マルチクラウド環境の最強セキュリティソリューション「RedLock」のご紹介

パロアルトネットワークス 株式会社
技術本部　システムエンジニア
石川　幸平

金融機関を取り巻く環境と課題

金融機関のクラウドファースト

- ２０１７年のメガバンクの一つである三菱UFJフィナンシャルグループがAWSのIaaSの標準化・自動化を念頭に置いた「クラウドファースト」を打ち出した後、公開系のみならず、業務・勘定系へのクラウド利用が、業界的にも進んできている。
- 政府情報システムの「クラウド・バイ・デフォルト原則」もあり、もはやクラウドの利用は、社会的に必然となってきている。
- それに伴い、金融機関の取り巻く課題・環境も変化している。

金融機関の取り巻く環境の変化・課題

現在

- 第３者評価によるセキュリティ対策の見直し
- 入口・出口対策の投資効果判断、運用コスト、フローの見直し
- クラウド向けセキュリティ対策の検討を開始
- CSIRT 体制整備・運用改善
- 金融ISAC、地域金融間の連携
- 仮想通貨対応

今後

- IT資産を持たない戦略へのシフト
- デジタルトランスフォーメーション
- クラウド利用のITガバナンス整備
- 働き方改革への対応
- 脅威インテリジェンスの導入
- SSL復号
- セキュリティ製品の有効活用

金融機関様から聞こえてくる声・・・

クラウドの利用者側の責任範囲はどこ？

パブリッククラウドの脅威ってなに？

現場は理解しているんですけど、、上が

コスト削減のためにクラウド使ってる
のにセキュリティ投資？

それ、外部にアウトソースできるの？

クラウドインシデント

クラウドインシデントの特徴

“2022年までに起こるクラウドでのセキュリティ事故の95%はユーザー起因によるもの”

- GARTNER

アカウント情報の漏洩

27%

- 主な事例:
  Uber, OneLogin, Tesla, Aviva, Gemalto
- Redlockによる調査結果:
  平均で27%の組織でアカウント情報の漏洩を経験

仮想通貨マイニング

25%

- 主な事例:
  Tesla, Gemalto, Aviva
- Redlockによる調査結果:
  平均で25%の組織が仮想通貨マイニングの被害を経験

設定ミスの危険性

51%

- 主な事例:
  Deep Root Analytics, FedEx, Under Armour
- Redlockによる調査結果:
  平均で51%の組織が最低でも一つ以上のストレージの一般公開による情報漏洩の可能性を経験

脆弱性

24%

- 主な事例:
  MongoDB, Elasticsearch, Intel, Drupal
- Redlockによる調査結果:
  24%の組織でパブリッククラウド上のホストへの最大深刻度のパッチ未適用

事例研究：某大手自動車メーカーによるAWS S3からの個人情報漏洩(2018年6月)

- モバイルアプリにより自分の自動車の情報を把握することが可能なサービスを提供
- アプリに登録しているユーザーの個人情報5万人分以上がクラウドサービス上で公開されていた
- **Amazon AWS S3上にデータを保存**。そのディレクトリ「Buckets(バケット)」の設定を誰でも閲覧できる「**公開状態**」にしていたのが原因
- 閲覧できる状態だったデータは、アプリに登録した名前・電話番号・パスワード・性別・メールアドレス・連絡先。また、車に関する情報の車両識別番号・アクセスIDなども含まれていた
- これらの情報が漏洩して悪意のある攻撃者に渡った場合、データベース内に記載されているすべてのスマートフォンにアクセスできる可能性。自動車の使用履歴から、自動車の所有車の住居・仕事・買い物・遊ぶ場所など、ユーザーの日々の活動を知ることが可能。

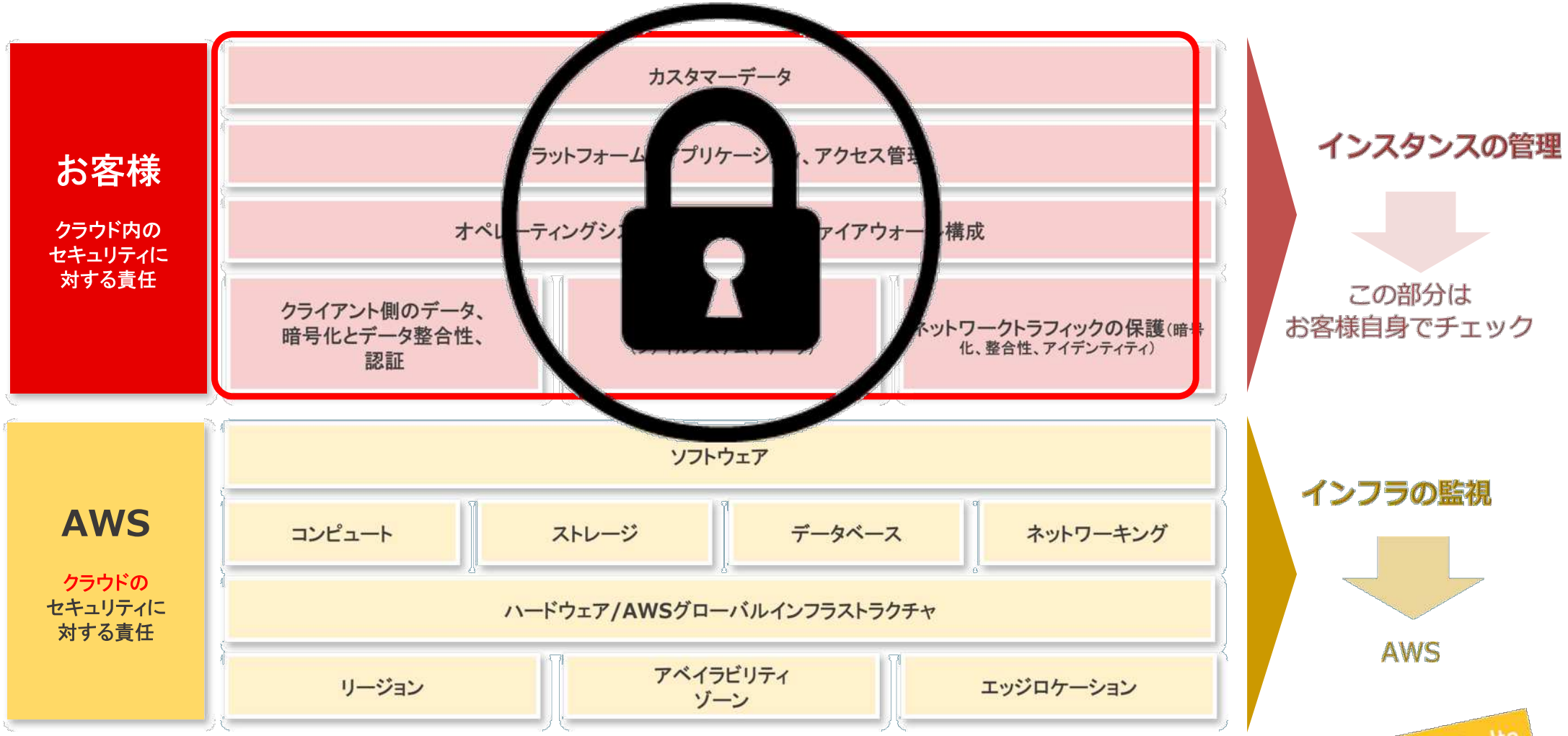
注：Gigazine記事より抜粋

このような事態を防ぐためにも
設定ミスによるインシデントを防ぐための
継続的なセキュリティ対策は必須

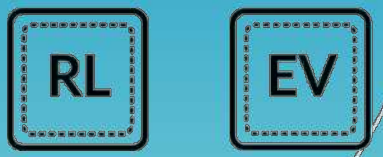
注：Gigazine記事より抜粋

守るべきポイント

パブリッククラウドにおける責任共有モデルのおさらい



RedLockとは



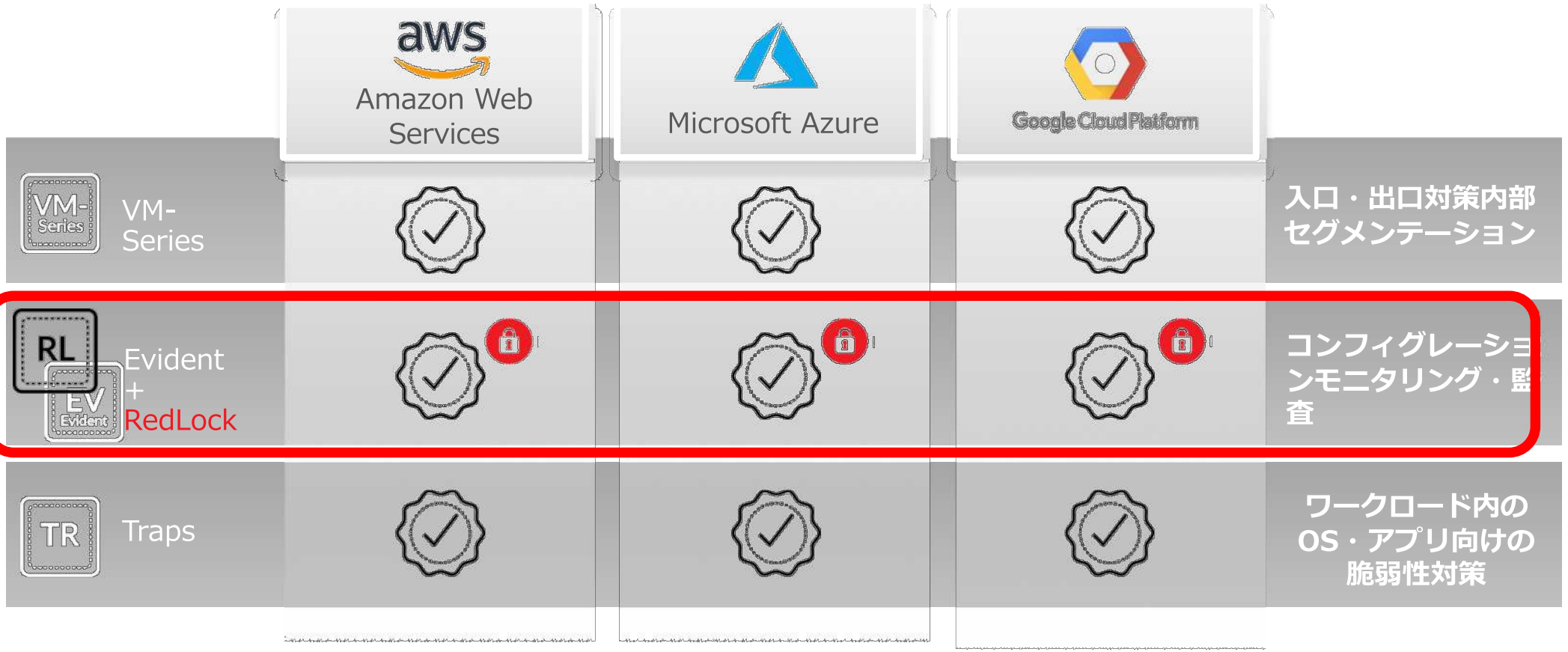
RedLock: クラウドセキュリティ解析

クラウドリソースとアプリケーションの検知と分類

リスクのある設定やネットワークの脅威、疑わしいユーザの振る舞い、ホストの脆弱性や不正アクセスを検知

リスクの優先順位づけ、インシデントの調査や脅威の修復

一貫したマルチクラウドの保護



RedLockを語る上で、

パロアルトネットワークス が提供するもう一つのセキュリティ製品を

紹介する必要があります。

それが、

Evident IO

Evident: クラウドコンプライアンス

継続的かつリアルタイムな
コンプライアンス監視と レポート

様々な規定や業界標準に準拠した、
カスタマイズ可能なコンプライアンス
レポートと制御

コンプライアンスポリシーを
自動的に適用可能

これら2種類のクラウドセキュリティ製品をまとめて提供

EvidentとRedLockの機能統合

RedLockのここが凄い！

コンプライアンス監査のための
ガイドラインを標準で提供
レポート出力も可能！

SOC ,NIST CSF,PCI DSS v3.2,HIPAA,GDPR,
DEVOP-Blue,CIS v1.0 (Azure),
CIS v1.0.0 (GCP),CIS v1.2.0 (AWS)
（*1）

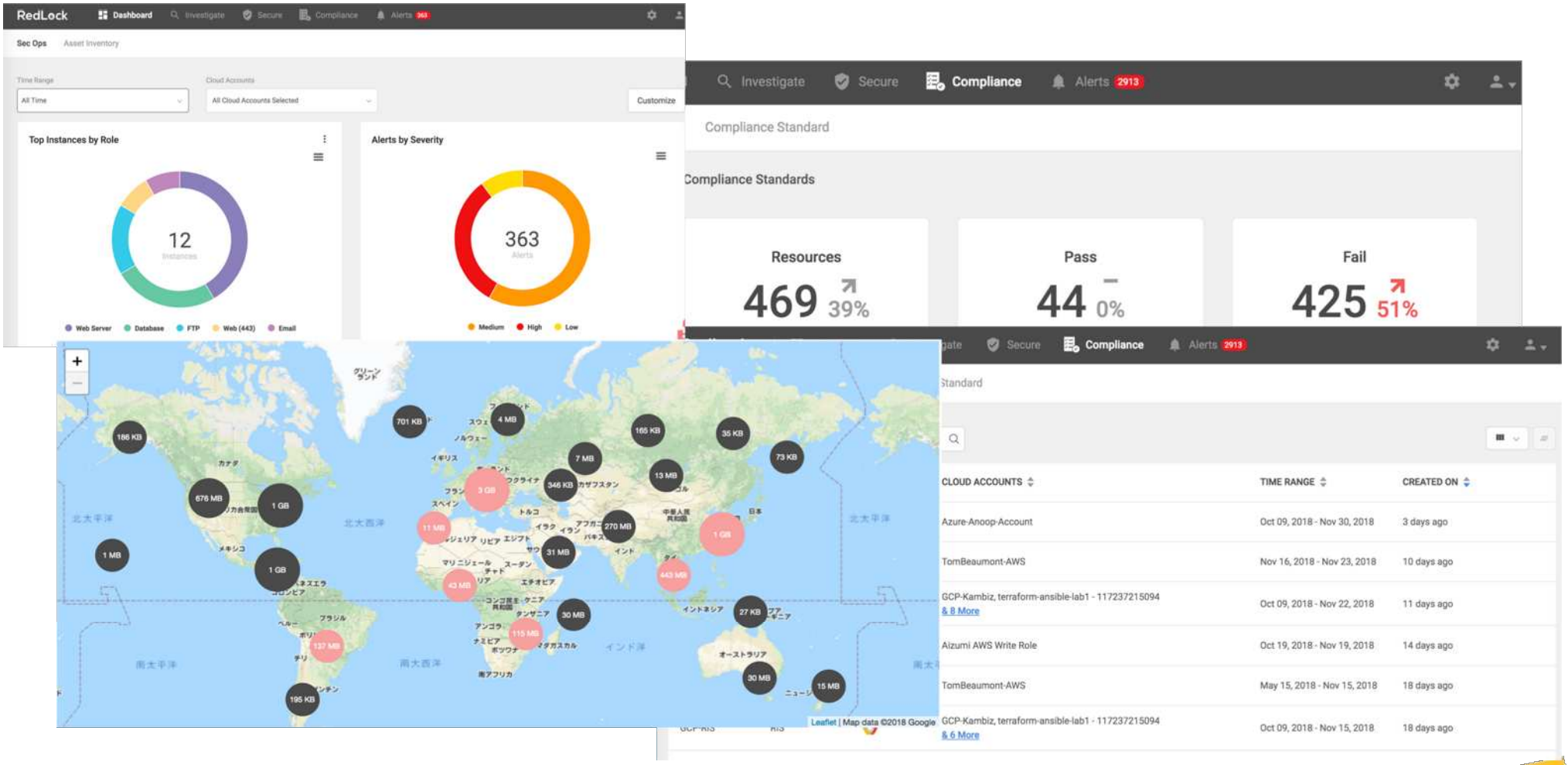
スペシャリストが定めた
マルチクラウドセキュリティ
ポリシー（判断基準）を標準実装

アラートに対して自動的に修復、
もしくは修復のために
必要なアドバイスを提供

独自のポリシーや監査基準も
カスタマイズ可能（※2）

※1・・・2018/12/12時点での対応
※2・・・専門的な知識とシステムへの理解が必要なため、セキュリティコンサルタントや運用が可能なSIへの相談をお勧めします。

RedLockの画面イメージ



どのようなシナリオで有効なのか？

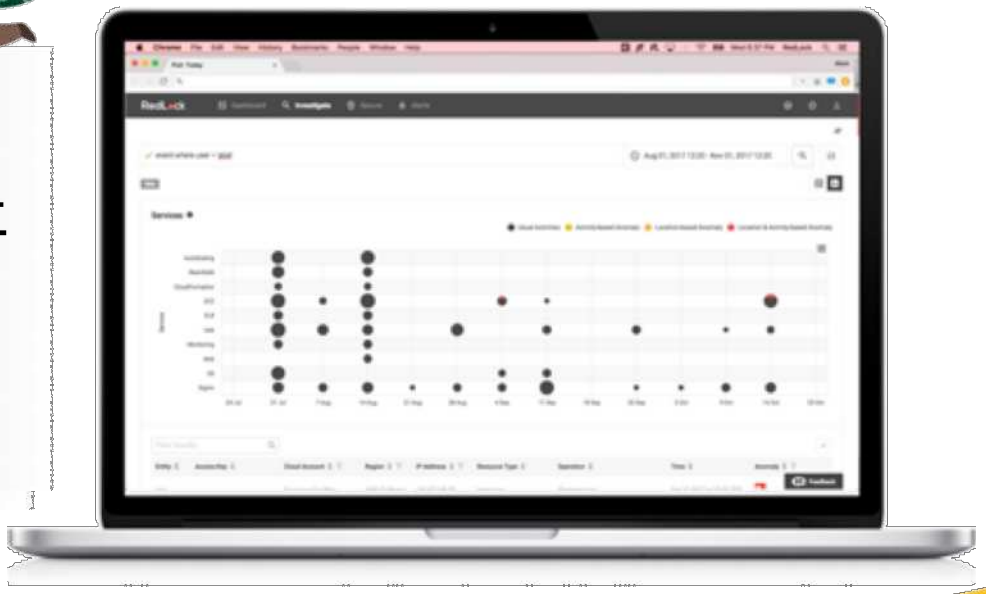
UEBA(User & Entity Behavior Monitoring)を利用したシナリオ例

開発者が誤って
GitHubのクラウド　アク
セスキーを漏洩

攻撃者がクラウド
アカウントからログインし、
データを盗む

RedLockは通常でない
場所からのキー利用を
検出し、異常な処理を実
行

RedLockはSOCチーム
に警告し、このキーに
関連する全ての
活動の完全な履歴も
提供

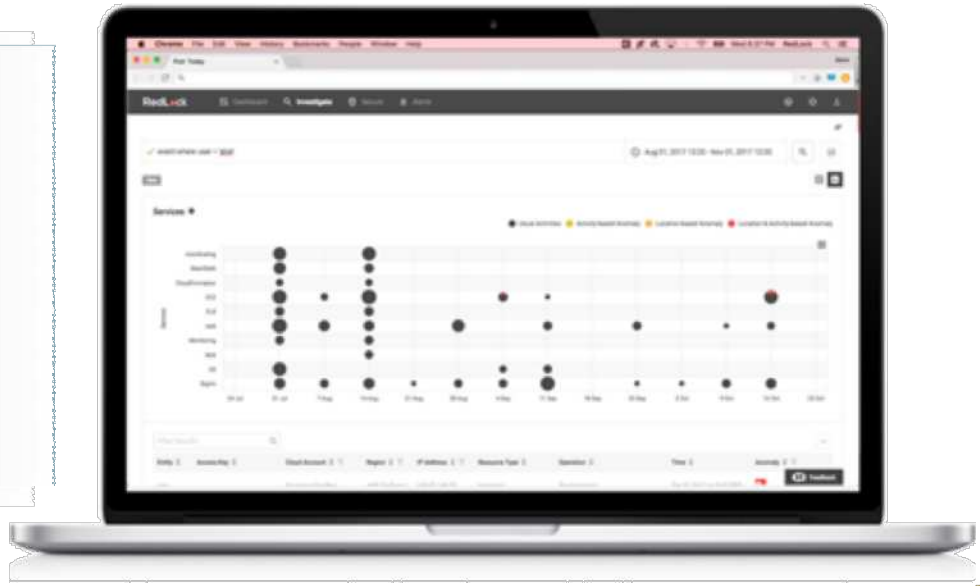


ネットワークモニタリングを利用したシナリオ例

ユーザーがセキュリティグループを作成するが、セキュリティグループは解放したまま

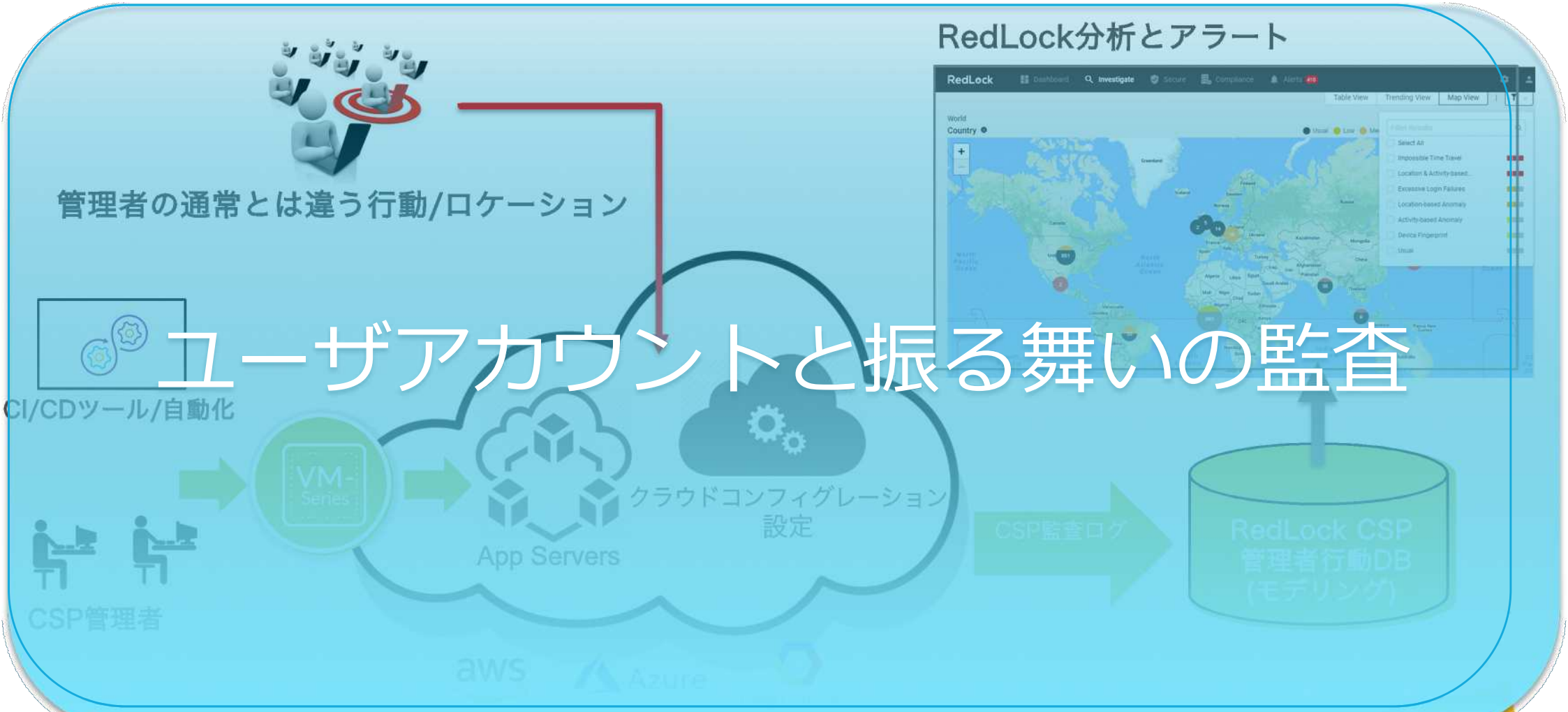
RedLockがMongoDBを実行しているVMに関連づけられていることを検出し、既知の悪意のあるIPアドレスからインターネットトラフィックをデータベースが受信していると判断

RedLockは自動的にデータベースをプライベートセキュリティグループへ移動させ、リスクを修復



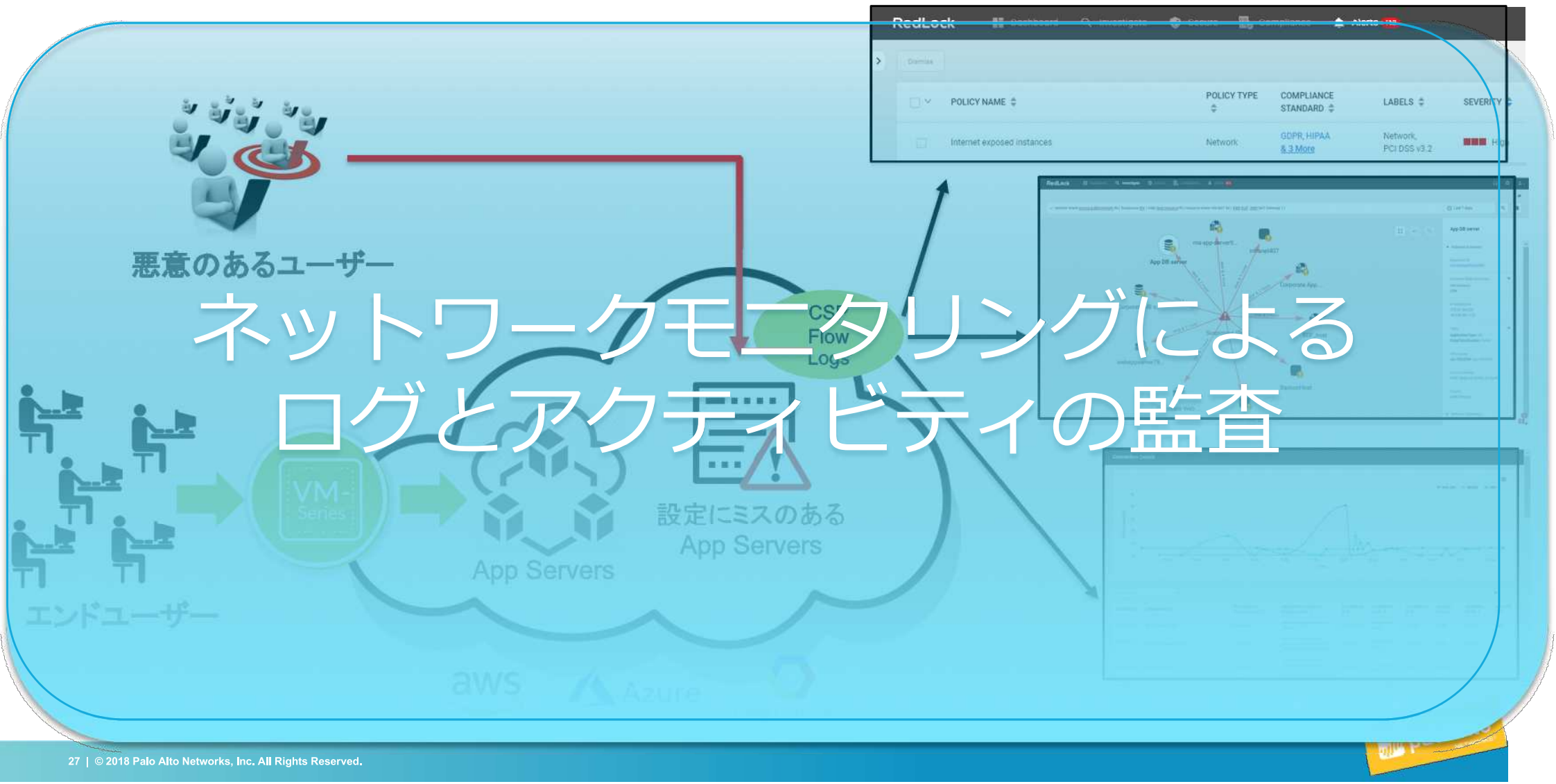
RedLockの機能

UEBA(User & Entity Behavior Monitoring)ワークフロー

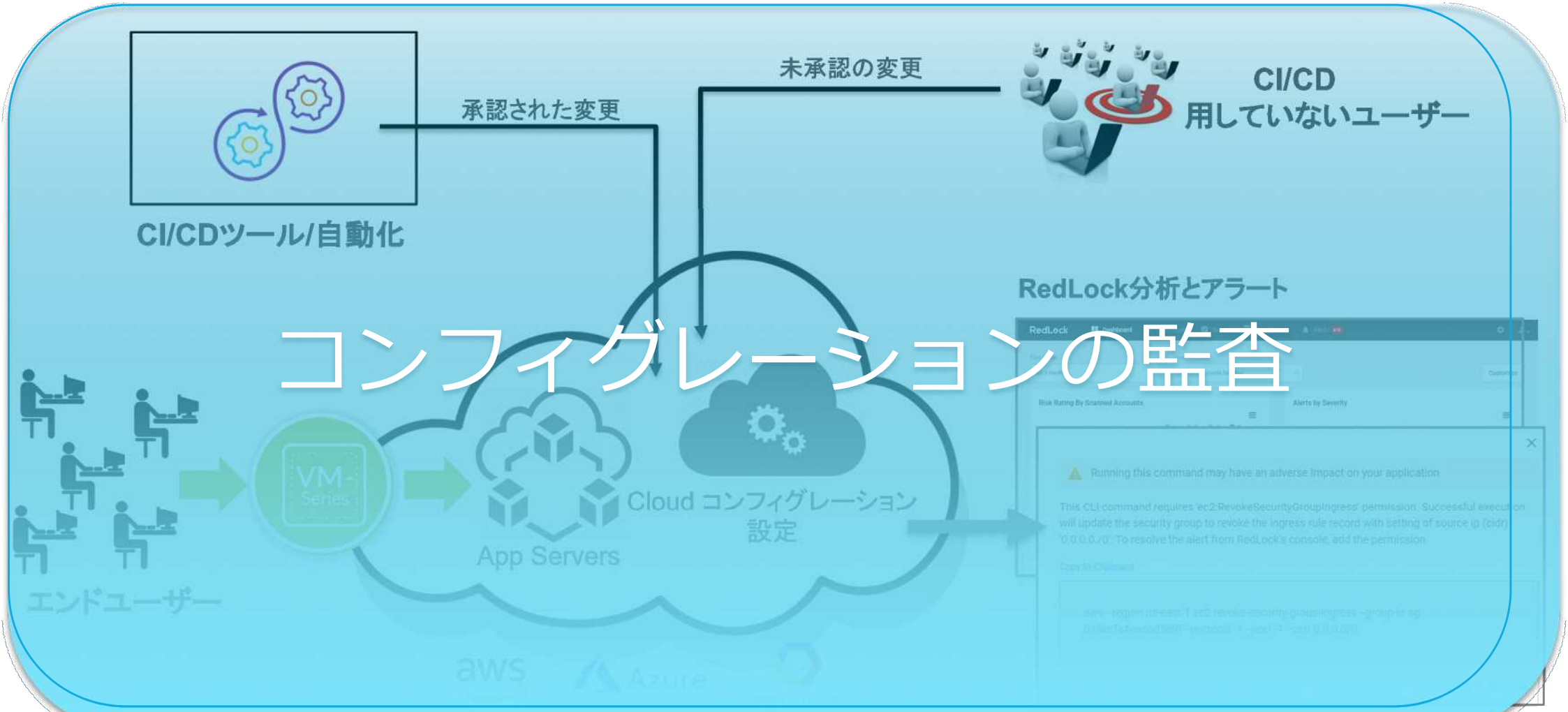


ユーザアカウントと振る舞いの監査

ネットワークモニタリングと分析ワークフロー



設定状態を監査



Demo & PoC

デモ

PoCの申し込みについて

- RedLock のPoCで貴社のパブリッククラウドの状況を診断して見ませんか？

お申し込みはネットワンシステムズ様の担当営業までどうぞ！