

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



We make the digital world work

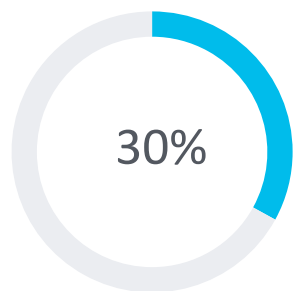
- Cisco SecureApplicationとAppDynamics
- AppDynamicsとは
～ビジネスオブザーバビリティプラットフォーム
- Cisco SecureApplicationご紹介
- デモ



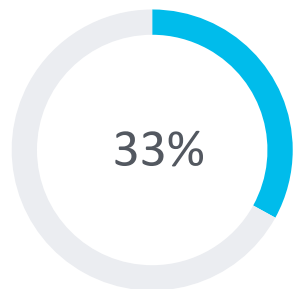
We make the digital world work

- 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

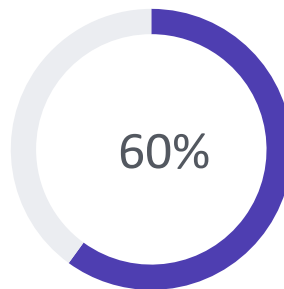
Security – 高く付く課題・代償



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

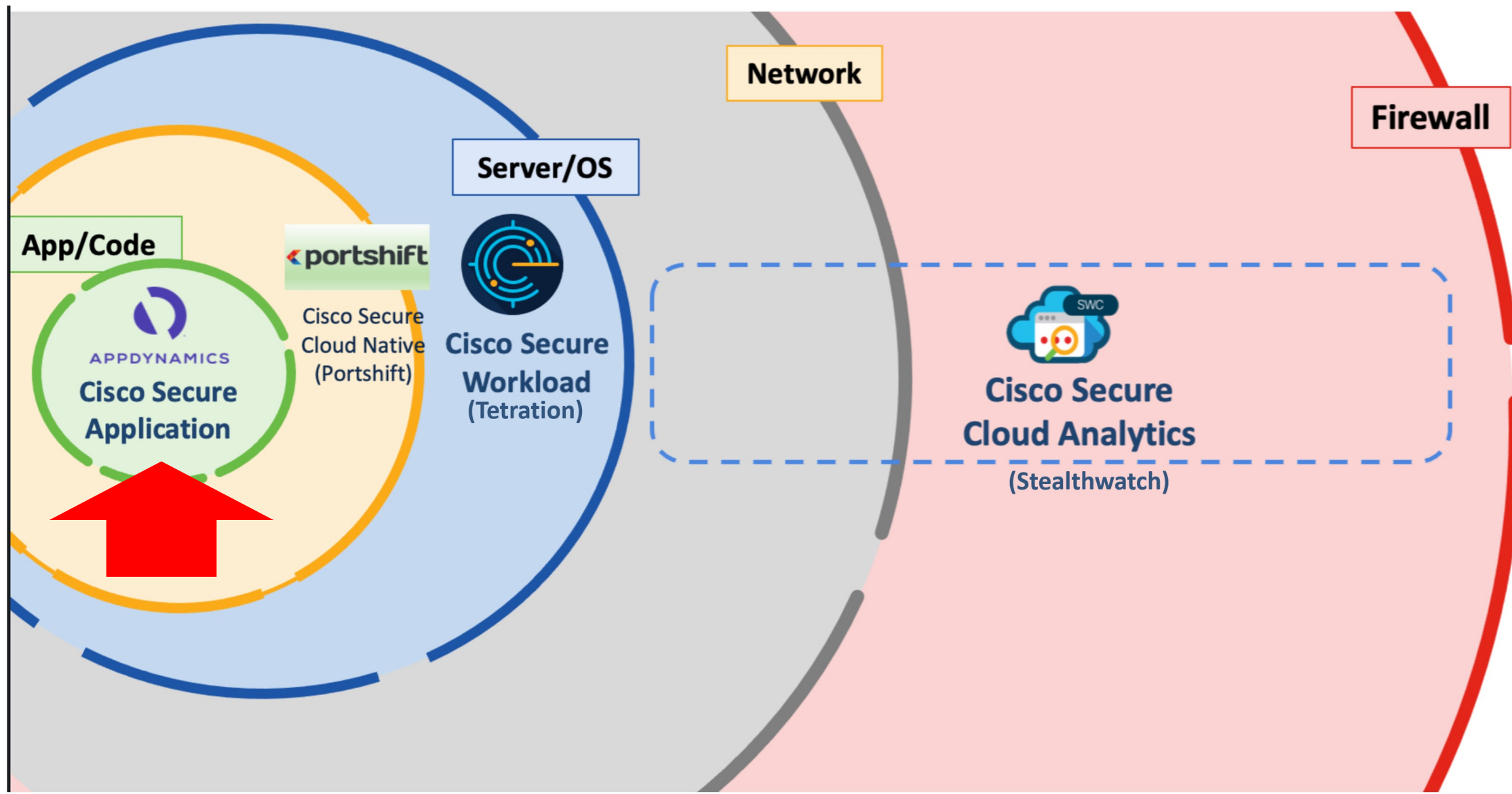
~\$4M

侵害を特定し
封じ込めるまでの時間

270+ days



Cisco Secure Applicationの位置づけ





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。

ユーザー情報や端末情報を捕捉。障害や性能低下

SAP や z/OSメインフレームとの透過的監視。

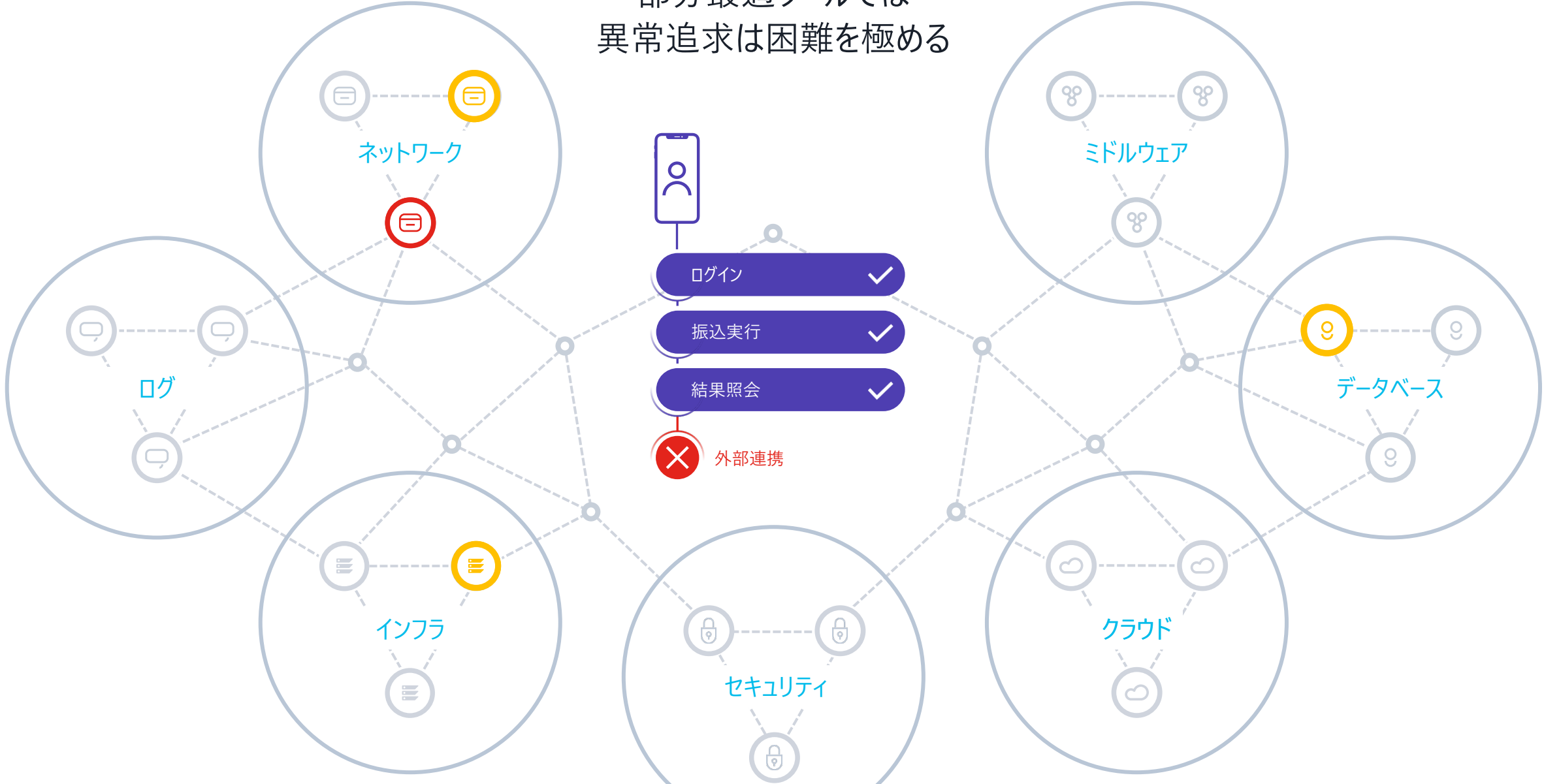
性能指標とともに、ビジネス指標も相関分析

下による サービス影響範囲を迅速に特定

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





開発部門
(アプリケーション開発に注力)

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)

インフラ部門
(技術スタックとシステム負荷に)

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)

ミドルウェア

データベース

ログ

クラウド

セキュリティ

クラウド

インフラ

ネットワーク

社内で無実を証明するまでの長い時間 (MTTI)



そのころ...



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

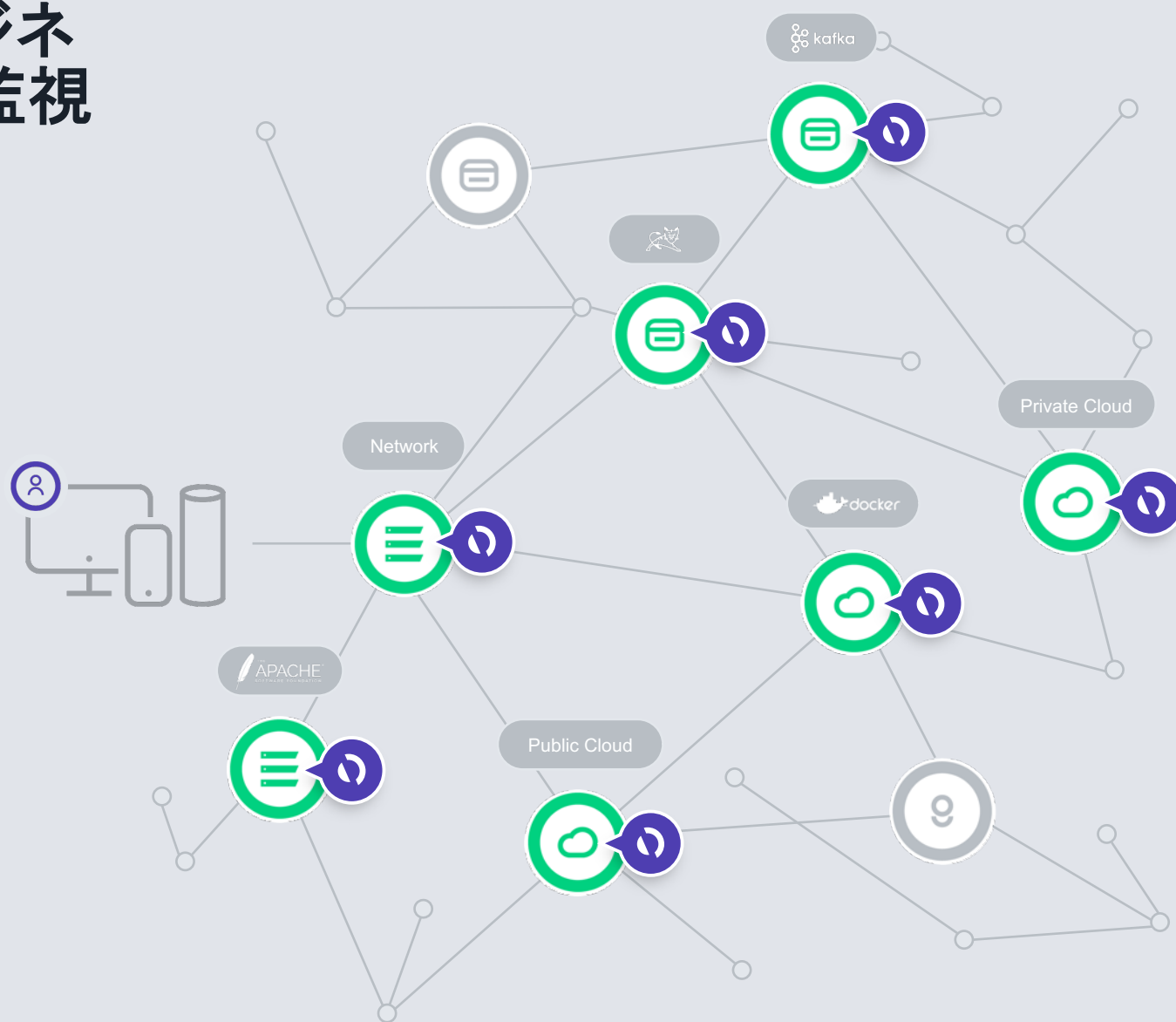
顧客が体験する全ビジネス・トランザクションを監視

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

— 自動インストルメント | 自動設定





App IQ

Map

Baseline

Diagnose

Enterprise

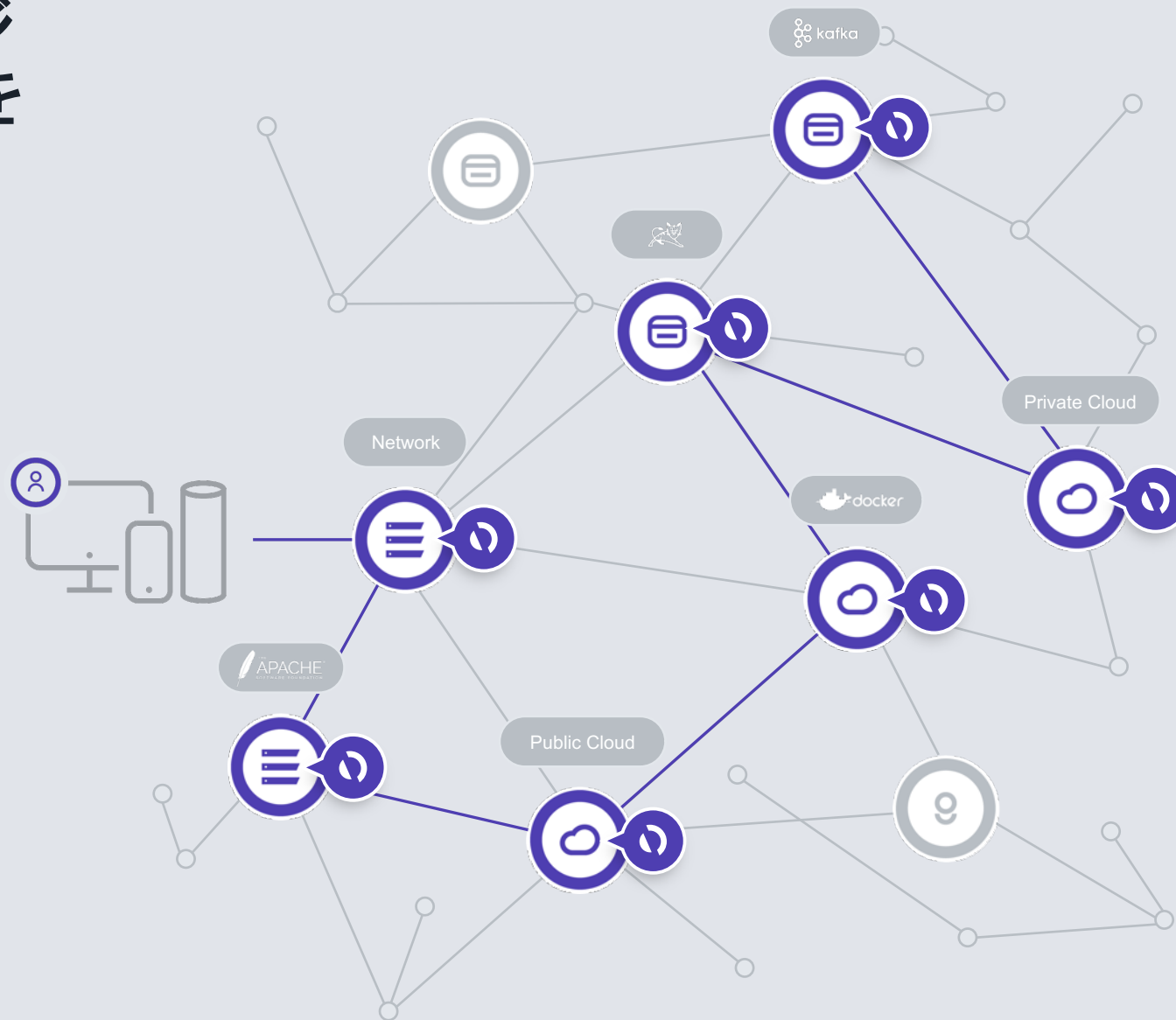


Business IQ

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

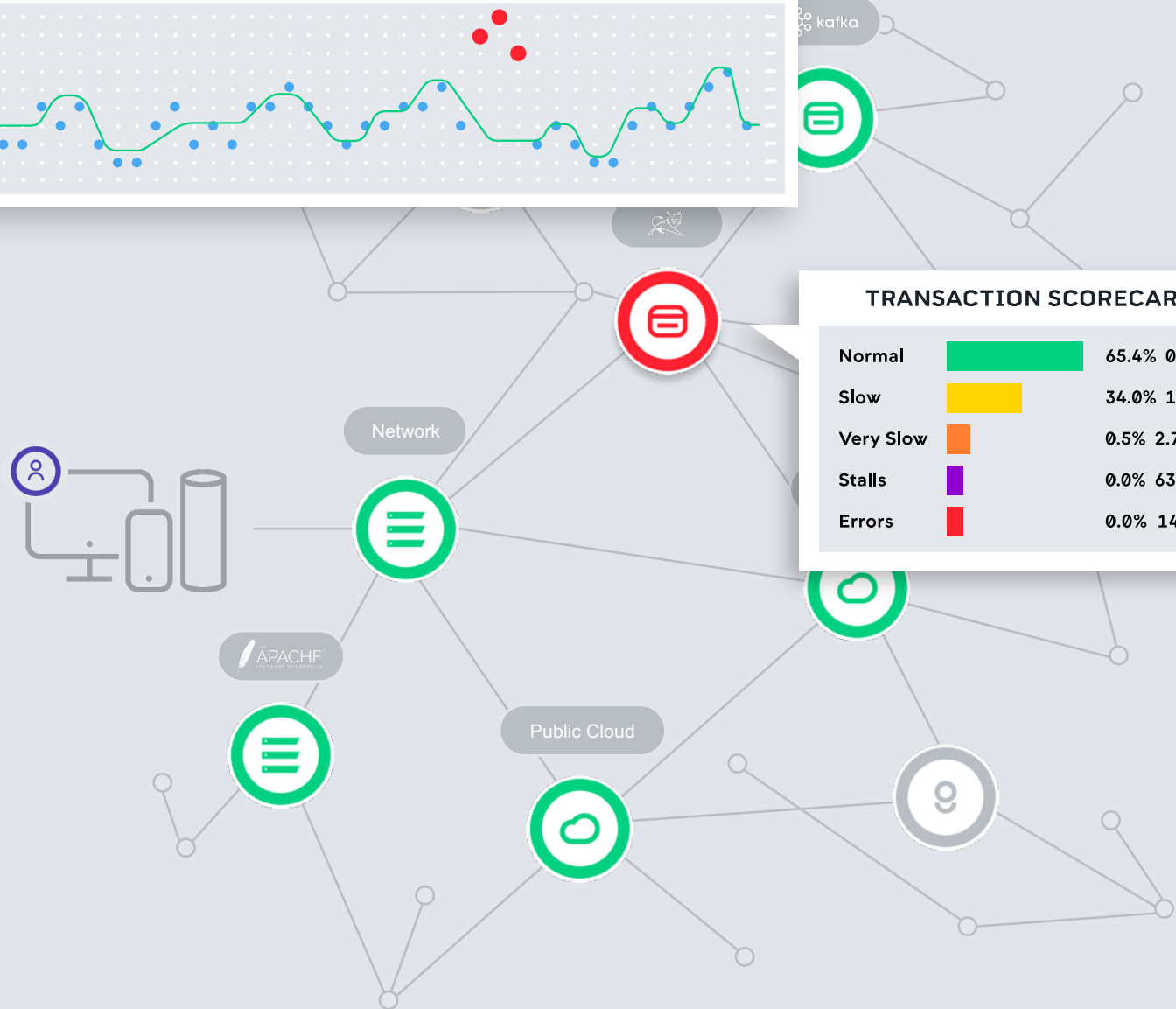
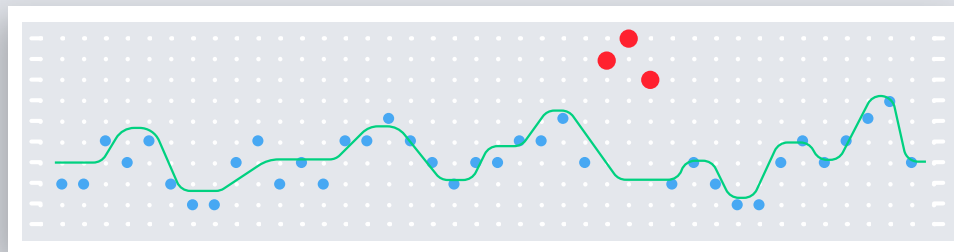


Business iQ

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



TRANSACTION SCORECARD

Normal	<div style="width: 65.4%; background-color: green;"></div>	65.4% 0.3m
Slow	<div style="width: 34.0%; background-color: yellow;"></div>	34.0% 168.7k
Very Slow	<div style="width: 0.5%; background-color: orange;"></div>	0.5% 2.7k
Stalls	<div style="width: 0.0%; background-color: purple;"></div>	0.0% 63
Errors	<div style="width: 0.0%; background-color: red;"></div>	0.0% 140



App iQ

Map

Baseline

Diagnose

Enterprise

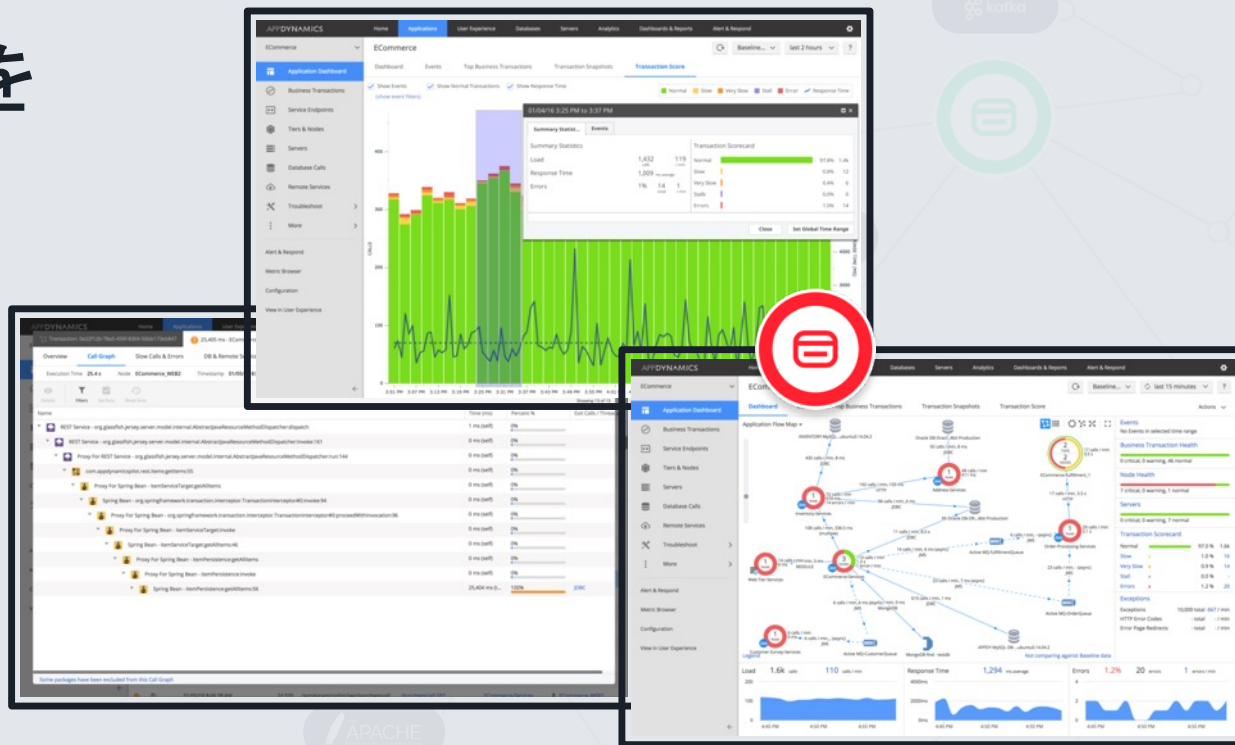


Business iQ

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

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

Application Components

10s

100s

1,000s

10,000s

Network

kafka

Private Cloud

docker

APACHE

Public Cloud



App IQ



Business IQ

Enterprise

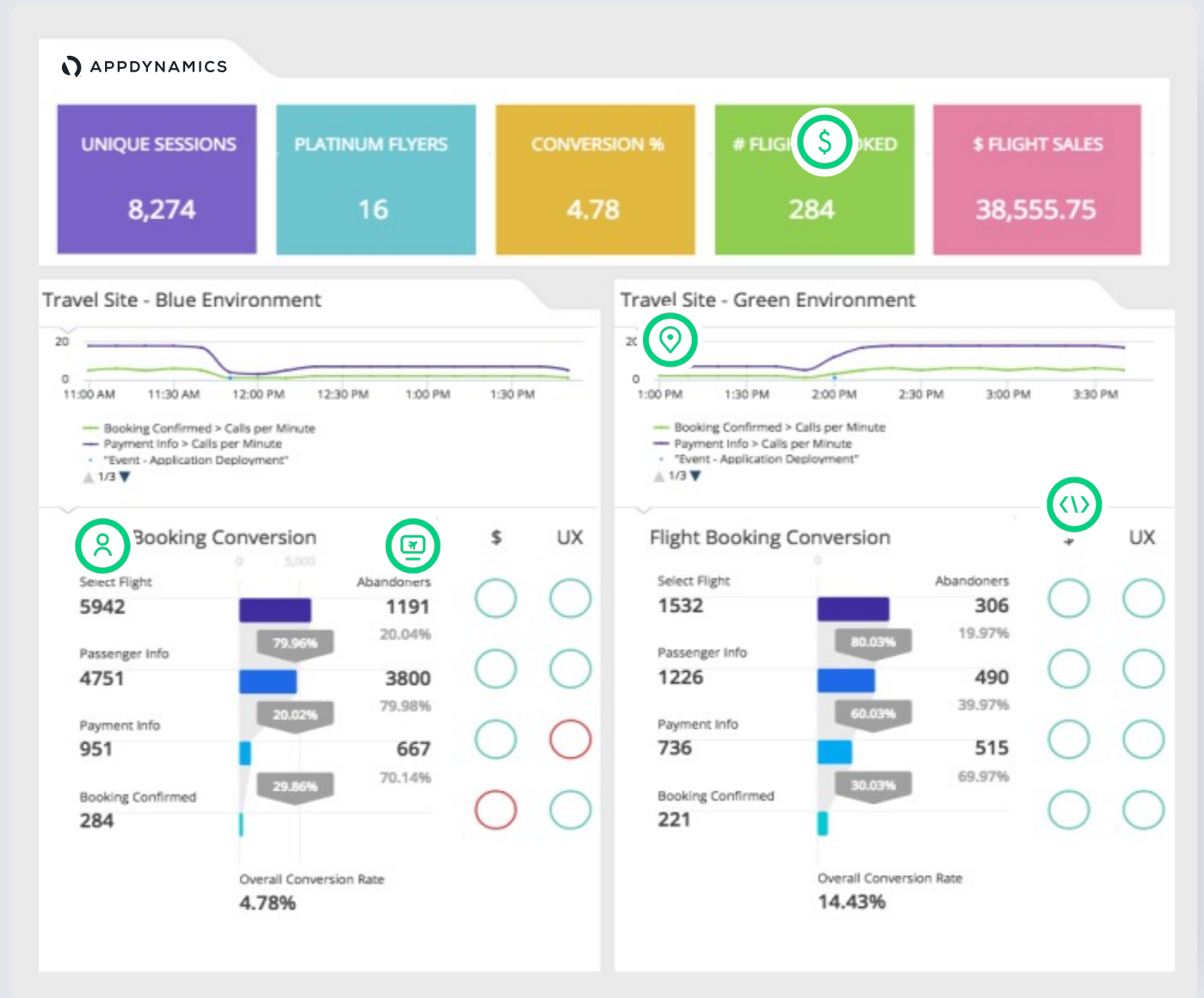


Business IQ

リアルタイム ビジネス インテリジェンス

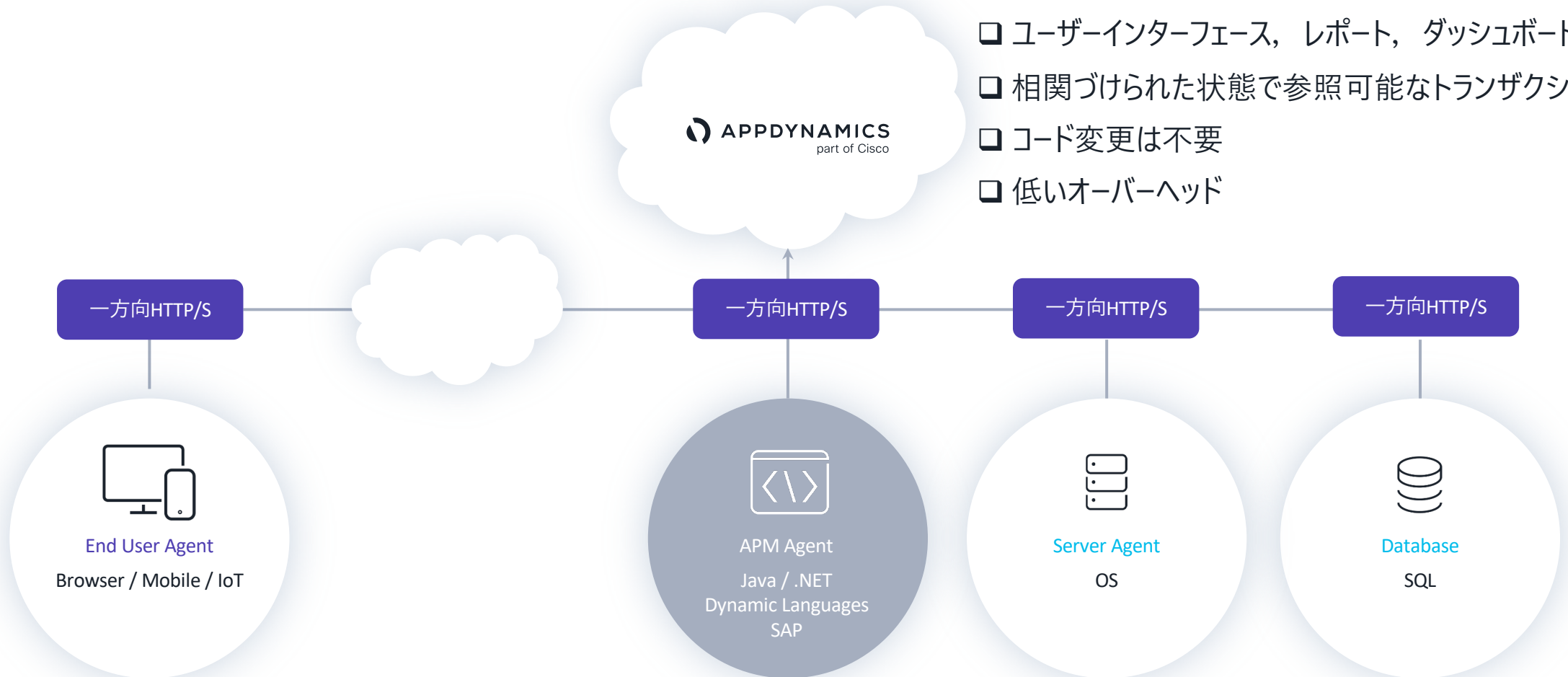
Move Fast,
Follow Everything &
Focus on What Matters Most

- 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



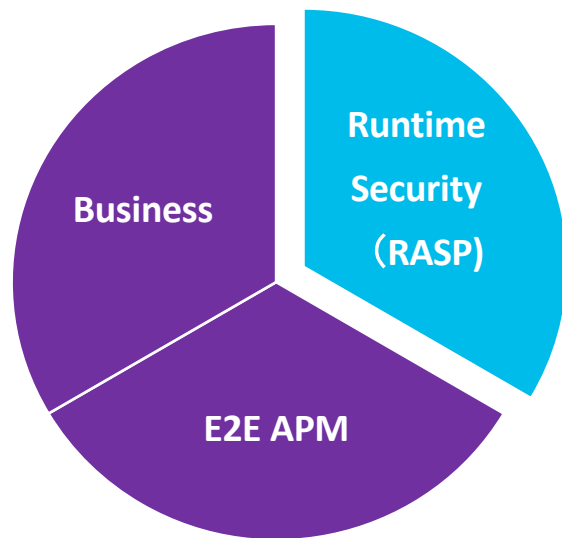


We make the digital world work

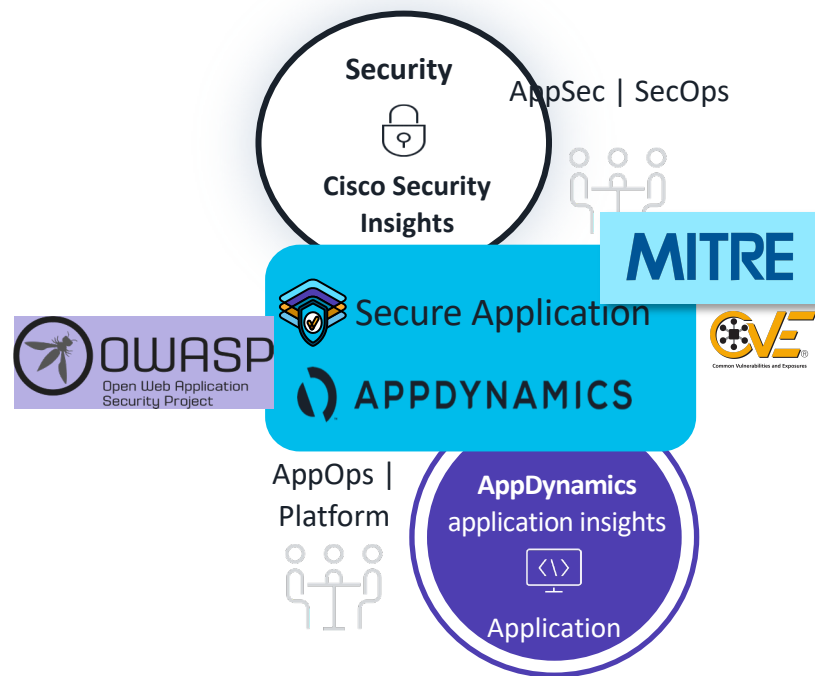
- Cisco SecureApplicationとAppDynamics
- AppDynamicsとは
～ビジネスオブザーバビリティプラットフォーム
- Cisco SecureApplicationご紹介
- デモ

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

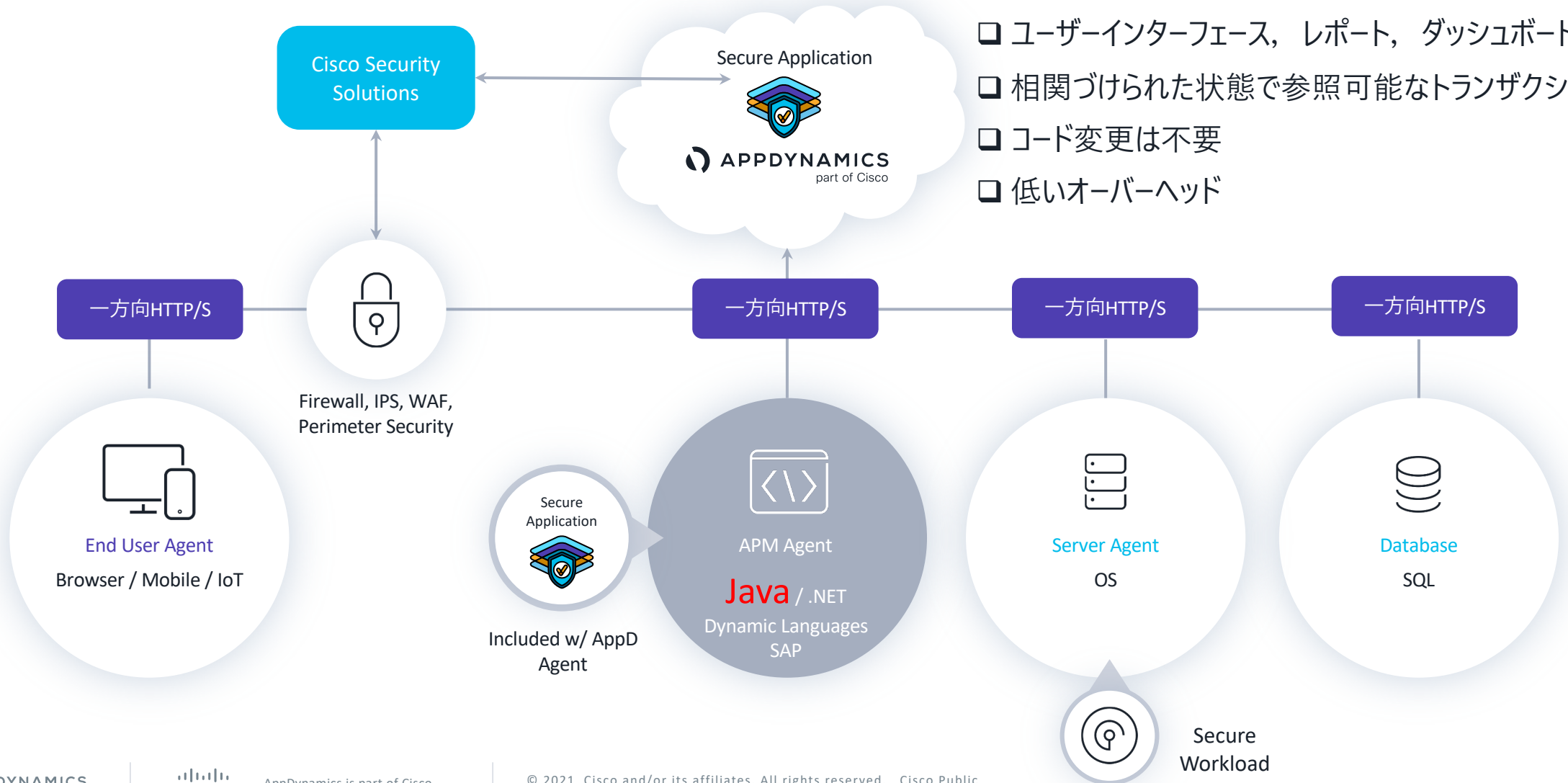
ユースケース

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

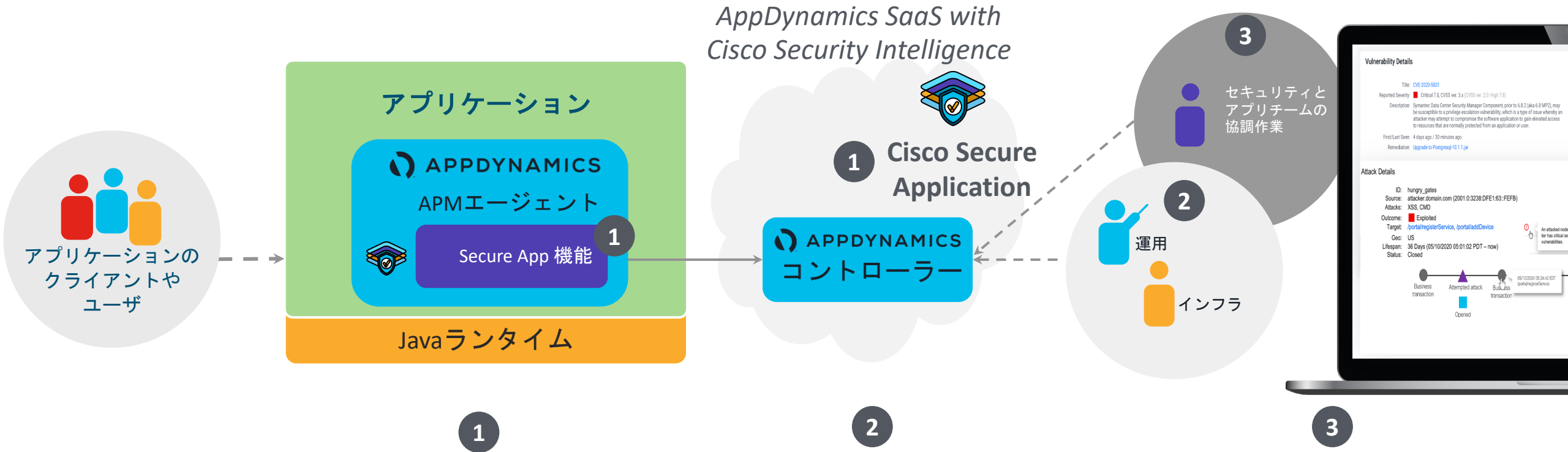
AppDynamicsアーキテクチャとセキュリティソリューション



- 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
- 関連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



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

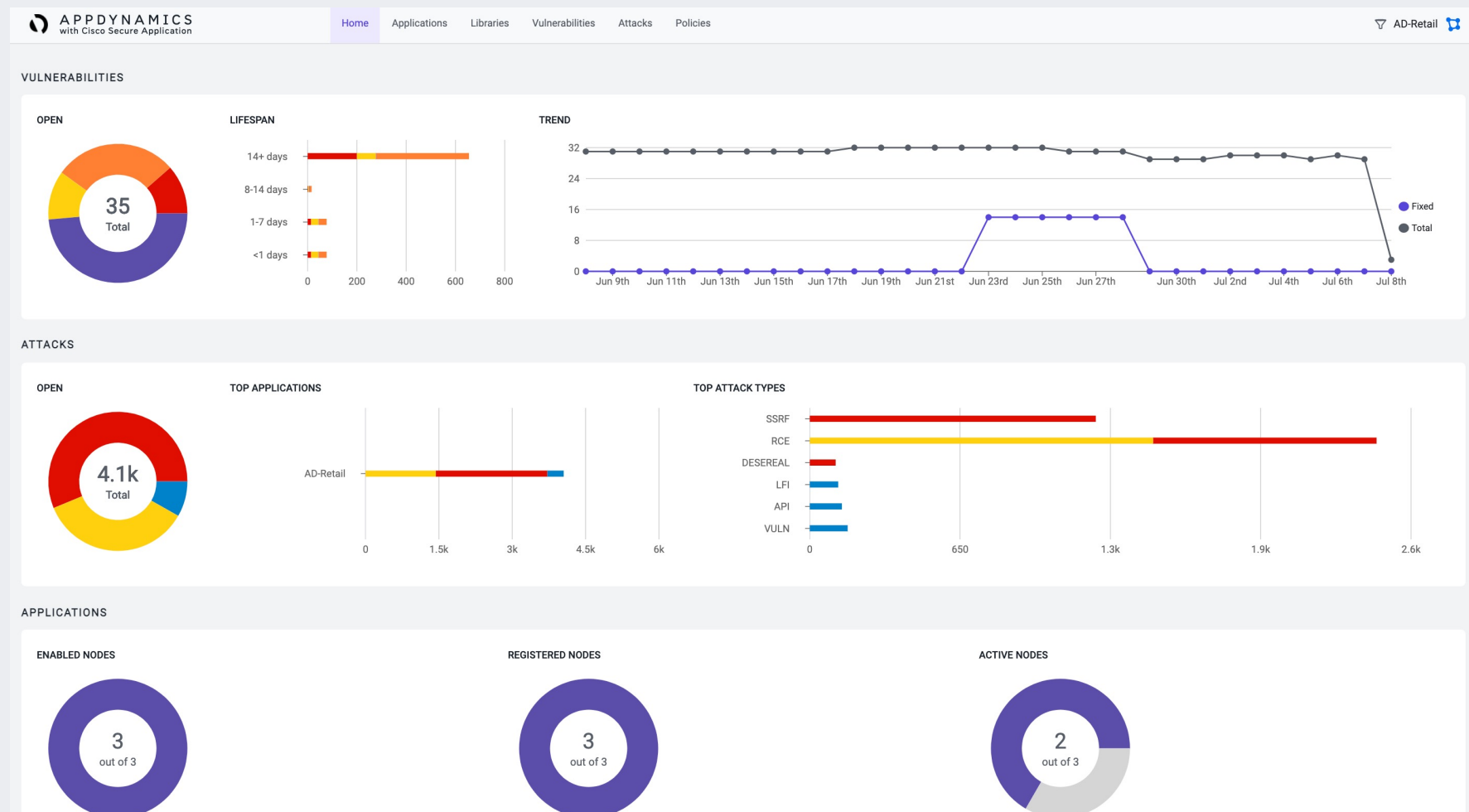
運用、インフラチームへの
セキュリティアラート機能
どのアプリのどの処理で発生し
たかを明示

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

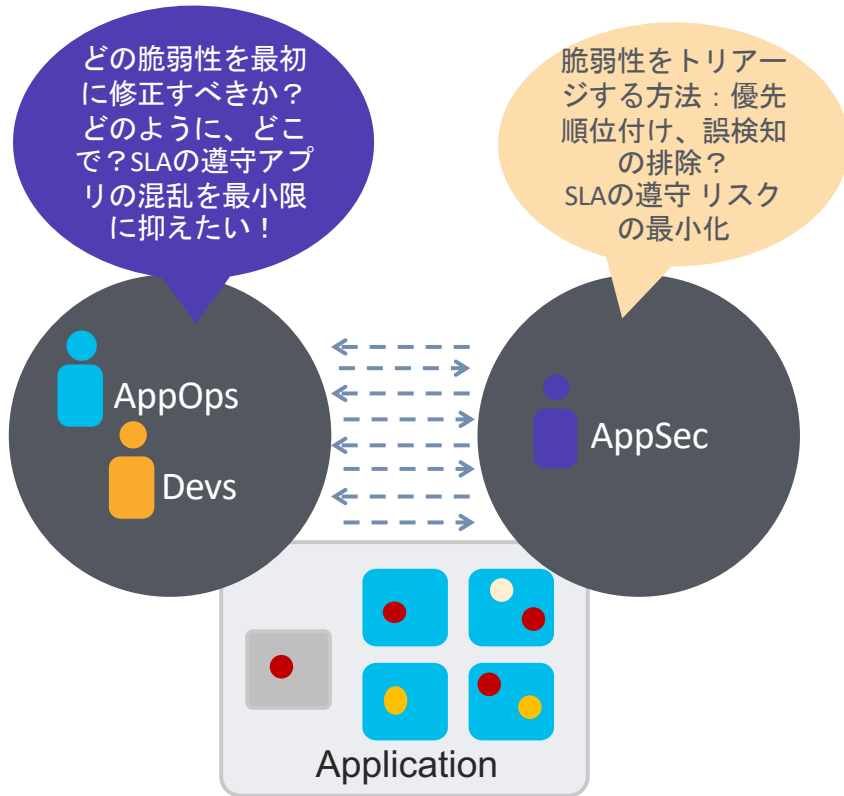
アプリの概要とセキュリティ詳細

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

CVE-2015-7501

Title: CVE-2015-7501 [🔗](#)

Reported Severity: ■ Critical

Description: Red Hat JBoss A-MQ 6.x; BPM Suite (BPMS) 6.x; BRMS 6.x and 5.x; Data Grid (JDG) 6.x; Data Virtualization (JDV) 6.x and 5.x; Enterprise Application Platform 6.x, 5.x, and 4.3.x; Fuse 6.x; Fuse Service Works (FSW) 6.x; Operations Network (JBoss ON) 3.x; Portal 6.x; SOA Platform (SOA-P) 5.x; Web Server (JWS) 3.x; Red Hat OpenShift/xPAAS 3.x; and Red Hat Subscription Asset Manager 1.3 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.

First/Last Seen: 2 months ago / 12 hours ago

Remediation: org.apache.commons:commons-collections4:4.1
commons-collections:commons-collections:3.2.2

Vulnerability Notes
Dummy note [📄](#)

Risk 評価

状態表示

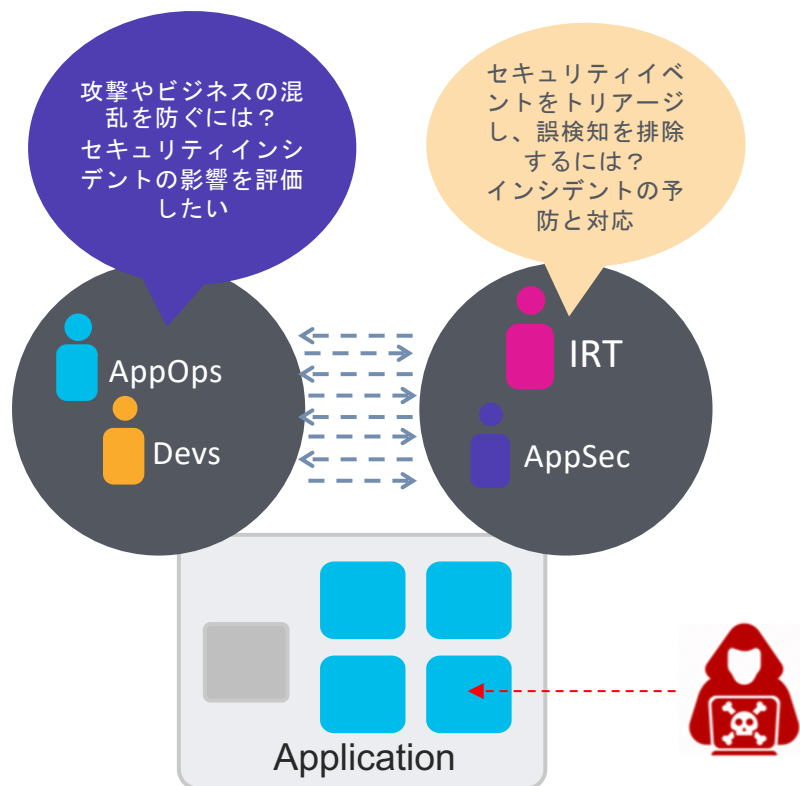
関連アプリケーション

影響を受けたライブラリ

AFFECTED TIERS (1)

<input type="checkbox"/>	Affected Tiers (Nodes)	Severity ↓	Existing Libraries	Risk	First Detected	Status	Note
<input type="checkbox"/>	AD-Retail / Inventory (1) 🔗	■ Critical	commons-collections:commons-collections 3.2.1	9.8	2 months ago	Discovered	

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衛

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

The screenshot displays the Cisco Argento interface for an attack named 'hungry_gates'. The interface is divided into several sections:

- Attack Details:** Shows the attack ID, source (External), outcome (Exploited), attack types (LFI (100), RCE (3)), application (AD-DevOps-Offers), affected services/tiers (AvailabilityService (3), OfferService (1)), lifespan (36 Days), and status (Open).
- Events:** A table listing individual attack events with columns for Type, Outcome, Affected Service / Tier, Risk, and Timestamp.
- Related Attacks:** A section for viewing related attack events.
- Stack Trace:** Provides a detailed view of the exception in the main thread, including the class/method and parameters.
- Vulnerabilities:** Lists the specific vulnerabilities exploited, such as postgresql-9.0.1.jar, commons-1.2.3.jar, and HTTP-X-XSS.
- Client IP and Network Flow:** Shows the source IP (19.32.33.22) and the network flow path.

Annotations in the image highlight key features:

- An orange box labeled "影響のあった対象" (Affected Object) points to the 'Application' field.
- A blue box labeled "相関関係にあるイベント発生順" (Order of event occurrence in related relationships) points to the 'Events' table.
- A blue box labeled "セキュリティとアプリの洞察力" (Security and application insight) points to the 'Stack Trace' section.

Type	Outcome	Affected Service / Tier	Risk	Timestamp
<input checked="" type="checkbox"/>	Exploited	AvailabilityService	13	05/10/2020 05:01:02 EDT
<input type="checkbox"/>	Exploited	AvailabilityService	13	05/10/2020 05:03:03 EDT
<input type="checkbox"/>	Exploited	AvailabilityService	13	05/10/2020 05:03:03 EDT
<input type="checkbox"/>	Exploited	AvailabilityService	13	05/10/2020 05:03:04 EDT
<input type="checkbox"/>	Blocked	OfferService	28	05/10/2020 05:04:23 EDT
<input type="checkbox"/>	Blocked	OfferService	28	05/10/2020 05:04:54 EDT
<input type="checkbox"/>	Exploited	AvailabilityService	5	05/10/2020 05:12:17 EDT
<input type="checkbox"/>	Exploited	AvailabilityService	5	05/10/2020 05:54:43 EDT
<input type="checkbox"/>	Exploited	OfferService	28	05/10/2020 05:54:44 EDT
<input type="checkbox"/>	Exploited	AvailabilityService	13	05/10/2020 05:54:01 EDT

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



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！