シスコエンタープライズ企業向けマンスリーウェビナー
2025 February

Splunk で実現するオブサーバビリティ：ビジネスとIT オペレーションの統合

Takashi Sekido
Observability Advisor, Splunk Services Japan

2025年2月19日

免責事項

- 当資料に掲載されている情報の正確性については万全を期しておりますが、シスコシステムズ合同会社 (以下、弊社) は利用者が当情報を用いて行う一切の行為について、何らかの責任を負うものではありません。当資料に起因して利用者に生じた損害につき、 弊社としては責任を負いかねますので御了承ください。
- 当サイトの情報やURL、過去に公表した資料は、予告なしに変更または削除される場合があります。
- 当サイトに掲載されている情報には、将来の予定に関する事項が含まれている場合があります。こうした事項には不確実などが含まれており、将来提供される製品、機能と必ずしも一致するものではありません。また現在提供されている製品、機能についても同様となります。
- 資料それぞれのページで上記以外の注意事項を記述してある場合がありますので、併せてお読みください。

Publickey Enterprise IT Technologies

シスコがSplunkの買収を発表、約4兆円で。同社の歴史上最大規模の買収

2023年9月21日

シスコシステムズは、ログの収集解析ツール大手として知られるSplunkの買収を発表しました。

買収金額は280億ドル（1ドル145円換算で4兆600億円）。ブルームバーグの報道によると、これは同社の歴史上最大規模の買収とのこと。

THE WALL STREET JOURNAL.

English Edition | Print Edition | Video | Audio | Latest Headlines | More

Latest World Business U.S. Politics Economy Tech Markets & Finance Opinion Arts Lifestyle Real Estate Personal Finan

CIO JOURNAL

Cisco Closes $28 Billion Acquisition of Splunk, Betting Big on AI

Cisco and cybersecurity and analytics company Splunk will use generative AI to simplify complex tools so that non-technical people can use them

By Steven Rosenbush Follow

March 18, 2024 5:15 pm ET

可視性を高めて、より多くの問題を解決。

「Splunk を当社に正式に迎えることができ、大変嬉しく思います。世界最大級のソフトウェア企業となることで、データ活用のあり方を刷新し、組織のあらゆる側面をつなぎ保護し、AI 革命の推進と安全性の確保を支援していきます。」

会長兼 CEO Chuck Robbins

シスコ

市場を牽引するセキュリティおよびオブザーバビリティ ソリューションを組み合わせてネットワークを最大限に活用することで、安全でシームレスなお客様体験および従業員体験を提供できます。

セキュリティを強化

お客様のセキュリティ運用の規模にかかわらず、クラウドおよびネットワークテレメトリに対する可視化機能で脅威を防ぎます。

優れたオブザーバビリティによる可視性の向上

フルスタック オブザーバビリティ ソリューションによって貴重なインサイトを取得することで、卓越した体験を提供できます。

ネットワーク インフラストラクチャを再構築

インテリジェントでレジリエンスが高く、常に最適化されるネットワーク インフラストラクチャにより、自信を持って運用できます。

AI の力を活用

安全かつ信頼性の高い方法で AI を展開できます。より優れたデータによって、差別化されたインサイトを得ることができます。

https://www.cisco.com/site/jp/ja/about/corporate-strategy-office/acquisitions/splunk/index.html

Splunkとは？

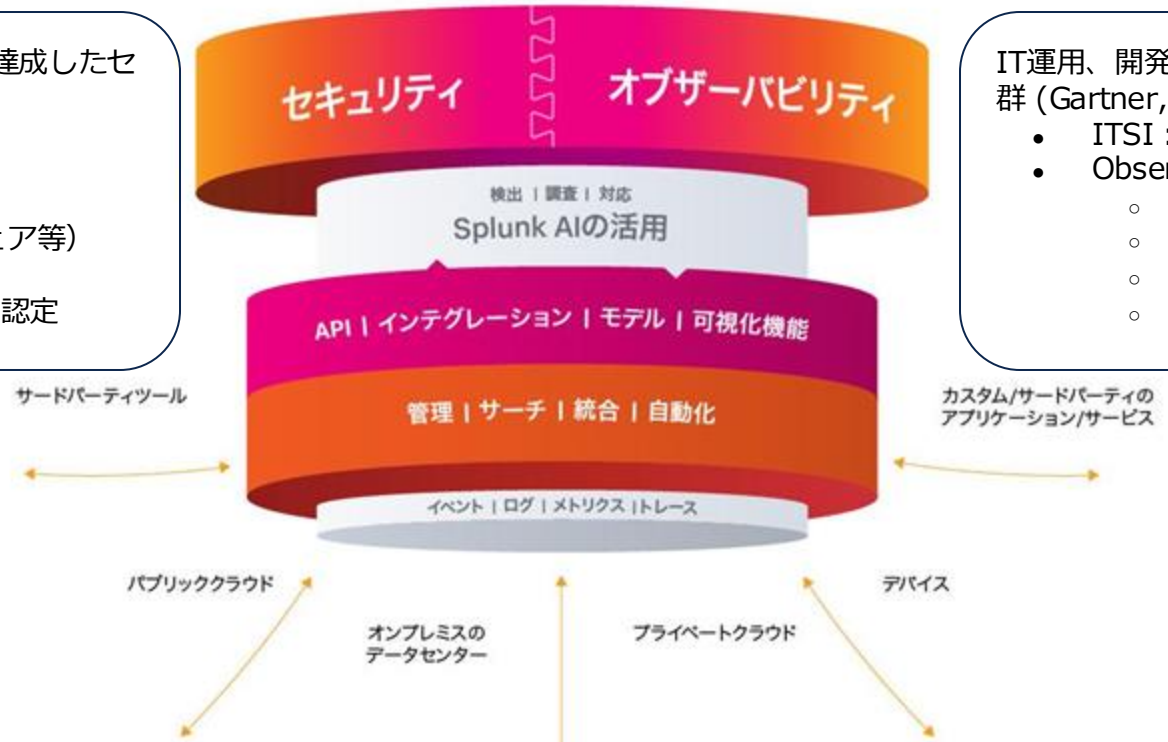
Splunkは、
より安全で
レジリエントな
デジタル世界の
構築を目指します

セキュリティとオブザーバビリティの統合プラットフォーム

- セキュリティとITサービスのデータを一つのプラットフォームで分析、技術を一石二鳥で取得
- AI技術（自動化技術やマシンラーニング技術）で、予兆や運用効率の向上

セキュリティ業務をご支援するハットトリック*を達成したセキュリティ製品群
- Enterprise Security （ES）
- SOAR
- UEBA
- Attack Analyzer （フィッシング、マルウェア等）
- Mission Control

* Gartner, IDC, Forrester Wave3社よりリーダー認定



IT運用、開発業務をご支援するオブザーバビリティ製品群 (Gartner, GigaOmにてリーダー評価)
- ITSI：SI for SAPなど
- Observability Cloud / AppDynamics
  - APM（性能管理）
  - IM：Infrastructure Monitoring
  - RUM (Real Time User Monitoring)
  - Synthetic (外形監視)

統合プラットフォームとそれを支える**AI機能**
- Splunk Cloud
- Splunk Enterprise

エコシステム
- 1,800種類を超えるSplunk Base アプリケーション
- パートナー様

パブリッククラウド　ハイブリッド環境　オンプレミス型データセンター　アプリケーション/サービス　エッジ・IoT

Splunk独自のデジタルレジリエンス

デジタルフットプリント
全域を**エンドツーエンドで**
可視化してインサイトを提供

脅威の検出/調査/対応の統合
をネットワークインサイトに
まで拡大することで
未来志向のSOCを強化

企業全体に
オブザーバビリティを
取り入れてあらゆる環境で
計画外のダウンタイムを防止

エンタープライズ規模のデータ管理機能を提供する柔軟なプラットフォームで統合

デジタルレジリエンス強化のジャーニー

セキュリティ
セキュリティチーム

オブザーバビリティ
IT運用チーム、
エンジニアリングチーム

環境の可視化

環境全体を可視化

サーチ、監視、調査によるリアルタイムでのセキュリティ監視

ミッションクリティカルなAppとインフラをトラブルシューティング

ガイド付きのインサイト

脅威や問題をコンテキスト付きで検出

AI/機械学習で強化された検出機能によって、ノイズを減らし、より多くの脅威を検出し、リスクを見極める

ビジネスへの影響に基づいて問題の優先順位付け

プロアクティブな対応

問題に先手を打つ

インシデントの調査と対応を自動化によって迅速化

重要なAppの信頼性を確保して障害を防止

ワークフローの統合

シームレスなコラボレーション

脅威の検出、調査、対応を統合することでSOCの効率を最大化

オブザーバビリティの運用方法をチーム間で統一

SplunkのAIによってスピードアップ

Splunkオブザーバビリティとは？

オブザーバビリティその前に：
そもそもなぜ、デジタルレジリエンス強化に取り組むのか

（IT側から）お客様とのビジネスや、従業員の皆様の業務を滞りなく推進、事業目標の達成のため

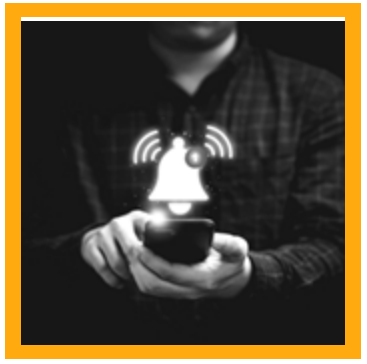
オブザーバビリティその前に：
デジタルレジリエンス強化を阻害する事象・困難

IT部門が直面する主な事象・困難

オンプレから、クラウドjへ拡大、システムの複雑化が増し、復旧に時間がかかってしまう

SAPやO365などに対するサービス健全性の可視性が不足している

アラートノイズとスタッフの疲労を軽減するのに苦労している



類似インシデントの繰り返しに対してリアクティブに対応している

ITとビジネスの優先度を合わせるのに苦労している

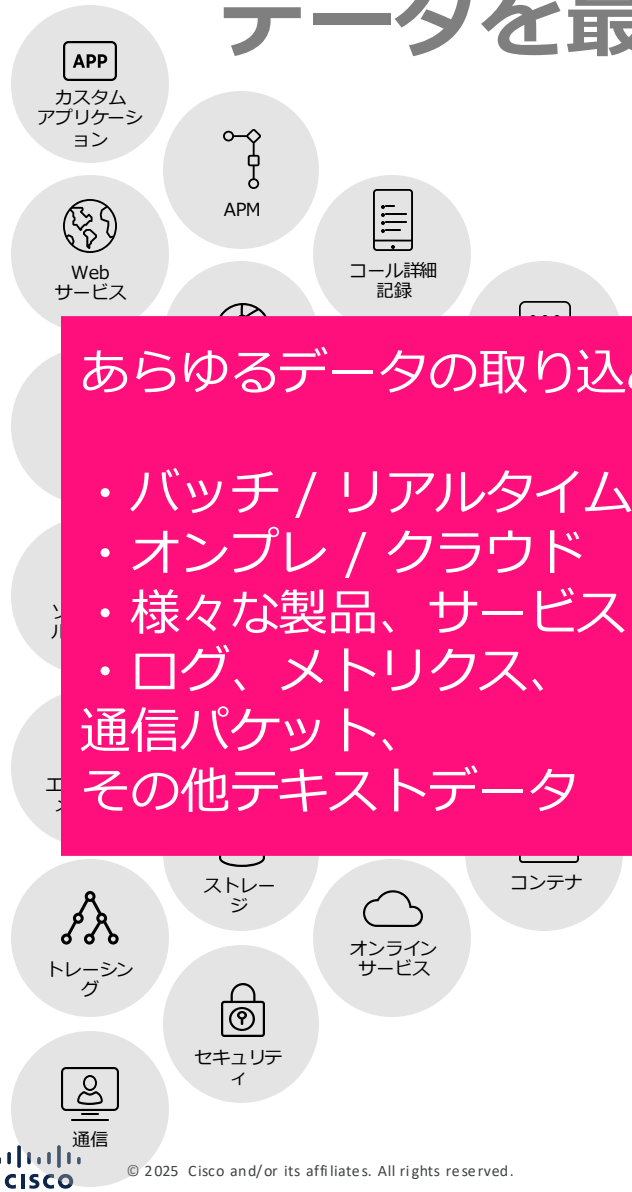
オブザーバビリティを活用することで、何が発生し、何が真因か、何すべきか、洞察を得て、事象・困難を乗越えていく

Splunkのオブザーバビリティへのアプローチ

問題の特定、根本原因の究明、是正措置の実施といった
労力のかかる作業について**ソフトウェア**での対応を拡張することで
デジタルシステムの**レジリエンス**を確保し**人手による運用負荷**を軽減する。

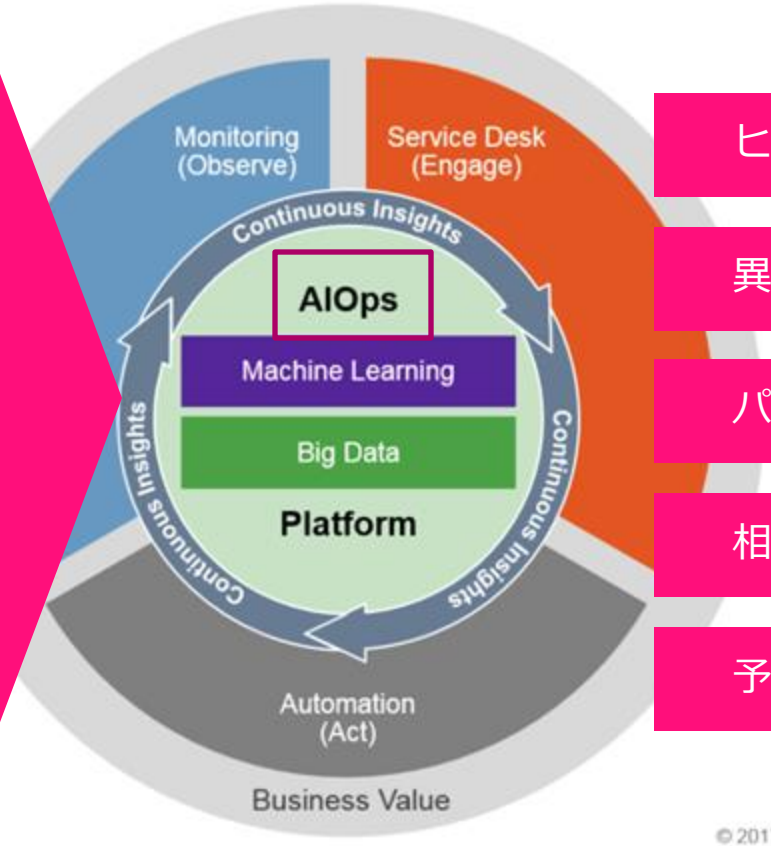
パフォーマンスに関するあらゆる問題の**ビジネスへの影響**を把握

データを最大限活用し、正しい観察から行動へ！



あらゆるデータの取り込み

・バッチ / リアルタイム
・オンプレ / クラウド
・様々な製品、サービス
・ログ、メトリクス、
通信パケット、
その他テキストデータ



© 2017 Gartner, Inc.

- ヒストリカル分析
- 異常検出
- パフォーマンス分析
- 相関とコンテキスト付け
- 予兆・予測分析

効果的な対応
↓
MTTR削減
↓
ビジネス影響最小化
人員の有効活用

Splunkの祖業はオブザーバビリティ

2025年1月29日 ZDNET社の記事より
https://japan.zdnet.com/article/35228675/

Splunkはセキュリティとログ管理のITベンダーとして広く知られているが、その本来の目的は現在で言うところのオブザーバビリティにある。

Splunkが2003年に設立された際、創業者たちは開発したアプリケーションのトラブルシューティングを迅速化することを目指してスタートした。当時はアプリケーションの状態を把握し、いつ注意を払うべきかを理解し、問題を解決するためにデータと分析が必要とされていた。

シスコによる近年の買収の多くは、オブザーバビリティ関連

APPDYNAMICS
ビジネスおよびアプリケーション監視のリーダー($3.7B)
2017年1月

ThousandEyes
ネットワークとグローバルパスの可視化
2017年10月

KENNA Security
セキュリティリスクスコアとビジネス優先順位付け
2020年5月

replex
クラウドネイティブコスト分析
2020年12月

PERSPICA
機械学習とAIによるデータ分析、APM強化
2021年5月

dashbase
イベントとメトリクスの分析
2021年8月

epsagon
最新型マイクロサ
オブザーバビ
2021年10月

opsani
クラウドネイティブのパフォーマンスとコストのチューニング
2022年1月

smartlook
セッションプレイバックとユーザー傾向
2023年3月

SamKnows
ラストマイルのネットワークとモバイル監視
2023年4月

splunk>
オブザーバビリティとセキュリティの統合プラットフォーム
$28B
2023年6月

Lightspin
クラウドネイティブ：エンドツーエンドのセキュリティと可視化
2023年6月

ACCEDIAN
5Gとサービスプロバイダー監視、大規模環境でマイクロ秒単位の観測
2023年8月

Code BGP
グローバルBGP監視、インターネット健全性
2024年3月

Splunkが目指すオブザーバビリティ

Observability
IT運用とエンジニアリング

基礎的な可視性

横断的に環境を見る

- ミッションクリティカルなアプリやインフラのトラブルシューティング
- クラウド監視の最適化

洞察の導出

文脈から脅威や問題を検出

- ITサービスの健全性を分析
- アラートノイズの低減
- リリースの影響を理解する

プロアクティブな対応

問題を先取り

- 障害の防止
- マイクロサービスの問題をデバッグする
- エンドユーザー・エクスペリエンスの最適化

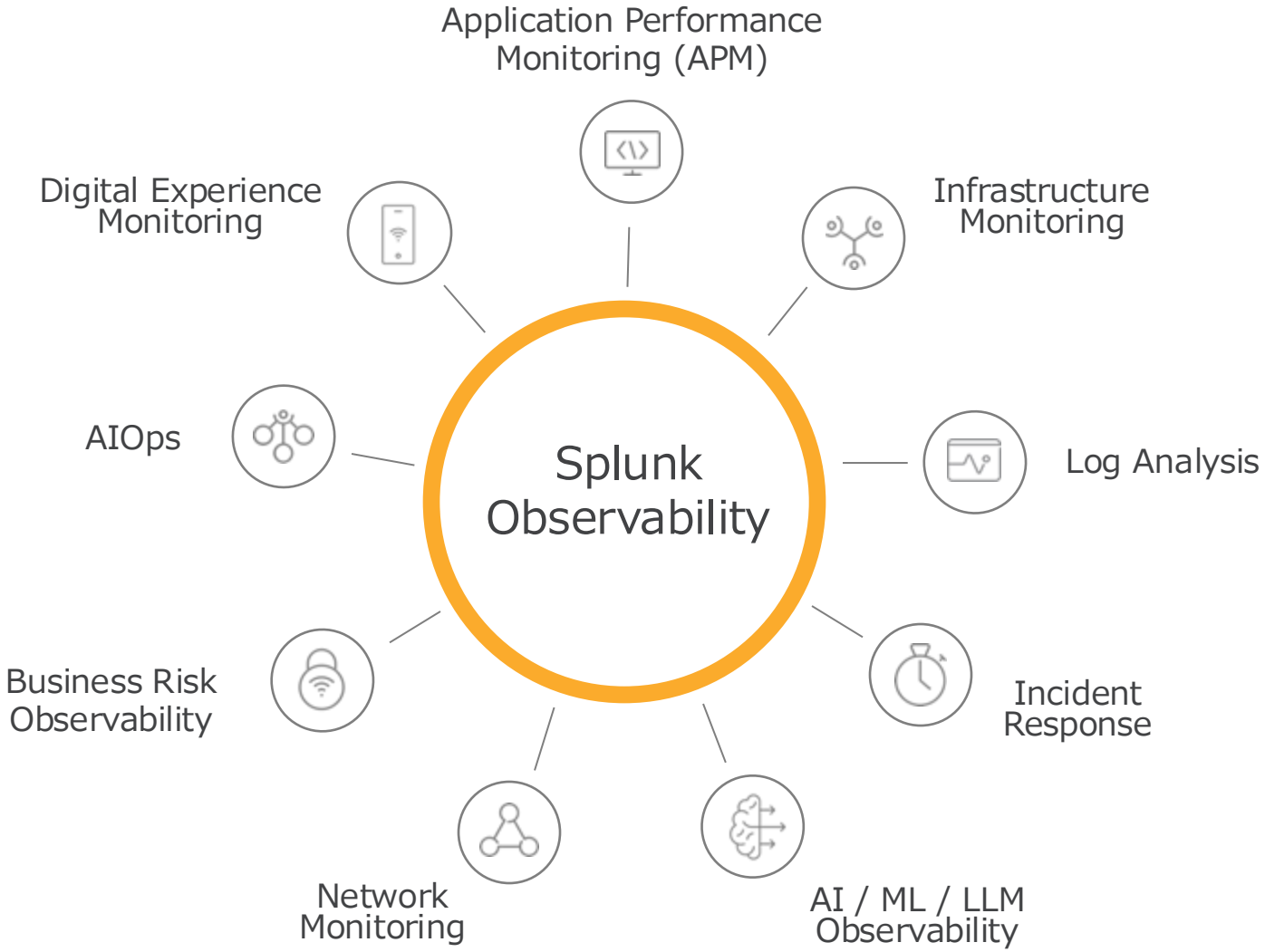
統一されたワークフロー

シームレスなコラボレーション

- ITとビジネスを連携させた　サービス監視
- オブザーバビリティを組織に展開する

Splunk AIが加速

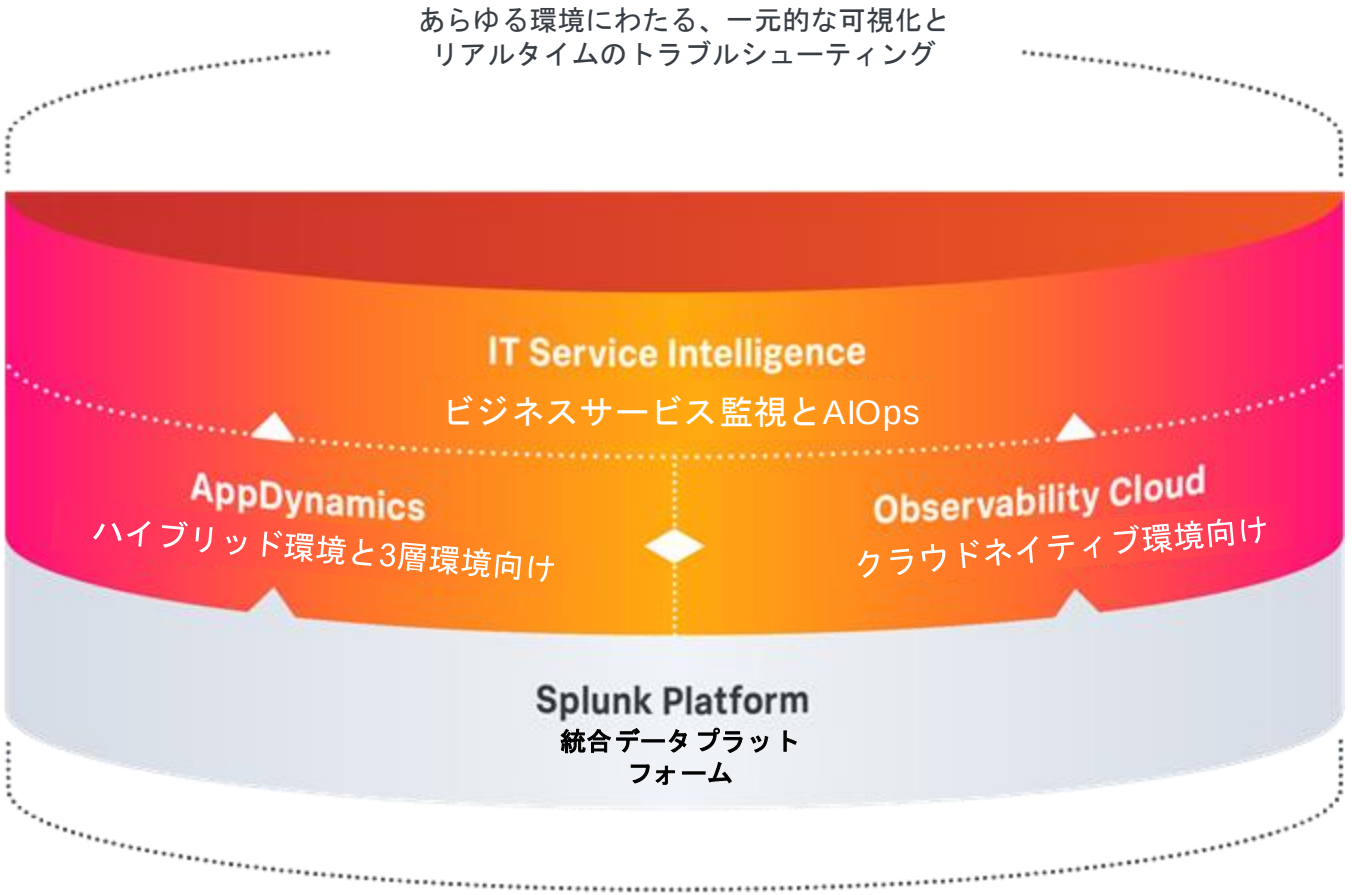
Splunk + Cisco =
あらゆる環境とスタックにわたる統合された可視性



- Real-Time Insights
- AI Powered
- Enterprise Grade
- Open Telemetry Native
- Extensible
- Cross MELT
- Business Context

オブザーバビリティの先進プラクティスの構築

デジタルフットプリント全体にわたる包括的な可視化



オブザーバビリティ業界のリーダーとして認定

統合されたメトリクス、イベント、ログ、トレース

AIガイダンスにより、未知の問題や根本原因を迅速に特定

OpenTelemetryのネイティブかつ主要な貢献者

Splunk + Ciscoによるエンド・ツー・エンドのオブザーバビリティ

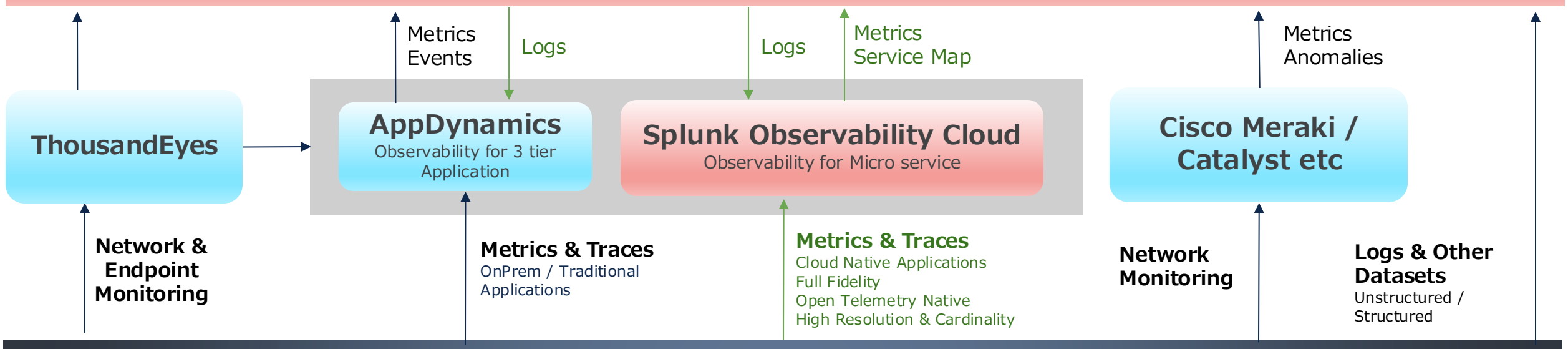
Splunk | Cisco

Splunk IT Service Intelligence
Executive Visibility | Proactive RCA | Event Management

OnCall

Enterprise Security

Splunk Core Platform
3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion



Real-time Data Sources
Hybrid Cloud Infra | Microservices | Applications | Services | Users | Network Devices | SaaS | Monitoring

Splunk

ITSI:
データを統合し俯瞰的な監視を実現する

OnCall:
オンコール管理・自動架電

ES:
セキュリティ監視
（SIEM）

Splunk

Splunk IT Service Intelligence
Executive Visibility | Proactive RCA | Event Management

OnCall

Enterprise Security

Splunk Core Platform
3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion

Metrics
Events

Logs

Logs

Metrics
Service Map

Metrics
Anomalies

ThousandEyes

AppDynamics
Observability for 3 tier Application

Splunk Observability Cloud
Observability for Micro service

Cisco Meraki / Catalyst etc

ThousandEyes:
ネットワーク監視

AppD:
モノリシックアプリに強い
オブザーバビリティツール

o11y cloud:
マイクロサービスに強い
オブザーバビリティツール

Cisco製品データ

Monitoring

Network Monitoring

Logs & Other Datasets
Unstructured / Structured

Real-time Data Sources
Hybrid Cloud Infra | Microservices | Applications | Services | Users | Network

その他、あらゆるテキスト・マシンデータ

Splunk

ITSI:
データを統合し俯瞰的な監視を実現する

OnCall:
オンコール管理・自動架電

ES:
セキュリティ監視
（SIEM）

Splunk

Splunk IT Service Intelligence
Executive Visibility | Proactive RCA | Event Management

OnCall

Enterprise Security

Splunk Core Platform
3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion

Metrics
Events

Logs

Logs

Metrics
Service Map

Metrics
Anomalies

ThousandEyes

AppDynamics
Observability for 3 tier Application

Splunk Observability Cloud
Observability for Micro service

Cisco Meraki / Catalyst etc

ThousandEyes:
ネットワーク監視

AppD:
モノリシックアプリに強い
オブザーバビリティツール

o11y cloud:
マイクロサービスに強い
オブザーバビリティツール

Cisco製品データ

Monitoring

Network Monitoring

Logs & Other Datasets
Unstructured / Str...

Real-time Data Sources
Hybrid Cloud Infra | Microservices | Applications | Services | Users | Networ...

その他、あらゆるテキスト・マシンデータ

本日の主なご説明

Splunk Observability Cloudについて

Cloud Nativeやマイクロサービス可視化に強いオブザーバビリティソリューション

Splunk Observability Cloudによるクラウド環境中心のエンド・ツー・エンドの可視性

エンドユーザーの経験から、アプリケーション、インフラまでをコンテキストを共有したトラブルシューティング

- ユーザー体験の可視化による インシデントの即時検知
- トラブルシューティングの 迅速化
- 根本原因の即時究明
- サイロ化の解消

Service Dashboard

ビジネスメトリクスや、フロントエンドからバックエンドまでの
メトリクス、トレース、ログ、イベントを集約したサービス状況の統合ビュー

ユーザー体験	アプリケーション	インフラ	ログ	サービスレベル
Synthetics / RUM (Real User Monitoring)	APM (Application Performance Monitoringi)	IM (Infrastructure Monitoring)	Log Observer Connect	SLO

ノーサンプリングによる一貫したコンテキスト

ユーザージャーニーの
シミュレートによる
能動的なユーザー体験監視

ブラウザ、モバイルアプリの
実ユーザーの体験を監視
セッションリプレイによる
操作状況の再現

アプリ間の関連性の自動マッピングと問題切り分け、DBクエリ分析、コードレベルのボトルネック分析

クラウドサービス、
Kubernetes、OS、ミドルウェア、DBなどのインフラメトリクスのダッシュボード化

アプリ、インフラと連動した
ログの特定と分析
(Splunk Cloud/Enterpriseと連携)

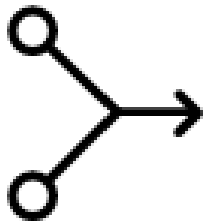
SLOの自動計算、アラートによるサービスレベルの維持

Splunk Observability Cloudの特長

エンタープライズのためのオブザーバビリティプラットフォーム

OpenTelemetry
準拠・フルサポート

ベンダーニュートラル
ロックイン回避



ノーサンプリングで
示唆型の原因究明

“再現待ち”を回避
問題解決を誰でも可能に

予測可能な課金体系

予期せぬ請求を
発生させない

企業全体の
データ統合分析

オブザーバビリティに
留まらない拡張性

Splunk IT Service Intelligenceについて

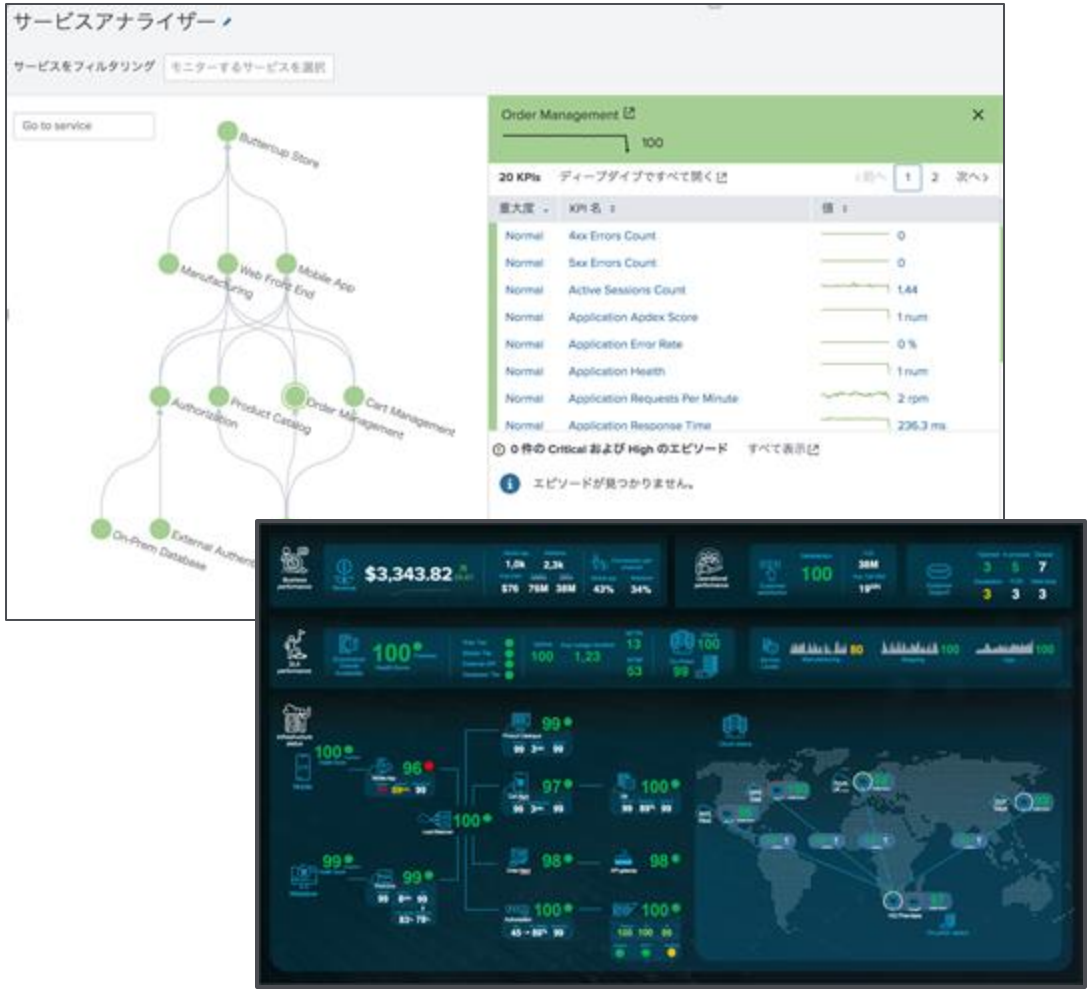
ビジネスとIT オペレーションの連携と深い洞察、AIOPS・運用プロセスの改善を図る

Splunk IT Service Intelligence

データに基づいた運用による、AIOpsの実現

ITSIがもたらす効果

- **死活監視からサービス健全性監視への変革**
- **MTTRの削減**
- **効率的な障害対応の実現**



ITSIの機能

サービス全体の健全性を可視化：ITサービスの構成要素をツリー構造で管理。KPIによるサービス健全性の管理によって、サービスの稼働状況を一目で確認可能。

メトリクス/イベントの時系列探索：複数のメトリクスやイベントログを一度に時系列探索が可能。

アラートノイズの削減：ルールエンジン、機械学習によりアラートを削減し、意味あるアラートに集約。

予兆検知：機械学習を用い、異常をいち早く検知することで、障害予兆の実現が可能。

ITSIによる統合監視ダッシュボード

Splunk で収集したデータを統合し、利用者視点でのカスタムViewを提供可能

Splunkによる組織全体のデータ統合分析

売上: ERPなど

コスト: ERP, AWS

問い合わせ・クレーム数:
CRM, ServiceNow

デプロイ状況:
CI/CD

SLA/SLO:
AppD/o11y cloud

セキュリティ:
ES, Cisco Security

システム連携:
HULFT

ジョブ管理:
JP1

状況俯瞰し、問題発生個所から
適切なツール、ダッシュボード
へドリルダウンし詳細調査

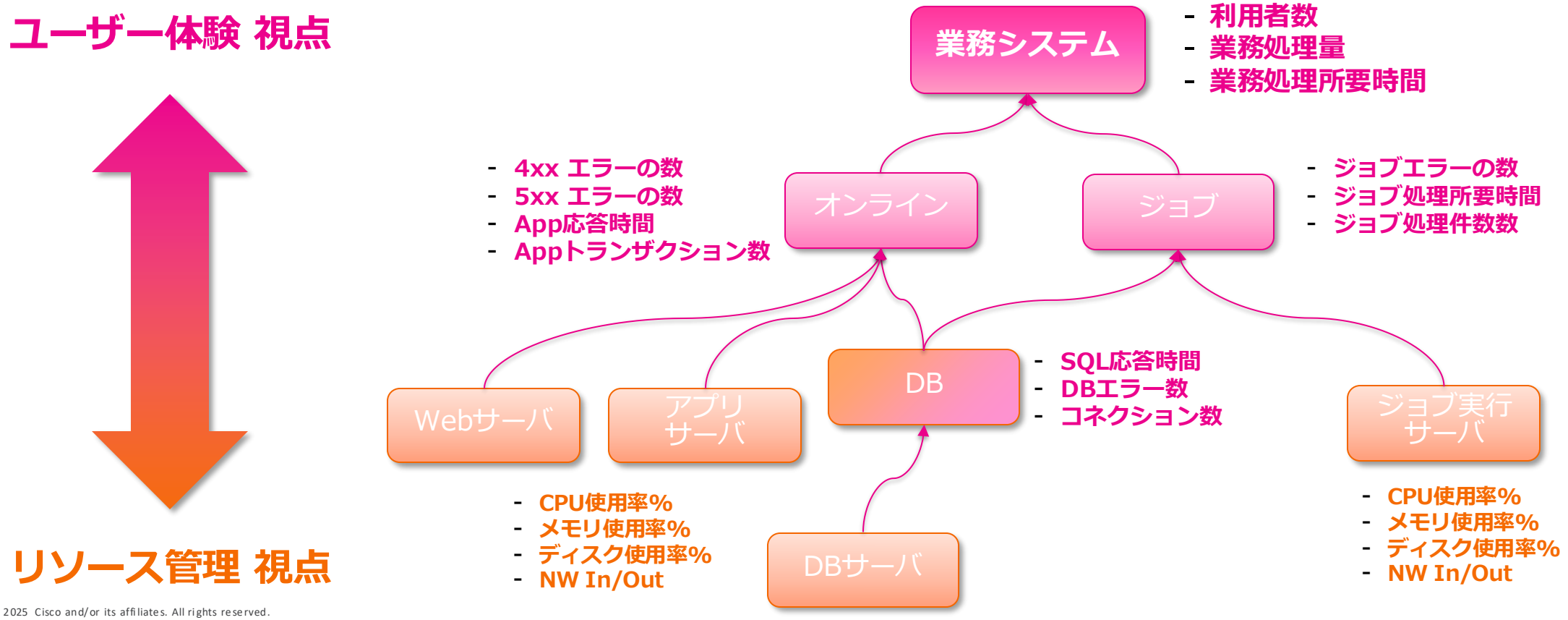
ユーザー体験:
AppD/o11y Cloud

アプリ・インフラ: AppD/o11y Cloud
ネットワーク: Cisco, ThousandEyes

拠点間・システム間の通信:
ThousandEyes

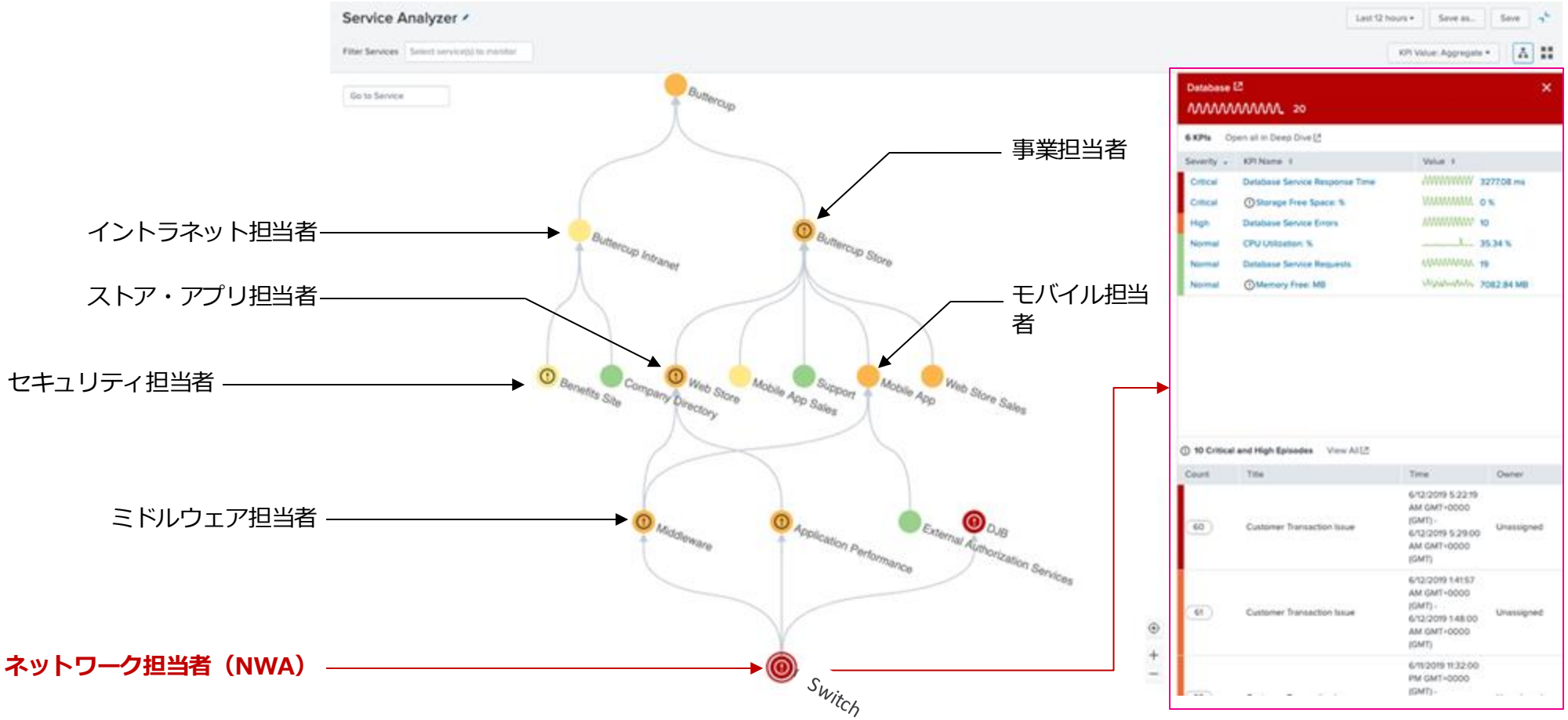
Splunk ITSI を中核とする新たな監視

ユーザー体験視点での監視・管理を重視、リソース視点での監視はそれを補完するものとし、
それぞれについてKPIベースの監視・管理を行う



IT基盤を通じて提供されるあらゆるサービスを管理

稼働環境（スタック）や技術ドメイン、担当組織の違いに関わらず
あらゆる状態を盲点なく、統合的に管理、可視化する仕組みの実現



AI含めたKPI計算により健全性スコアを自動計算
どのKPIが悪化しているか即時に特定

関連するイベント・アラートの一元管理

迅速に問題箇所を切り分け問題調査を迅速化

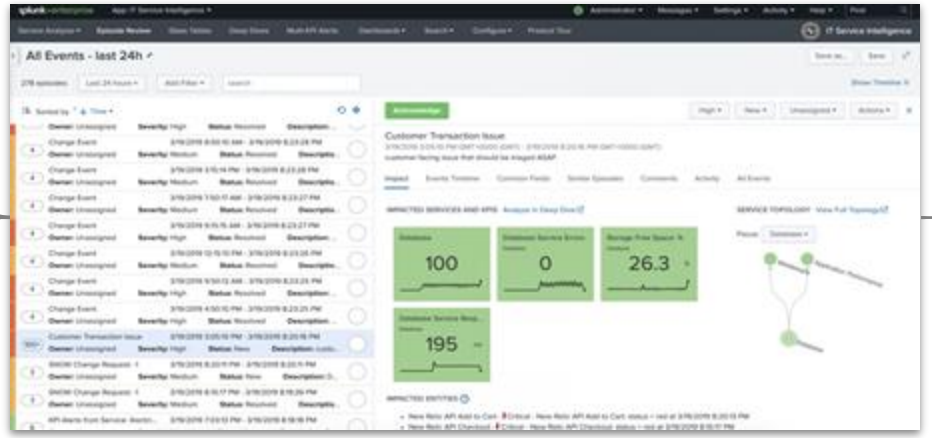
アラートノイズによる「アラート疲れ」を排除

既存の監視ツールからのアラートを統合、集約し必要なアラートのみにフォーカス。
サービス健全性との相関分析によりアラートにコンテキストを与える。

監視ツールのアラート

- Splunk
- Zabbix
- Nagios
- JP1
- Hinemos
- OpenView
- NetCool
- SNMP Trap
- etc

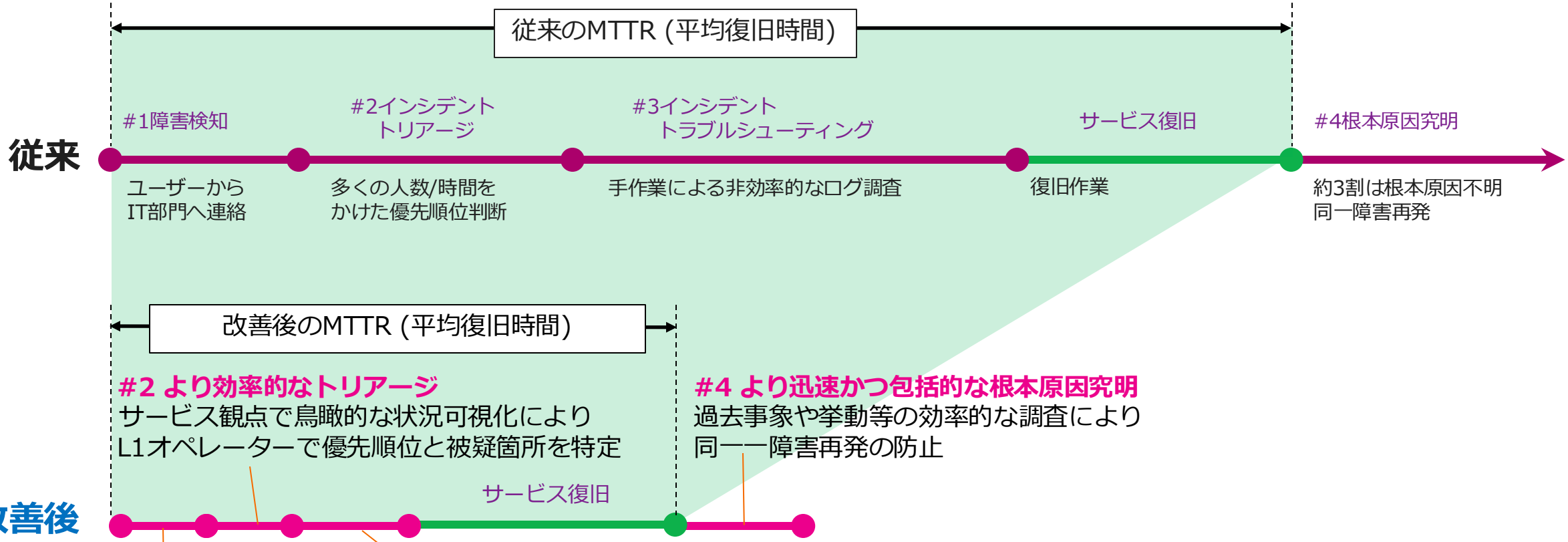
各監視ツールのアラート取り込み、
正規化、エンリッチメント、
類似イベント集約（アラートノイズ除去）



通知・他ツール連携

- Splunk OnCall
- Chat (Slack, Teams)
- ITSM (ServiceNow)

Splunk AIOps プラットフォームによる運用プロセスの改革



事例：SBペイメントサービス株式会社

オンライン取引のサービス監視とシステム状況を可視化

“経験豊富な有識者でなくとも、誰が見てもどの値が問題になっているのか、サービスレベルの状態が一目で分かるようにようになりました。“

- システム本部　システム運用統括部　運用課　鈴木彰氏

- 事業拡大*に伴い、増大するミドルウェアのアラートの分析・調査にSplunkを利用開始
- 利用範囲をCPUやメモリ等のシステムリソースのリアルタイム監視からサービス視点のシステムステータスの可視化へ拡大
- 異常検知時には相関分析により迅速に原因を究明
- 機械学習への取り組みも加速

*）提供オンライン決済手段: 40超。2017年取扱実績: 2兆5334億円。導入店舗数: 100,474（2018年度10月）

国内金融会社

国内金融会社

大量アラートの集約・自動電話による「意味あるアラート発報」を実現

課題

- 大量アラートによる障害対応の遅延
- アラート内容について口頭で伝達をしており、アラートの重大度について認識齟齬が発生

ご提案内容

- 監視ツールから発報されるアラートについてSplunkに集約し、ルールに基づいてアラート集約
- アラート内容に応じて、適切な相手への自動電話を実施
- アラート内容をTeamsへ自動投稿

見込まれる効果

- アラート対応作業の省力化
- 情報伝達の精度向上

Cisco製品とのインテグレーション

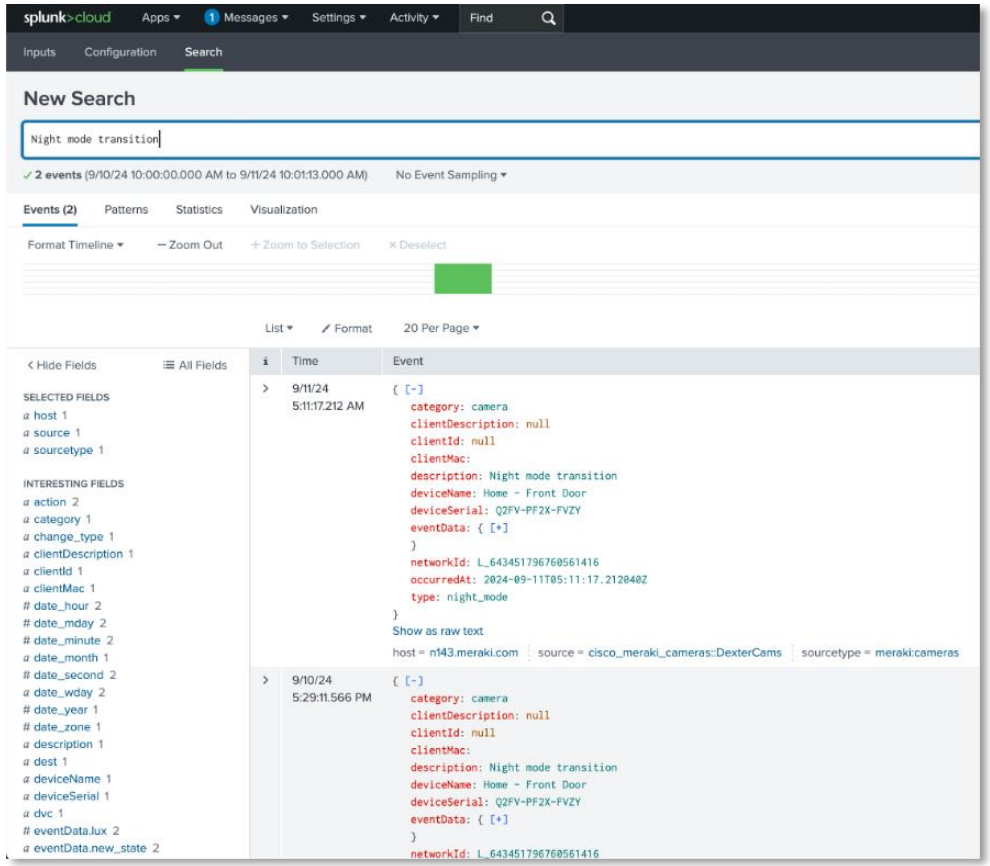
日々ご利用のCisco製品をSplunkの統合監視・運用プロセスに組み込む

Cisco + Splunk Integration roadmap

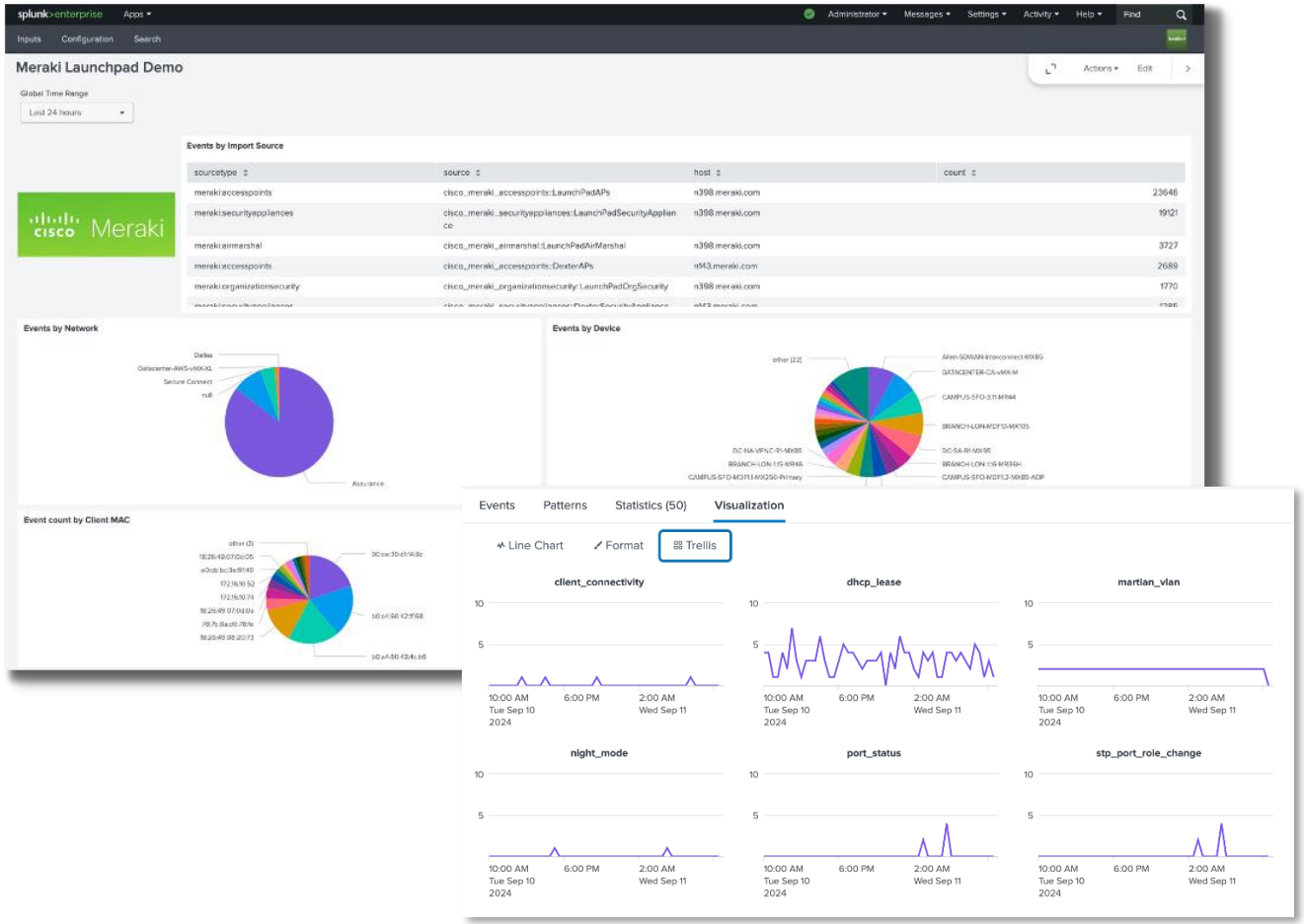
	AppDynamics + Splunk Platform	AppDynamics + Observability Cloud	Cisco + ITSI
DELIVERED Generally available (GA)	❑ AppDとSplunkプラットフォーム間でコンテキストを保持したディープリンクによるログ調査 ❑ AppDとSplunkプラットフォーム間のシングルサインオン		❑ アラートノイズの軽減とサービスの健全性向上のため、AppDアプリケーションのアラートとメトリクスをITSIに統合
DEVELOPING NOW Preview or GA within 6 months		❑ 共通の外観と操作性 ❑ シングルサインオン	❑ データベースやインフラにも拡張された、AppDアラートとメトリクスのITSI統合
NEXT Preview or GA within 6-12 months	❑ Splunkプラットフォームに保存されたログを調査するためのAppD内のログサマリーUI	❑ Observability CloudへのThousandEyesの統合、豊富なデジタルエクスペリエンス管理（DEM）のためのモバイルRUM	❑ ThousandEyes、Catalyst Center for Enterprise、アクセスネットワークの可視性をITSIに統合
FUTURE Preview or GA beyond 12 months		❑ AppDとObservability Cloud間のコンテキストを保持したディープリンク ❑ Observability Cloudに組み込まれたビジネスリスクの可視化とコスト・リソース最適化機能	❑ データセンター、ワイヤレス、SD-WANネットワークの可視性向上のため、ACI、Meraki Controller、vManageをITSIに統合

Observability with Meraki + Splunk

データを集約し、ネットワークイベントの簡単な検索と分析

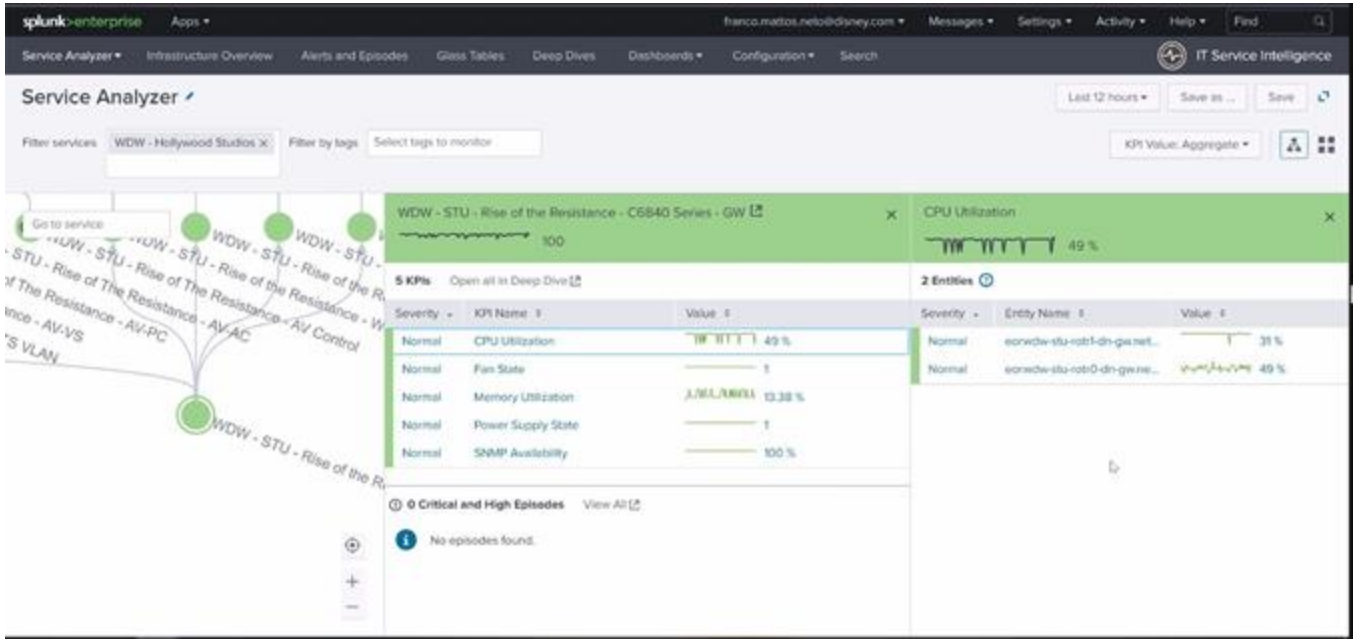


重要なデータにフォーカスしたカスタムダッシュボードの作成



ウォルト・ディズニー・ワールド：
ネットワークサービスの健康状態がビジネスサービスに影響を与える

- パーク内のライドコントロールネットワーク（AV、VLAN、GW）の全体的なヘルス状態を監視し、各アトラクションが正常に機能するようサポート
- この健康状態を、特定のアトラクションやパークのビジネスへの影響として示す
- ネットワークのヘルスパラメータには、可用性、CPU、メモリ、ファン、電源、温度が含まれる
- ITSIで高レベルの可視性を得た後、NW監視ツールでルーターやスイッチなどの詳細を調査



まとめ

Splunkで実現するオブザーバビリティは・・・

・Splunkはセキュリティのみならずオブザーバビリティ観点でもシステムのレジリエンス（回復力）を高めるための統合基盤です

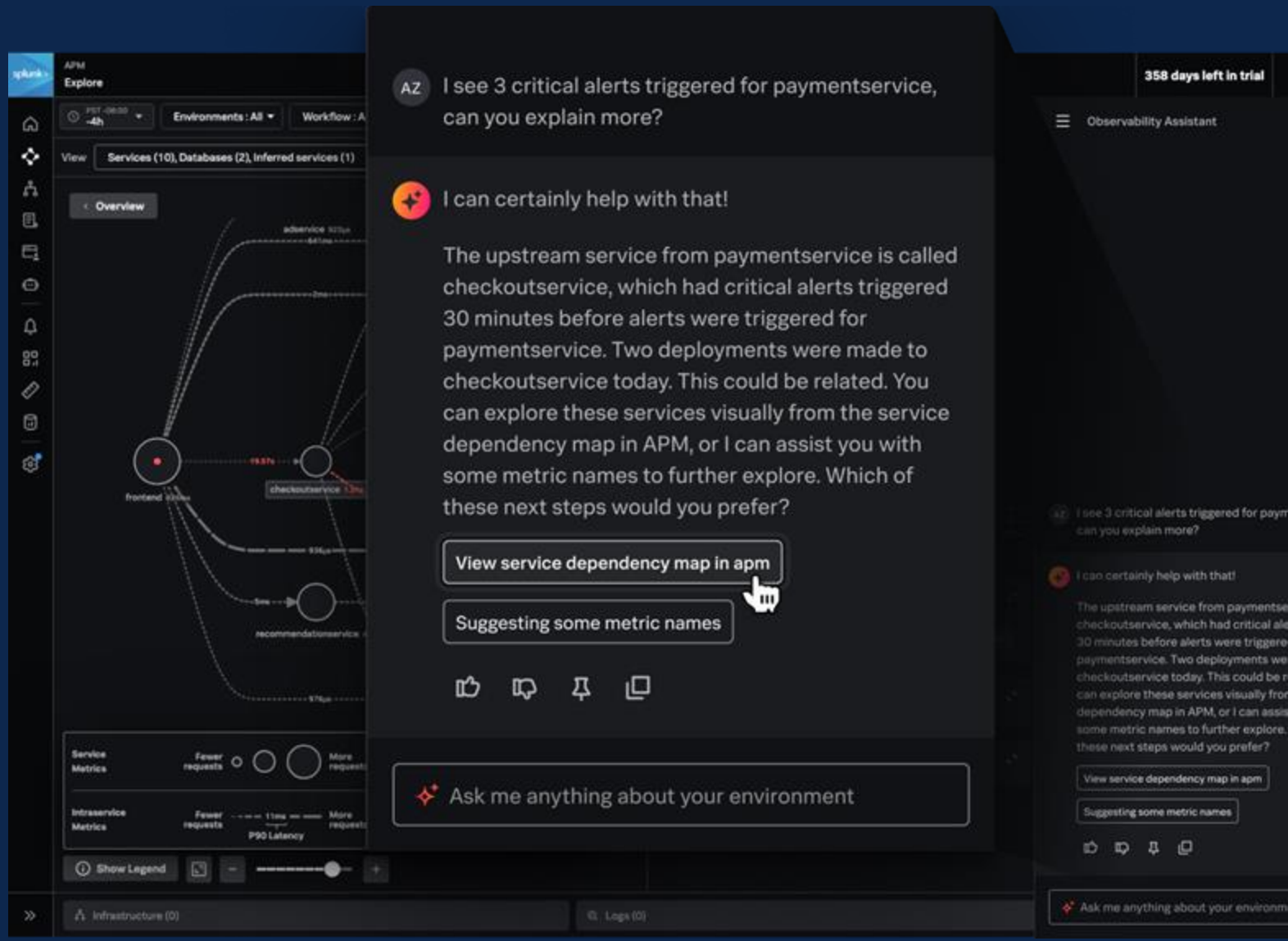
・ITオペレーションみならずビジネスデータも統合・効率化が図れ、お客様のビジネスを支えます

・Ciscoとの統合により更に包括的になりました
（ Catalyst、Meraki、ThousandEyes、AppDynamics etc ）

紹介：
Splunk AI Assistant for Observability

自然言語を使い、Splunk Observability Cloudでの問題の特定と解決を迅速化

- データとやり取りすることで、主要なインサイトを発掘
- チャートを作成して、調査を迅速化
- トラブルシューティングに際して、コンテキストやサポートを活用



CABへの影響


CISCO