

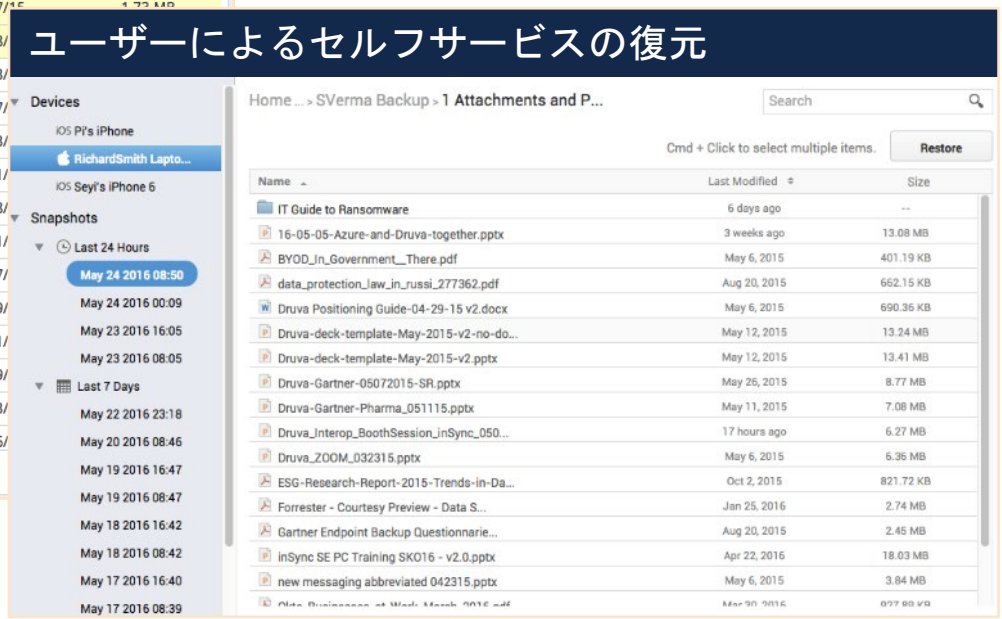


管理者やユーザーによるファイル単位の復元

管理者によるユーザーデータ復元の代行

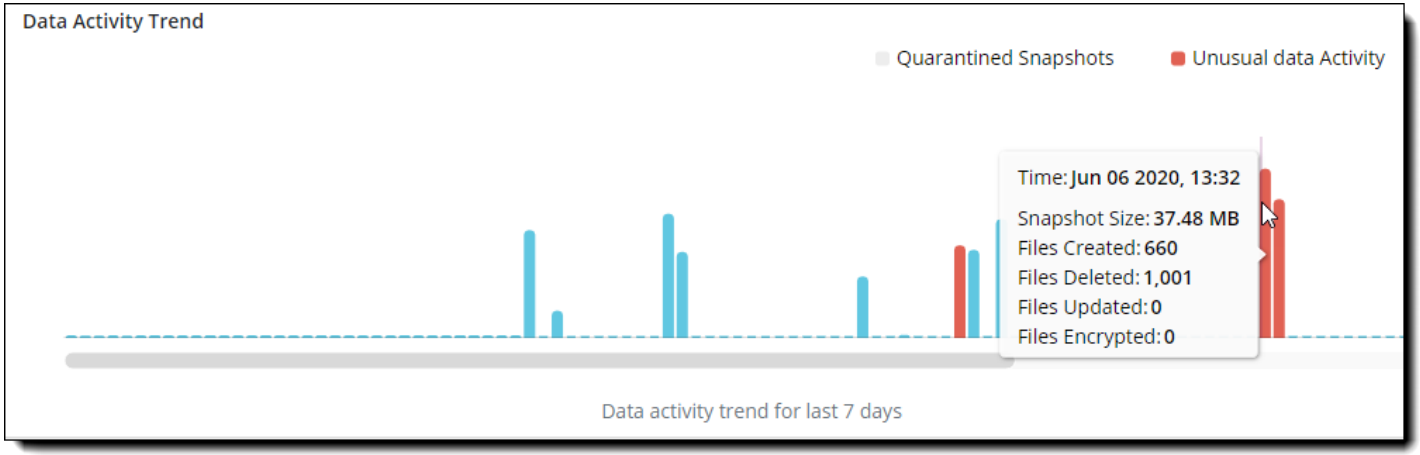


ユーザーによるセルフサービスの復元



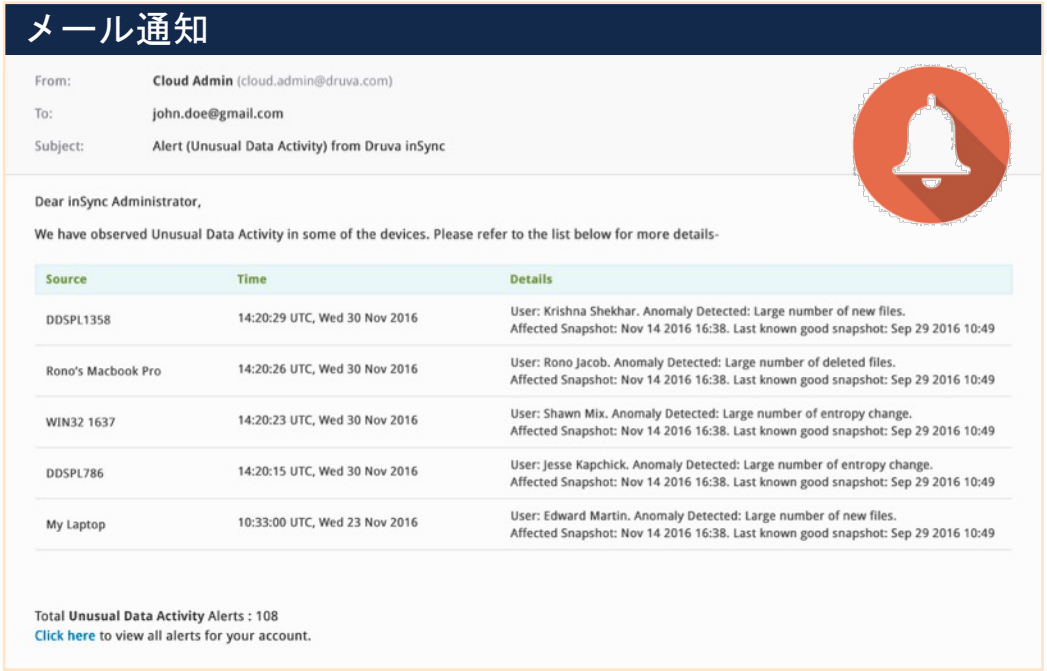
ランサムウェアの容易な検出、対応

- 完全分離された変更不可能なスナップショットにより元データを確実にリカバリ
- 異常データアクティビティの監視と潜在的な脅威に対するIT部門へのアラート
- 検疫機能: 影響あるファイル/端末のリストア制限、スナップショット削除
- リストア時のアンチウイルススキャン、ハッシュによるファイル除外
- 横断検索機能により情報セキュリティ部門の調査と対処を実現



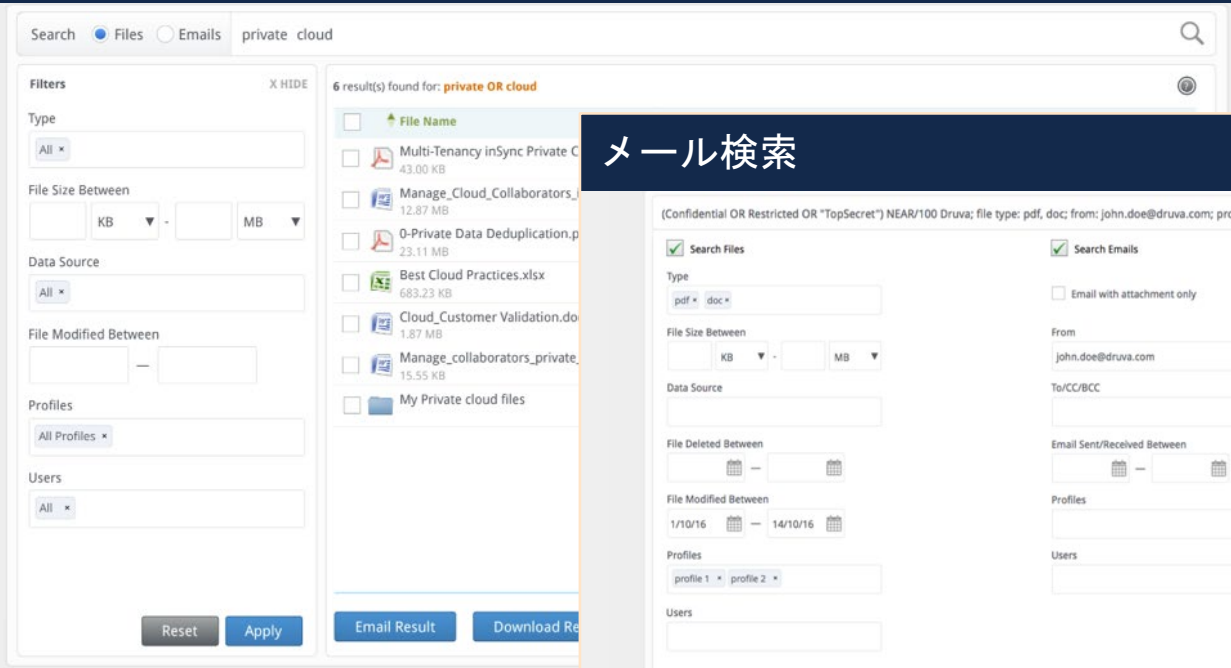
レポートと通知

- データ操作の通知
  - ファイル削除
  - ファイル変更
  - ファイル暗号化



ファイルとメールの横断検索

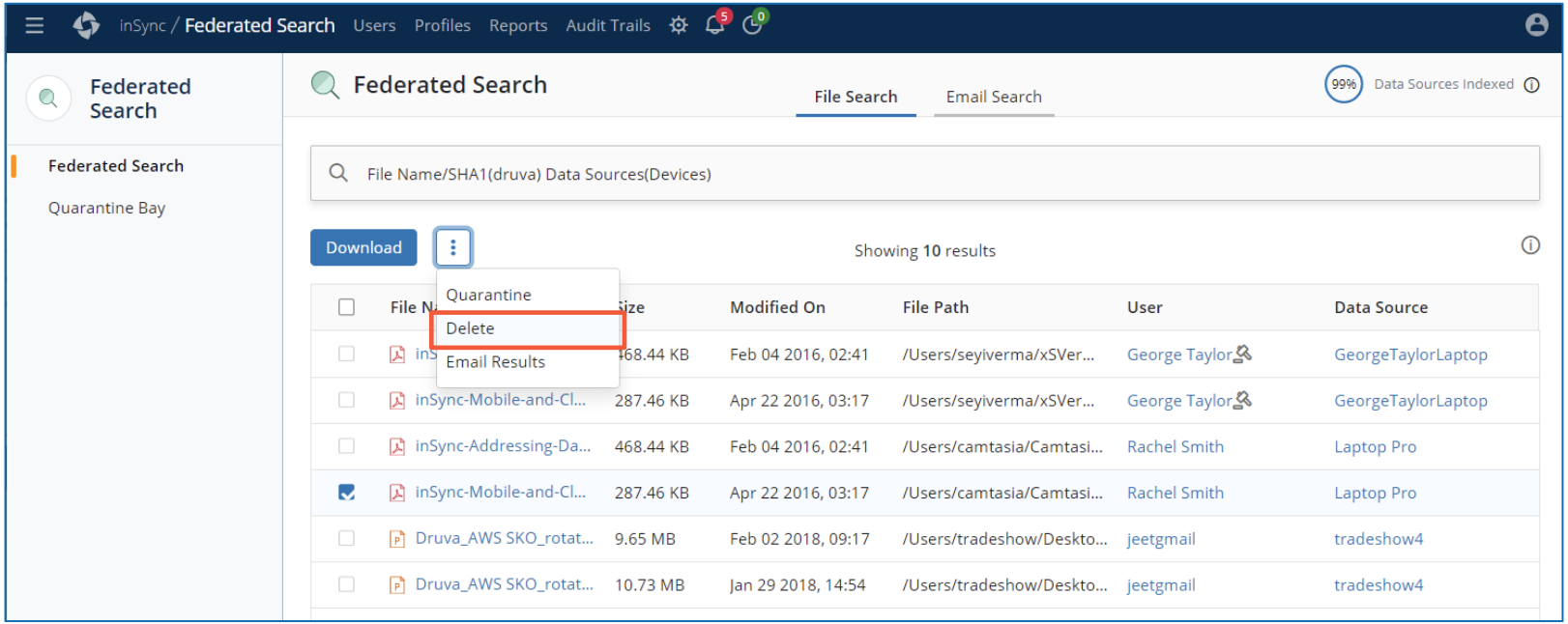
横断メタデータ検索



メール検索

druva

マルウェア (ランサムウェア) 感染ファイルの削除



druva

大量データ損失 / 破損対策への応用

マルウェア

恒久的なデータ損失の可能性ある
ランサムウェアやその他の標的型攻撃

退社する社員

社員が退職する際の知的財産
盗難や削除の可能性

悪意ある内部者

たとえば不満を持った従業員や
悪意を持った請負業者

事故による削除

誤った情報の上書きや
共有フォルダの誤削除

druva

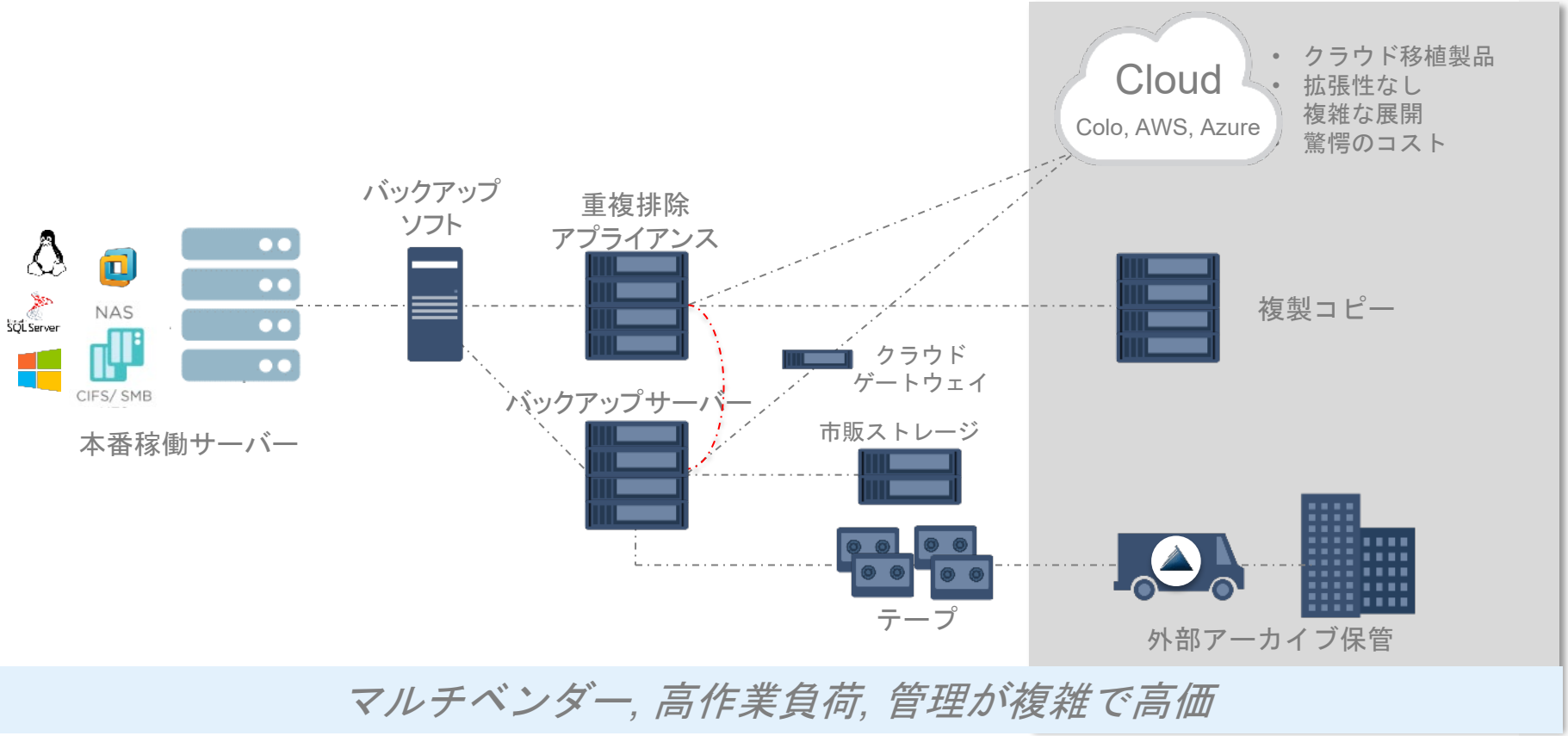
inSyncのエディション

	Enterprise	Elite
データソースごとのデータ保護（バックアップ、リストア、アーカイブ）		
エンドポイントデバイス Windows、Mac OS X、Linux、Android、iOS	○	○
Microsoft 365（Exchange Online, OneDrive, SharePoint Online, Teams）/ Google Workspace（Gmail, Google Drive, Google Share Drive）	○	○
Salesforce.com 自動日次バックアップ、メタデータリストア、複数 Organization	○	○
情報ガバナンス機能（全データソース向け）		
メタデータによるファイル / メールの検索 ファイルおよびメールのメタデータ横断検索、検疫、削除		●
eDiscovery 対応 訴訟ホールド、事前カリング選別、HTTPS コネクタ		●
自動コンプライアンス監視 コンプライアンステンプレート、機密データ全文検索、違反レポート、違反アラート	オプション	オプション
導入と管理向けの拡張機能（全データソース向け）		
複数リージョン選択 / Microsoft Active Directory（AD）連携 / シングルサインオン / SCIM 連携 / 管理者ロール	●	●
退職者用ライセンス 退社したユーザーのデータ保持	● ※1	● ※1
エンドポイント向けの拡張機能		
デバイス更改 / OS 移行 / MDM 連携 MobileIron、AirWatch、Mass360 との連携	●	●
情報漏えい対策（DLP） 位置情報追跡、ファイル強制暗号化、リモートワイプ、自動削除	●	●
統合一括導入 msi ファイル配布後のサイレントインストール	●	●
ランサムウェア対策 異常振舞検知、SIEM 連携、スナップショットの検疫とマルウェアスキャン	オプション	オプション

druva

Phoenixのご紹介

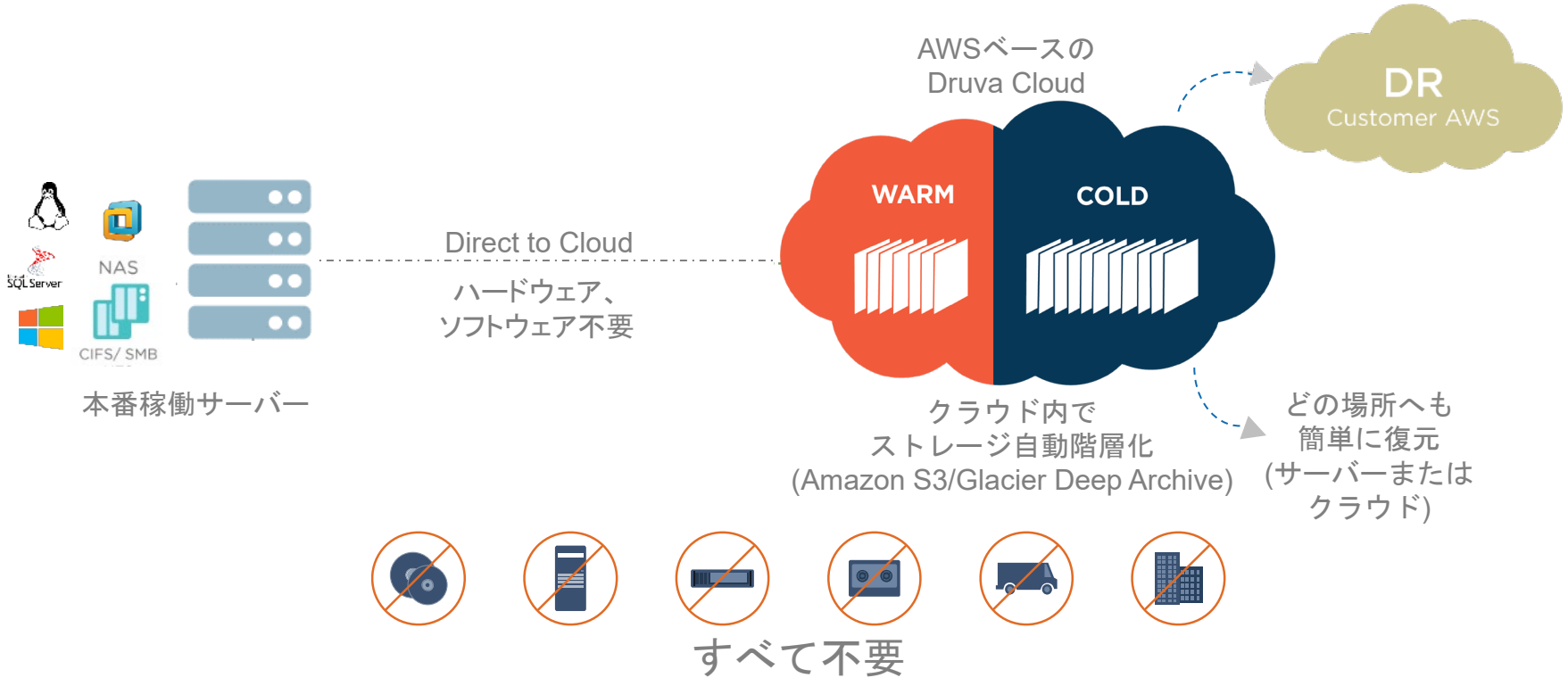
従来のサーバーデータ保護



マルチベンダー, 高作業負荷, 管理が複雑で高価

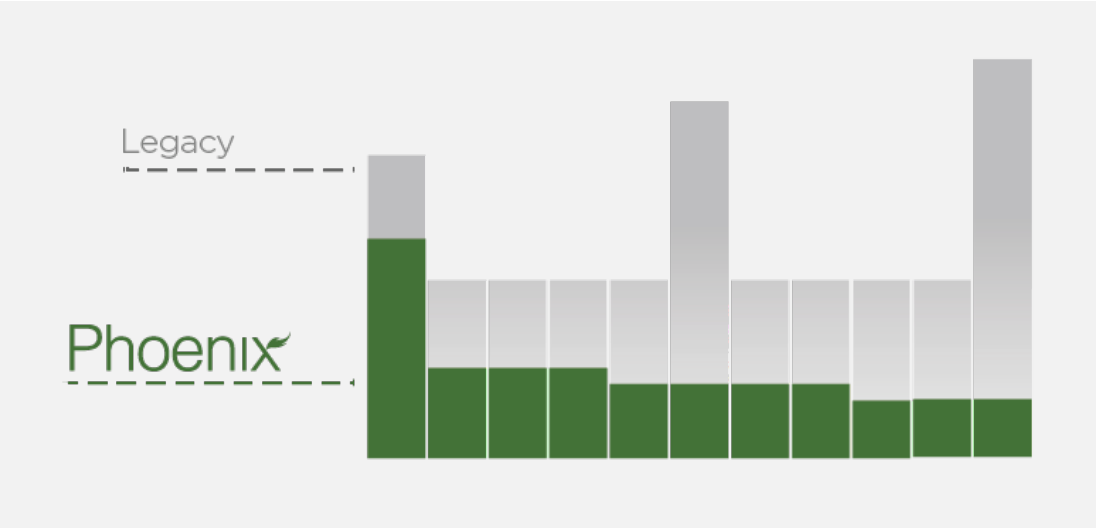
druva

Druva データ保護 – ダイレクトツークラウド (Direct to Cloud)



druva

効率的なストレージ: 最小のバックアップデータ総量



グローバル
重複排除

ボトルネックなしに拡張可能

可変長ブロックの
ソース重複排除

ユニークなデータのみ送信して保存
ストレージと帯域を80%以上削減

定期的な
フルバックアップ不要

永久増分バックアップ
ストレージ削減効果50倍以上

druva

クラウド上で利用された容量のみ課金

完全な対容量使用率

- 最小の総量 – グローバル重複排除
- オンデマンドの拡張性
- データが保存されるほど削減されていく
- 購入容量の無駄遣いが一切ない

従来

Phoenix

Phoenixのバックアップ対象

- ファイルサーバー: Linux, Windows Server (物理、仮想)
  - PhoenixエージェントをOSにインストール
  - ファイルベースのバックアップ
- ハイパーバイザー
  - VMイメージのエージェントレスバックアップ, 自動検出 – vCenter, ESXi, Hyper-V
  - MS-SQLのApplication awareバックアップ
  - VMware向けCloud DRオプション
- データベース: MS SQL , Oracle
  - アプリケーション対応 (動作させながらバックアップ)
- NAS: CIFS/SMB および NFS

ランサムウェア対策機能 (ファイルサーバー、NAS)

- セキュリティ・インサイト・ダッシュボード
  - データアクセス、管理者ログイン、APIリクエスト、異常データ操作の可視化
- 検疫
  - ランサムウェアやマルウェア感染から解決までのスナップショットについて検疫対象とすることでリストア不可に
- 感染時のスナップショット検出
  - リストアに使える暗号化前のスナップショットを提示
- ファイルを復元する前にアンチウイルススキャン
- 各種アラートについて管理者にメール通知
  - SIEMツールと連携

Phoenixのエディション

バックアップ、アーカイブ、DR			
プラン名	Business	Enterprise	Elite
ファイルサーバーのバックアップ Windows Server と Linux のバックアップ	●	●	●
データベースサーバーのバックアップ MS SQL Server / Oracle のアプリ対応バックアップ	●	●	●
VMware / Hyper-V のバックアップ 仮想マシン (VMDK, VMX, VHDX) のバックアップ	●	●	●
NAS 共有のバックアップ CIFS/NFS による NAS のバックアップ	●	●	●
Snowball Edge 連携 大容量の初回バックアップやリストア	●	●	●
クラウドキャッシュ機能 社内サーバーへの一時的な保存による高速化		●	●
マルチサイト管理のサポート サーバーやバックアップポリシーの論理分割		●	●
マルチリージョンのサポート 複数の AWS リージョンが使用可能		●	●
Cloud DRaaS（ディザスタリカバリ） VMware 仮想マシンを顧客 VPC 上で立ち上げ		オプション	●
データの分析と検索			●

Druvaが解決できることとは？

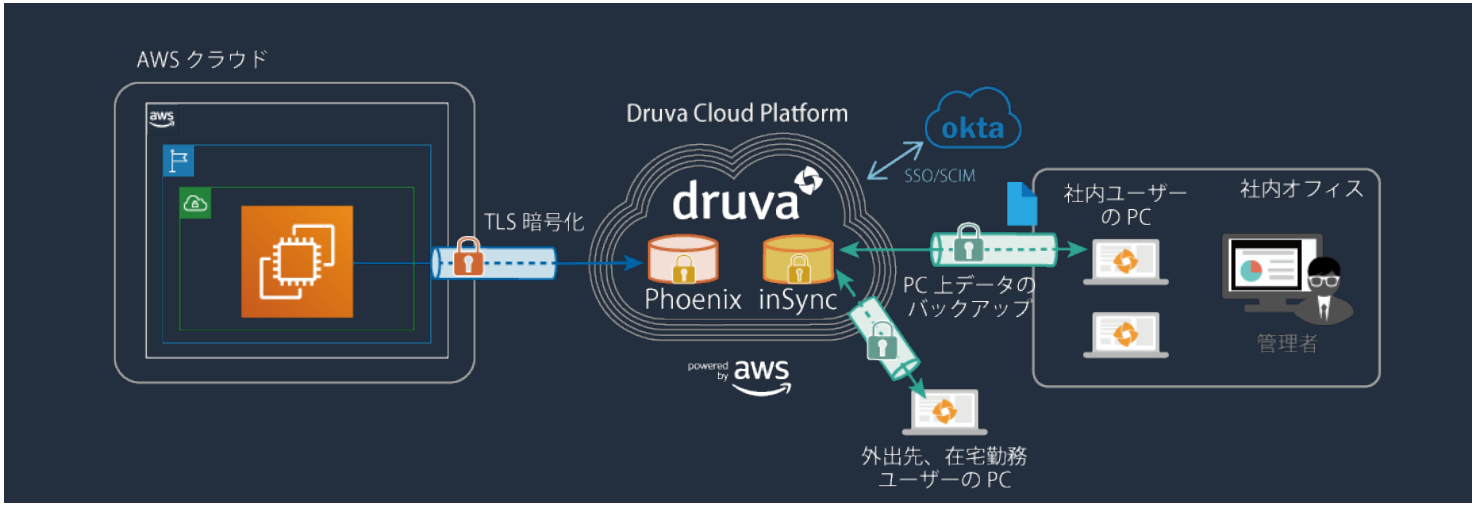
- データ保護のコストを削減し、複雑さを解消する
  - データの総量と重要性が増す中で、管理性を向上し、既存アーキテクチャを簡素化
- サイバーレジリエンスを向上し、コンプライアンスを維持する
  - 組織の従業員とデータ資産を確実に保護し、レスポンス対応
- クラウドプロジェクトの加速と保護を支援する
  - アジリティの高いクラウド中心の環境要件を満たし、実現
  - すでにクラウド上にあるか、移行中であるかは問わない

お客様がなぜDruvaを選んだか

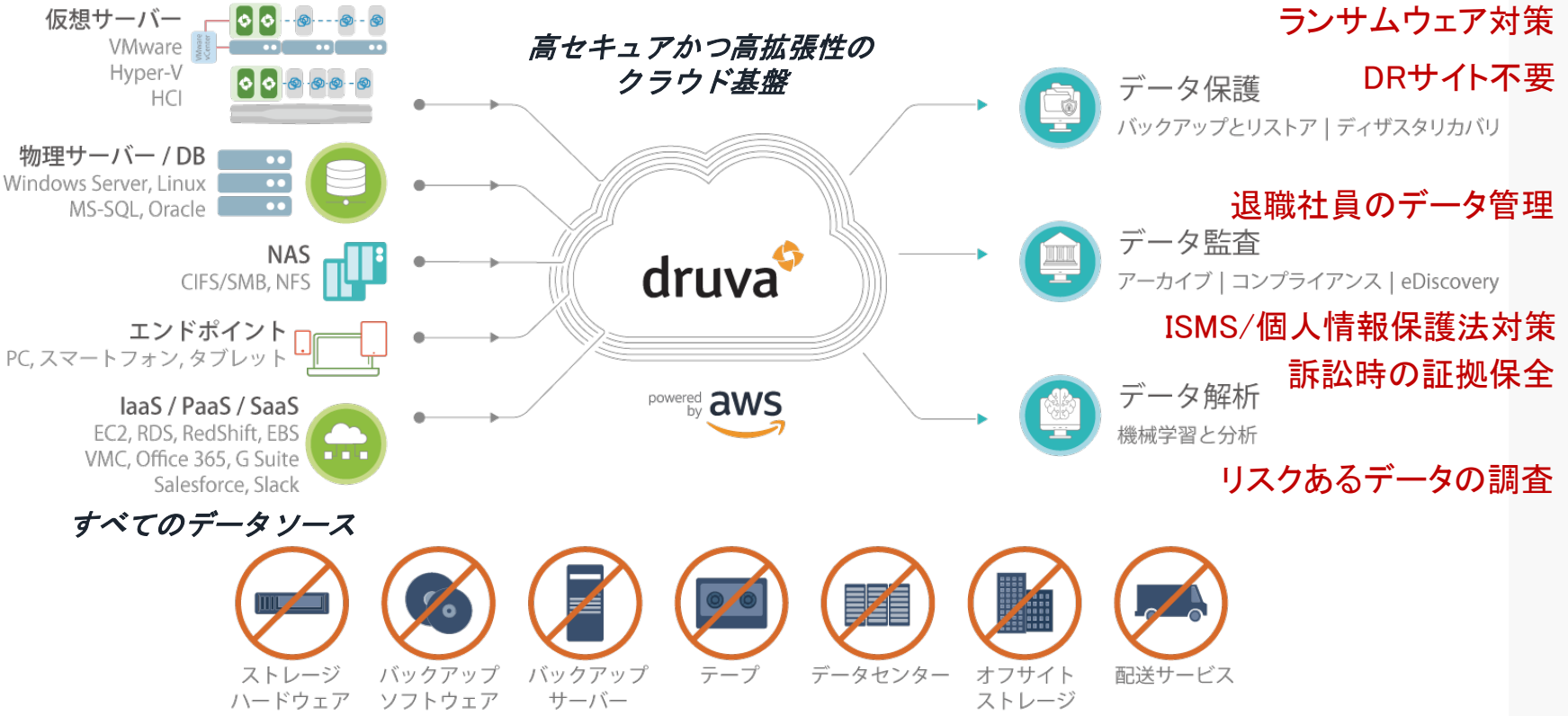
単一プラットフォーム	• 広範なワークロードを単一のプラットフォームで保護、管理できる
信頼性が高い	• ランサムウェア保護 – データ分離 & 改ざん不能 • セキュリティ & プライバシー標準, 暗号化, Fed Ramp
バックアップデータから 別の価値を得られる	• eDiscovery -- コストと時間を削減 • コンプライアンス -- 一元的な監視と違反への対処
簡単な設定管理	• 15分で設定可能な簡単さ • 複数ワークロード全体で単一ダッシュボード
TCO (コスト) 削減	• クラウドでクラウドを保護 • ハードウェア/ソフトウェアのインストール/メンテナンス不要、隔週のアップデート • 自動スケーリング、キャパシティプランニングやクラスタリング不要 • どこからでも管理と利用が可能。WANやVPN通信への影響なし

お客様事例

- 化学系製造業様
  - 課題: データ増加によるバックアップ費用の増大、散在する重要データの一元的な保護ができない、リストアに時間がかかる
  - ソリューション: Phoenix + inSync
  - 結果: 日々の運用管理工数の大幅な削減、バックアップデータの統合的な可視化、ユーザーによるセルフサービスのリストアとスマホ上でPCデータが参照できることによる生産性向上



Druvaクラウドプラットフォーム



Thank you!

www.druva.com/ja/ をご参照ください