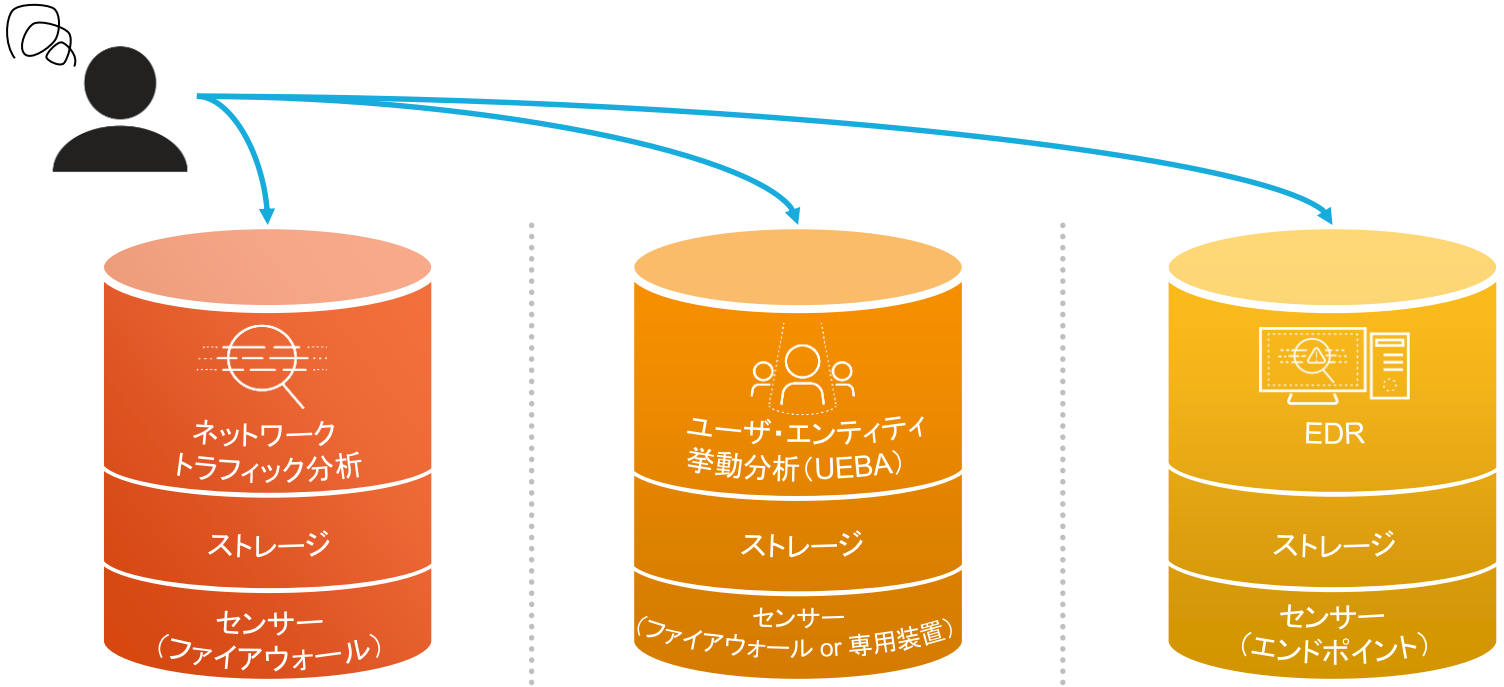
まだEDR？
パロアルトネットワークスの
推奨するXDRとは？

高度なサイバー攻撃にはディテクション(検知)とレスポンスが必要

99%以上のサイバー攻撃は
正しいツールを使うことで阻止可能

1%未満の
サイバー攻撃

課題：サイロ化された各セキュリティ機能。。。

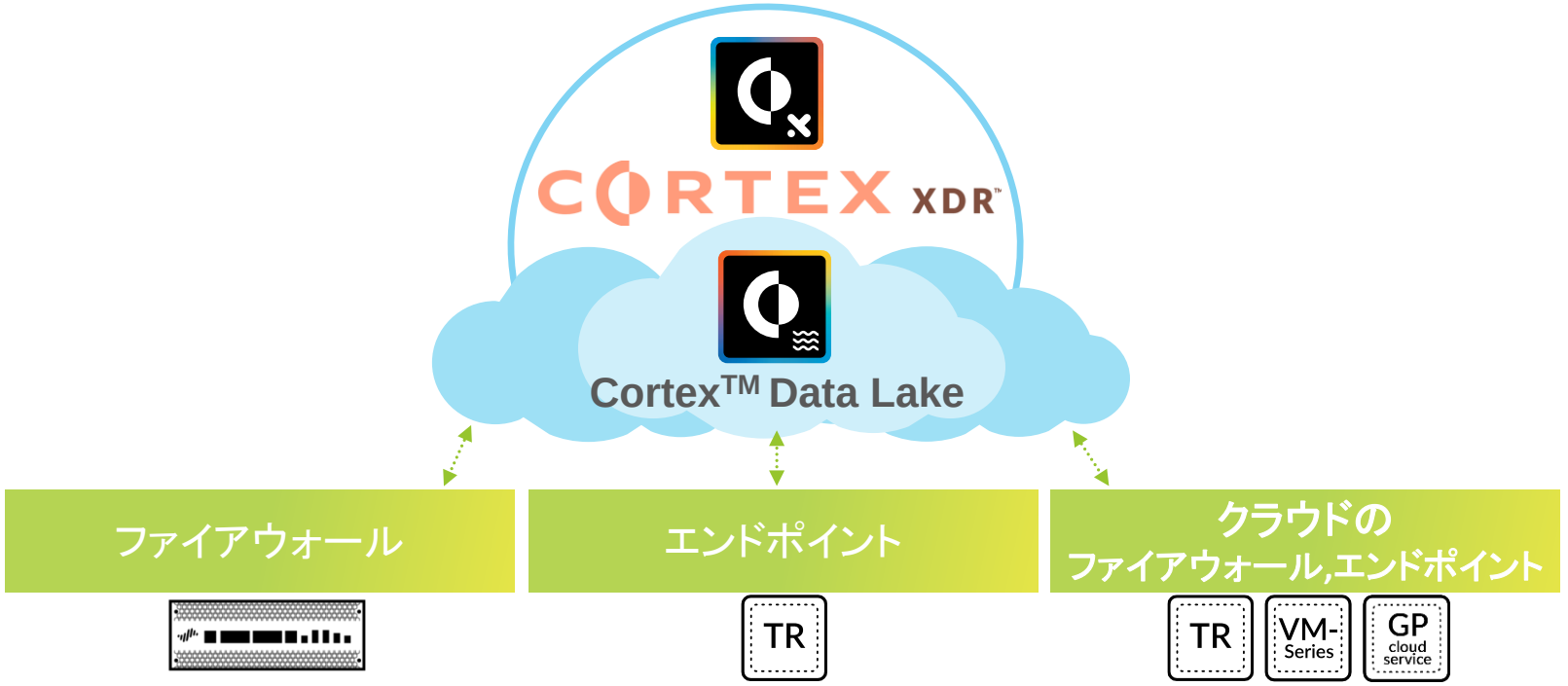


大量のアラート生成

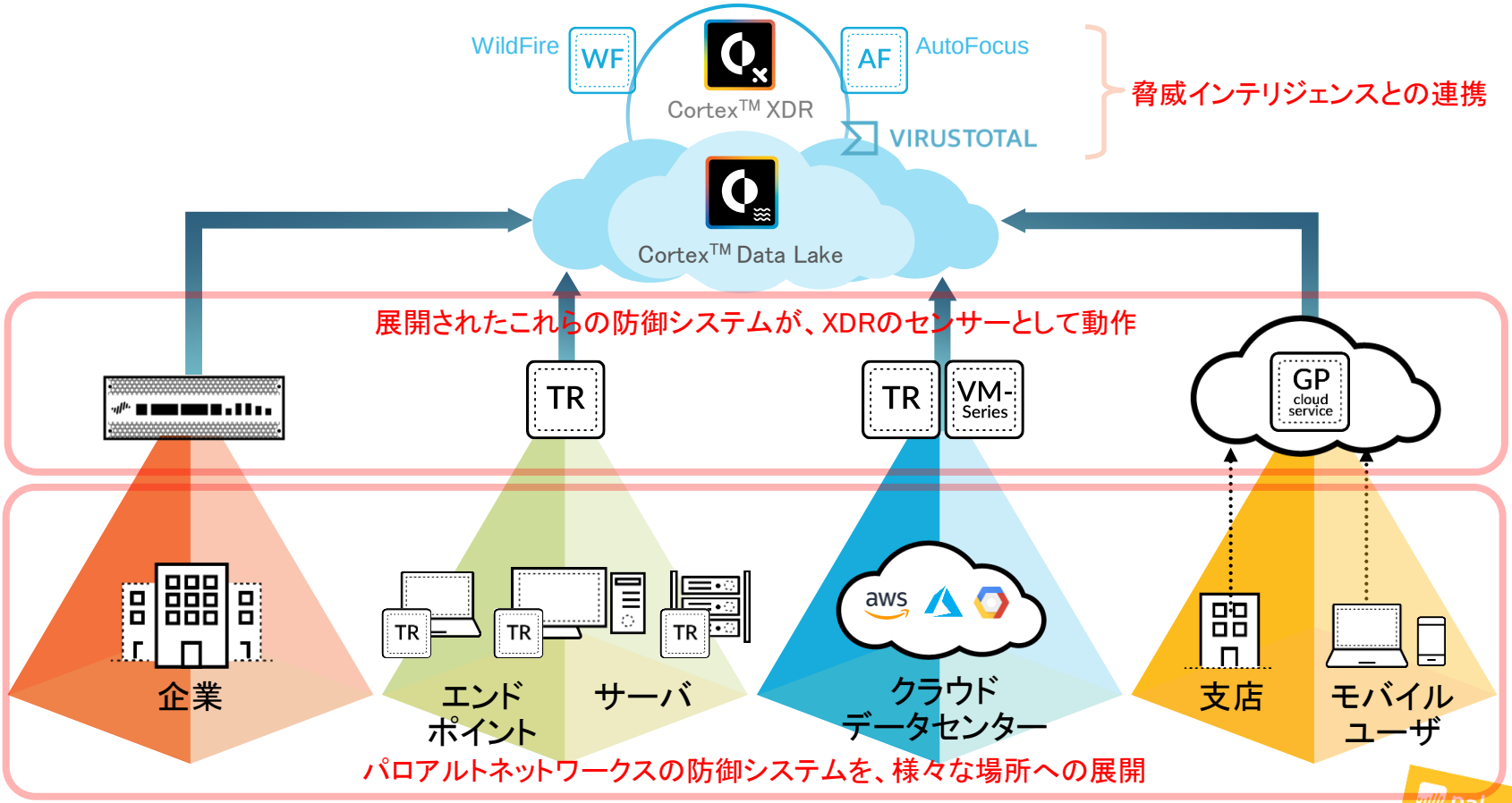
アラートに関連すると思われるデータを手動収集

人海戦術での相関分析が難しい

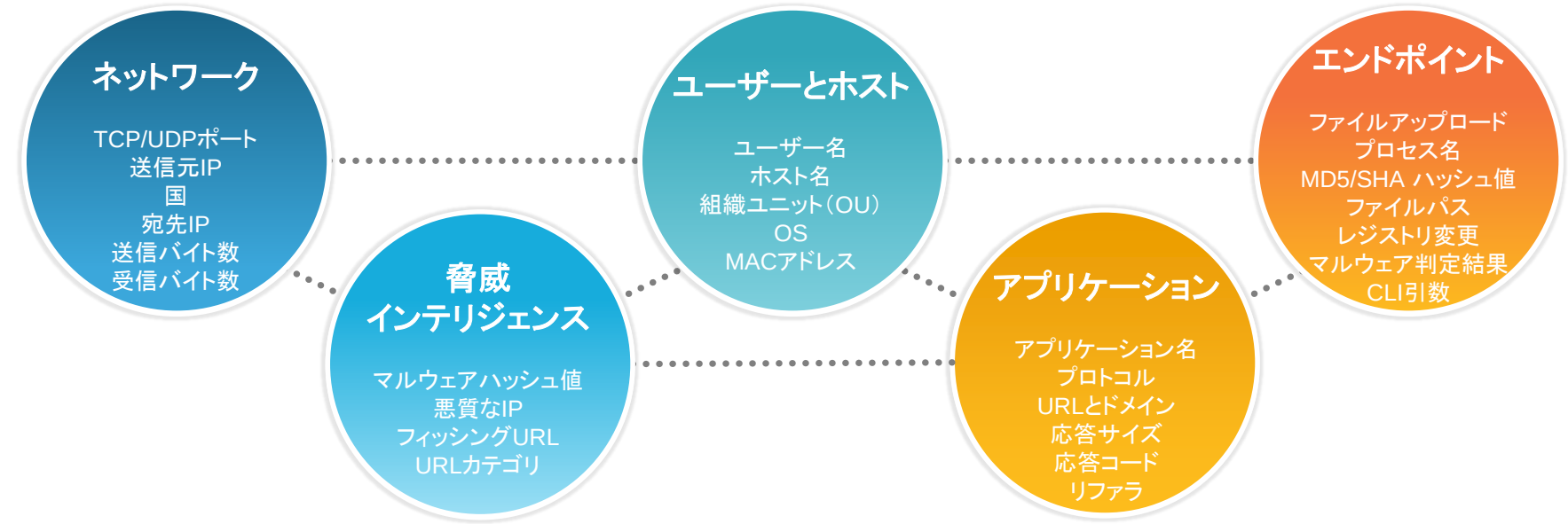
解決策：Cortex XDR 単一ベンダーによる包括的なディテクション&レスポンス



ネットワーク、エンドポイント、クラウド全ての脅威を可視化



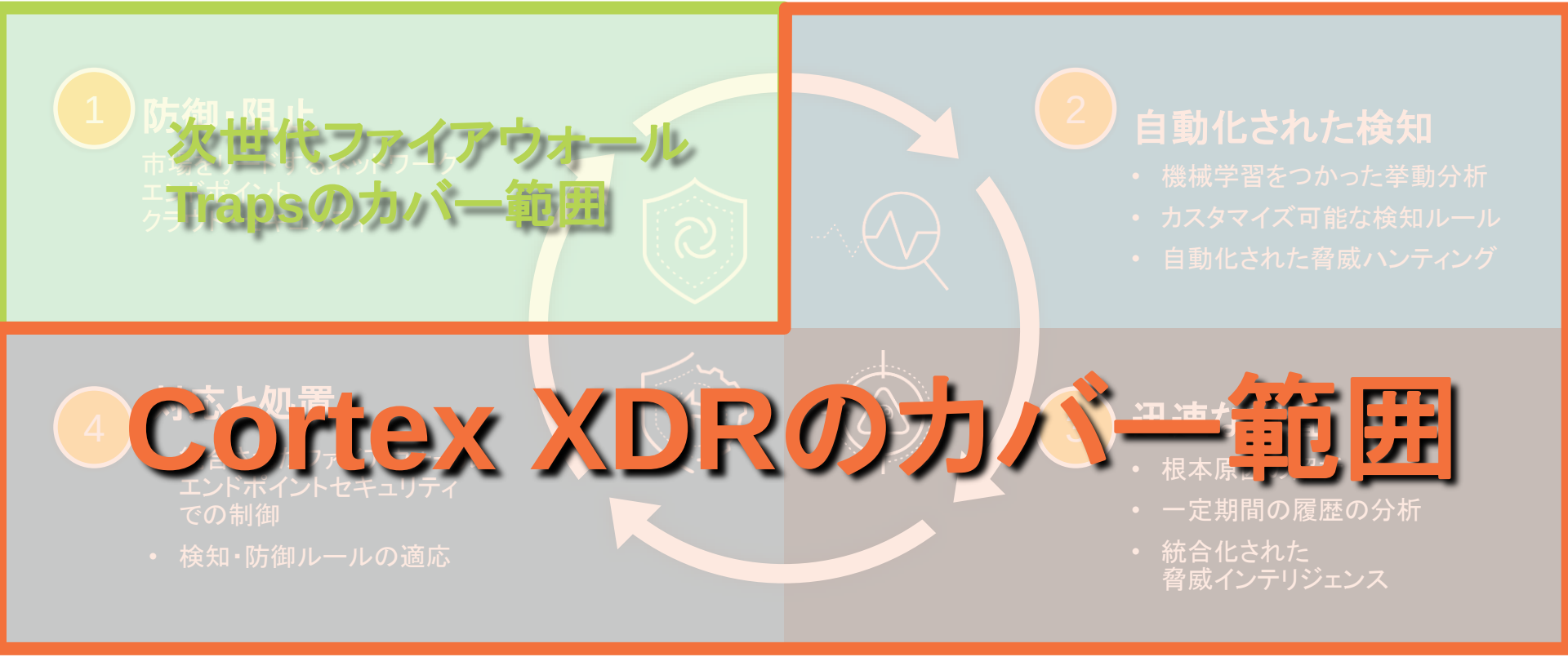
リッチデータとビッグデータでデータドリブン



AIの学習と調査に必要な
リッチデータを収集

自動的にデータを相関させ
わかりやすい前後関係情報を構築

Cortex XDR で組織のセキュリティを総合的かつ効率的に高める



次世代ファイアウォール
Trapsのカバー範囲

Cortex XDRのカバー範囲

Cortex XDR で組織のセキュリティを総合的かつ効率的に高める

1 **防御・阻止**

市場をリードするネットワーク
エンドポイント、
クラウド・セキュリティ

2 **自動化された検知**

- 機械学習をつかった挙動分析
- カスタマイズ可能な検知ルール
- 自動化された脅威ハンティング

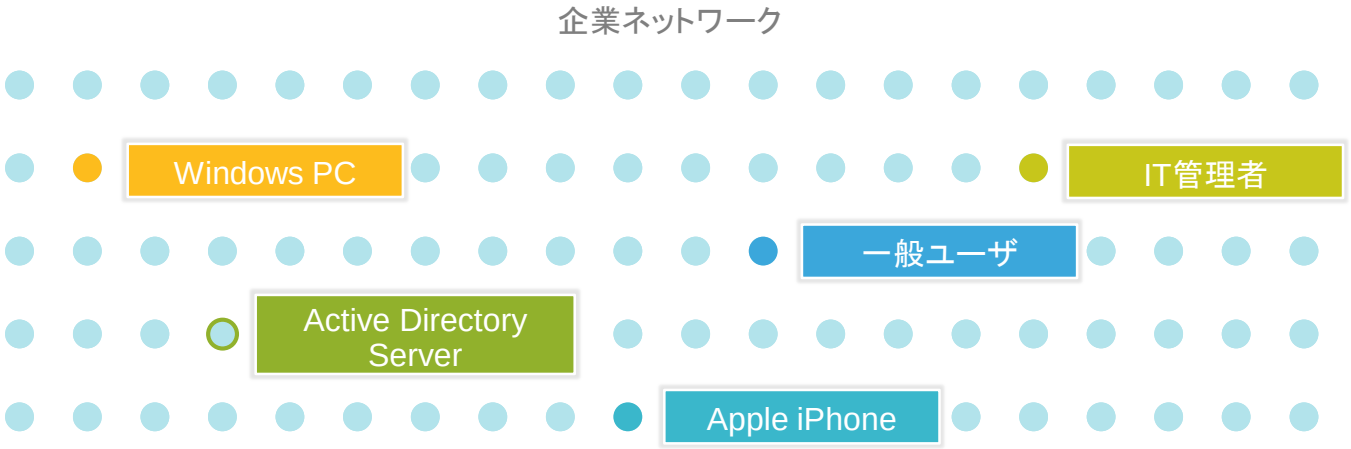
3 **迅速な調査**

- 根本原因の解析
- 一定期間の履歴の分析
- 統合化された
脅威インテリジェンス

4 **対応と処置**

- 統合されたファイアウォール、
エンドポイントセキュリティ
での制御
- 検知・防御ルールの適応

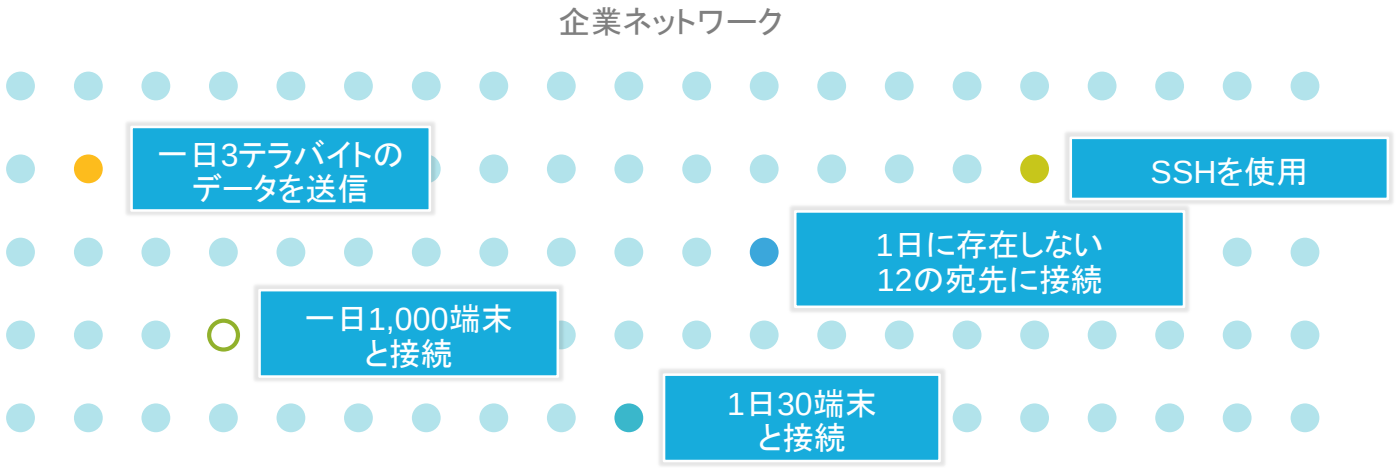
AIによる分析で攻撃を自動検知



1

ユーザとデバイスの
アクティビティを分析

AIによる分析で攻撃を自動検知



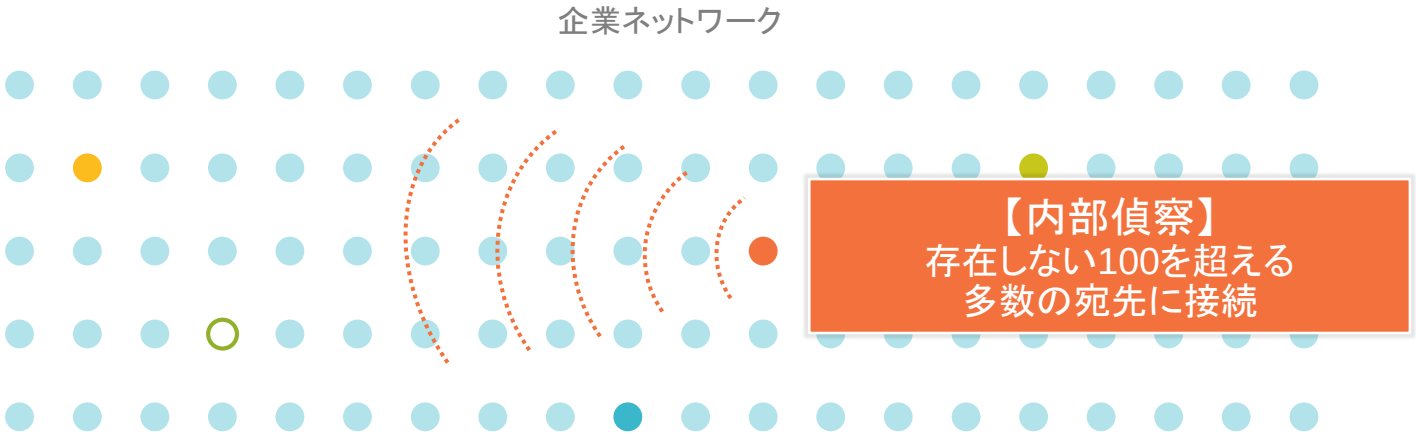
1

ユーザとデバイスの
アクティビティを分析

2

ユーザやデバイスの
ふるまいをプロファイル化

AIによる分析で攻撃を自動検知



1
ユーザとデバイスの
アクティビティを分析

2
ユーザやデバイスの
ふるまいをプロファイル化

3
攻撃の可能性を示唆する
不審な行動を見つけ出す

Cortex XDR で組織のセキュリティを総合的かつ効率的に高める

1

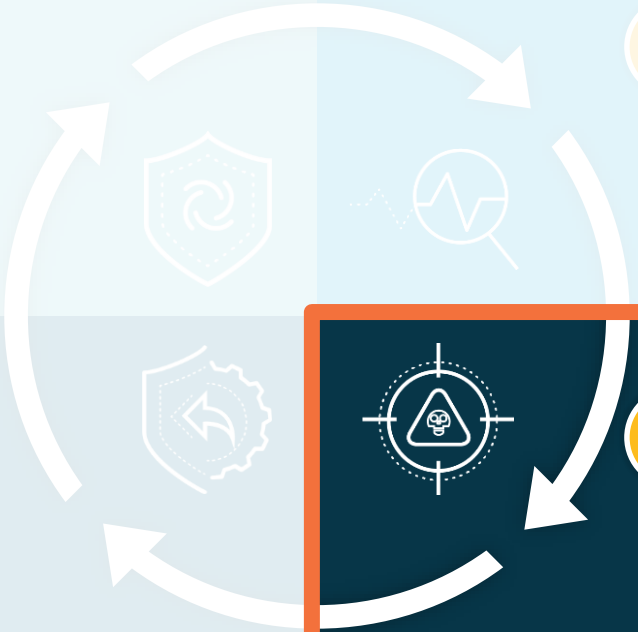
防御・阻止

市場をリードするネットワーク
エンドポイント、
クラウド・セキュリティ

2

自動化された検知

- 機械学習をつかった挙動分析
- カスタマイズ可能な検知ルール
- 自動化された脅威ハンティング



3

迅速な調査

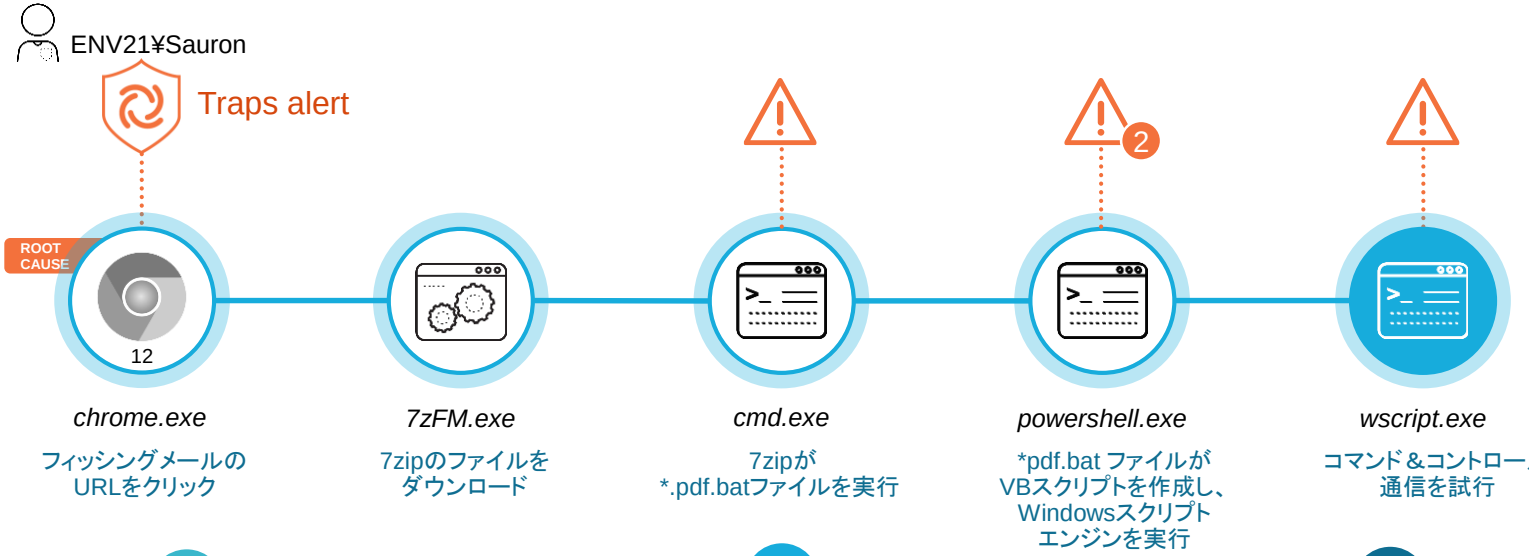
- 根本原因の解析
- 一定期間の履歴の分析
- 統合化された
  脅威インテリジェンス

4

対応と処置

- 統合されたファイアウォール、
  エンドポイントセキュリティ
  での制御
- 検知・防御ルールの適応

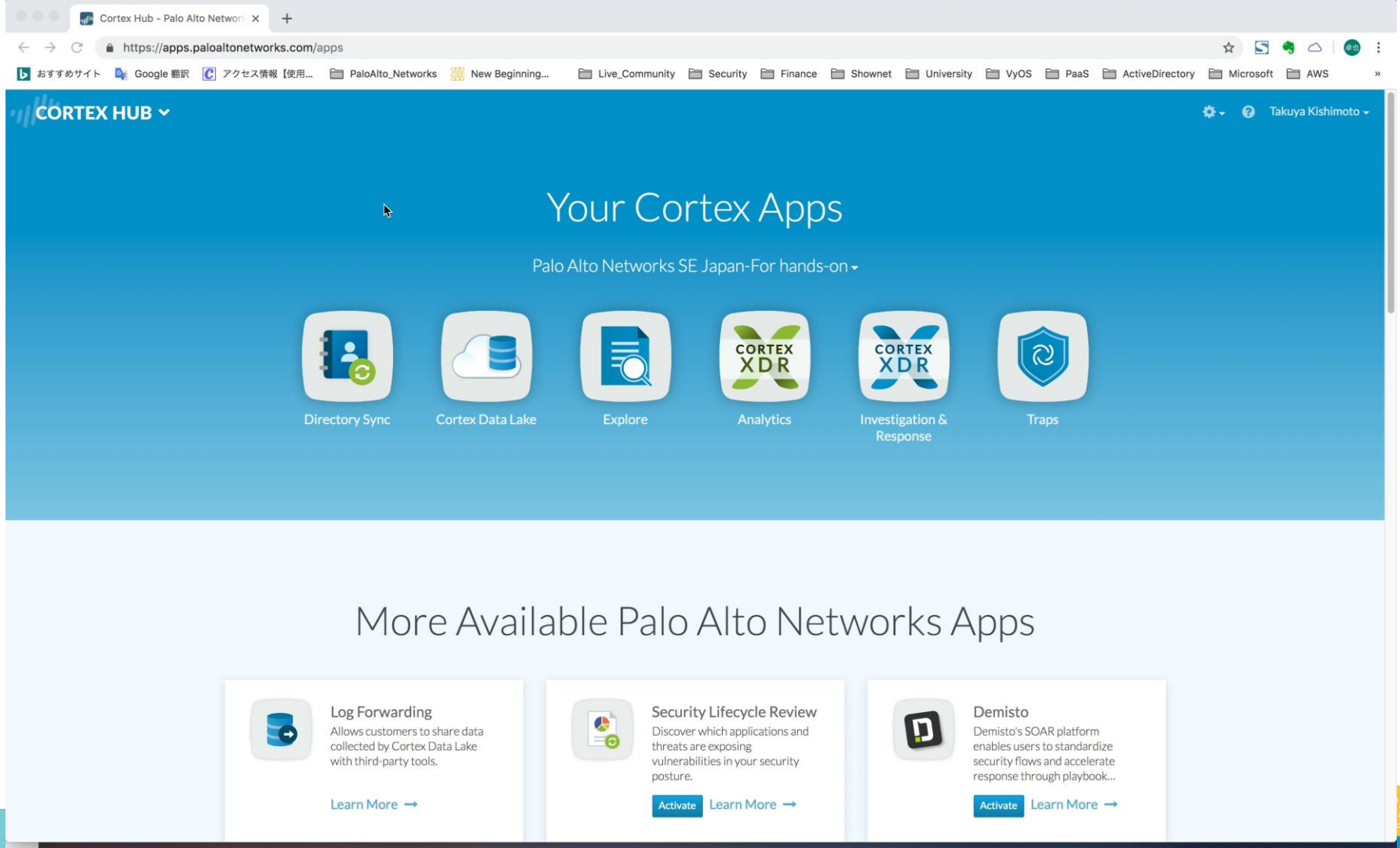
迅速な調査：調査作業を簡素化、迅速化



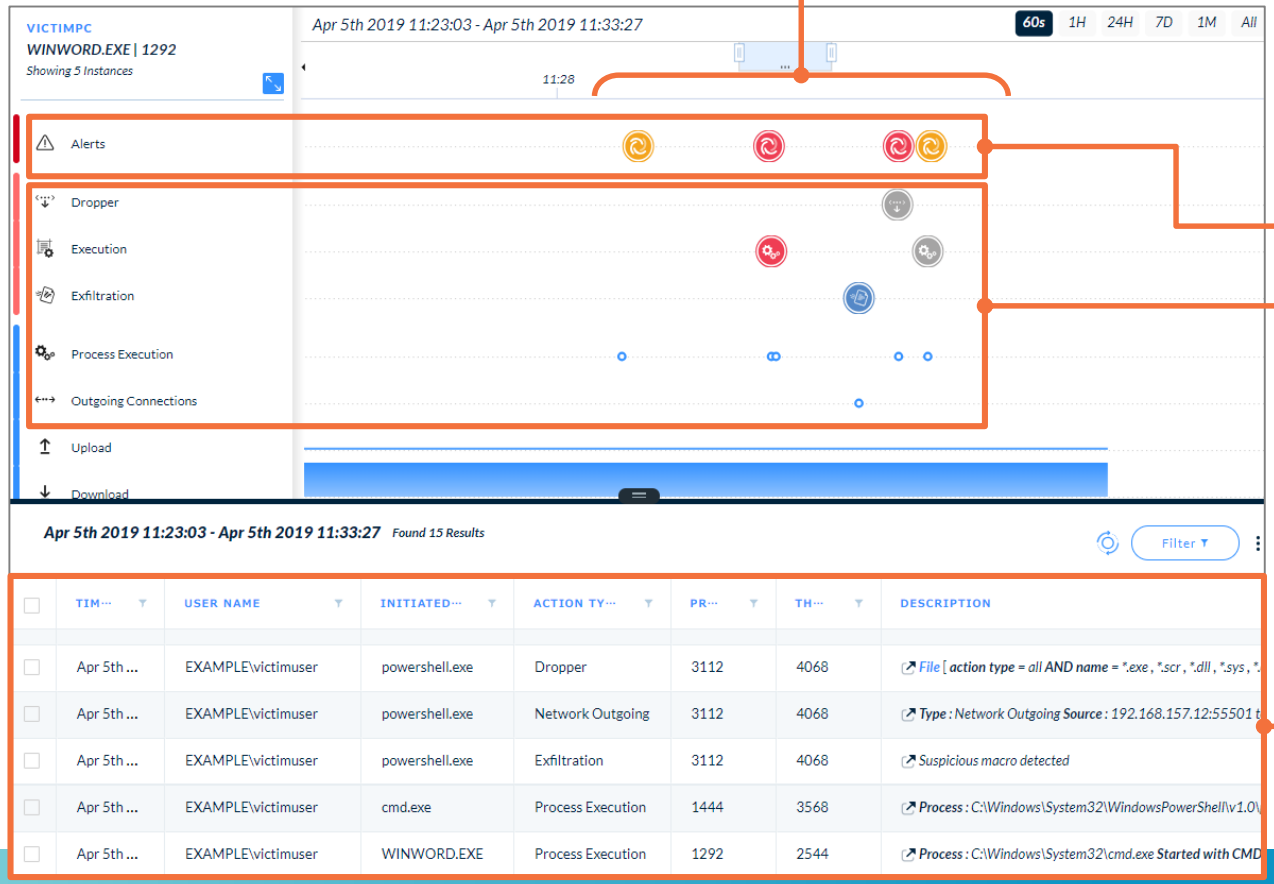
1 様々なアラートを ワンクリックで調査

2 自動的にアラートの 根本原因を明確化

3 脅威インテリジェンスや 前後関係でインシデント特定 と重要度を判定


Cortex Hub - Palo Alto Networ
https://apps.paloaltonetworks.com/apps
CORTEX HUB
Takuya Kishimoto
Your Cortex Apps
Palo Alto Networks SE Japan-For hands-on
Directory Sync
Cortex Data Lake
Explore
Analytics
Investigation & Response
Traps
More Available Palo Alto Networks Apps
Log Forwarding
Allows customers to share data collected by Cortex Data Lake with third-party tools.
Learn More
Security Lifecycle Review
Discover which applications and threats are exposing vulnerabilities in your security posture.
Activate
Learn More
Demisto
Demisto's SOAR platform enables users to standardize security flows and accelerate response through playbook...
Activate
Learn More

タイムライン調査



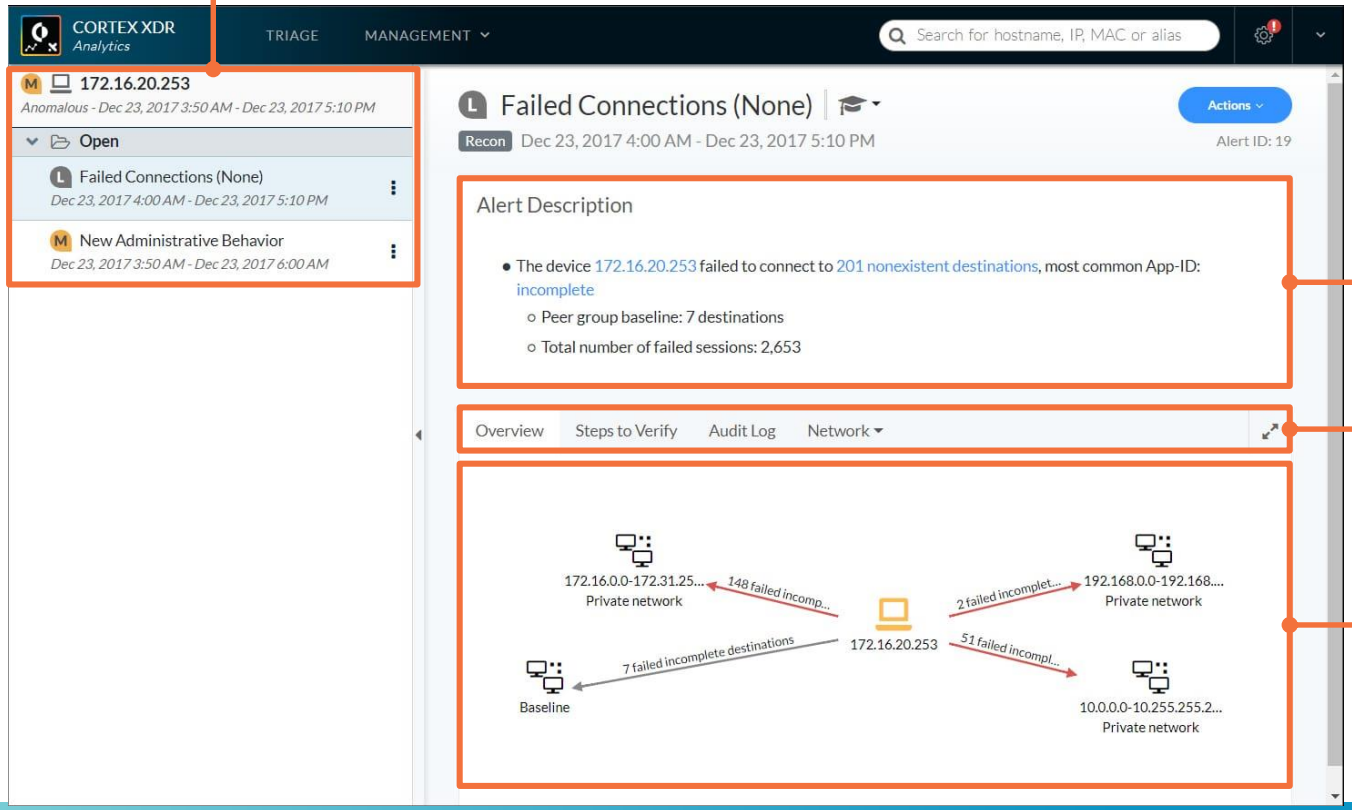
タイムライン

検知したアラート

マルウェアの
活動を攻撃フェーズ毎に
応じて自動分類

各プロセス動作
の分析

内部監視／内部不正対策



不審な行動を検知した
アラートを確認

検出理由

通信先の情報など
詳細内容の確認

動作の可視化

Cortex XDR で組織のセキュリティを総合的かつ効率的に高める

1 防御・阻止

市場をリードするネットワーク
エンドポイント、
クラウド・セキュリティ

2 自動化された検知

- 機械学習をつかった挙動分析
- カスタマイズ可能な検知ルール
- 自動化された脅威ハンティング

3 迅速な調査

- 根本原因の解析
- 一定期間の履歴の分析
- 統合化された
  脅威インテリジェンス

4 対応と処置

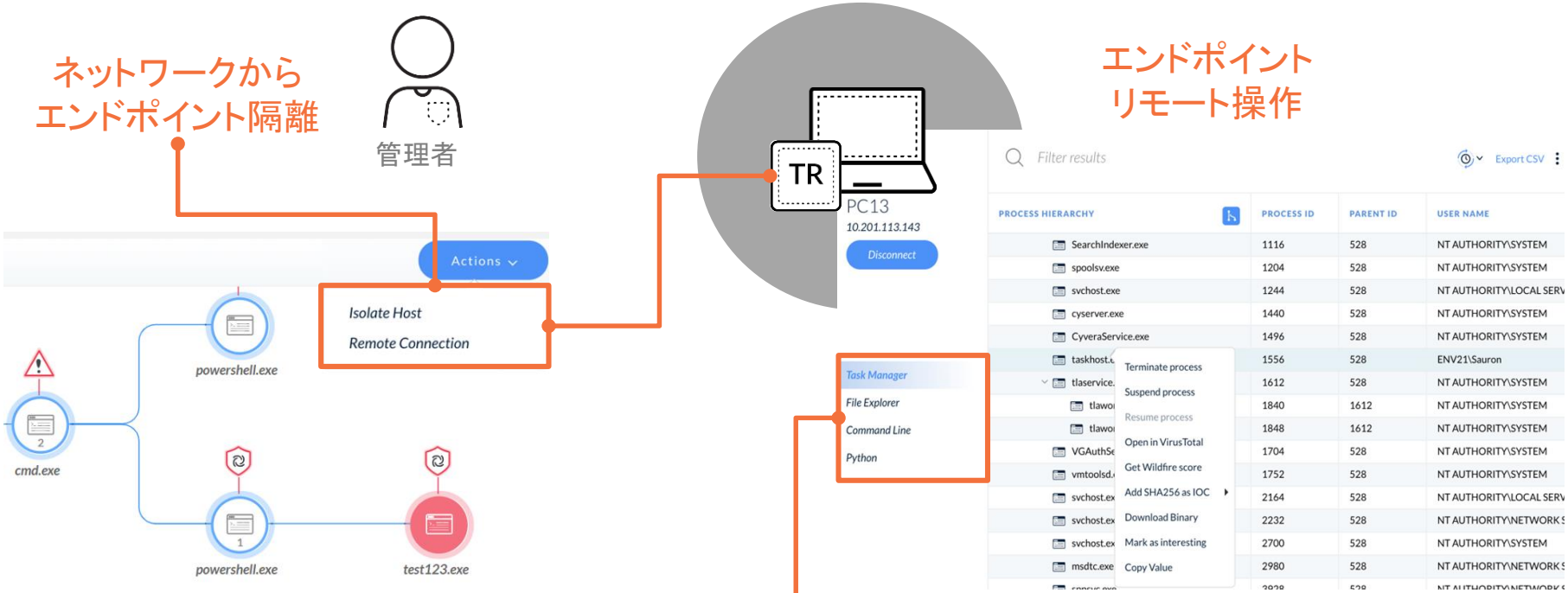
- 統合されたファイアウォール、
  エンドポイントセキュリティ
  での制御
- 検知・防御ルールの適応

簡単なレスポンス

ネットワークから
エンドポイント隔離

管理者

エンドポイント
リモート操作

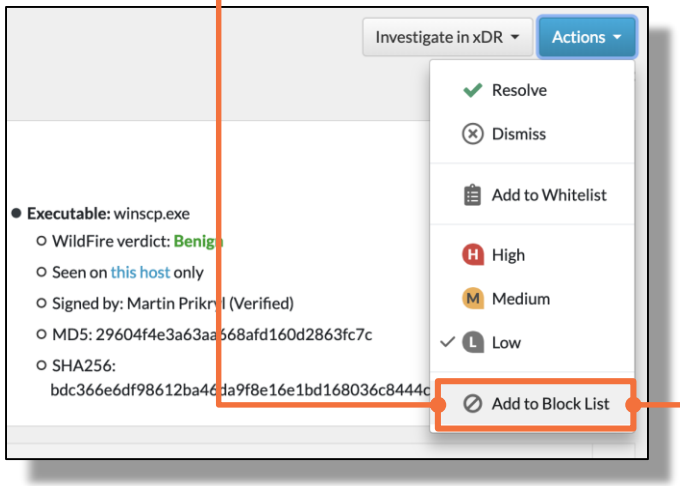


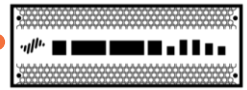
・プロセスの停止、調査
・ファイル操作
・コマンドライン操作

簡単なレスポンス

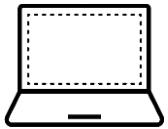
ネットワーク上で
通信を遮断

管理者





次世代ファイアウォール



CORTEX XDR により

エンドポイント、ネットワーク、クラウドを可視化し、
AIにより、効率的な運用性を持つ
ディテクション＆レスポンスを実現

 |

 |