クラウドファースト &
働き方改革を実現する
パロアルトネットワークスの
クラウドサービス

PRISMA
BY PALO ALTO NETWORKS

パロアルトネットワークス株式会社

「クラウドシフト」と「モバイルシフト」が急速に拡大

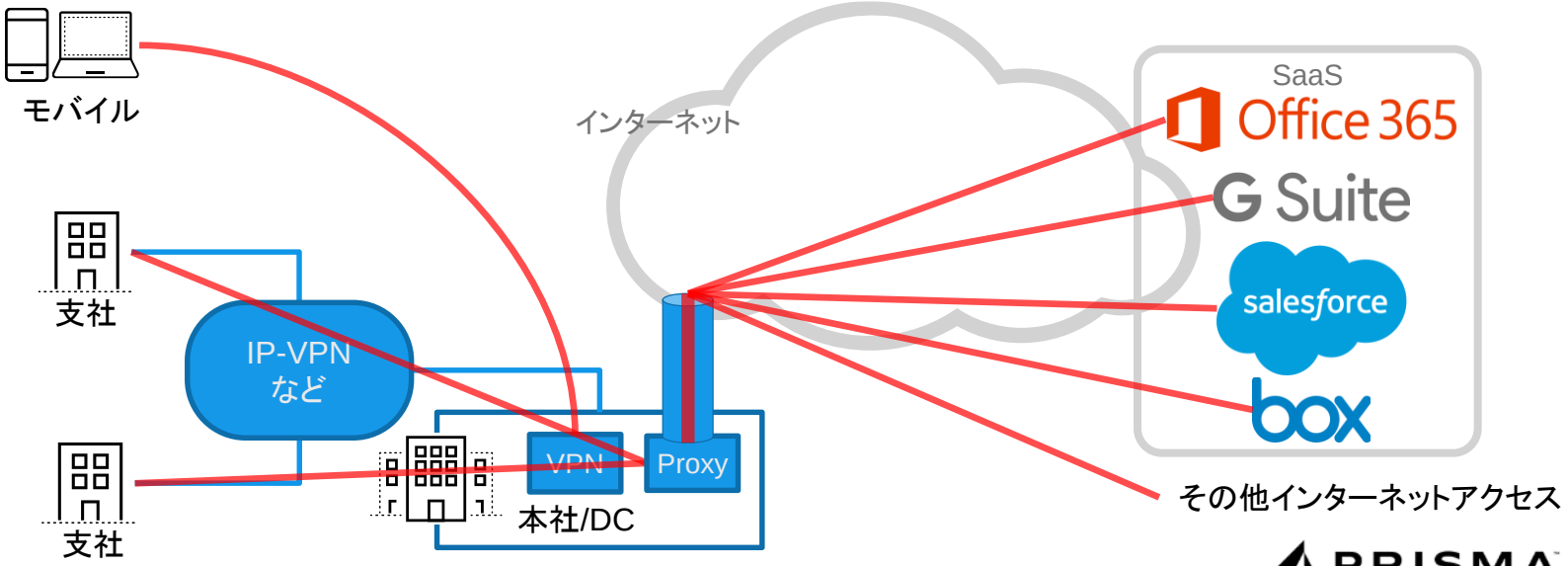
- オフィスアプリケーションの多くが、クラウドサービスにシフト
  - Office 365 / G Suite
  - オンラインストレージ
  - Web会議 / ビジネスチャット
  - イントラネット(社内情報共有)
  - 業務系アプリケーション
  - IaaS・PaaS (AWS / Azure / GCP)

- 「働き方改革」「デジタル化」により、
  スマートデバイスの活用やモバイル利用が活発に
  - 自宅からPCでアクセス
  - カフェからタブレットでアクセス
  - 移動中にスマートフォンからアクセス

PRISMA BY PALO ALTO NETWORKS

「クラウドシフト」と「モバイルシフト」の課題①：ネットワークの負荷

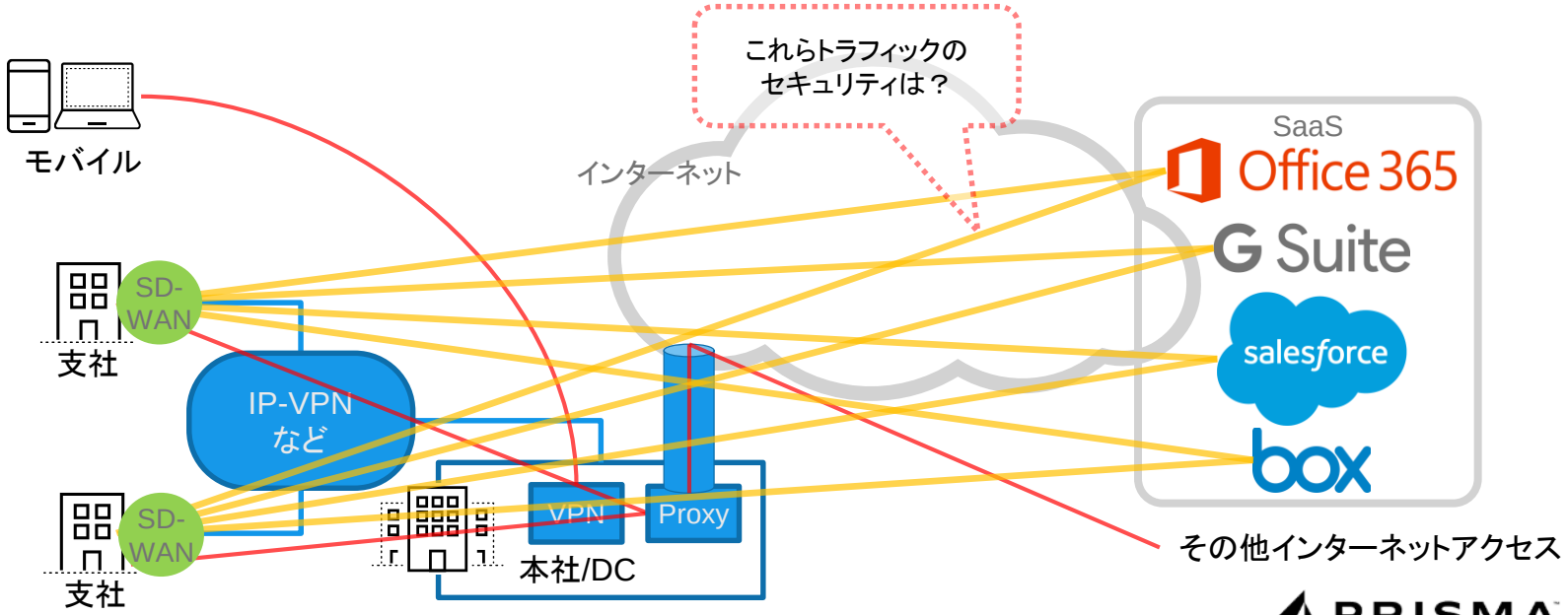
- クラウドアクセス増加によるネットワーク帯域の消費
  - 社内で閉じていたアクセスが、すべてインターネットに出ていく
  - 拠点間の閉域網やインターネットアクセス回線の帯域や遅延が問題に
- Office 365のセッション増加によるWebプロキシサーバの性能問題
  - Office 365は、多くのコネクションを使用（Outlookだけでも1ユーザあたり20～30本）
  - Webプロキシサーバ（オンプレミス）の台数を増やしても追い付かない



PRISMA
BY PALO ALTO NETWORKS

SD-WANの利用で回避？

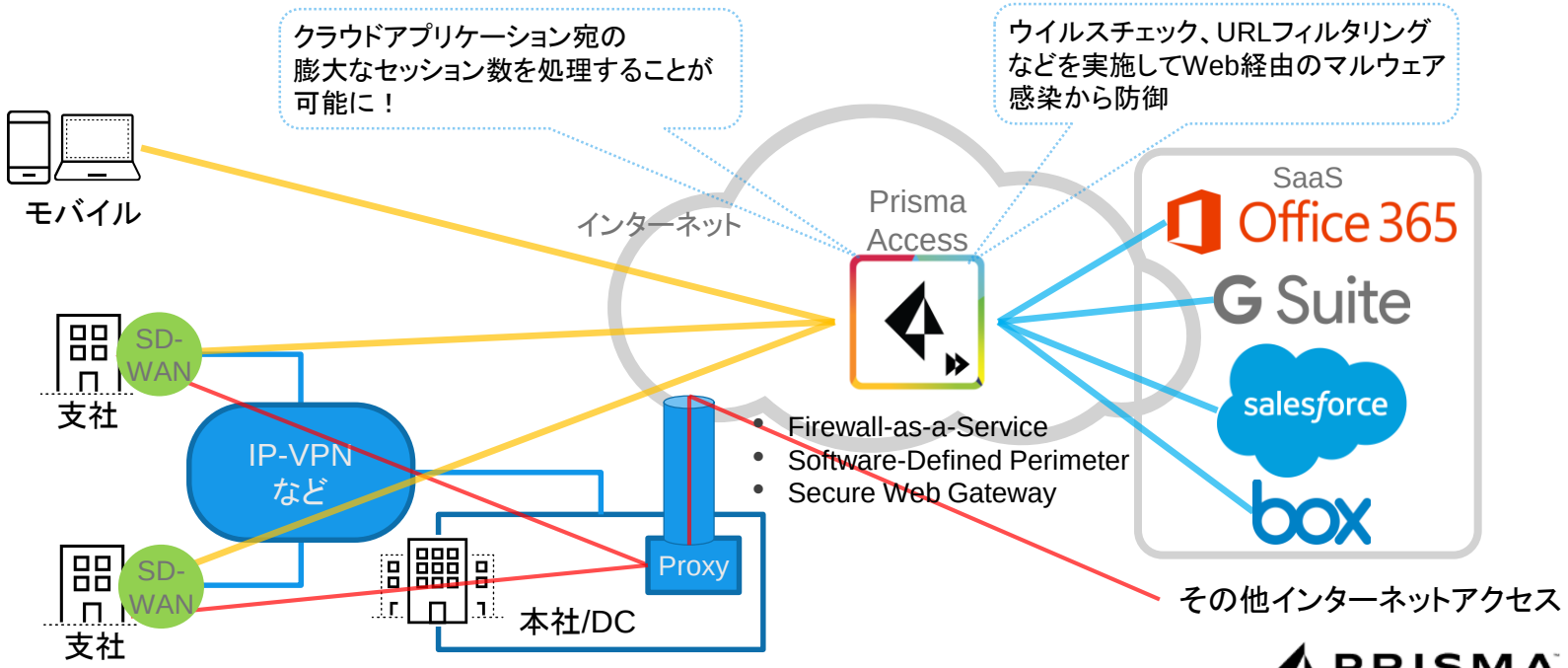
- SD-WANで、各拠点からSaaSトラフィックをインターネットにブレークアウト
- 「その他インターネットアクセス」トラフィックは、従来通り本社/DCのプロキシ経由
- ［課題］ブレークアウトしたトラフィックのセキュリティはどうする？



PRISMA
BY PALO ALTO NETWORKS

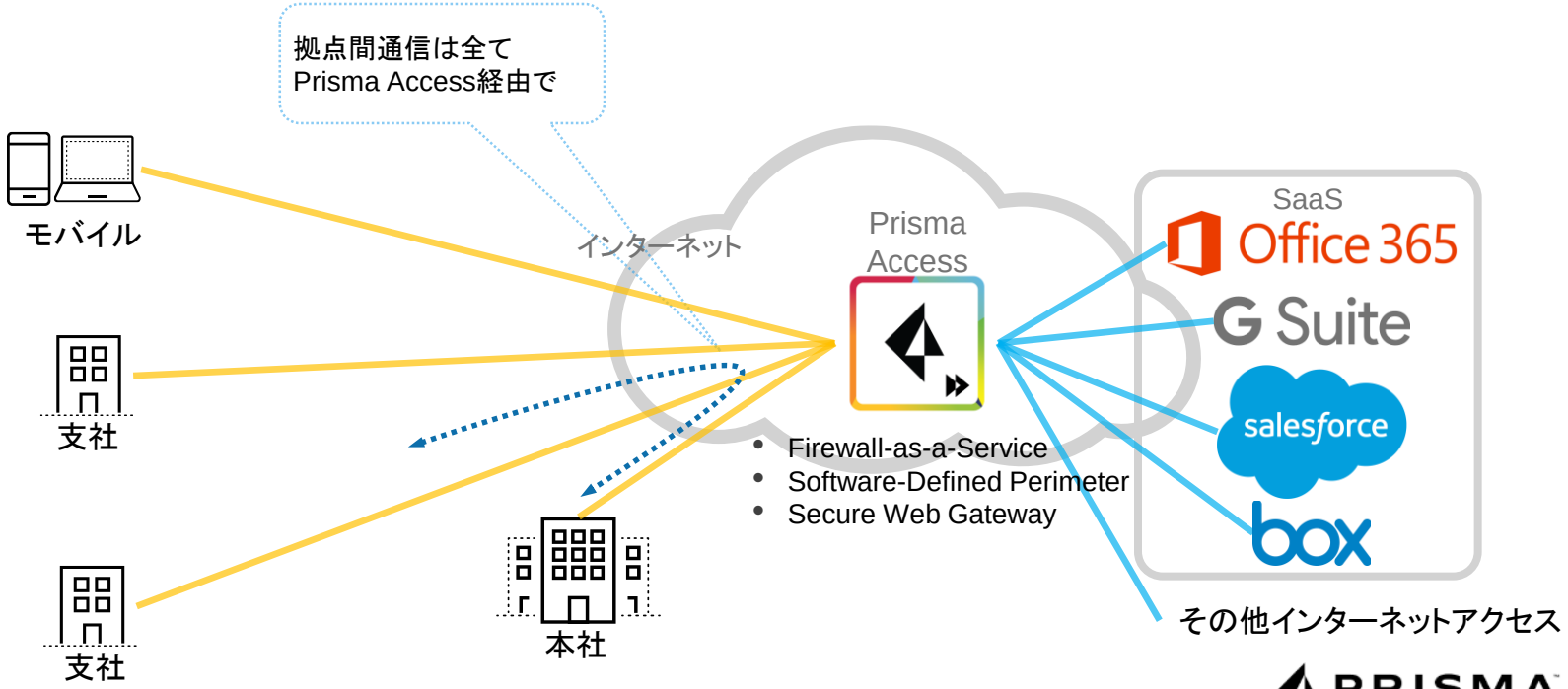
「クラウドシフト」と「モバイルシフト」に対応したネットワーク構成 (1)-1

- SD-WANでブレークアウトされた通信は、Prisma Accessにてセキュリティを確保
- モバイル端末は、直接Prisma AccessへのVPN接続が可能



「クラウドシフト」と「モバイルシフト」に対応したネットワーク構成 (1)-2

- 拠点間通信もPrisma Access経由に変更 → コスト削減
- SaaS以外のインターネットアクセスもPrisma Access経由でセキュリティを確保



Prisma Accessの特長

- パロアルトネトワークスが運営するクラウド型Next Generation Firewallサービス
  - スケーラブル (Firewall キャパシティ拡張の柔軟性)
  - クラウドサービスなので、展開が容易
  - SaaSアプリの許可・不許可の制御と利用状況の可視化
- モバイルユーザー向け:
  - GlobalProtectエージェントソフトウェアを介して、IPSec/SSL-VPNトンネルで
  - Prisma Accessに接続
  - App-IDや脅威防御などのセキュリティサービスを提供
  - 従来のオンプレミス型のGlobalProtectに代わるクラウド型ソリューション
- 社内ネットワーク向け:
  - オフィス等の拠点に設置された、業界標準の IPsec VPN 対応ルータ等を介して、IPSecトンネルでPrisma Access に接続
  - App-ID や脅威防御などのセキュリティ サービスを提供

「クラウドシフト」と「モバイルシフト」の課題②：SaaS特有のセキュリティ

- SaaS内でマルウェアが伝播する可能性
- 意図せず、データ(ファイル)が公開・共有設定になっている＝情報漏洩
- 悪意のある部外者によるデータ搾取

マルウェアの伝搬

アクシデント的なデータ漏洩

悪意あるデータ搾取

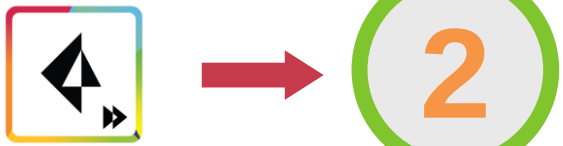
SaaSセキュリティのベストプラクティス

Prisma SaaS

1

SaaS アプリケーション内データやファイルの脅威や不備を検出する

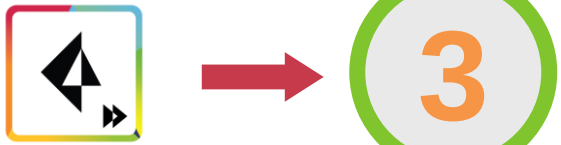
Prisma Access



2

SaaSの利用状況を知る

Prisma Access



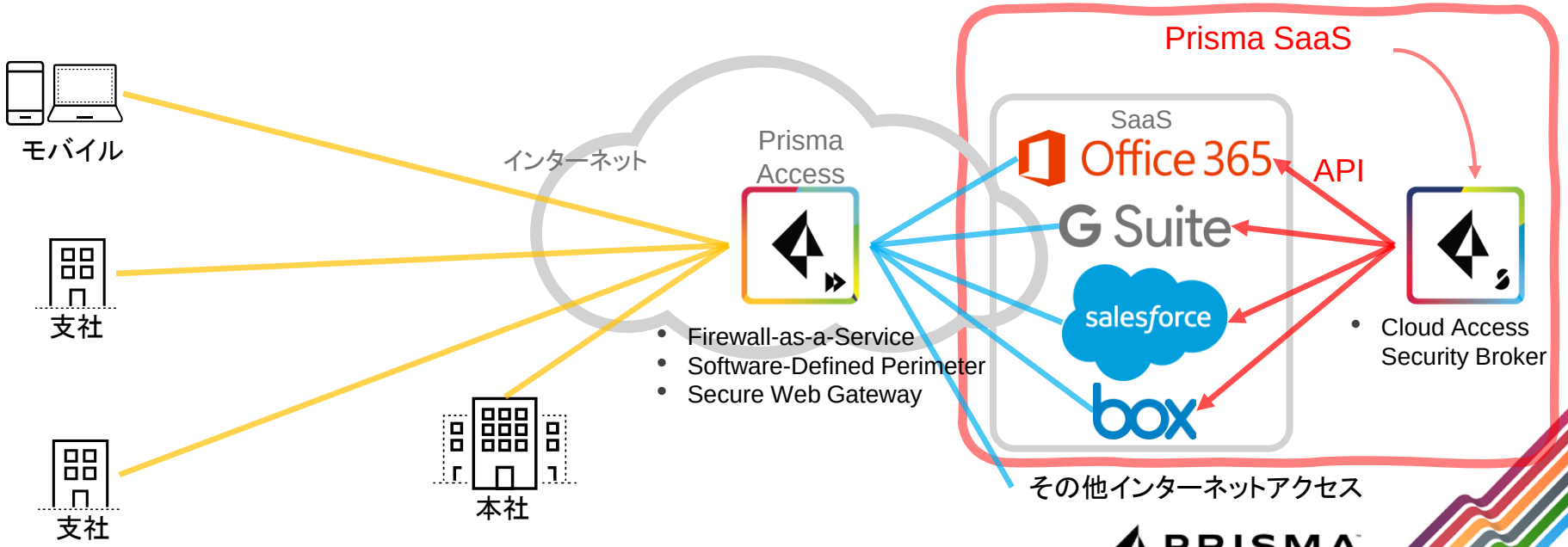
3

SaaSの使用をコントロールする

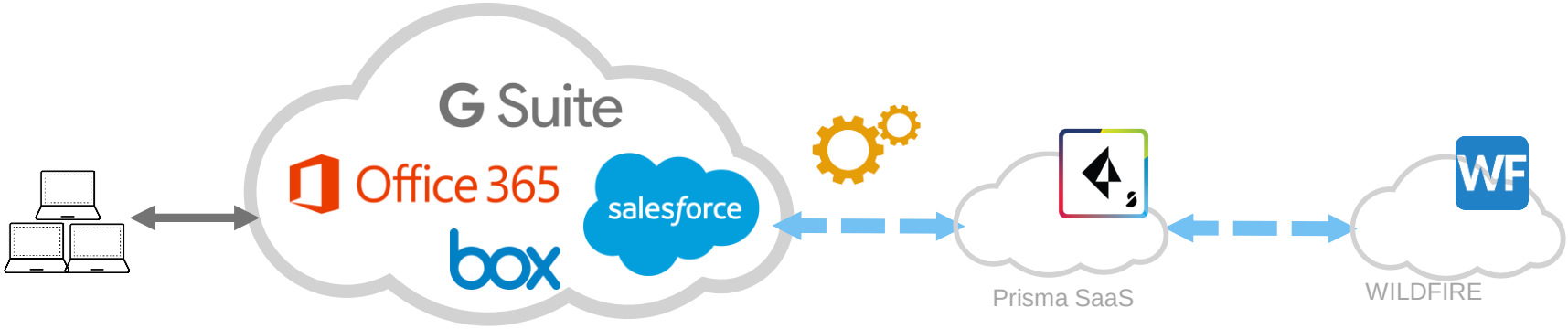
PRISMA BY PALO ALTO NETWORKS

「クラウドシフト」と「モバイルシフト」に対応したネットワーク構成 (2)

- Prisma SaaSがSaaSアプリケーションに直接接続して、データ分類、データ漏洩防止、脅威検出の機能を提供
- Office 365、G Suite、Salesforce、BoxなどSaaSアプリケーションの意図しないデータ公開、悪意のある部外者を排除



Prisma SaaSの特長



ユーザに囚われない

エージェントも不要で、
アプリの制限もなし

デプロイメントに囚われない

ネットワークの変更も、
HW/SWのインストールも
必要なし

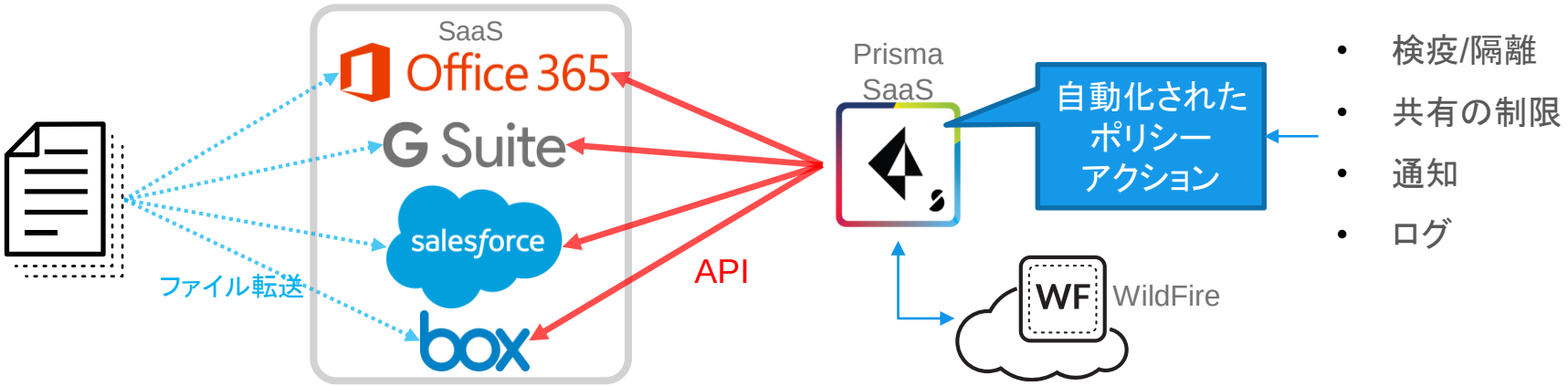
脅威の防御

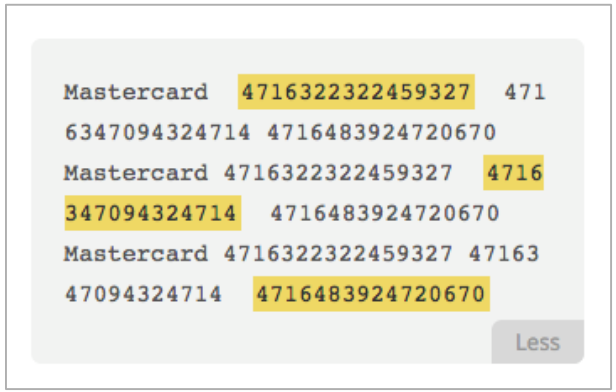
Wildfireを通じて、
マルウェアを検知

既存ファイルへもポリシー適用

未来のファイルだけでなく
サービス開始前に存在していた
ファイルに対しても
ポリシーを適用可能

Prisma SaaSによるリスク軽減





- 高度なデータ分類
  - 財務書類や法的文書など、機密ドキュメントを自動的に識別
  - ドキュメント分類のカスタマイズも可能
- 機密データ漏洩の防止
  - クレジットカード番号、SSH 鍵、社会保障番号など、一般的な機密データ文字列がないか、ドキュメントを検査
- Wildfire統合によるマルウェアの排除

「クラウドシフト」と「モバイルシフト」の課題③：IaaS/PaaS特有のセキュリティ

パブリッククラウドの責任共有モデル

カテゴリ	パブリッククラウドの責任範囲
データ	自己責任
アプリケーション	
ミドルウェア	
OS	
サーバ	クラウドベンダー責任
ストレージ	
ネットワーキング	
仮想化	

攻撃者

パブリッククラウドベンダーは、自身が提供する
全てのサービスを実行するインフラストラクチャの保護に
責任を負います。
しかし、クラウド内のOS以上のアプリケーションやデータは、
お客様自身で保護する必要があります。

① 管理機能と可視化の不足

- パブリッククラウド環境の構成管理情報、リアルタイムにリソースやネットワーク構成を把握するための仕組みがない
- 多くの特権管理者に対するガバナンスの不足
- (困)未検知の設定ミス増加
- (困)リスク予測管理が困難

② コンプライアンス対応が困難

- 日々変化、拡大するクラウド環境へのコンプライアンス対応は非常に困難
- コンプライアンス基準を実環境へ反映するには、コンサルタントとアーキテクト両方の知識が必要
- (困)コンプライアンス対応へかかるコストが大きい

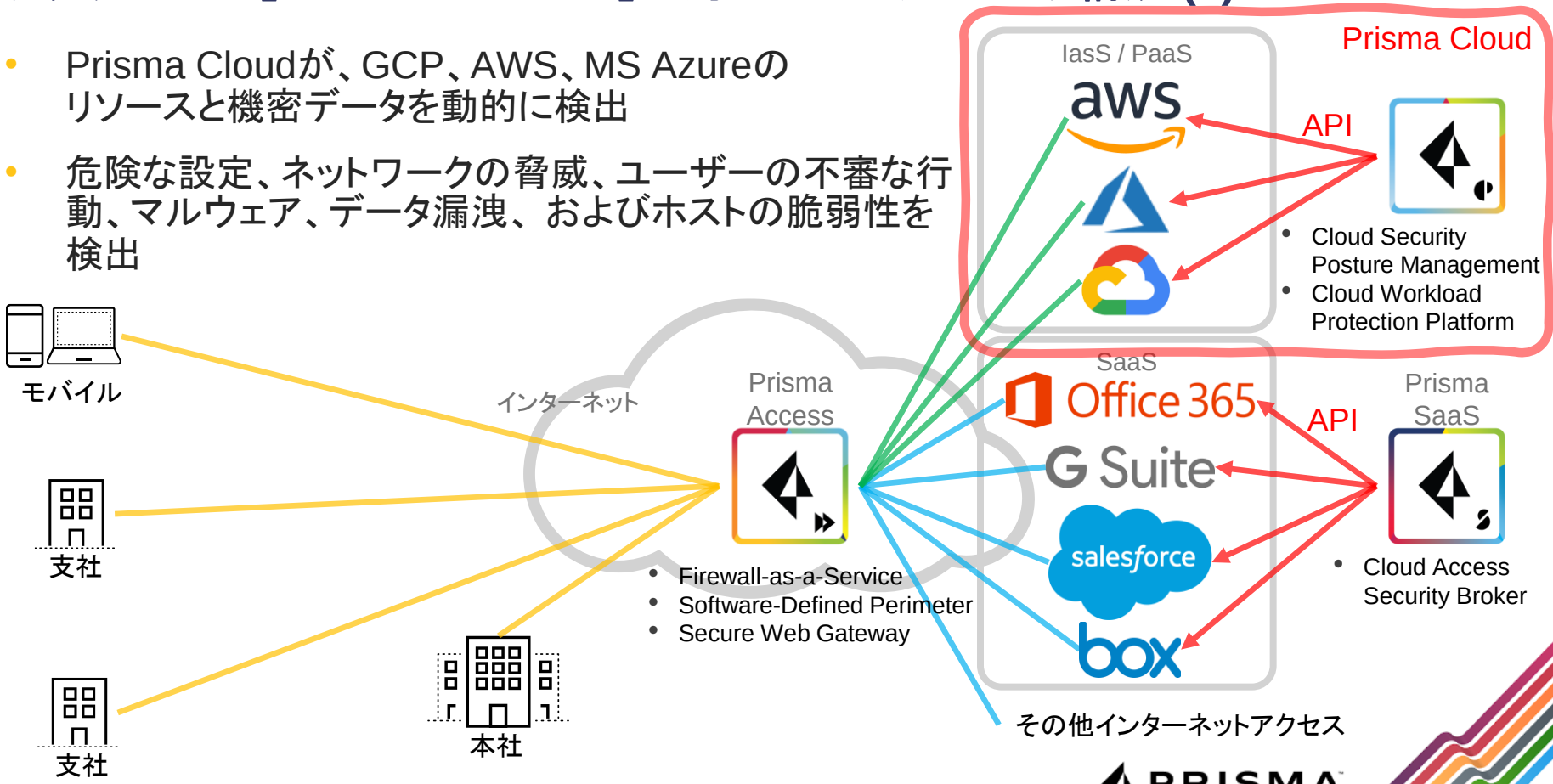
③ 脅威の発見・対応の遅れ

- 典型的なSEIMはクラウドに対応しておらず、パブリッククラウド上の大量のデータと変化対応スピードが問題に
- (困)オンプレには無かった、クラウド特有のアラート対応が必要
- (困)原因詳細や対処方法なしのアラートによる対応の遅延

PRISMA BY PALO ALTO NETWORKS

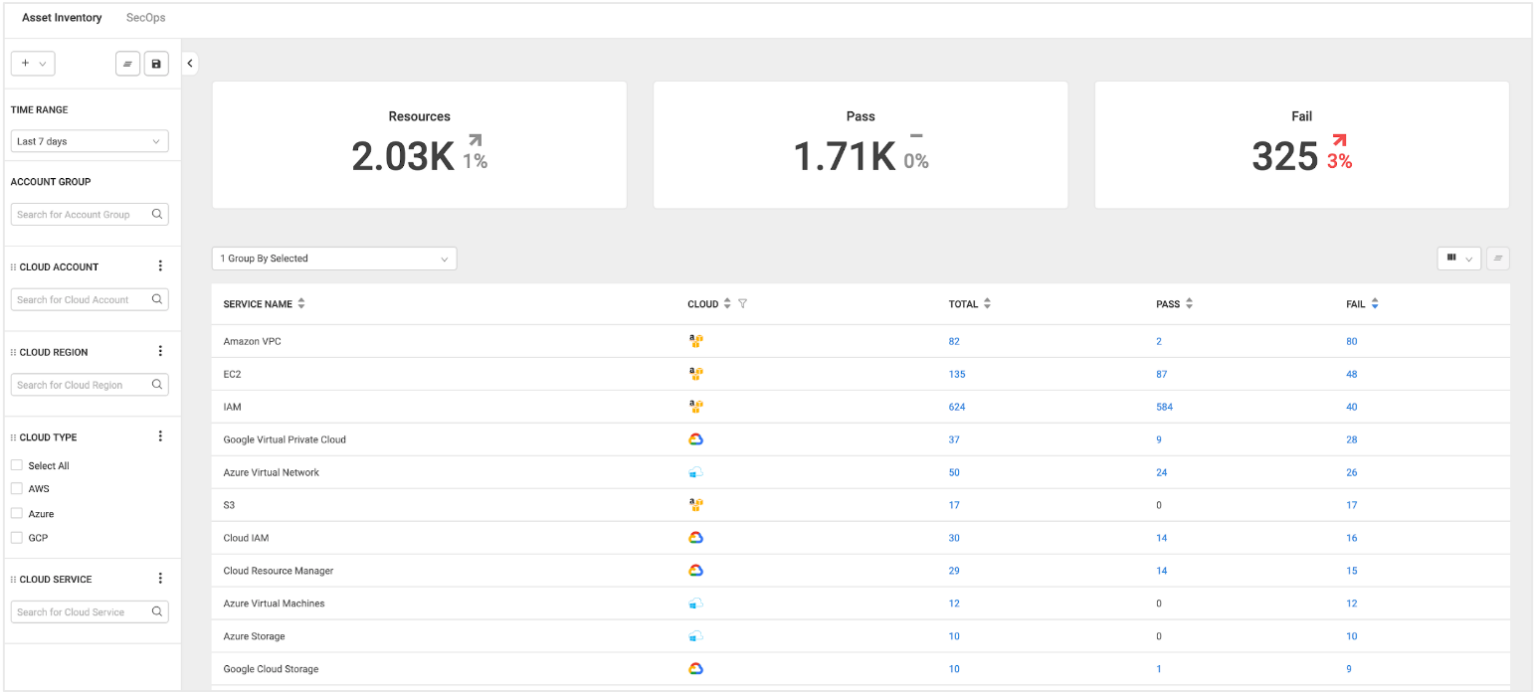
「クラウドシフト」と「モバイルシフト」に対応したネットワーク構成 (3)

- Prisma Cloudが、GCP、AWS、MS Azureのリソースと機密データを動的に検出
- 危険な設定、ネットワークの脅威、ユーザーの不審な行動、マルウェア、データ漏洩、およびホストの脆弱性を検出



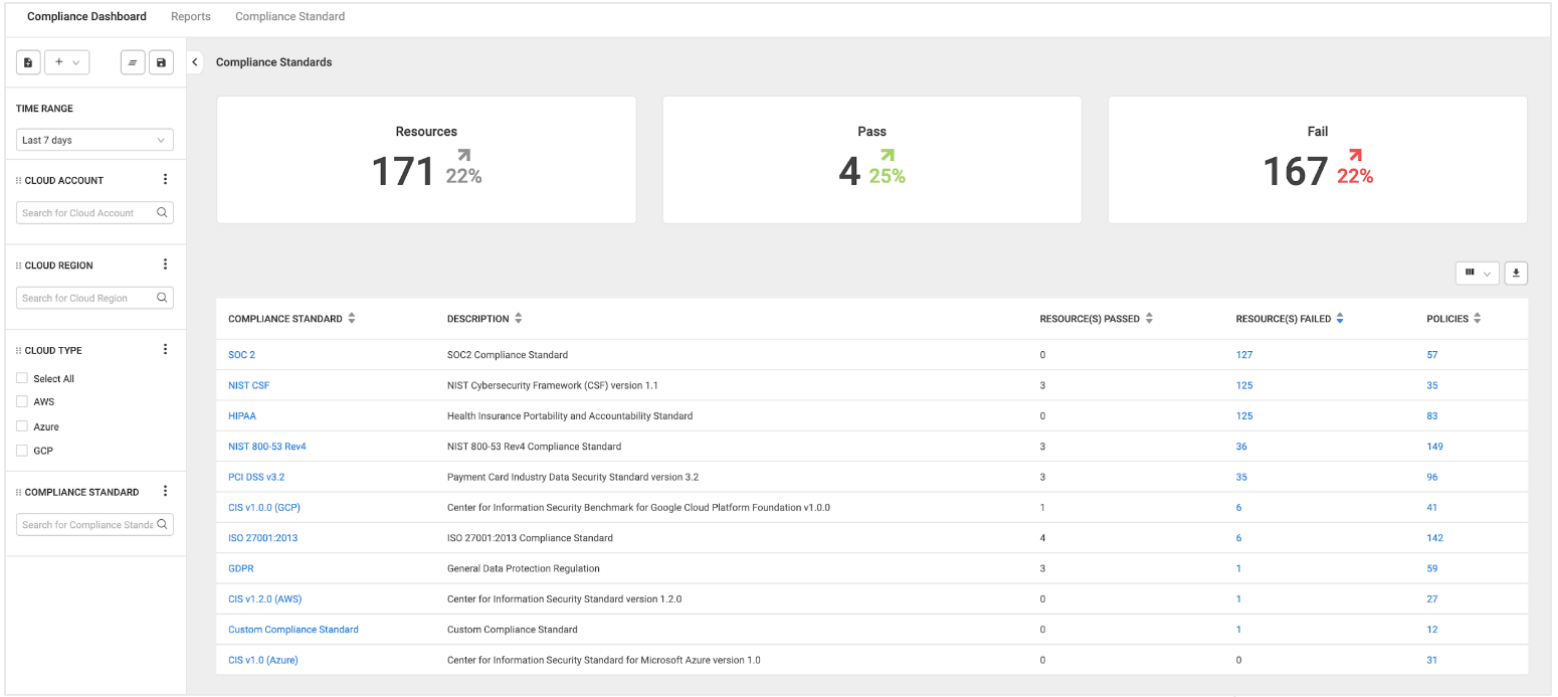
① クラウド上のどこに何があるのかを可視化

- リアルタイムのアセットインベントリー/CMDB
- アプリケーションの識別
- 変更履歴の管理



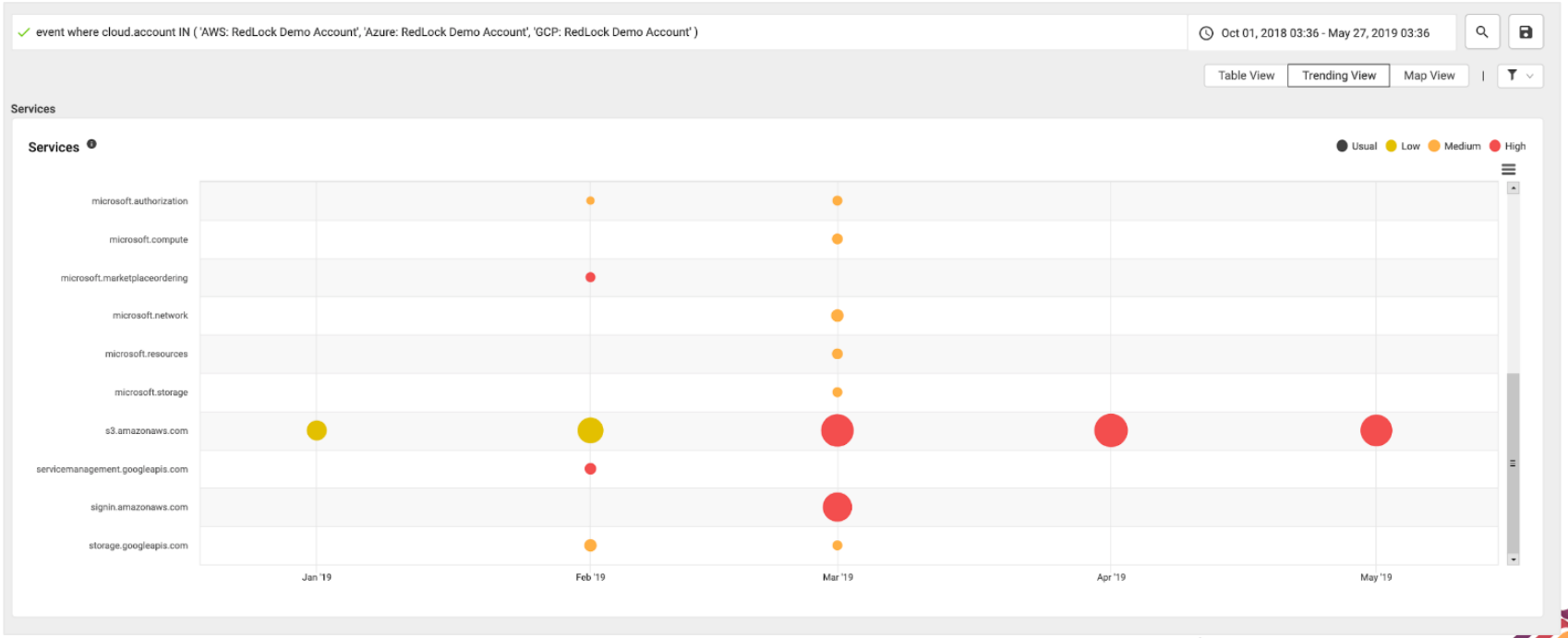
② セキュリティとコンプライアンスの要件を容易にモニタリング

- 業界標準コンプライアンスの監視とレポート
- アクセス・ガバナンスの有効化
- 構成の差異を検出



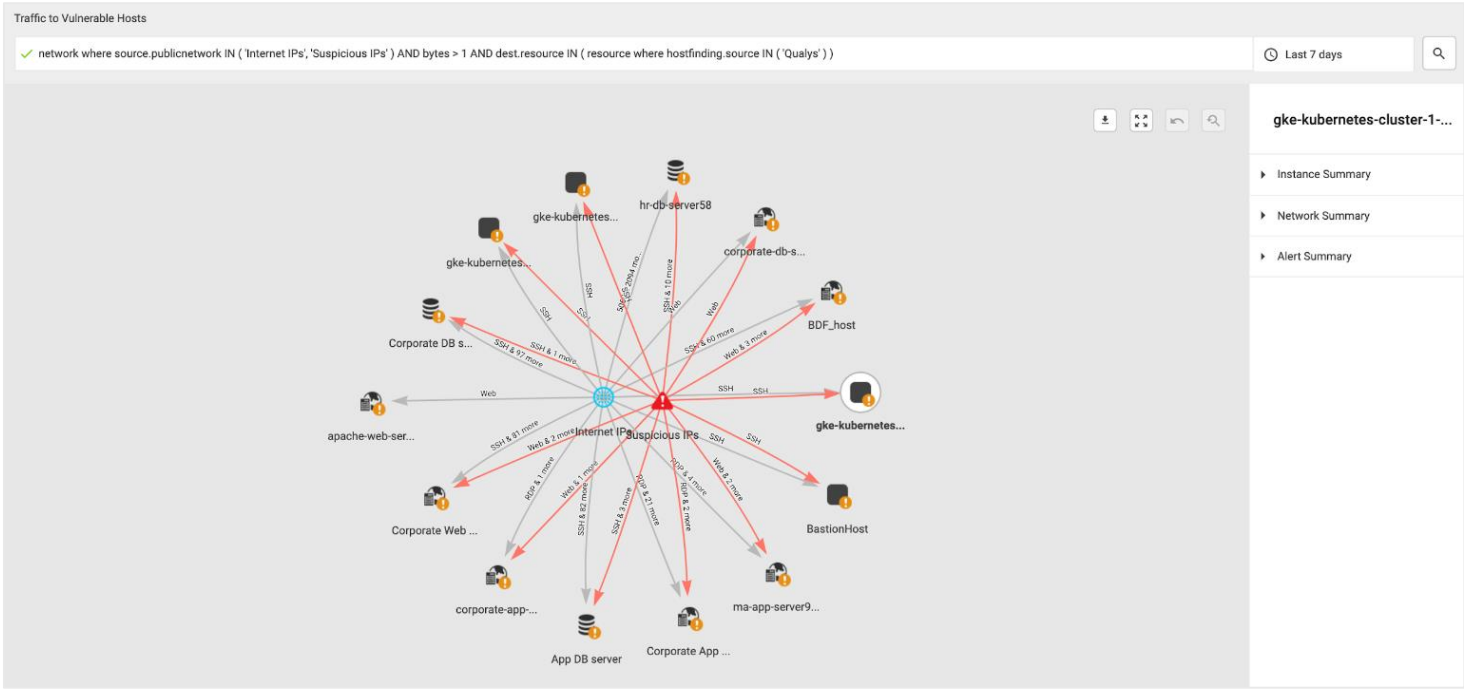
③-1 クラウドの脅威からの保護 (検知)

- ユーザー/エンティティの行動監視
- ネットワーク脅威検知
- 脆弱性のあるホストのリスク評価



③-2 クラウドの脅威からの保護 (インシデント調査)

- クエリによるデータ抽出と可視化
- 現在から過去に渡るインシデントの調査
- ドリルダウンと影響範囲の分析



まとめ：Prisma導入によって得られること

データ、資産、リスクの
可視性

一貫性のある包括的な
セキュリティ

スピードと俊敏性

運用コストと複雑さの
軽減

Thank You