rubrik | Zero Trust Data Security™

確実な復旧のために
今求められる
“ゼロトラストな”バックアップ

Rubrik Japan株式会社
セールスエンジニア
中井 大士

ランサムウェアからの復旧/対策事例

復旧成功事例

ダーラム市

- 金曜日にネットワーク全体で感染
- 約80台のサーバーがランサムウェアに感染、市のサービスがダウン

- 週末に感染されていないバックアップデータからサーバーを順次リストア
- 月曜日にはサービスを開始

0%
感染されたバックアップデータ

<2日
システムの復旧にかかった実際の日数

ラングス ビルディング サプライ

- メールを経由して感染。数十万のファイルが暗号化
- ビットコインで約15億円相当の身代金要求

- 感染されていないバックアップデータから24時間以内にすべてのサービスを再開

0%
データロス実績

<1日
復旧にかかった実際の日数

事後対策事例

国内企業（感染を契機に対策）

- 本番環境だけでなくバックアップデータも暗号化
- 約３週間業務が停止

- 早期に対策可能なシステムを導入
  - 迅速な復旧のため、誰でも復旧操作可能に
  - クラウドへのリカバリも確保

1/3
リカバリにかかる工数削減目標

<3日
復旧目標

rubrik

感染の現場で実際に起きたこと

データは復旧可能か?

IT担当者

バックアップはとっていたが
バックアップデータが暗号化

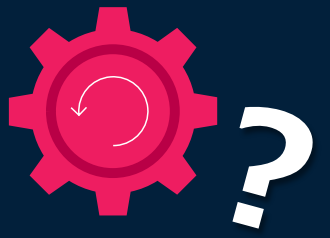
OS管理者権限が奪われて
バックアップソフトが
アンインストールされてしまった

攻撃/影響の範囲は?
データの重要度は?

セキュリティ担当者

どこまで暗号化されたのか、
どこまでリストアすればいいのか

暗号化されたデータに
機密情報が入っているのか、
身代金を支払うに値するのか



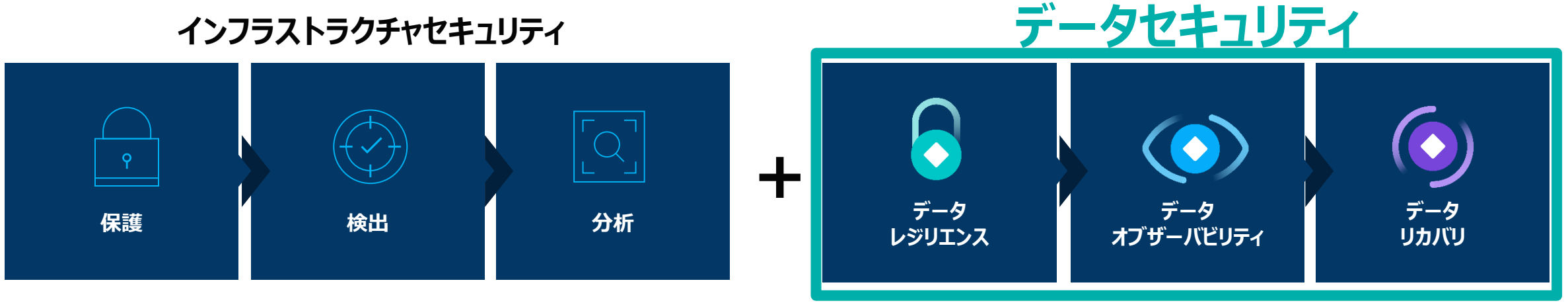
復旧により再感染しないか?
迅速に復旧できるか?

インシデント担当者

どのバックアップデータなら
安全にリストアできるのか

バックアップデータは
厳重に保管されており、
まずは取り出すことが必要

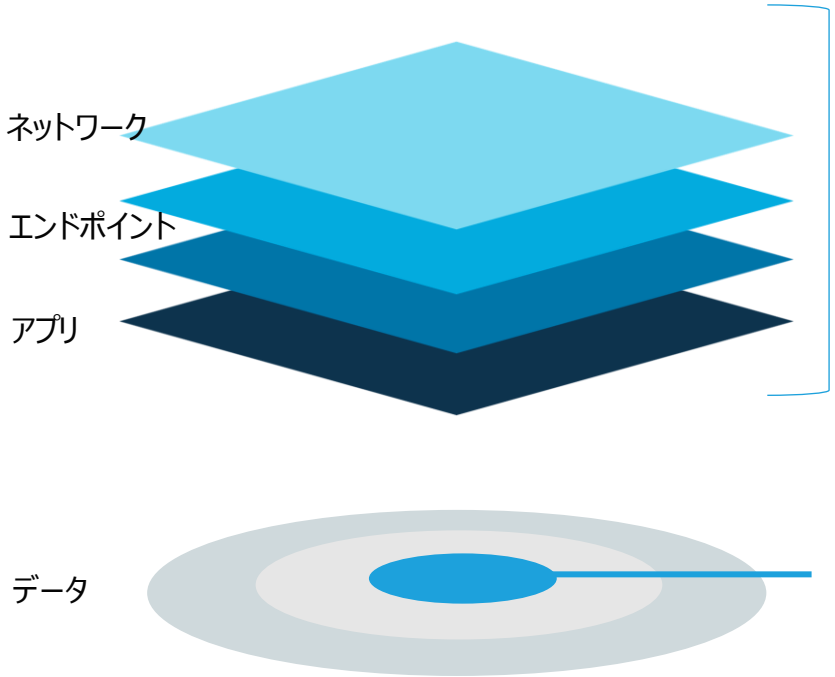
単なるバックアップではない、
確実な復旧のために、データに対する新たなアプローチが必要



rubrik

データセキュリティにより、企業の”復旧力”を強化

Rubrik ゼロトラスト データセキュリティ



インフラストラクチャセキュリティ（防御、検知のためのセキュリティ）

データセキュリティ（復旧のためのセキュリティ）

Rubrikは、バックアップを通じた高度なデータセキュリティにより、サイバーアタックからの確実かつ迅速な復旧を実現

- **Data Resilience（データレジリエンス）**
  - バックアップシステムやデータを堅牢に保護し、継続的なデータ保護とデータ復旧手段を確実に確保
    - **イミュータビリティ / エアギャップ技術 など**
- **Data Observability（データ可観測性）**
  - 機械学習を活用したバックアップデータの分析を通じて、脅威の監視と検出、重要なデータに対するリスクを可視化
    - **ランサムウェア検出機能 など**
- **Data Recovery（データリカバリ）**
  - リスクあるデータを隔離し、安全に、迅速かつ自動的なデータの復旧を実現
    - **インスタントリカバリ機能 / 自動的なデータリストア など**

rubrik

感染の現場で実際に起きたこと

データは復旧可能か?

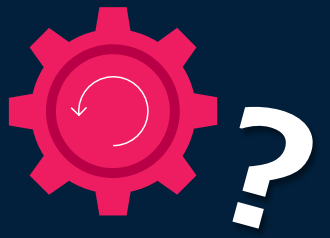
IT担当者

データ
レジリエンス

攻撃/影響の範囲は?
データの重要度は?

セキュリティ担当者

データ
オブザーバビリティ



復旧により再感染しないか?
迅速に復旧できるか?

インシデント担当者

データ
リカバリ

GLOBAL DASHBOARD

DATA PROTECTION ›

Protected Objects

969
Objects

Data Centers

10 Connected 2 Disconnected

Past 24 hours

Cloud	SaaS	Data Center
11 +0 Objects	803 +2 Objects	155 -134 Objects
13.3 TB +32.2 GB	0 B +0 B	226.9 TB -268.7 TB

Tasks

All clusters

RANSOMWARE INVESTIGATION ›

Pipeline health 95%

104
Objects

1
Anomaly event

INVESTIGATE

DATA DISCOVERY ›

FILES

Past 7 days

35 Open Access Se... 2.4k Stale Sensitive... 3.6k Sensitive Files

APPLICATION RECOVERY ›

82%

10

0

RANSOMWARE INVESTIGATION

DASHBOARD INVESTIGATIONS

Anomalies > rdp-win2k19-atlanta-35

rdp-win2k19-atlanta-35

VIEW OLDER ANOMALIES | DOWNLOAD CSV | RECOVER FULL SNAPSHOT

SUMMARY BROWSE

rdp-win2k19-atla... > C: > File Shares

RECOVER | Search

Anomaly Details

Anomalous Snapshot
Sep 14, 4:01 PM

Base Snapshot
Sep 13, 4:01 PM

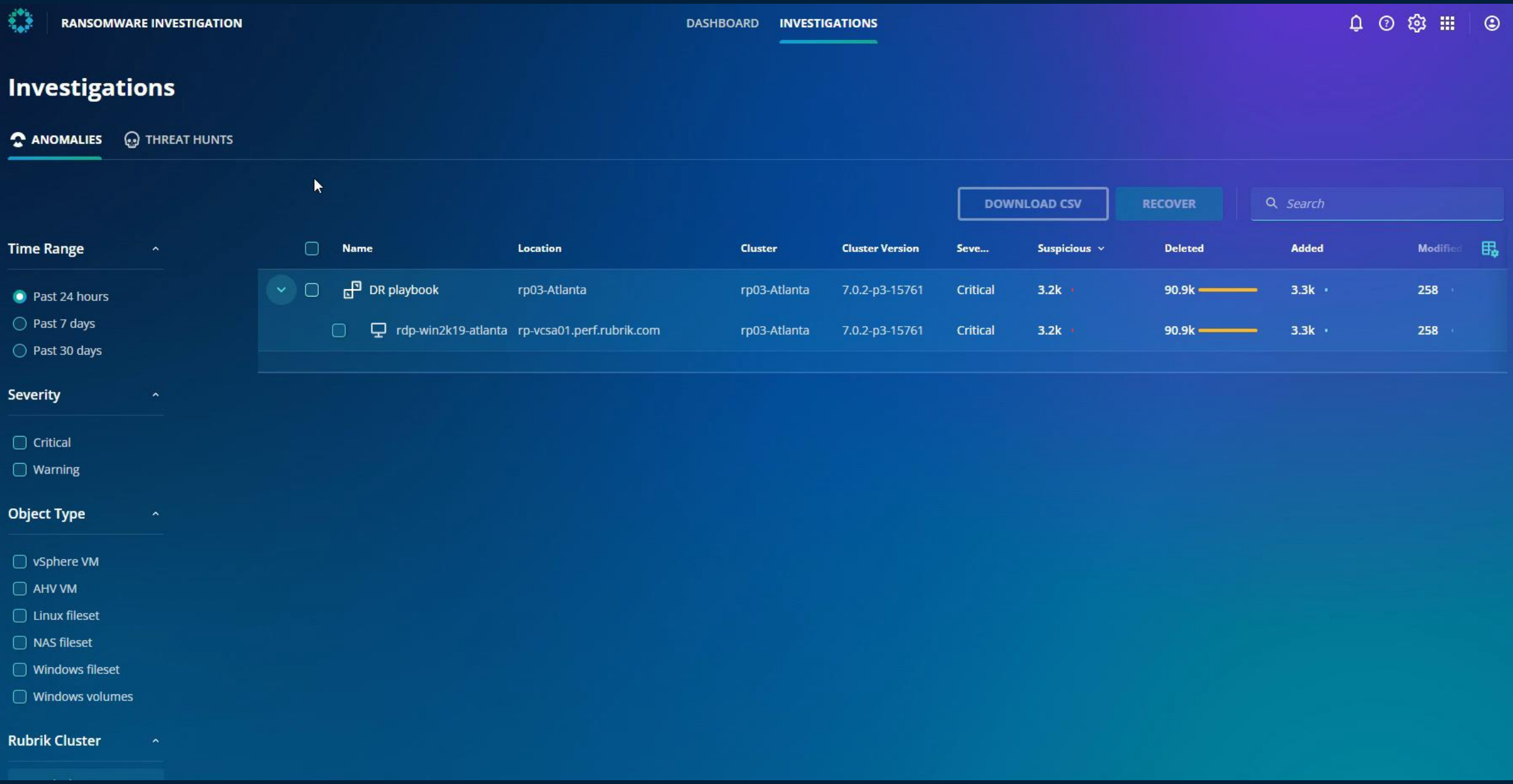
Suspicious

- [ ] Suspicious

File Changes

- [ ] Added
- [ ] Deleted
- [ ] Modified

Name	Suspicious	Deleted	Added	Modified	Size Change	Total Size	Last Modified
Engineering Department	28	28	28	0	+789 B	62.81 MB	Sep 14, 7:02 AM
Finance Department	22	22	22	0	+640 B	63.06 MB	Sep 14, 7:02 AM
HR Department	623	623	623	0	+19.23 kB	921.38 MB	Sep 14, 7:02 AM
IT Department	382	384	382	1	- 27.86 kB	627.86 MB	Sep 14, 7:02 AM
Legal Department	424	424	424	0	+14.11 kB	516.39 MB	Sep 14, 7:02 AM
Marketing Department	457	462	457	6	- 239.81 kB	931.79 MB	Sep 14, 7:02 AM
Public Share	982	985	982	2	- 92.2 kB	1.44 GB	Sep 14, 7:02 AM
Sales Department	268	268	268	0	+7.55 kB	681.2 MB	Sep 14, 7:02 AM


RANSOMWARE INVESTIGATION
DASHBOARD
INVESTIGATIONS
Investigations
ANOMALIES
THREAT HUNTS
DOWNLOAD CSV
RECOVER
Search
Time Range
Past 24 hours
Past 7 days
Past 30 days
Severity
Critical
Warning
Object Type
vSphere VM
AHV VM
Linux fileset
NAS fileset
Windows fileset
Windows volumes
Rubrik Cluster
Name
Location
Cluster
Cluster Version
Seve...
Suspicious
Deleted
Added
Modified
DR playbook
rp03-Atlanta
rp03-Atlanta
7.0.2-p3-15761
Critical
3.2k
90.9k
3.3k
258
rdp-win2k19-atlanta
rp-vcsa01.perf.rubrik.com
rp03-Atlanta
7.0.2-p3-15761
Critical
3.2k
90.9k
3.3k
258

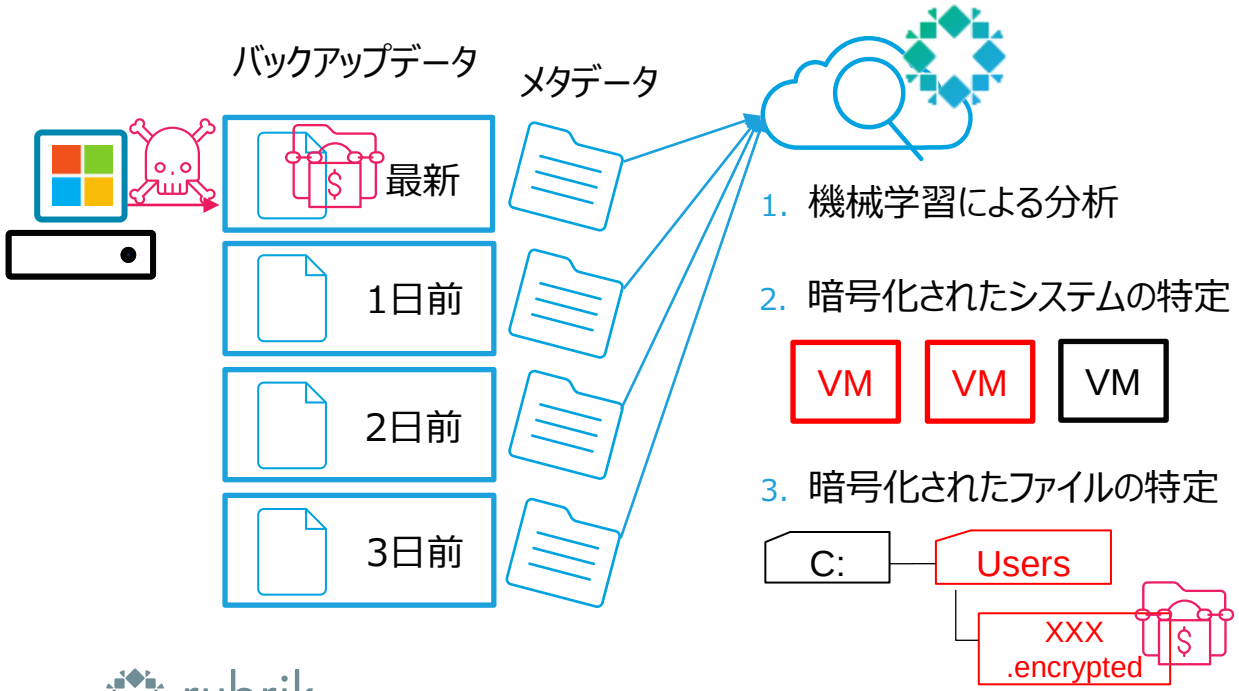
データオブザーバビリティ

感染したシステムの検出と影響範囲を特定

2つの方法でバックアップデータを分析し、ランサムウェア感染を検知

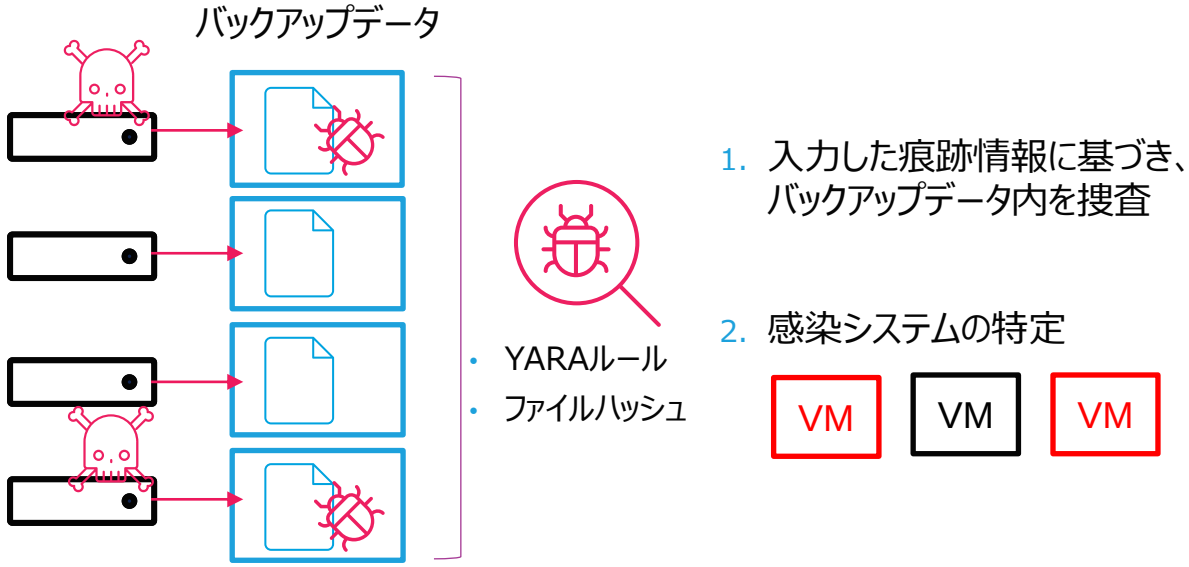
ふるまい検知 (Anomaly Detection)

メタデータを機械学習で分析し、ランサムウェアにより
暗号化されたシステム / ファイルを検出し影響範囲を特定



脅威ハンティング（Threat Hunting）

入力されたYARAルールなどの痕跡情報とバックアップデータ
を照合し、いつからランサムウェアが侵入したかを検出



rubrik

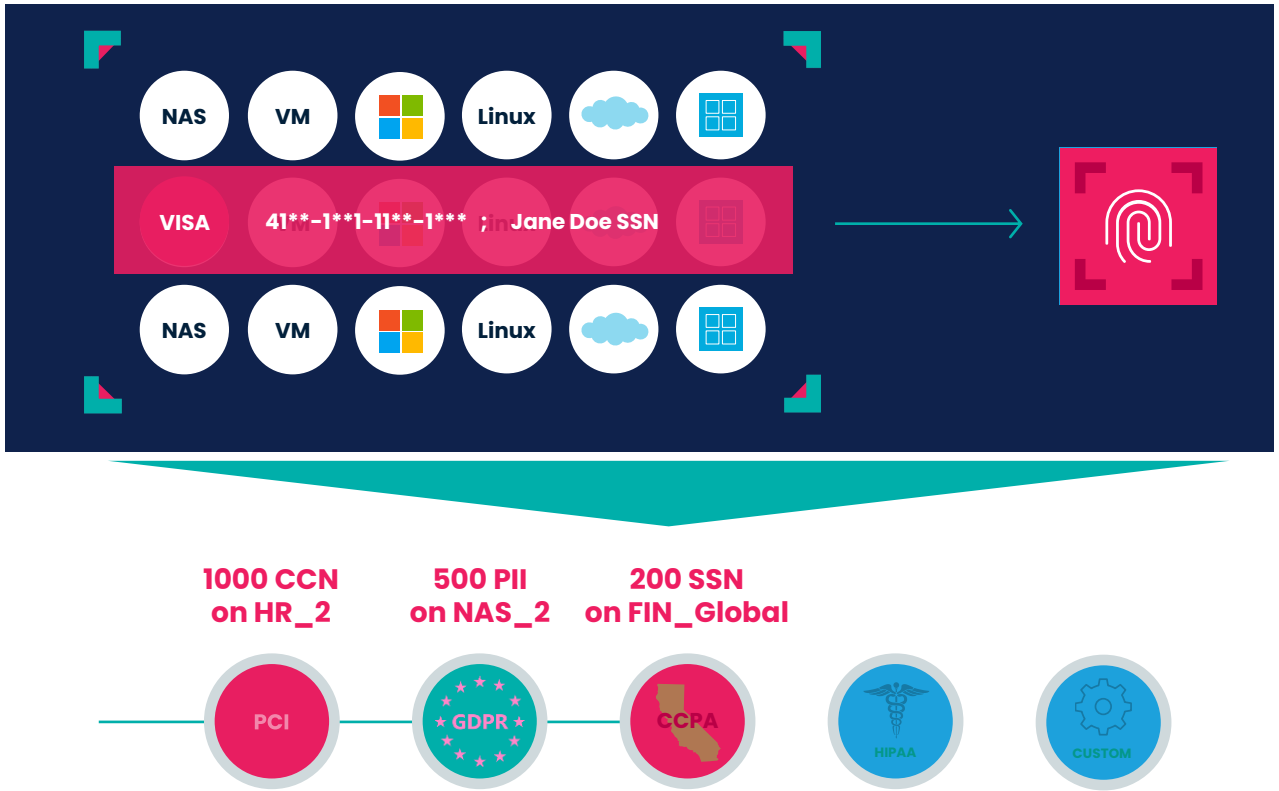
データオブザーバビリティ

機密情報を可視化し、リスクの回避と対応を迅速化

Rubrik Sensitive Data Discovery

- **データのリスクアセスメントサービス**
  - バックアップデータに対して、ポリシーに基づいて自動的にキーワード検知と分類を実施
  - 機密データへのアクセス状況を可視化
  - 情報保護規制の遵守を促進

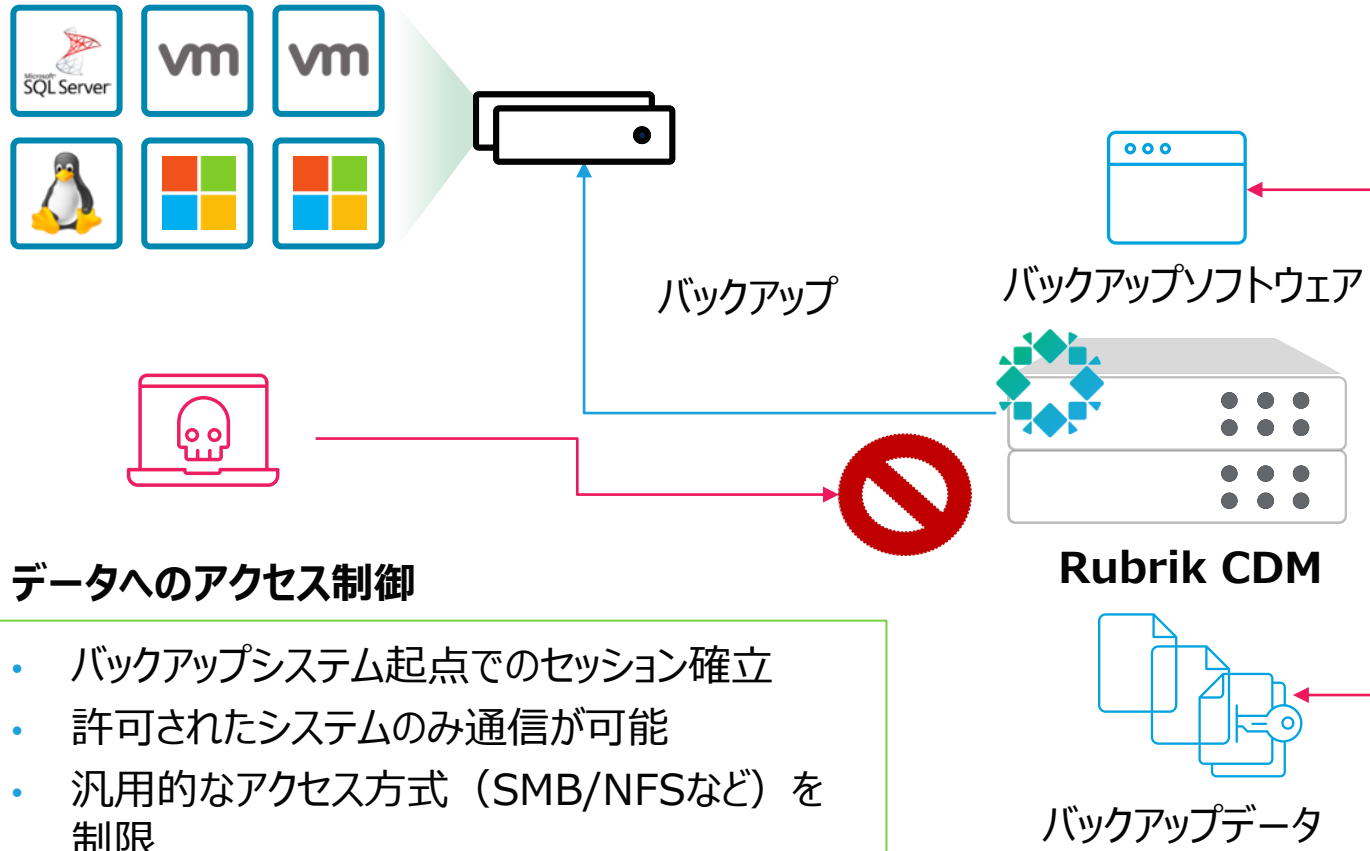
- **機密データの可視化を支援**
  - どの機密データか
  - どこに保存されているか
  - どれだけのデータが公開されているか
  - 誰がアクセスできるか



rubrik

Rubrik CDMのデータセキュリティを実現する機能

バックアップデータ / バックアップシステムを確実に保護



なりすましの防止

- ベースOSの管理者権限は利用不可
- 多要素認証によるなりすましの防止
- ファイルの保存期間の変更を禁止

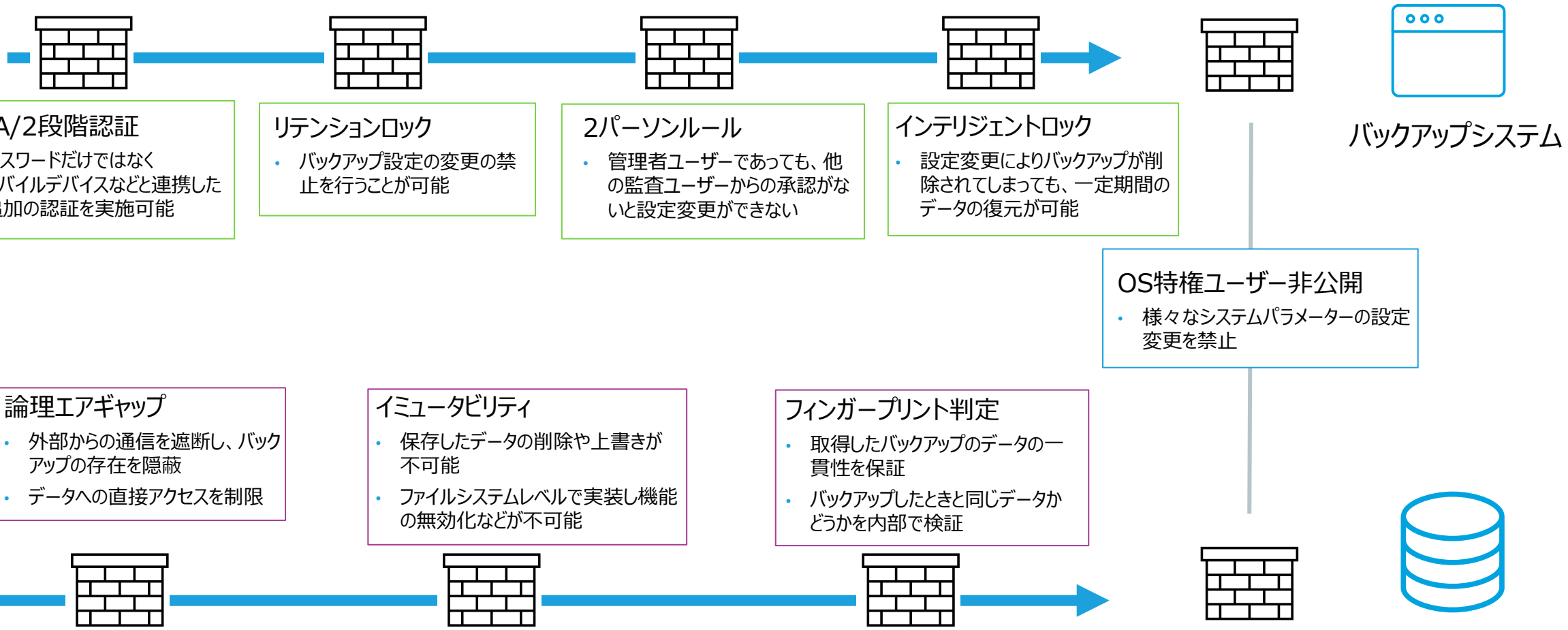
データへのアクセス制御

- バックアップシステム起点でのセッション確立
- 許可されたシステムのみ通信が可能
- 汎用的なアクセス方式（SMB/NFSなど）を制限

データの改ざん防止 / 一貫性

- 独自OSを採用
- Rubrikが許可したソフトウェアのみ実行許可
- データの上書きや削除が不可能なイミュータブルなファイルシステムにより暗号化を防止

多重の（ゼロトラストな）セキュリティ対策



MFA/2段階認証
- パスワードだけではなくモバイルデバイスなどと連携した追加の認証を実施可能

リテンションロック
- バックアップ設定の変更の禁止を行うことが可能

2パーソンルール
- 管理者ユーザーであっても、他の監査ユーザーからの承認がないと設定変更ができない

インテリジェントロック
- 設定変更によりバックアップが削除されてしまっても、一定期間のデータの復元が可能

バックアップシステム

OS特権ユーザー非公開
- 様々なシステムパラメーターの設定変更を禁止

論理エアギャップ
- 外部からの通信を遮断し、バックアップの存在を隠蔽
- データへの直接アクセスを制限

イミュータビリティ
- 保存したデータの削除や上書きが不可能
- ファイルシステムレベルで実装し機能の無効化などが不可能

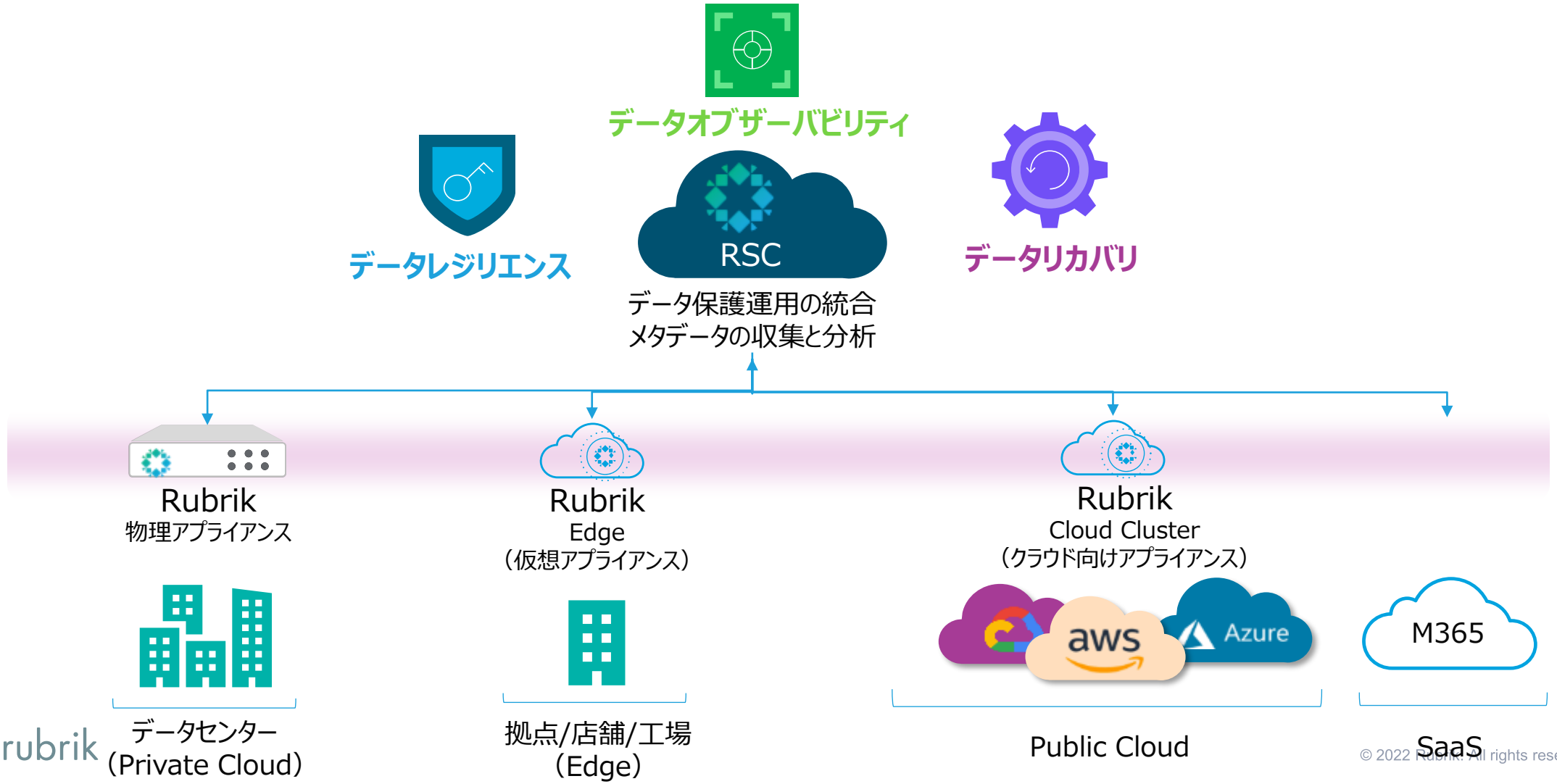
フィンガープリント判定
- 取得したバックアップのデータの一貫性を保証
- バックアップしたときと同じデータかどうかを内部で検証

バックアップデータ

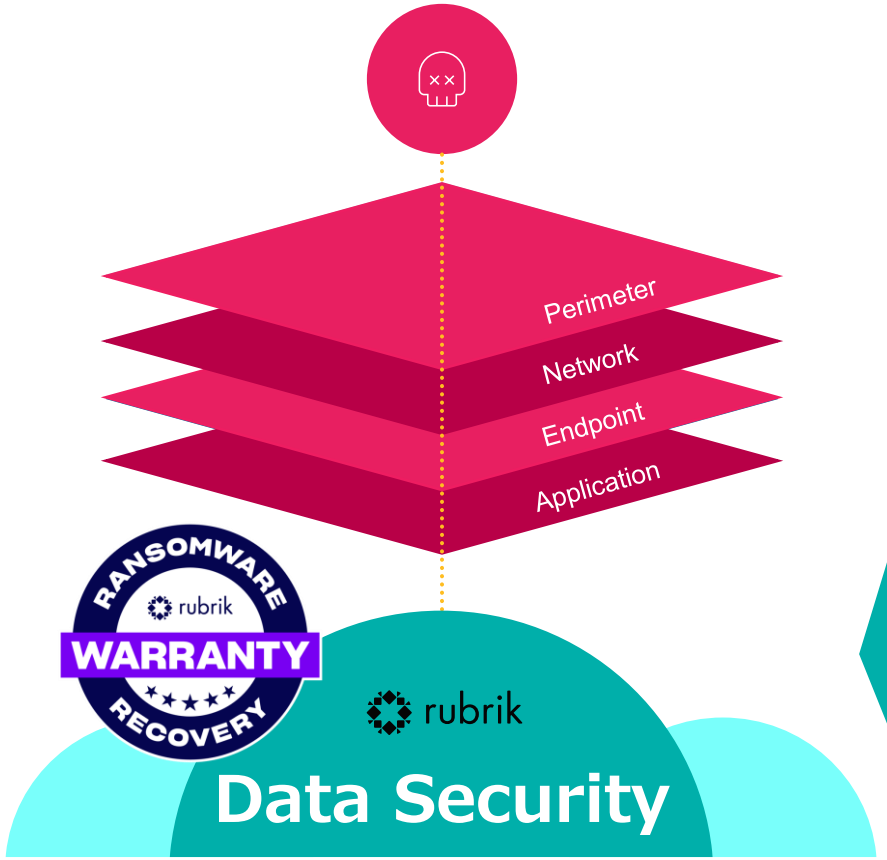
rubrik

あらゆる場所でデータセキュリティを強化

SaaSコントロールプレーンから、バックアップを通じて企業内のデータのセキュリティを強化



データセキュリティにより、企業に”復旧力”を提供



サイバーアタックから お客様の早期のサービス/データの 確実、かつ迅速な復旧を支援

データ レジリエンス

サイバー脅威から データを守る

データ オブザーバビリティ

サイバー脅威を 継続的に監視し、 迅速に分析する

データ リカバリ

数時間以内に 業務を復旧させる

Don’t Backup.

Go Forward.

rubrik