APPDYNAMICS
part of Cisco

シスコオンラインセミナー

Ciscoの新・セキュリティソリューション「Cisco SecureApplication」ご紹介

森下 貢孝
シニアマネージャー セールスエンジニアリング
AppDynamics Business Unit

APPDYNAMICS
part of Cisco

We make the digital world work

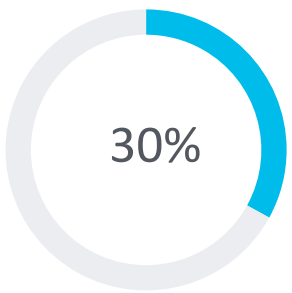
- Cisco SecureApplicationとAppDynamics
- AppDynamicsとは
  ～ビジネスオブザーバビリティプラットフォーム
- Cisco SecureApplicationご紹介
- デモ

APPDYNAMICS
part of Cisco

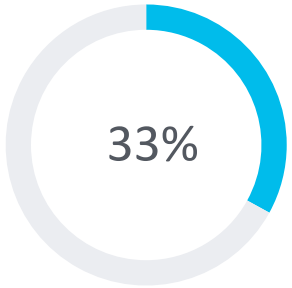
We make the digital world work

- Cisco SecureApplicationとAppDynamics
- AppDynamicsとは
  ～ビジネスオブザーバビリティプラットフォーム
- Cisco SecureApplicationご紹介
- デモ

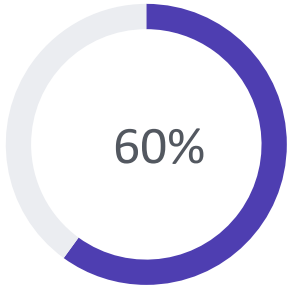
Security – 高く付く課題・代償



セキュリティ侵害の可能性



インハウス・モニタリングにより成功した攻撃の検知



最初の24時間でデータが失われた侵害事案

セキュリティホールの値段:

- ❑ CVE-2017-9805 $700M
- ❑ SQL Injection + XSS $300M
- ❑ Remote Access Trojan $200M

データ侵害発生による
平均総コスト

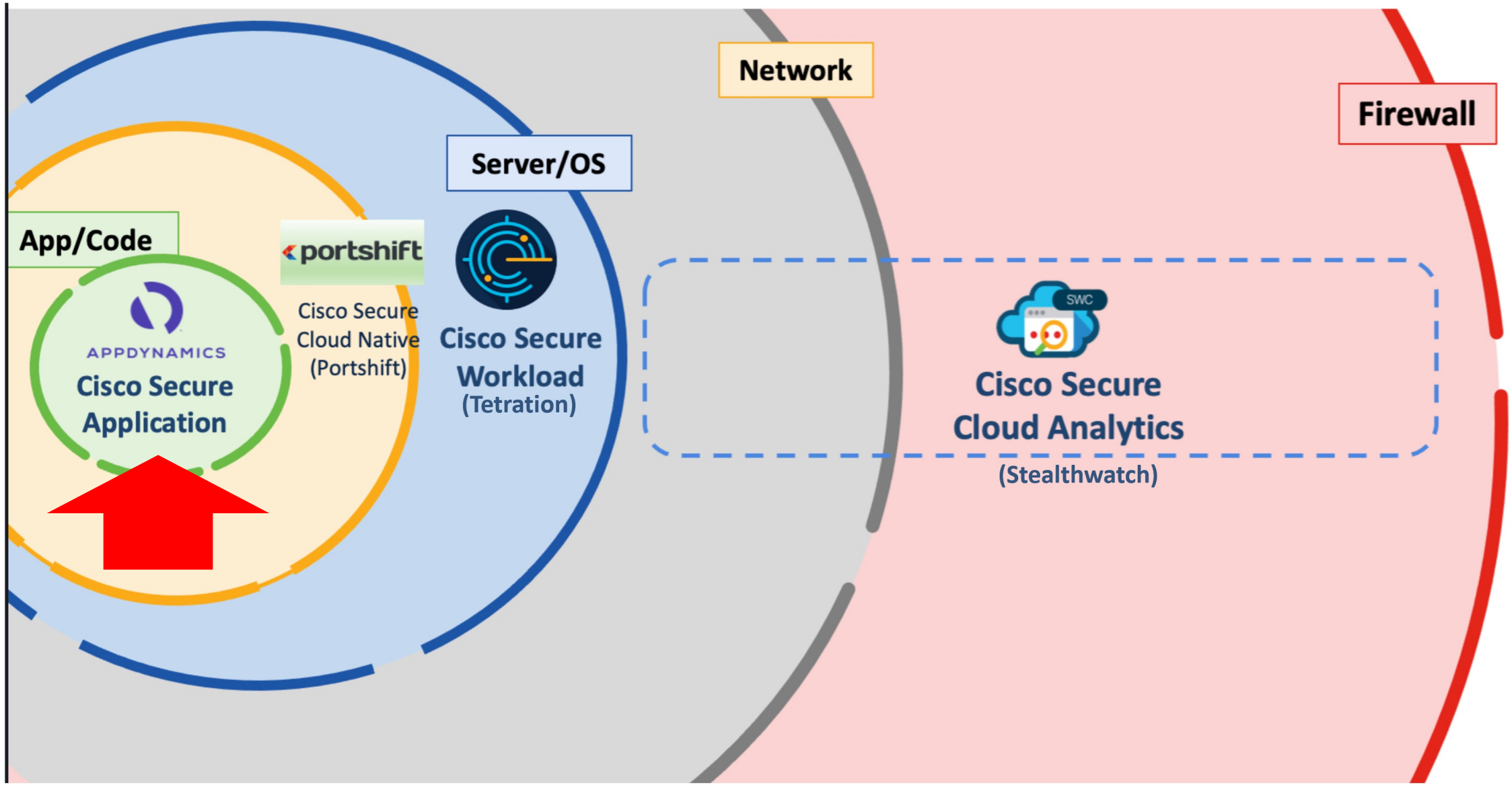
~$4M

侵害を特定し
封じ込めるまでの時間

270+ days

Sources: Cost of a Data Breach Report, Ponemon 2019
https://www.varonis.com/blog/data-breach-response-times/

Cisco Secure Applicationの位置づけ



APPDYNAMICS
part of Cisco

We make the digital world work

- Cisco SecureApplicationとAppDynamics
- AppDynamicsとは
  ～ビジネスオブザーバビリティプラットフォーム
- Cisco SecureApplicationご紹介
- デモ

AppDynamicsソリューションとは

2008年創業。アプリケーション性能をコードレベルで自動監視

Java / .NET / PHP / Node.js / Python / Go / C & C++ アプリケーションを監視。カスタムコードも標準でサポート

2014年に、監視範囲を拡大。エンド-to-エンドでフルスタックを監視

ブラウザ、モバイルアプリ、IoTのエンドユーザーエクスペリエンスを監視

データベース、サーバー、OS、ネットワーク等もフルスタックで監視

2016年に、監視している全ユーザー、全トランザクションからデータを捕捉し、ビジネスインパクトを分析する機能を追加

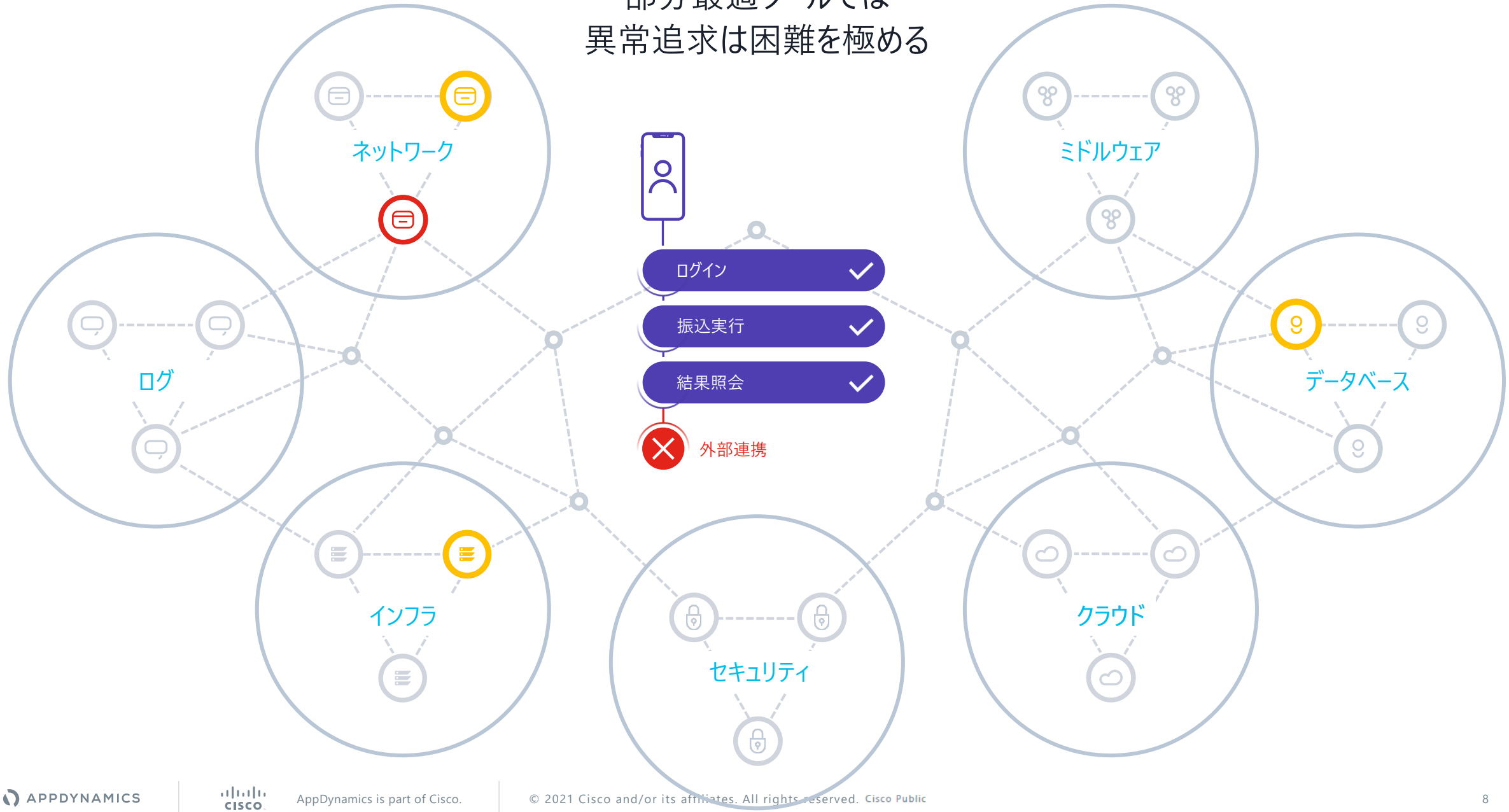
トランザクションからビジネスデータを抽出。
性能指標とともに、ビジネス指標も相関分析

ユーザー情報や端末情報を捕捉。障害や性能低下による サービス影響範囲を迅速に特定

SAP や z/OSメインフレームとの透過的監視。
ビジネス部門との連携をさらにサポート

①**インフラ資源**の視点 x ②**サービス性能**の視点 x ③**ビジネス指標**の視点
の**3つの視点**でアプリケーション性能とユーザー・ジャーニーを**横断監視**する統合型プラットフォーム。

部分最適ツールでは
異常追求は困難を極める




事業部
(売上とコンバージョンに関心)
ネットワーク部門
(N/W接続に責任)
ネットワーク
開発部門
(アプリケーション開発に注力)
ミドルウェア
データベース
ログ
クラウド
セキュリティ部門
(セキュリティ侵害と脆弱性対策に集中)
セキュリティ
インフラ部門
(技術スタックとシステム負荷に)
クラウド
インフラ
社内で無実を証明するまでの長い時間 (MTTI)

顧客は待たされ、事業部門は顧客からのクレームと売上逸失のダブルパンチ

App iQ

Map

Baseline

Diagnose

Enterprise

Business iQ

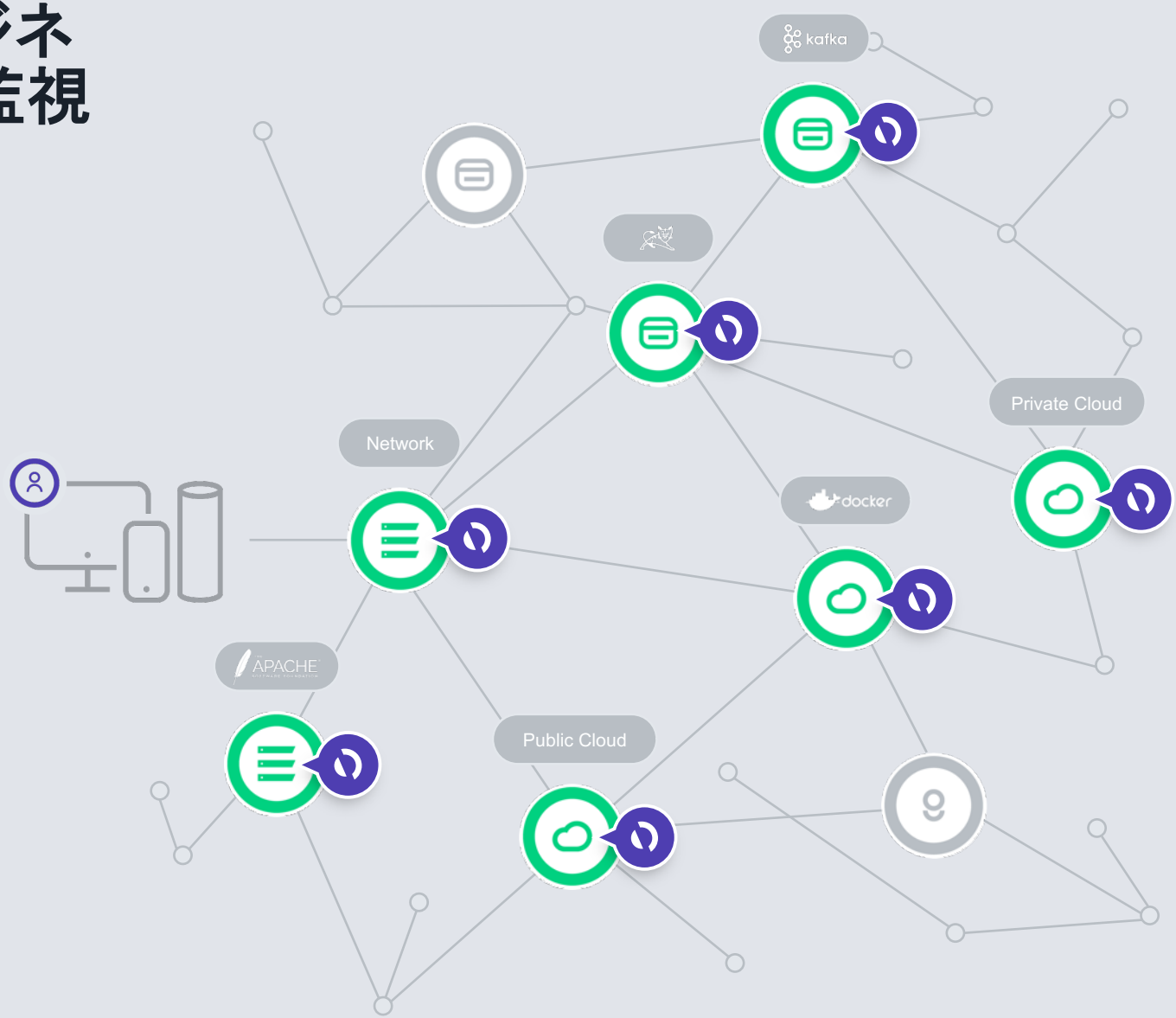
顧客が体験する全ビジネス・トランザクションを監視

Move Fast,
Follow Everything &
Focus on What Matters Most

— 低負荷のAgent

— アプリケーション環境全体にわたる導入

— 自動インスツルメント | 自動設定



App iQ

Map

Baseline

Diagnose

Enterprise

Business iQ

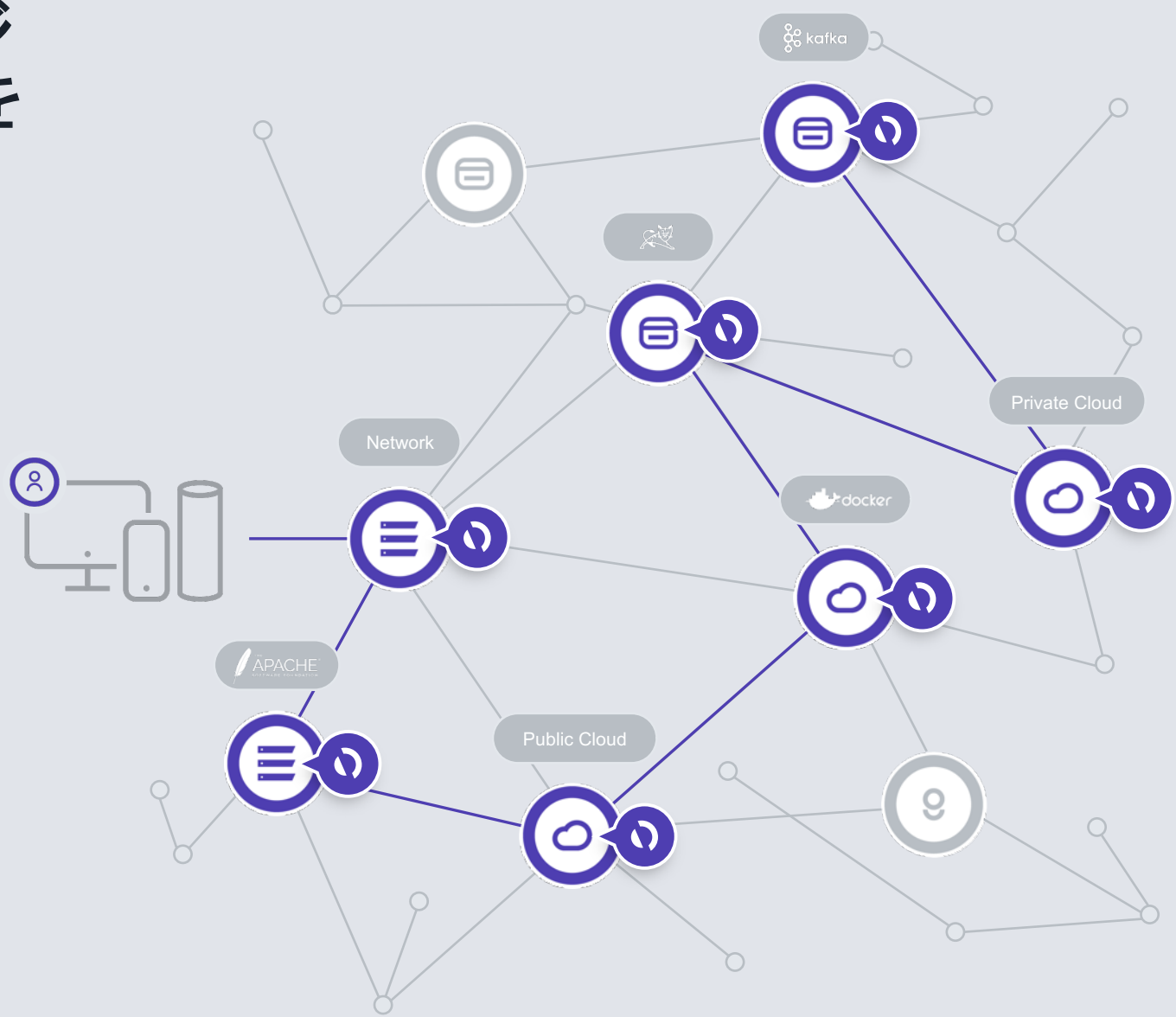
顧客が実行する全ビジネス・トランザクションを監視

Move Fast,
Follow Everything &
Focus on What Matters Most

— 全てのユーザの全てのトランザクション

— 自動的にビジネストランザクションを検知し関連付け

— 動的な情報更新



App iQ

Map

Baseline

Diagnose

Enterprise

Business iQ

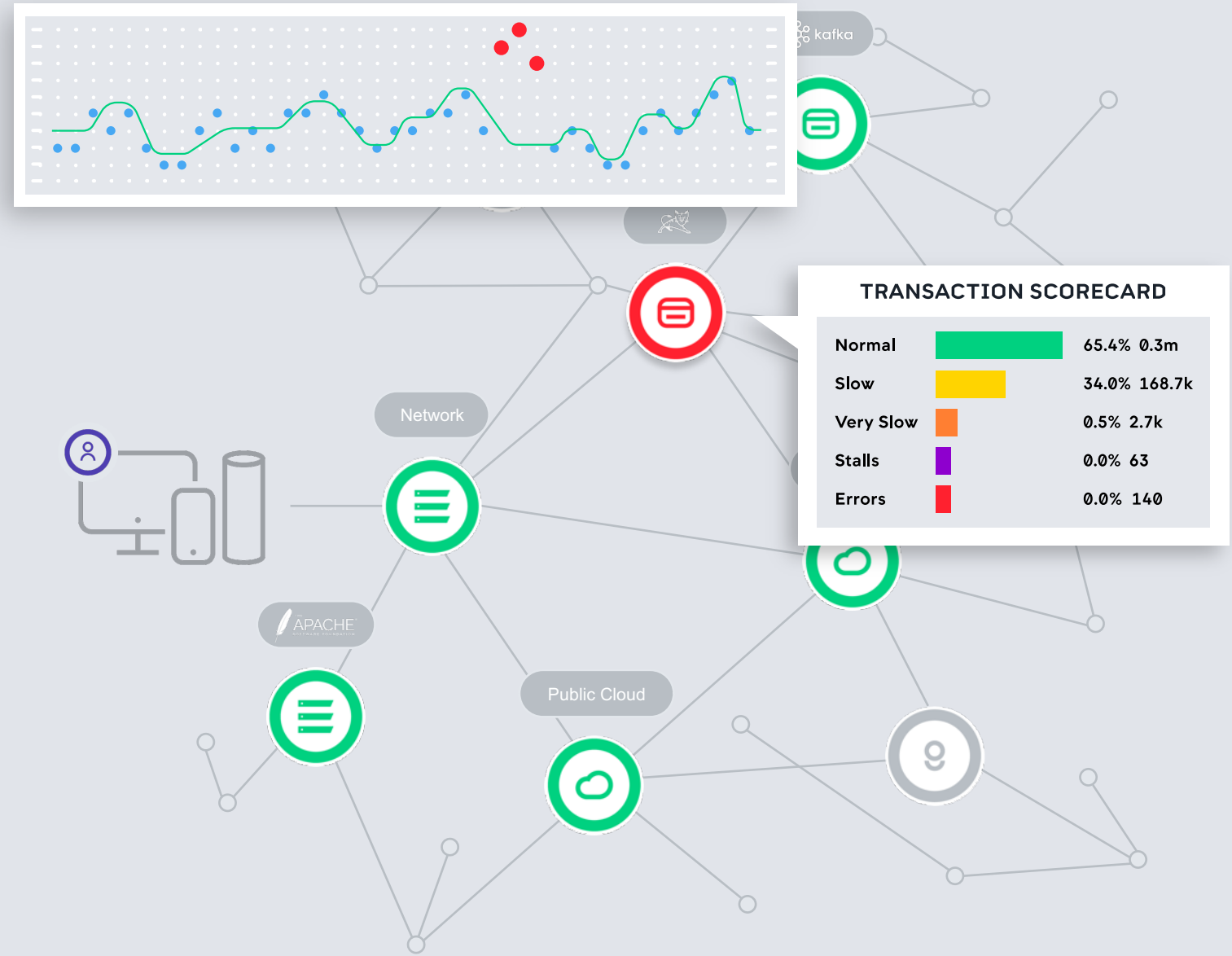
顧客に認知される前に問題を捕捉

Move Fast,
Follow Everything &
Focus on What Matters Most

— 全てのメトリックスについて自動ベースライニング

— 機械学習による自動検知

— 不要なアラートの削減



App iQ

Map

Baseline

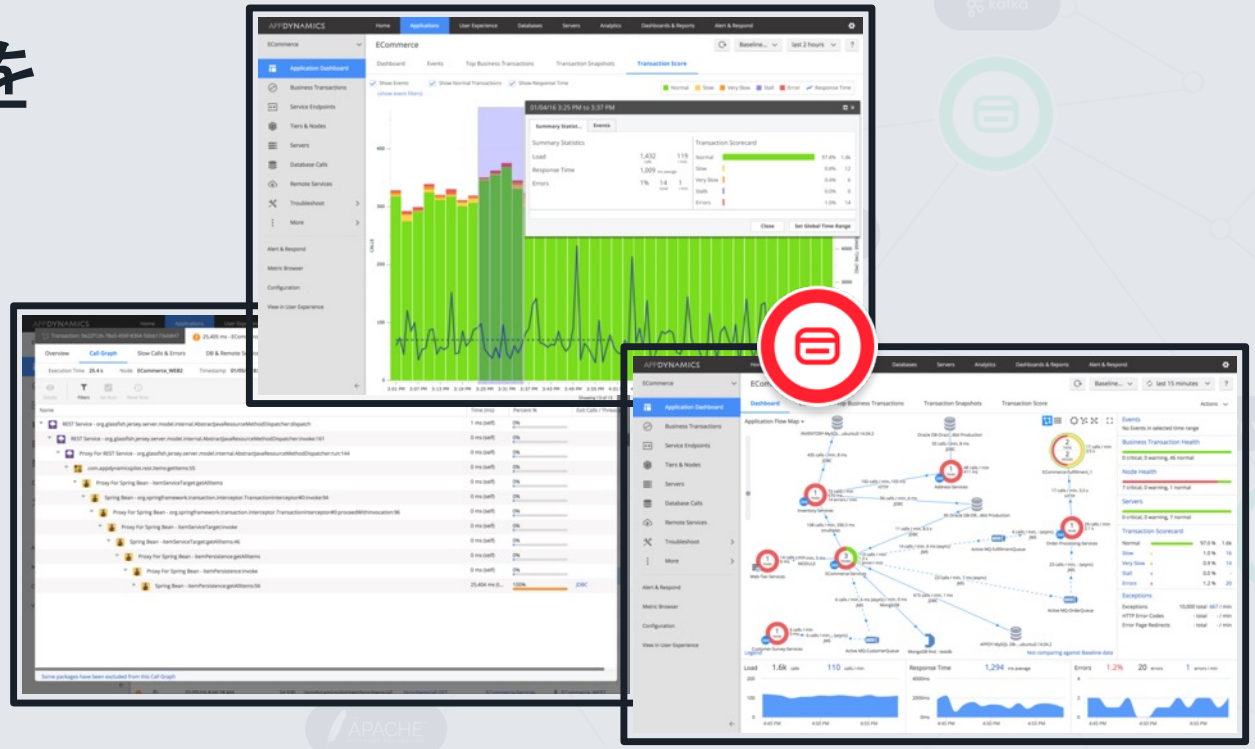
Diagnose

Enterprise

Business iQ

自動かつ瞬時にコードレベルの分析を実行

Move Fast,
Follow Everything &
Focus on What Matters Most



— 大量のログファイルの分析は不要

— 低いオーバーヘッド

— 本番環境、ステージング寛容の問題を解決

根本原因まで3クリック！

Down to the line-of-code

App iQ

Map

Baseline

Diagnose

Enterprise

Business iQ

顧客体験の拡張に即座に対応

Application Components

10s

100s

1,000s

10,000s

Move Fast,
Follow Everything &
Focus on What Matters Most

— 監視エージェントの拡張

— 可視性の拡張

— 監視範囲の拡張
オンプレ・クラウド・ハイブリッド

kafka

Network

Private Cloud

docker

APACHE

Public Cloud

App iQ

Business iQ

Enterprise

Business iQ

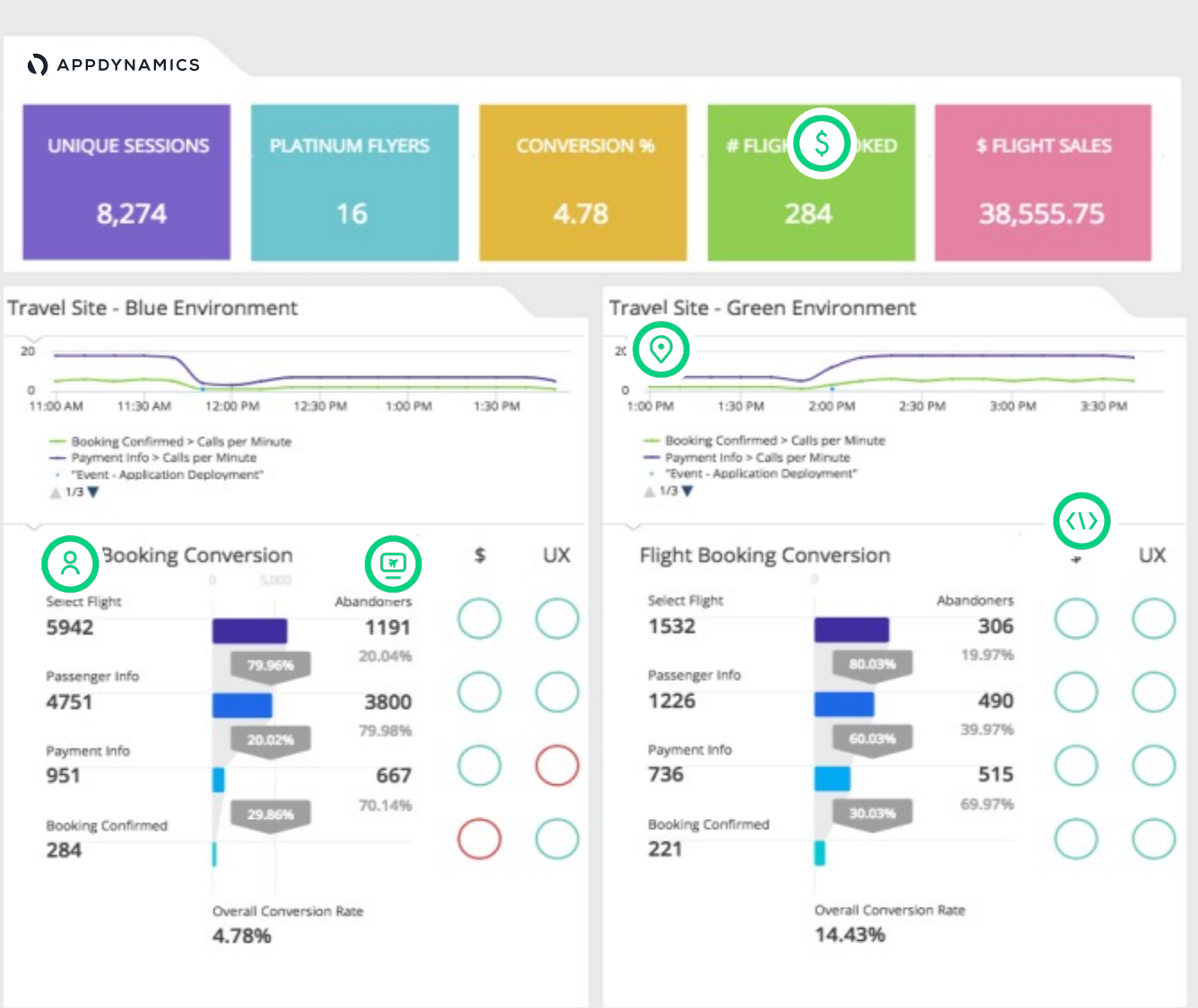
リアルタイム ビジネス インテリジェンス

Move Fast,
Follow Everything &
Focus on What Matters Most

— 自動的に情報収集

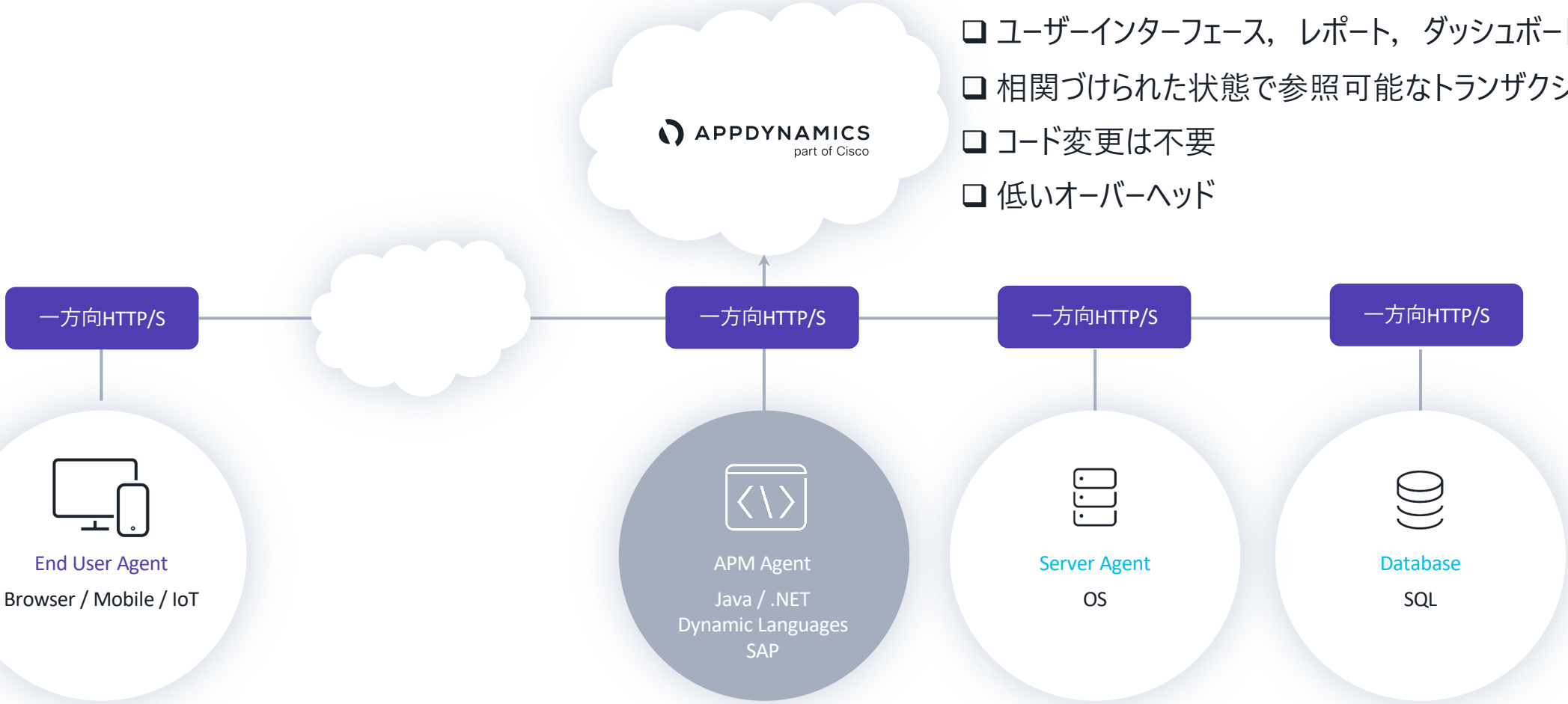
— ビジネスとITの相関関係把握

— リアルタイムでの情報洞察力



AppDynamicsアーキテクチャ とセキュリティソリューション

- ❑ SaaS上に配置されたコントローラー
- ❑ ユーザーインターフェース，レポート，ダッシュボード
- ❑ 相関づけられた状態で参照可能なトランザクション
- ❑ コード変更は不要
- ❑ 低いオーバーヘッド



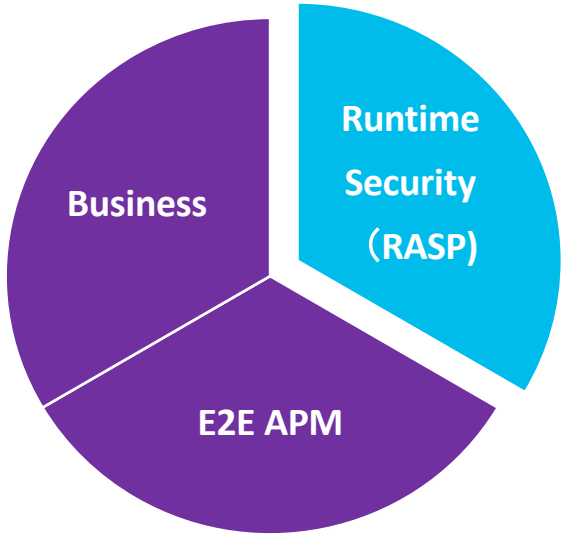
APPDYNAMICS
part of Cisco

We make the digital world work

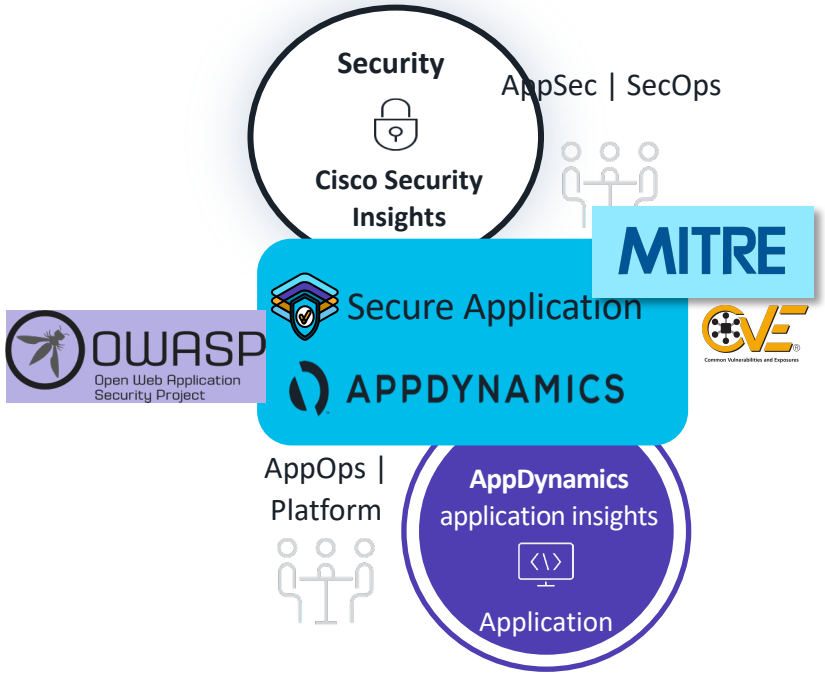
- Cisco SecureApplicationとAppDynamics
- AppDynamicsとは
  ～ビジネスオブザーバビリティプラットフォーム
- Cisco SecureApplicationご紹介
- デモ

Cisco Secure Applicationとは？

シスコAppDynamicsの
アプリケーション・セキュリティのアドオン



シスコのセキュリティと
AppDynamicsのアプリの専門性
+ セキュリティ標準の活用



AppDynamicsランタイムエージェントを使用したリアルタイムのアプリ保護を提供

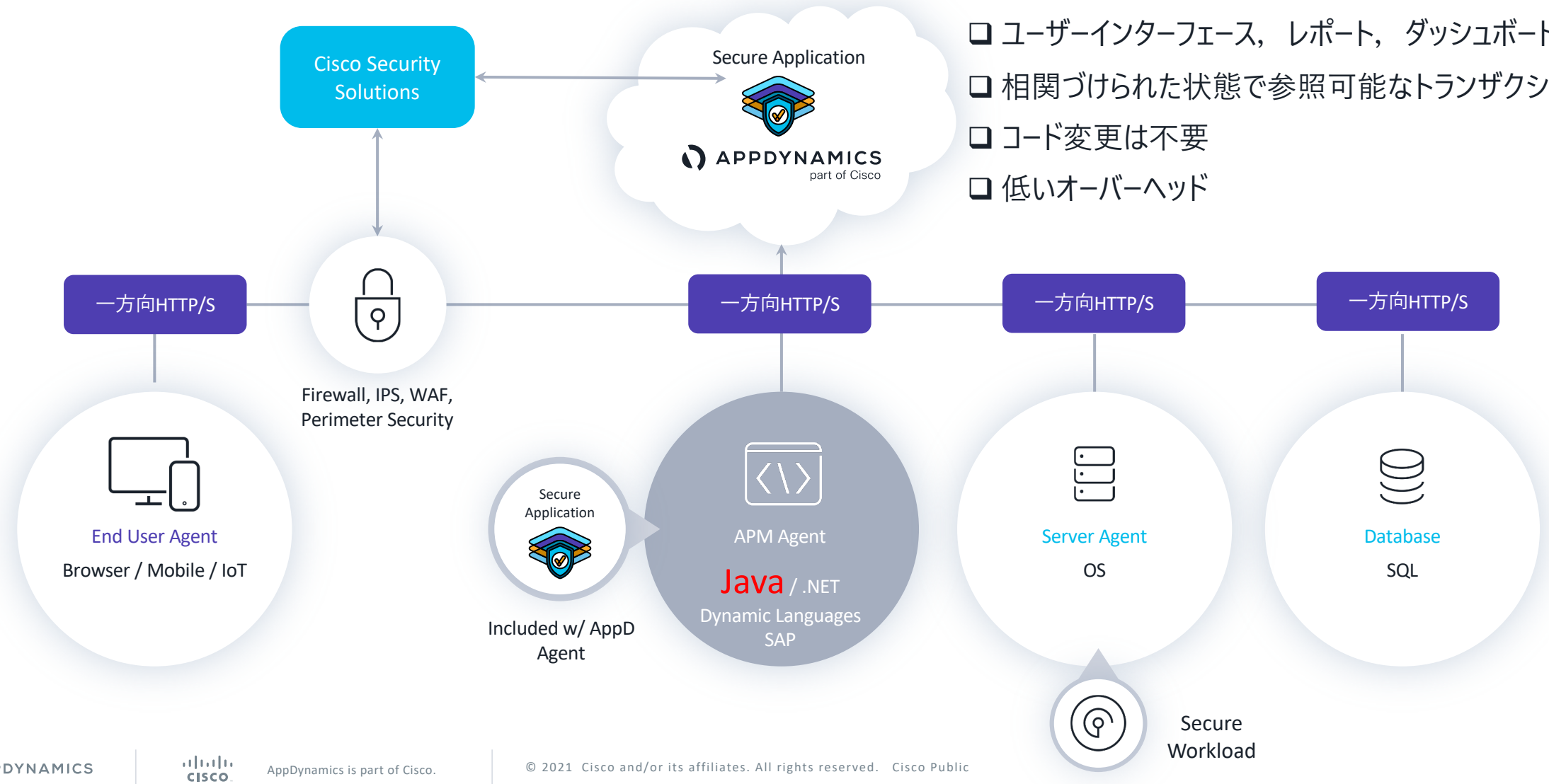
ユースケース

脆弱性の評価と修復、パッチの適用

攻撃の検知と対応

それぞれのアプリケーションに対する
セキュリティの可視化

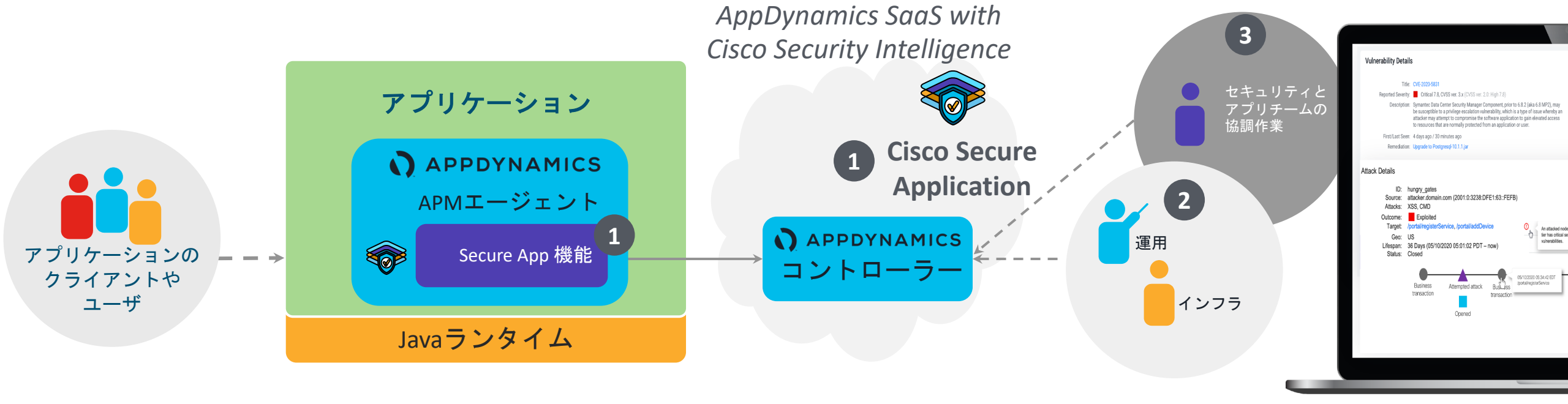
AppDynamicsアーキテクチャ とセキュリティソリューション



- ❑ SaaS上に配置されたコントローラー
- ❑ ユーザーインターフェース，レポート，ダッシュボード
- ❑ 相関づけられた状態で参照可能なトランザクション
- ❑ コード変更は不要
- ❑ 低いオーバーヘッド

Cisco Secure Application + AppDynamics

本番稼働中のアプリケーション上で 脆弱性や 攻撃を検知、防御



1

APMにセキュリティ機能を追加
AppDynamics内の機能
Secure Appとの連動

2

運用、インフラチームへの
セキュリティ アラート機能
どのアプリの どの処理で発生したかを明示

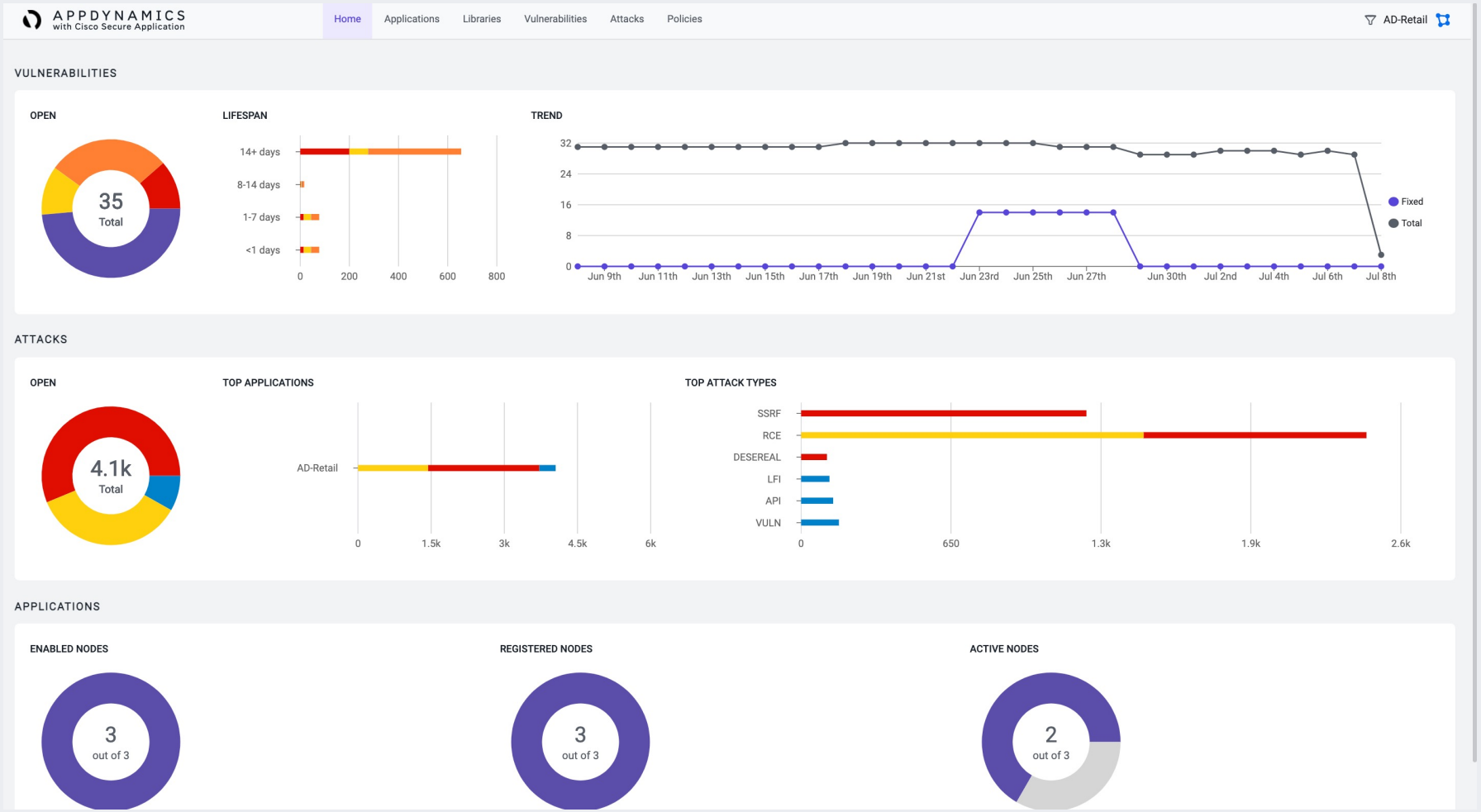
3

セキュリティチームと
アプリチームで問題解決
ポリシー設定、脆弱性修正、漏洩の確認

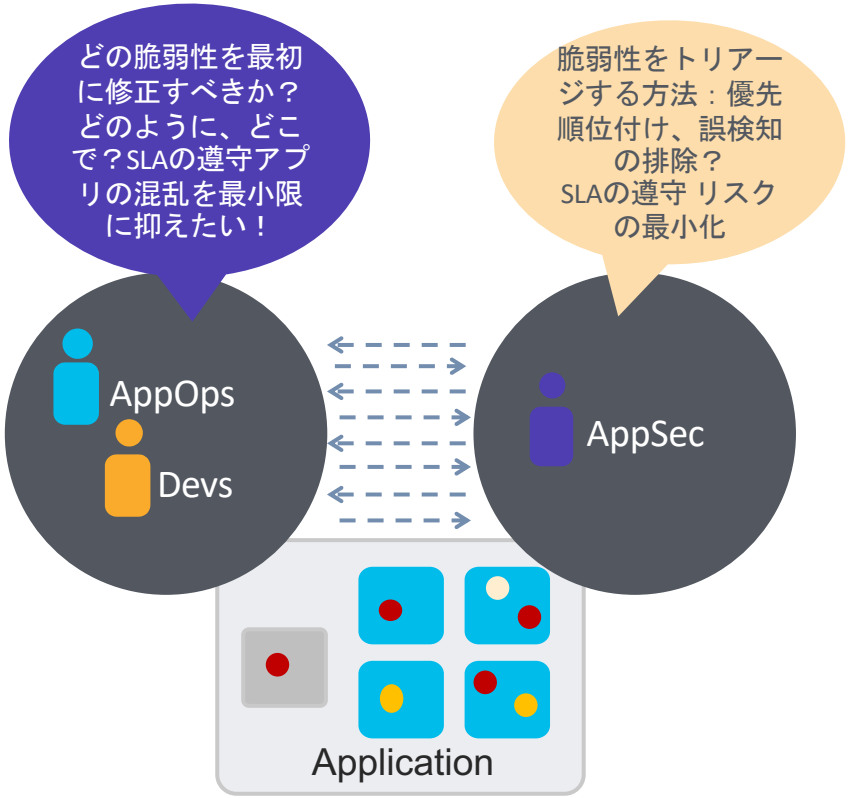
アプリの概要とセキュリティ詳細

SecureApp UI

- セキュリティ詳細
  - 詳細なポリシー、エージェントコントロール、ステータス
- アプリ概要
  - AppDへのリンク



Use case: ランタイムの脆弱性診断



課題

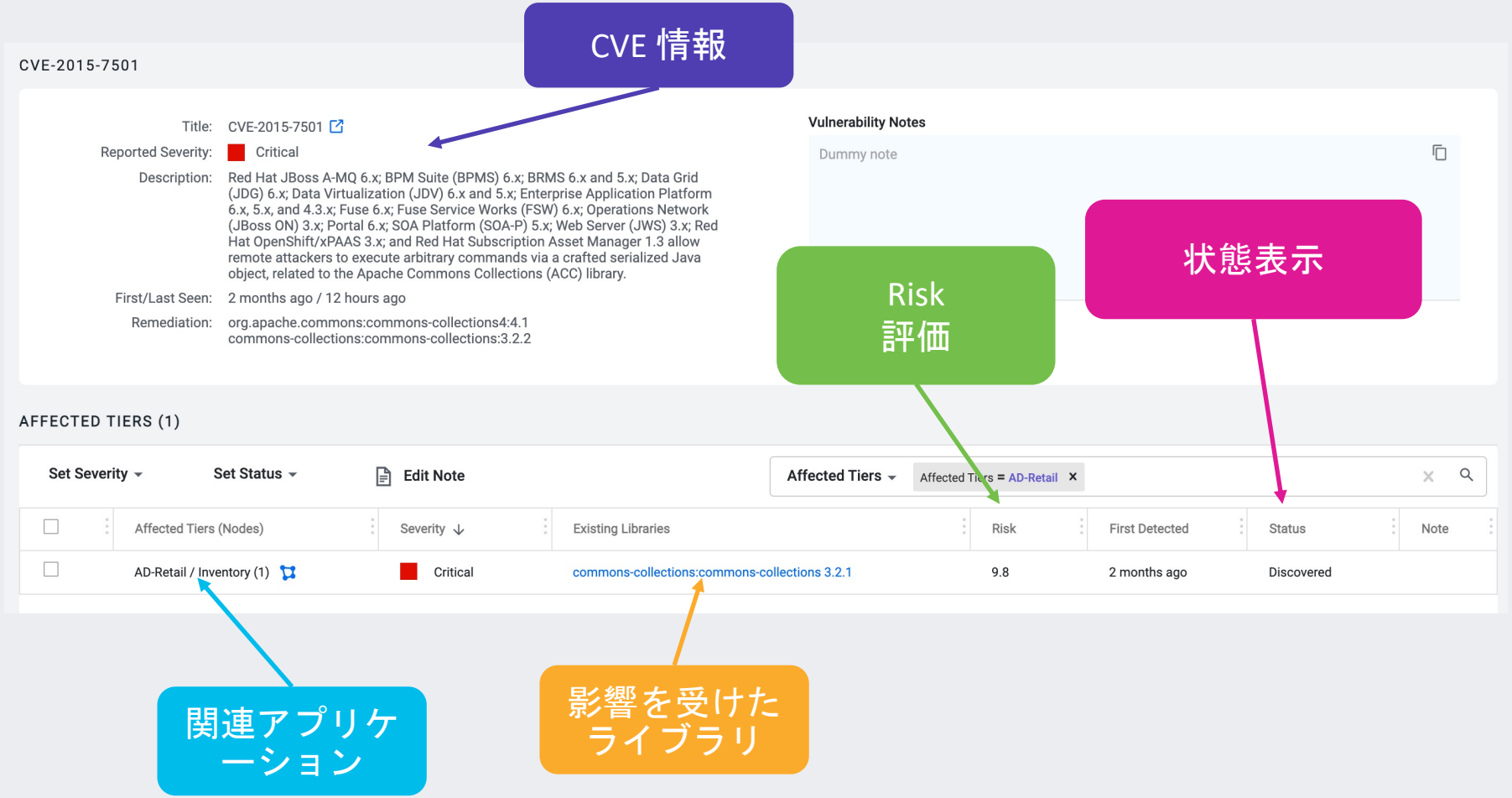
- ポイントインタイムの脆弱性スキャンのみ、通常は本番前に実施
- 導入後に多くの脆弱性が報告される
- 脆弱性のパッチ適用には数ヶ月を要する
- 報告された脆弱性を最初に利用するのはハッカー
- 面倒なプロセス、厳しい選択：リスクの増加か生産性の低下か？

実行中のコードのリスクをリアルタイムに評価するには？

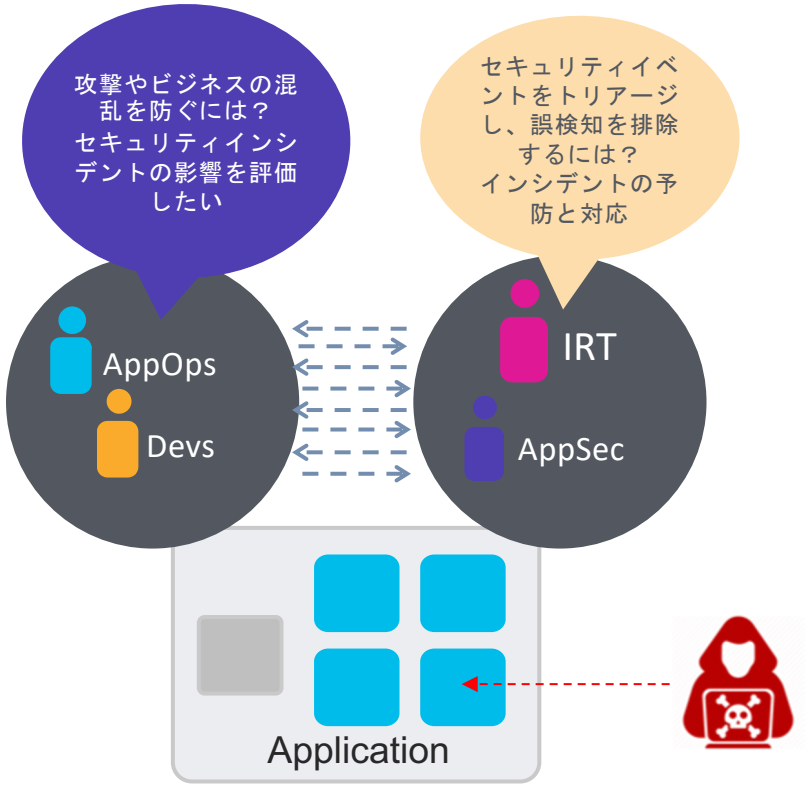
Use case: ランタイムの脆弱性診断
動作するアプリケーションの脆弱性の評価

迅速なトリアージと修復

- デプロイ時およびランタイム中に検出される
- CVE情報
- 影響を受けるアプリ/階層/ノード
- ライブラリ、ヘッダ、ロギング、例外処理
- リスクに応じた優先順位付け
- ステータス管理



Use case: リアルタイムでのアプリ攻撃の検知と防御



アプリケーションレベルの攻撃の爆発

- ハッカーはアプリレベルの新しい攻撃ベクターを使用
- ハッカーは数ヶ月間気づかれずに活動

既存ツールの課題

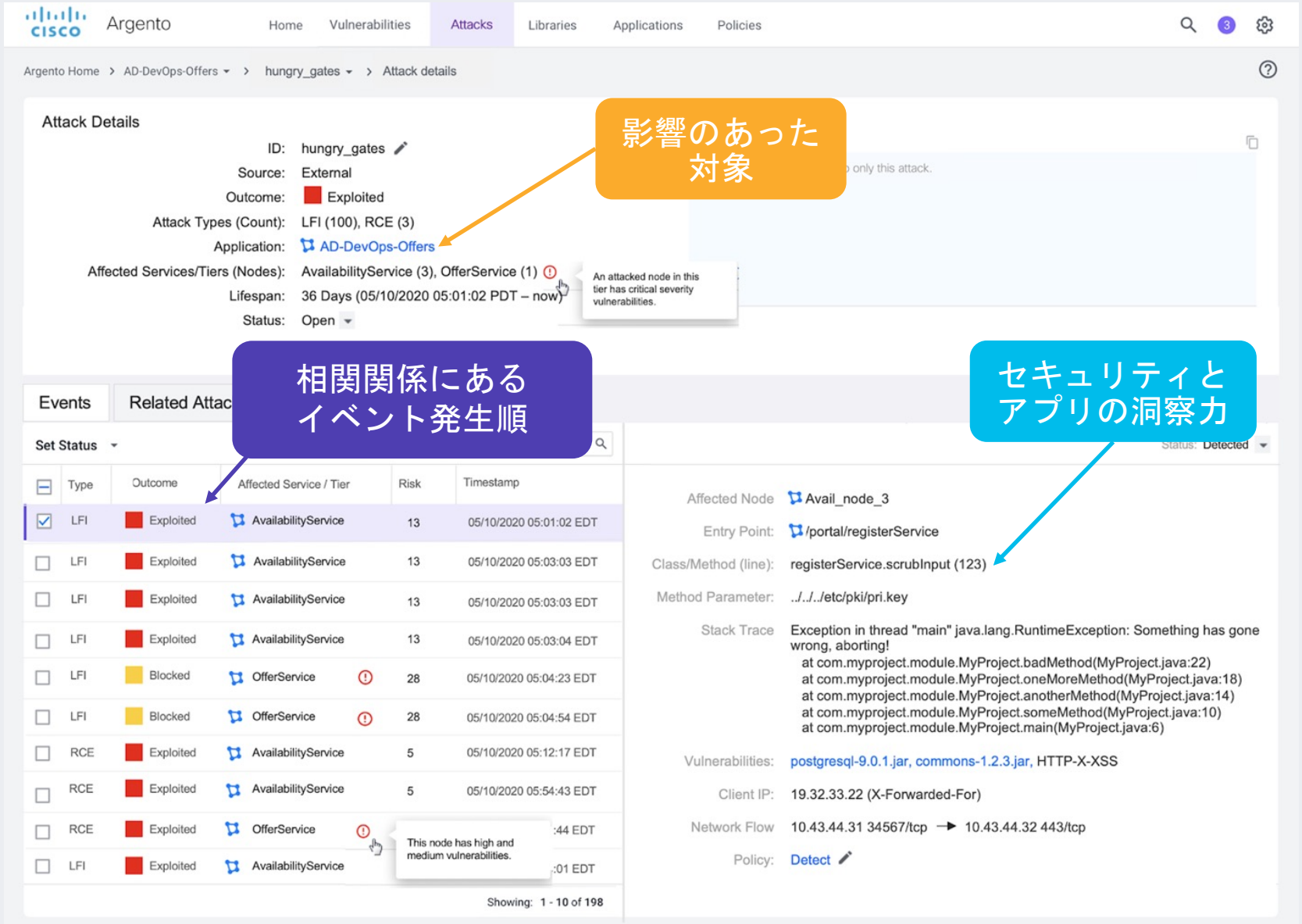
- アプリの洞察力が不足している、または開発者のかなりの関与を必要とする
- 過剰な誤検知が発生する

開発者への負担を最小限に抑え、アプリケーションセキュリティの洞察力を高めるには？

Use case: リアルタイムでのアプリ攻撃の検知と防御
アプリケーションの振る舞いに関連する攻撃

詳細分析

- イベントのタイムライン
- 攻撃元
- アプリの相関関係
- アプリ/階層/ノード/BT
- 攻撃の範囲と方法
- リスクの優先順位



攻撃の検知と防御

アプリケーション攻撃の検知と防御

- 13クラスのBCI（Byte-Code-Instrumentation）によりアプリの動作を可視化し、コントロール:

  例えば、コールグラフ、ファイルアクセス、リモート接続、終了コール、DB、エラー処理、プロセスの生成
- アプリとセキュリティに関する知見をもとにルールを構築
- アプリのパフォーマンスを考慮して構築された斬新なアプローチ

  APMエンジニアとセキュリティエンジニアによる共同設計
- Cisco TalosとNISTを活用した脅威のモデリングとインテリジェンス

検知、ブロック、パッチへの幅広い対応

- Remote code execution
- Path traversal
- Local file include
- Untrusted deserialization
- Insufficient logging / uncaught exceptions
- Non-parameterized SQL query
- SSRF
- Expression language injection
- Logging of sensitive information
- Malicious IP access
- HTTP security headers
- Detect exploit of vulnerable dependencies
- Vulnerability virtual patching

APPDYNAMICS
part of Cisco

We make the digital world work

- Cisco SecureApplicationとAppDynamics
- AppDynamicsとは
  ～ビジネスオブザーバビリティプラットフォーム
- Cisco SecureApplicationご紹介
- デモ

Thank you

AppDynamics及びCisco Secure Applicationにご興味頂いた皆様

appd-japan-sales@cisco.com

までどうぞ！