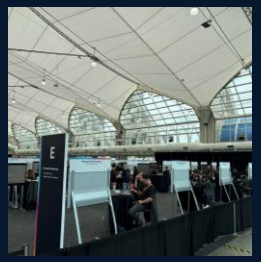
Cisco Live! とは

- Cisco Live! は、世界中の IT プロフェッショナルが一堂に会し、最先端のテクノロジーやソリューションに関する知識やスキルを習得する機会を提供するとともに、さまざまな分野のエキスパートとのディスカッション、ネットワーキングが可能なシスコが主催する世界最大級の IT イベントです。

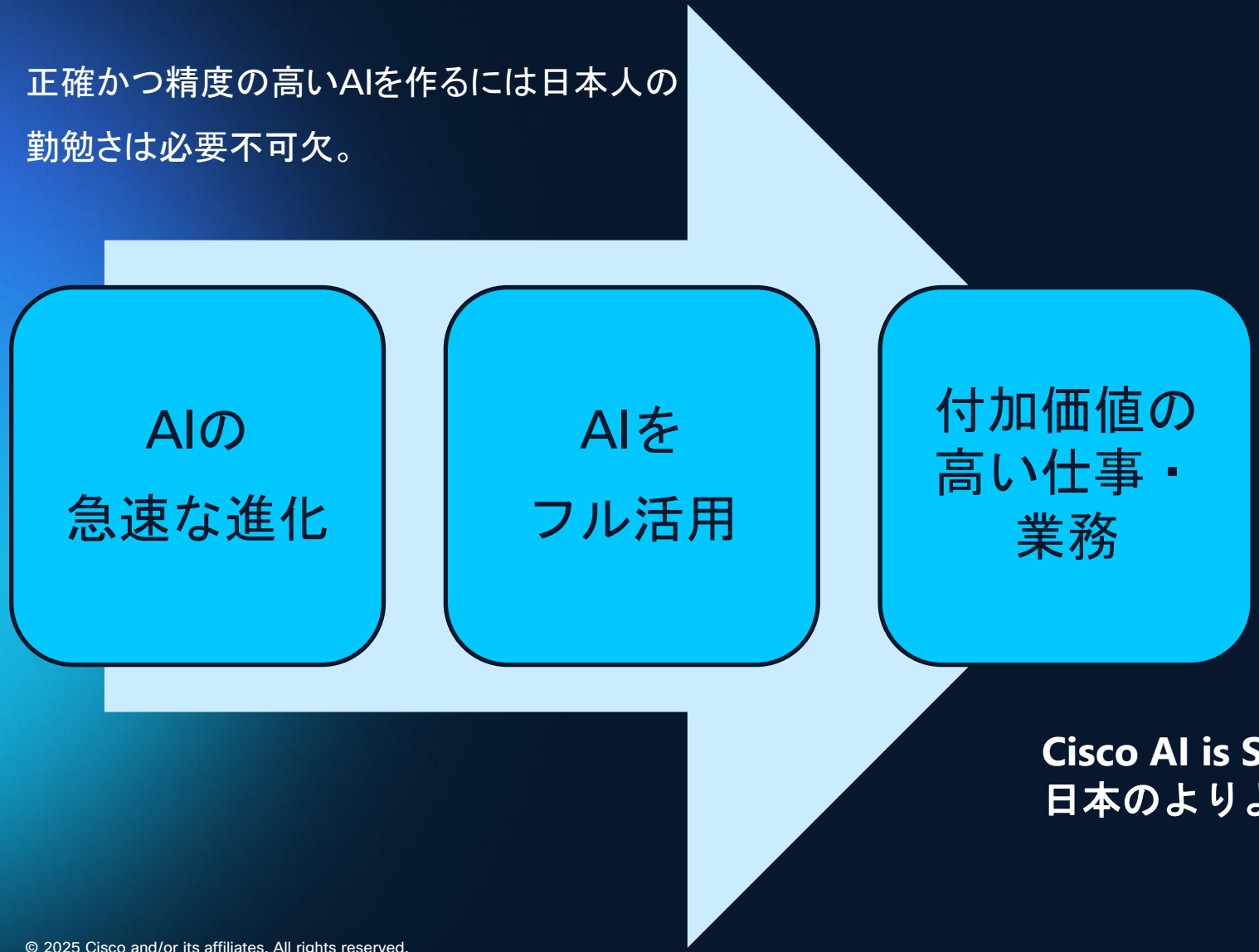
- サンディエゴでは米国を中心に約22,000名以上が訪れ、約1,700のセッションや、150社以上のパートナー企業による展示が行われました。

Japan Hosting program
参加者は195名、61社



世界でもっともAIの恩恵を受けるは日本

正確かつ精度の高いAIを作るには日本人の
勤勉さは必要不可欠。



✓一足飛びのデジタル化
✓人手不足の解消
✓国際競争力の強化

Cisco AI is Supporting Japan's Future
日本のよりよい未来のためにCisco＆AIで支援する

Cisco Live 2025 San Diego

Cisco Live Keynote セッションサマリ

2025年6月18日

長谷川 偉一

エンタープライズソリューションズエンジニアリング

シスコシステムズ合同会社

Jun 18, 2025

アジェンダ

- マーケットトレンドおよびシスコ戦略
- AI ready Datacenter
- Future Proofed Workplace
- Digital Resilience
- CX 戦略および対談内容の紹介

アジェンダ

- マーケットトレンドおよびシスコ戦略
- AI ready Datacenter
- Future Proofed Workplace
- Digital Resilience
- CX 戦略および対談内容の紹介

AI時代の変革はネットワークから
共に安全で革新的な未来を

AI活用が急速に拡大する中、堅牢かつ安全なネットワークがビジネスの成長と変革のカギとなります。シスコは、ネットワーク、セキュリティ、データ活用を統合したプラットフォームへの進化を加速しています

シスコが提供する3つの価値

・AI対応データセンター:
高性能・拡張性でAIワークロードに最適化

・未来を見据えたワークプレイス:
変化に強く、柔軟な働き方を支援

・デジタルレジリエンス:
ネットワーク全体でセキュリティと可視性を強化し、信頼性を確保

主な発表・取り組み

-AI時代のセキュアネットワークアーキテクチャ発表。トラフィック増加や高度なセキュリティ要求に対応

-セキュリティ機能をネットワークに深く統合し、ゼロトラストやAIによる脅威検知を実現

-データセンターのAI対応を強化。NVIDIAとの連携や「Cisco Silicon One」など最新技術で高性能・拡張性を実現

-Splunk & ThousandEyes連携でネットワーク可視化・障害対応力を向上

Cisco Live US 2025での主なメッセージ

グローバルでの AI レース

- AI活用への取り組みについて、参加者の98%が「強い緊急性を感じている
- 85%が「18か月以内に成果を出す必要がある」と考えている
- 世界的な AI 競争と地政学的リスクの高まりに触れ、各企業のCEOも「競合他社が先行してしまうこと」への恐れから迅速な対応を求めている

AIを支えるインフラの重要性

The Network Foundational for AI（ネットワークはAIの基盤）

- Ciscoはネットワーク企業として創業し、今も「ネットワークが全ての基盤」であると位置付けています。特にAgentic AI時代への移行においてネットワークはこれまで以上に重要であり、今回発表される全てのイノベーションもネットワーク抜きには語れない
- 調査結果として「モダンネットワークが不可欠だ」と答えた参加者が97%
- AI時代に向けてネットワークとセキュリティの融合（Security in the Network）が必須

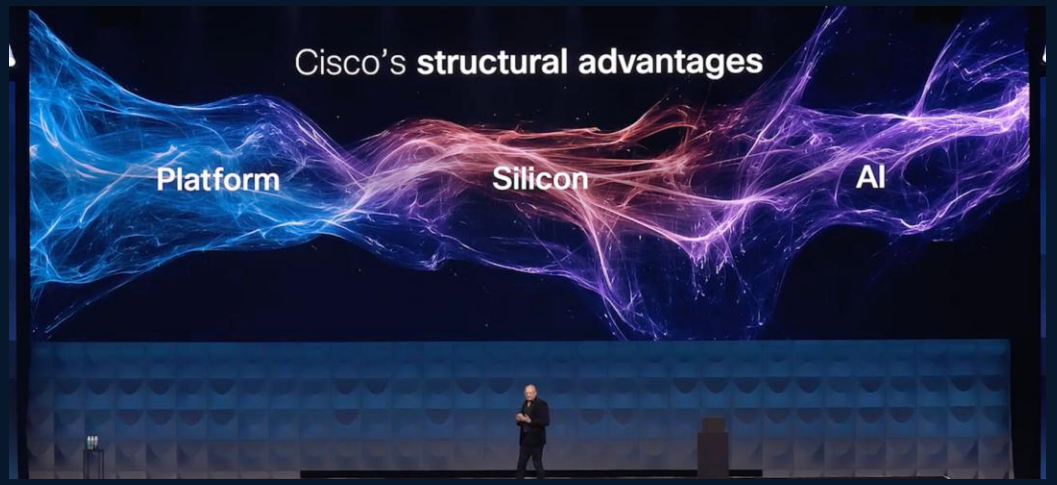
プライベートデータセンターの回帰

- 一時期はクラウド全面移行の圧力があったものの、現在は多くの企業がクラウドとオンプレミスを組み合わせたハイブリッド戦略に回帰
- 特に生成AIの推論（インフェレンス）ワークロードはレイテンシやコストの観点から自社データセンター内で行う需要が高まっており、小型モデルをエッジで動かすケースも増えるため、今後は自社インフラを再構築する動きが活発になると予測

Agentic AIを踏まえた Safety and Security

- 安全性とセキュリティの新たなアプローチが必要。
- 昨年の調査では、組織内でAIリスクを十分に理解している社員は半数に満たないと回答
- これはエージェントAI以前の話です。そこで、AIアプリケーションを動かしながら、ワイヤースピードでセキュリティサービスを適用するために、「セキュリティをネットワークに融合」

Cisco Live US 2025での主なメッセージ



Agentic AI 時代の到来

- 2020年11月のChatGPT登場以来、「チャットボットによる対話型AI」の時代から、今まさに「ヒトに代わってタスクを実行するエージェントAI」の時代へと進化
- この変化は単なるインタラクションの拡張ではなく、従来、人間が100%実施していたタスクにエージェントが加わることで、生産量が十倍以上に拡大

Agentic AI を踏まえたインフラでの考慮事項

- ネットワーク：エージェント間の「リアルタイム / 低レイテンシ通信」が頻発し、既存ネットワークでは帯域や遅延面でボトルネックに
- Compute：持続的な推論ワークロードが発生するため、GPUやサーバ容量の大規模拡張が不可欠
- 電力・コスト：大規模AI推論では消費電力が跳ね上がることから、エネルギー効率改善とコスト最適化が事業継続の分水嶺となる。
- セキュリティ：AIを安心して導入・利用いただくためには、「セキュリティがなければAIは採用されない」時代へ転換していると指摘しました プライベートDCのハイブリッド再評価

Cisco の強み

- Platform: ネットワーク、セキュリティ、コラボレーション、データセンター、AI を一気通貫で統合し、各製品を組み合わせるほど相乗効果が上がる“複合的な価値”を実現
- Silicon:自社開発ASIC（プログラム可能シリコン）により、新しいユースケース対応を後付けプログラムで実現。従来のシリコン“テープアウト”サイクルを大幅に短縮し、開発と導入の速度を加速
- AI: 製品設計からプロダクトライフサイクル、運用管理に至るまで、AIを基盤原則として組み込むことで、「作って終わり」ではない継続的イノベーションを可能に

Ciscoの戦略の柱

AI-Ready Data Center

Future-Proof Workplace

Secure Global Connectivity

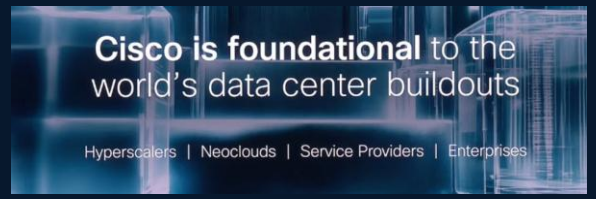
Digital Resilience

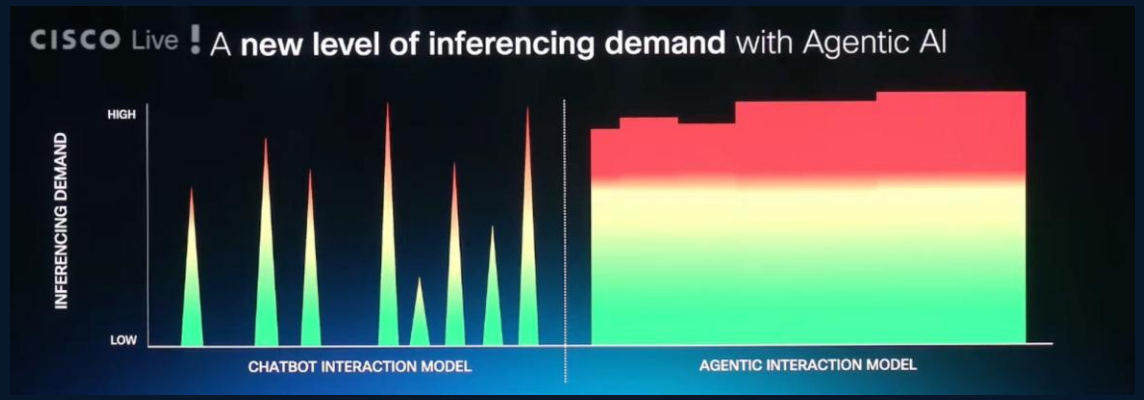
Accelerated by Cisco AI

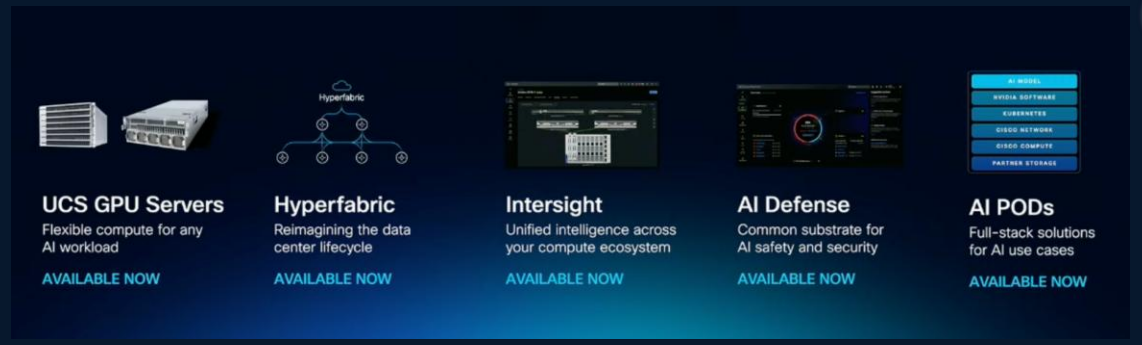
アジェンダ

- マーケットトレンドおよびシスコ戦略
- AI ready Datacenter
- Future Proofed Workplace
- Digital Resilience
- CX 戦略および対談内容の紹介

AI-ready Data Center







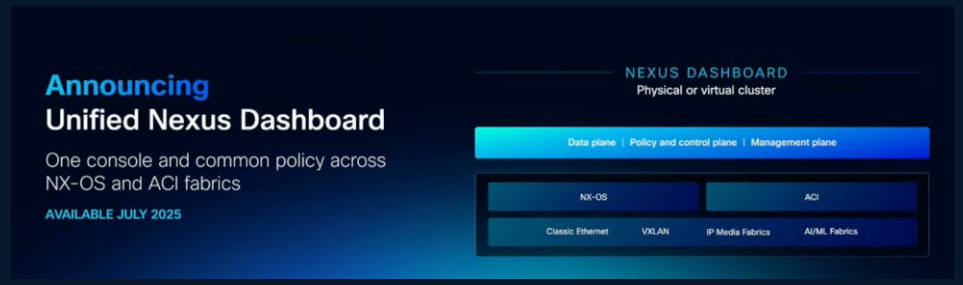
AI 需要の高まりと変化

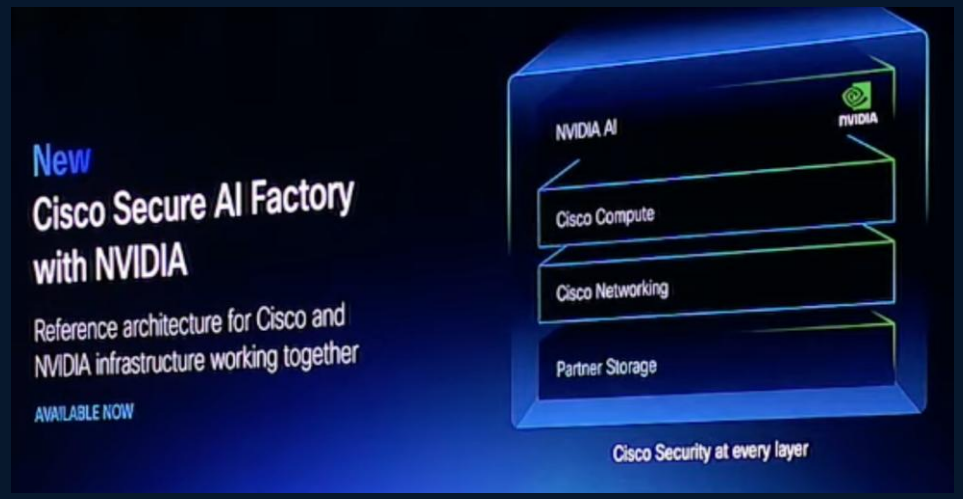
- **最大規模のデータセンター拡張期**：世界は歴史上最大規模のデータセンター拡大を迎えており、歴史的に見ても、今この瞬間が「かつてないほど急速にデータセンターが増設されている局面」であり、そのカーブは日々加速している。
- **トレーニング中心から推論中心へ**：過去数年間は大規模モデルのトレーニング需要がドライブしていたが、今後は「エージェントが常時ジョブを回す”推論ワークロード”」が継続的かつ大量に発生する。
  チャット：ユーザーが質問するたびにピークがぽつぽつ現れる一過性の需要
  AIエージェント：ピ「持続的かつ永続的な推論要求」が DC にのしかかる
- **アーキテクチャの再設計が必須**：突発的ピークではなく、24時間365日走り続ける推論パイプラインに耐えうるネットワーク、コンピュート、電力インフラを再構築し直す必要がある。

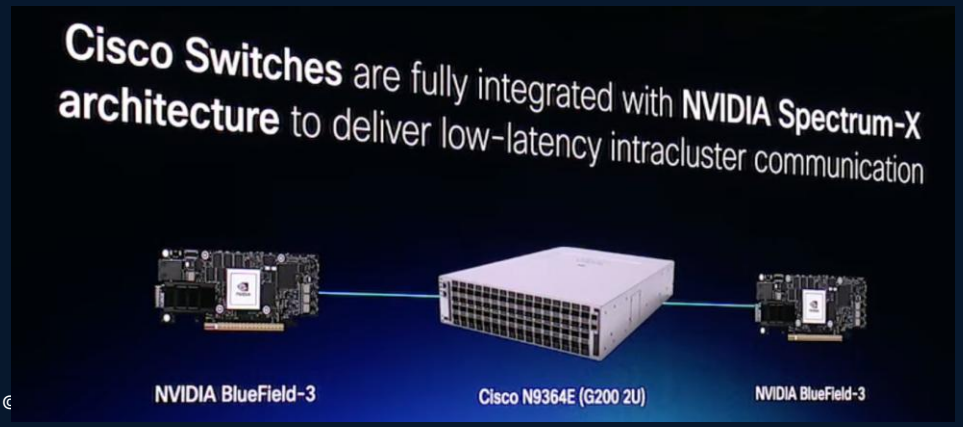
直近6ヶ月の主なイノベーション

- ニーズに合わせてGPUを2基→4基→8基とスケールアップ可能なサーバ(UCS Servers)
- データセンタネットワークをクラウドから素早く簡単に構築可能なソリューション(Hyperfabric)
- 進化し続けるUCSサーバ郡を管理するための統合管理プレーン(Intersight)
- AI自体を保護するためのセキュリティ製品(AI Defense)
- Compute、ネットワーク、ストレージ、セキュリティを統合したリファレンスアーキテクチャ構成のフルスタックソリューション(AI PODs)

AI-ready Data Center







Unified Nexus Dashboardのリリース

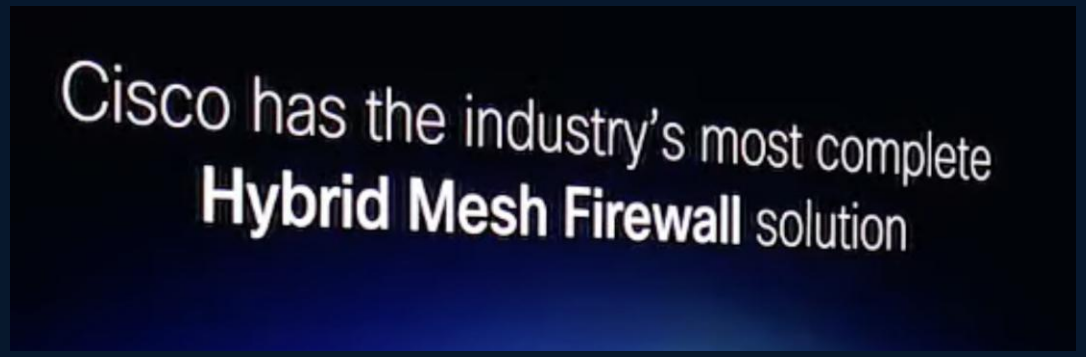
New

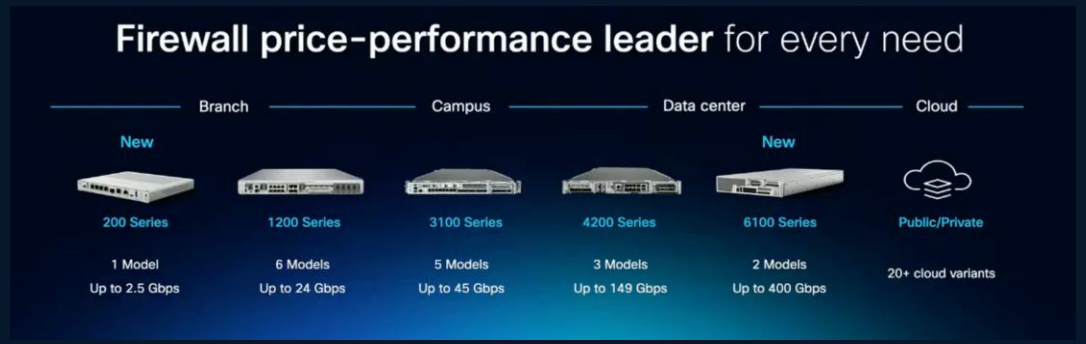
- Nexus OSとACIファブリックの管理を統一するNexus Dashboardの統合を発表(7月リリース予定)
- 統合コントローラにより、異なる種類のデータセンターネットワークファブリックの統合を実現

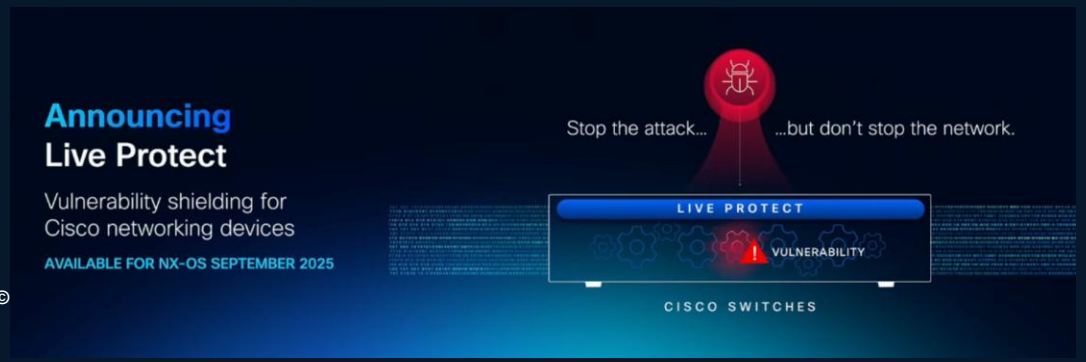
NVIDIA 社とのパートナーシップ強化

- すでにリリースしているSecure AI Factory、 NVIDIA Spectrum Xアーキテクチャへのスイッチ統合に加え、 Cisco AI DefenseとNVIDIA Nemoの連携を発表
- NVIDIA Spectrum XアーキテクチャにCiscoスイッチ統合され、低遅延のクラスター無い通信実現
- Cisco AI Defenseが、NVIDIAのNemoフレームワークで開発されたオープンモデルを検証・保護可能 (Secure AI Factoryの強化)
- これによりAIモデル自体のセキュリティ強化が可能となり、AIシステム全体の信頼性を高める事が可能

AI-ready Data Center







Security Cloud Controlの進化

- Cisco Security Cloud 全体を設定、管理、監視が可能
- 各種AI Assistant機能を搭載
- ルール、ポリシー、設定の最適化、重複や設定ミスの検出、エレファントフローのような異常をAIにより検出

Hybrid Mesh Firewallの進化

- Hybrid Mesh Firewall の実現に向けて対応製品と機能を拡張
- Security Cloud Control対応製品の拡張(Cisco Secure Router, 3rd Party Firewall)
- ポリシー管理ポイントの拡張(Cisco Smart Switch, ACI, Secure Workload)

Cisco Secure Firewall のラインナップ拡大 New

- 1台あたり2Uで400Gbpsの処理性能を持つデータセンタ向け高性能Firewall、最大16台のクラスタリングで4Tbps以上のパフォーマンス(6100シリーズ)
- 1.5Gbpsの暗号化通信を処理可能なブランチ向けのハイパフォーマンスボックス(200シリーズ)

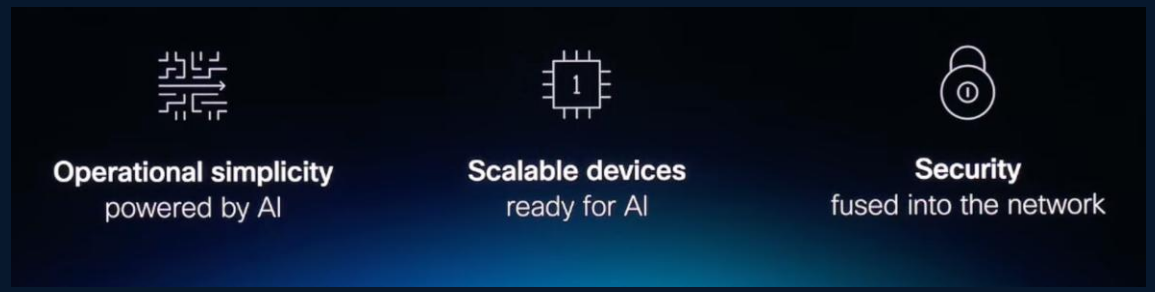
Live Protect New

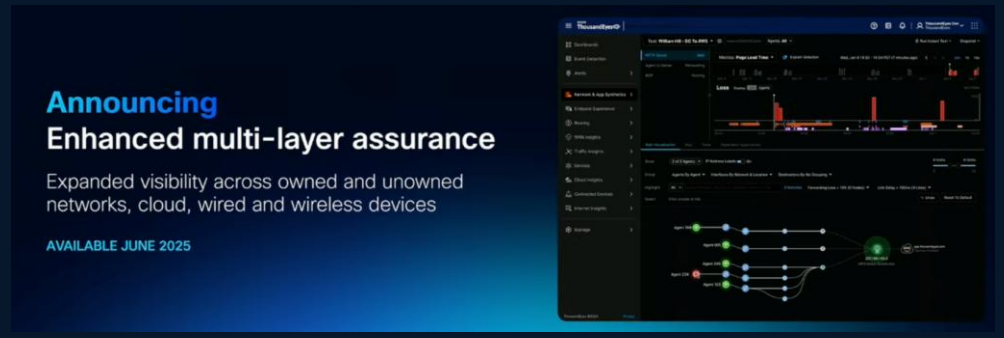
- ネットワーク機器のパッチ適用には平均45日だが、脆弱性悪用は公開から3日
- ネットワーク機器の脆弱性発見からパッチ適用までの期間にネットワーク機器を保護する仕組み
- eBPFを利用し、ネットワーク機器のOSを保護(NX-OSからリリース予定)

アジェンダ

- マーケットトレンドおよびシスコ戦略
- AI ready Datacenter
- Future Proofed Workplace
- Digital Resilience
- CX 戦略および対談内容の紹介

Future proofed-workplace





マーケットトレンドと戦略

- 未来の職場ではエージェント、ロボット、IoTデバイスの増加、人々の働き方の変化、電力に関する性ややセキュリティの脅威など、インフラに対して様々な要求が発生する
- Ciscoは3つの戦略で変化へ対応
  - Operational Simplicity (AIを利用した運用のシンプル化)
  - Scalable Devices (AI対応スケーラブルデバイス)
  - Security (ネットワークへのセキュリティ融合)

Operational Simplicity

Catalyst と Meraki の統合

- CatalystとMerakiのハードウェア、ライセンス、管理の統合を進めている
- CatalystとMerakの統合管理を実現し、クラウド・オンプレミス・ハイブリッドの統合管理を発表

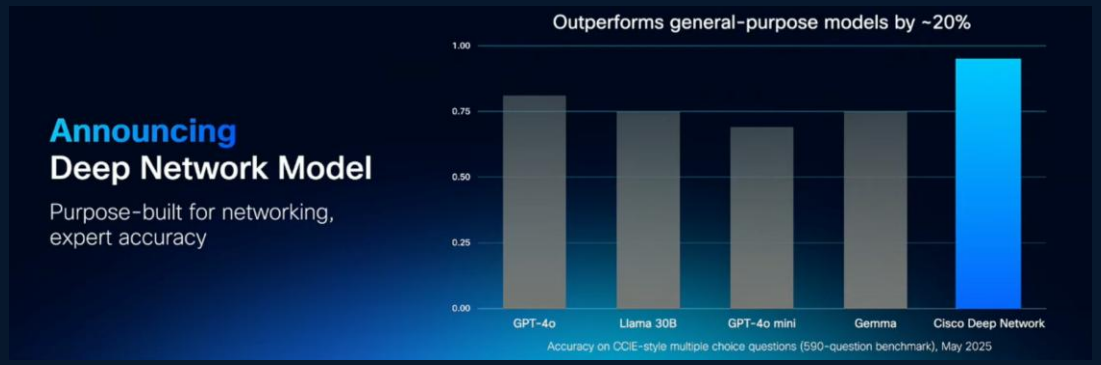
Operational Simplicity

マルチレイヤアシュアランス

New

- 自身が管理している企業ネットワークだけでなく、管理外のクラウドやエンドポイントを含めた可視化が必要
- 複雑化する環境においてマルチレイヤ（ネットワーク、クラウド、有線/無線デバイス）での簡単な管理の実現 - Splunkとの統合も可能

Future proofed-workplace



Scalable Devices

AgenticOpsの実現 New

- クロスドメインの可視性と管理、マルチプレイヤーでの協調作業を可能にするAgenticOpsの発表
- AgenticOpsの構成要素
  - 専用に構築されたAIモデル： Deep Network Model
  - 生成AIを利用したUI： AI Canvas

Scalable Devices

Deep Network Model リリース New

- Ciscoが開発した、ネットワーキングの専門家向けに設計
- ネットワーキングドメインにおいて他社のモデルより20%優れた精度を持つ、比較的小規模で効率的なモデル
- 6月末にCCIEユーザ向けに提供予定

Scalable Devices

AI Canvas New

- クロスドメイン・トラブルシューティングのためのGenerative UI
- AI Assistant により、自然言語での指示（例：「このチケットをトラブルシューティングして」）に基づいて、ServiceNow、Meraki、Thousand Eyes、Splunkなど様々なソースからデータを自動的に取得・相関させ、動的にUIウィジェットを生成
- これにより、NetOps、SecOps、IT、そして経営層を一つの環境に統合し、トラブルシューティングプロセスの簡素化

AI Canvas によるデモ内容

障害概要の取得
(Service Now 連携)

↓

障害内容の解析
被疑箇所の可視化

↓

関係者を招集

↓

追加の情報を確認

↓

問題の是正/結果表示
(切り戻しも可能)

↓

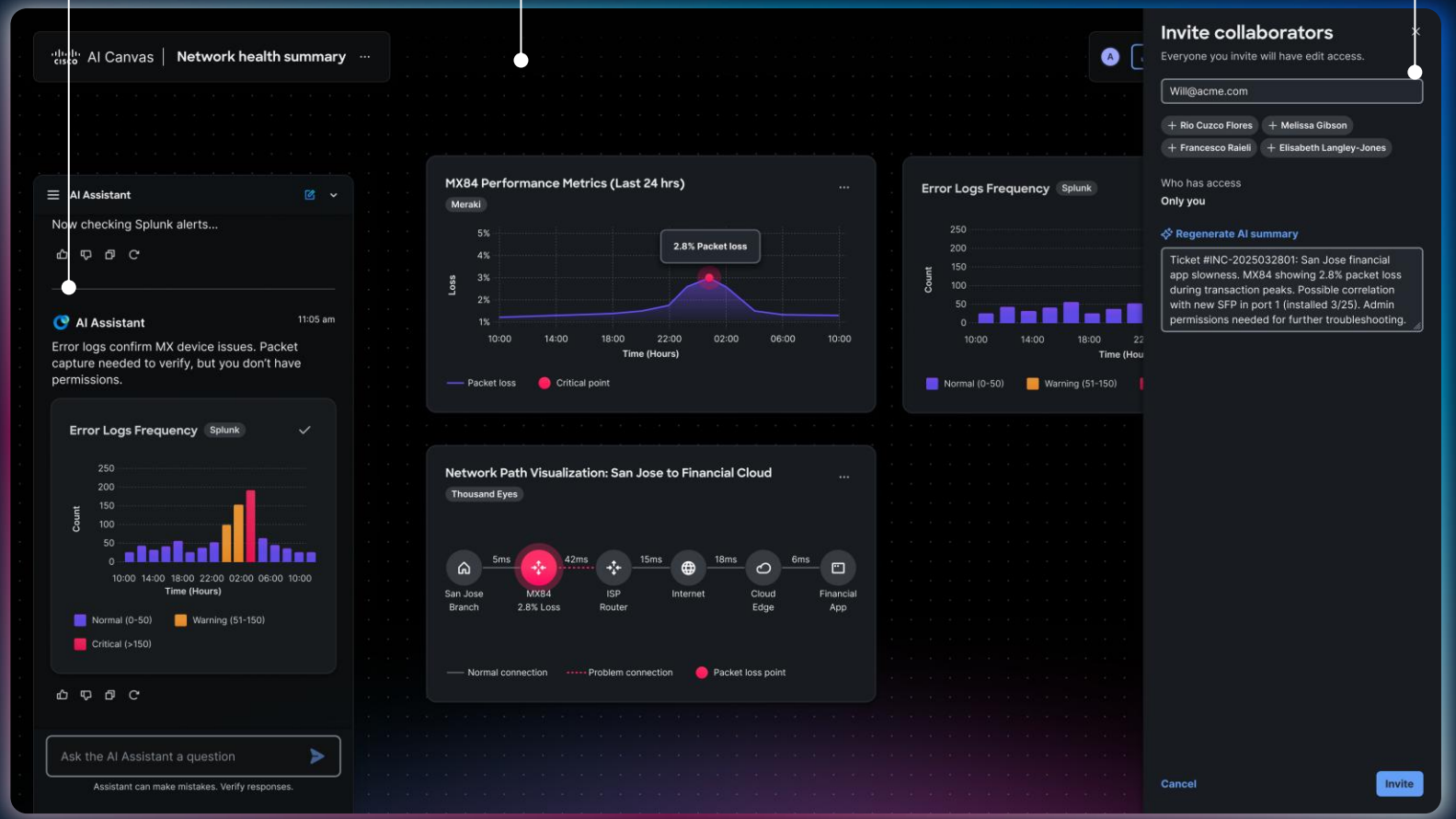
最終レポートの作成

https://www.youtube.com/watch?v=M3WSjEc30mk
(1:00:22 頃から)

ALPHA | OCTOBER

AI Canvas

- クロスドメイン・トラブルシューティングのための単一キャンバス
- 推論を組み込んだGenerative UI
- NetOps、SecOps、IT、そして経営層を一つの協調的な環境に統合
- AI Assistant 搭載



Many of the products and features mentioned are still in development and will be made available as they are finalized, subject to ongoing evolution in development and innovation. The timeline for their release is subject to change.

Future proofed-workplace

Cisco Room Vision PTZ

Cisco **Universal ZTNA**

Cisco **Security**

Scalable devices

AI時代向けのラインナップをリリース

New

- キャンパス、ブランチ、産業用IoTを含む新しいモデルのリリース
- 自社開発したSilicon One ASICを搭載に加え、コンテナ化されたサービスや、リアルタイムの遠隔測定、AI分析に基づいて、動的に適応するダイナミックQoSなど、OSのアップデートを実施

- Smart Switches：Silicon One ASIC を搭載し、スイッチ上でセキュリティワークロードを利用可能、ポスト量子暗号対応新世代スイッチ
- Smart Routers：高パフォーマンスかつインラインでのセキュリティ機能を搭載、ポスト量子暗号対応新世代ルータ
- Campus Gateway：最大5000台のAPに対応している、クラウドネイティブなワイヤレスコントローラ
- Large Venue Wi-Fi 7：スタジアムやアリーナなどの大規模空間に対応したWi-Fi 7アクセスポイント
- Scale OT for AI： PoE および UPoE を特徴とする 19 種類の新しい産業用スイッチと、Wi-Fi 7/CURWB（超高信頼ワイヤレスバックホールテクノロジー）を一台に組み合わせたアクセスポイントのリリース

Scalable devices

Cisco Room Vision PTZリリース

New

- NVIDIAチップセット搭載した、職場での体験に重要なAI対応コラボレーションデバイスのリリース(MS Teamsサポート)
- ネットワーク上のセンサーとしても機能して、施設データ（温度、通話品質、利用率など）を取得可能

Security

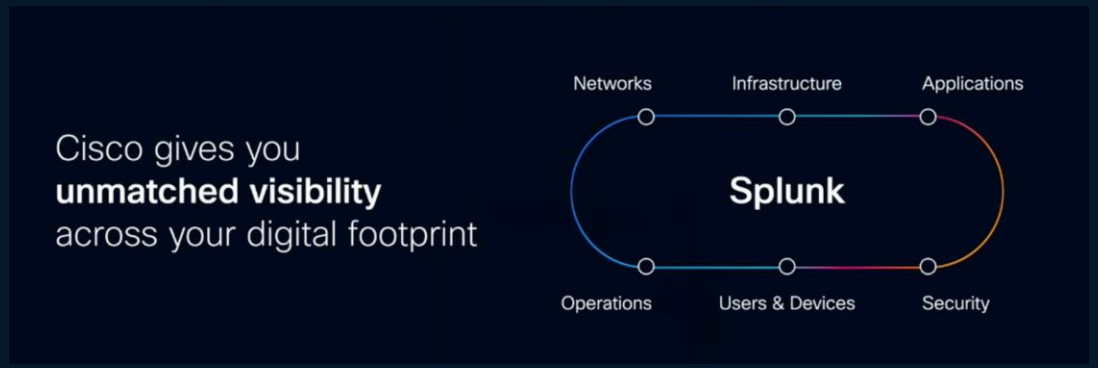
Universal ZTNAの進化

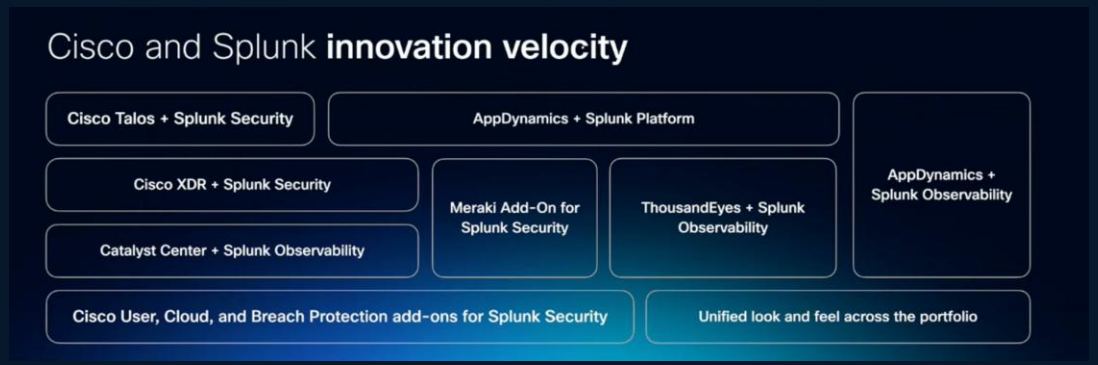
- ゼロトラストの概念をユーザだけでなく、モノ(Things)やエージェント(Agents)に拡張。Duo (IAM)、Thousand Eyesと連携
- ISEからのタグ情報を利用してユーザー、モノ、エージェントに対して同じポリシーと制御を適用可能。

アジェンダ

- マーケットトレンドおよびシスコ戦略
- AI ready Datacenter
- Future Proofed Workplace
- Digital Resilience
- CX 戦略および対談内容の紹介

Digital Resilience





デジタルレジリエンスの重要性

“何が原因か” を特定することの難しさ

- 組織内で障害が発生した際、時間を浪費しがちなのが「何が原因か」の特定作業
- ネットワーク障害か、セキュリティ侵害か、APIの過負荷か、あるいはアプリケーションのバグか、複雑なシステム環境では復旧までのリスクが飛躍的に高まる

データの分散配置による課題

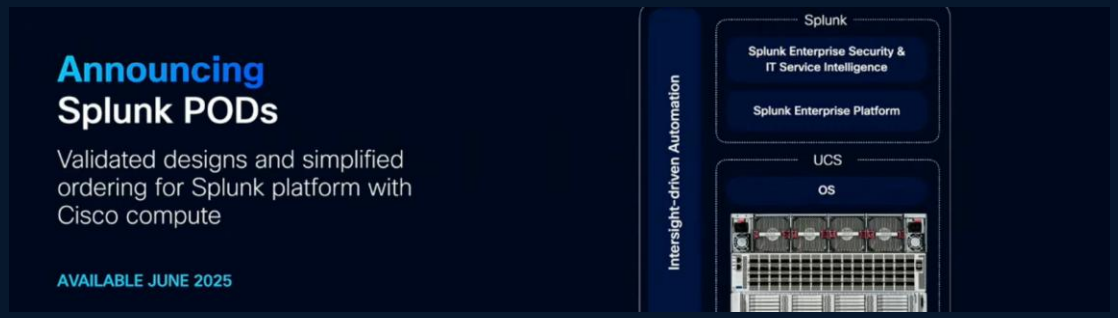
- これまで「データ」はデータセンターに集中していましたが、現在はエッジやクラウド、AIプラットフォームなどへ分散し、データ量も爆発的に増大
- データが分散先ごとにサイロ化すると、シグナル（本当に見るべき情報）をノイズ（不要なデータ）から抽出する難易度が急上昇

AIの適用（Unleash AI）

Splunk 連携により、ネットワーク / インフラ / アプリケーション / ユーザー / デバイス / IT運用 / セキュリティなど、多様なドメインのテレメトリデータを取り込み、シームレスに相関分析できる基盤を構築するため、以下３つのステップを実施

- Distill (データ精査)：膨大なログやテレメトリから、本質的なシグナルを抽出するために、前処理で不要ノイズを削ぎ落としつつ高精度なデータを残す。
- Correlate (分散データの相関分析)：データは元の場所（エッジやデータセンター、クラウド）に保持したまま、相関分析を実行できる仕組みを整備。データ移動の遅延や権限管理の煩雑さを最小化
- Unleash AI(AI適用によるインサイト創出)：相関後のデータに機械学習 / AIを適用し、異常検知や予測メンテナンス、攻撃パターンの自動識別など、運用効率と精度を一段と引き上げる

Digital Resilience



Splunk ObservabilityとCisco製品の統合

- Splunk Observabilityが、Thousand Eyesに加えてCatalyst、Merakiと統合(9月リリース予定)
- ネットワークデータやネットワークの状態を、ITサービスやビジネスの状態データと相関させることが可能

Cisco Firewall ログの無償化 New

- Ciscoファイアウォールからのログ取り込みを無料(8月リリース予定)
- 5GB/day までの取り込みが対象

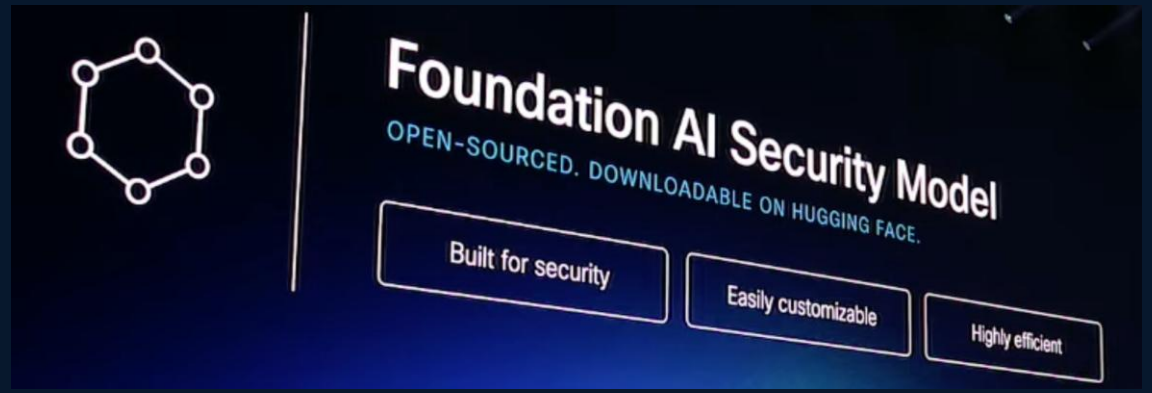
Splunk PODのリリース New

- オンプレミスでSplunkを利用する顧客向けに、Splunkプラットフォーム向けの検証済み設計とシンプルな発注を提供するSplunk Podを発表
- UCSサーバー上でのSplunk Podの検証済み設計として提供(6月リリース予定)

Observability for AI New

- 「Agentic AI」の利用が増えた際に必要となる、AIを動かしているGPUの利用状況やモデルの利用状況などを把握する機能 (8月リリース)

Digital Resilience



SOCの再構築

現状課題と SOC の再設計意義

- 悪意ある攻撃者は、マルウェア配布や認証情報悪用などをスクリプトやボットで自動化し、極めて短時間で大規模に攻撃を展開
- 従来のSOCでは、攻撃スピードに対して人手の処理能力は追いつかず、見落としや判断遅延が致命的リスクを生むため
- そこで「マシン×マシン」で高速に検出・相関・対応できるSOC再設計が不可欠

Splunk SIEM と XDR の融合

- 市場をリードしているSplunk SIEMと革命的なXDRを組み合わせた統合プラットフォームを提供

セキュリティモデル

Foundation AI Security Model

- Ciscoが開発したセキュリティ向けに目的別に構築されたオープンソースのAIモデル
- Hugging Faceで「foundation-sack」として公開され、40,000件以上のダウンロードの実績

アジェンダ

- マーケットトレンドおよびシスコ戦略
- AI ready Datacenter
- Future Proofed Workplace
- Digital Resilience
- CX 戦略および対談内容の紹介

Customer Experience (CX) 戦略

シスコの新たな CX 戦略を発表

お客様からが求められていることとこれまでの課題

- 従来からお客様がCiscoに求めてきた「レジリエンシー（高信頼性）」「シンプルさ」「導入から価値創出までの速さ」が、AI時代になり更に加速
- お客様からは「トラブル後の対応から予防保全・予測対応への転換」「導入からサポートに至るあらゆる局面でのハイパーパーソナライズ」「人による確認と信頼を確保しつつの高速な価値実現」といった要望
- 従来型のカスタマーサポートではこの複雑性とスピードに対応できず、「単に自動化ツールやAIを上乗せして人力で繋ぎ合わせても限界があった」

Agentic-Led CX

- 上記課題に対して必要となるのは Ciscoが提唱する「Agentic CX」、すなわちエージェント技術による新しい顧客体験
- 多くのIT運用管理者が、慢性的に生産性を奪ってきた問題群（例: 煩雑な設定ミス対応やチケット処理など）を根本的に変革可能
- Agentic CXによってCiscoは「リアクティブ（事後対応）」ではなく「インテリジェントな予測支援」へシフト
- Agenticシステムはデータ蓄積により時間とともに進化します。過去データ、リアルタイムのテレメトリ、インタラクションパターン、フィードバックループ等を継続分析し、人間では不可能な深さで各顧客環境を理解します 。その結果、お客様に合わせたパーソナライズや事前提案が可能となり、まるで「すべてのお客様が唯一の顧客であるかのよう」に感じていただくことがゴール
- また、すべてのカスタマーサービスおよびサポート対応のうち、68%は2028年までにエージェント型AIによって処理されると予想されています。

Kevin Weil氏 (Chief Product Officer, Open AI)との対談

Cisco 社外取締役に就任した Kevin Weil 氏と Jeetu 対談

AI最大の制約とComputeの重要性:
- OpenAIがStargateプロジェクトのような大規模投資（5000億ドル規模）を行っているのは、ComputeがAIの未来に不可欠だと考えており、多くのComputeがより強力なモデルを構築に貢献し、それによって多くの価値を個人やビジネスに提供できる。

ネットワークインフラとセキュリティの重要性:
- AIにはComputeだけでなく、超堅牢で高性能なネットワーキングインフラストラクチャと、あらゆる段階でのセキュリティが必要不可欠。
- OpenAIは、ユーザーが重要な情報を信頼して預けられるように、安全性とセキュリティを非常に重視しており、これら全てが組み合わさって初めて、人々が信頼し、ビジネスが依存できるアプリケーションが構築できる。

AI研究の役割とCodex:
- OpenAI Codex（コードエックス）は、自然言語（英語など）で指示するとコードを生成・修正・テストした上でプルリクエストの提案まで行う、クラウド実行型のソフトウェアエンジニアリング・エージェントであり、Ciscoは最初のデザインパートナー。
- これにより、製品マネージャーのような非エンジニアでもコードを書けるようになる可能性（少なくともプロトタイプレベル）があり、ソフトウェア開発が民主化されると考えている。

2025-2026年のAIの予測:
- AIが現在の質問応答から現実世界でのタスク実行へと進化し、ユーザーのデータに接続されたエージェントが多くの「忙しい仕事」を自動化すると予測している。これにより、人々はより高付加価値な活動や家族との時間に集中できるようになる未来が訪れると考えている。

まとめ：Ciscoの戦略の柱

AI-Ready Data Center

Future-Proof Workplace

Secure Global Connectivity

Digital Resilience

Accelerated by Cisco AI

Cisco Live US 2025

Networkingについての発表内容

未来を見据えたワークプレイス

渡部 周一
ネットワーキング事業
シスコシステムズ合同会社
2025年6月18日

AI時代において、組織をつなぎ、保護する

AI対応
データセンタ

未来を見据えた
ワークプレイス

安全なグローバル接続

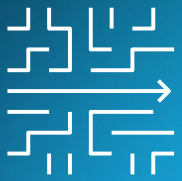
デジタルレジリエンス

Accelerated by Cisco AI

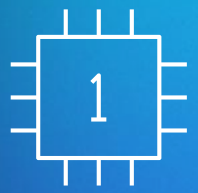
AIの時代に

AI 対応
セキュアネットワーク
アーキテクチャ

運用のシンプル化
powered by AI



拡張可能なデバイス
ready for AI



セキュリティ
fused into the network

cisco

運用のシンプル化
powered by AI

プラットフォーム統合による運用のシンプル化

Catalyst		Meraki
Catalyst Center	マネージメント	Meraki Dashboard
Catalyst License	ライセンス	Meraki License
Catalyst Hardware	Ciscoハードウェア	Meraki Hardware

シスコの統合されたプラットフォーム

プラットフォーム

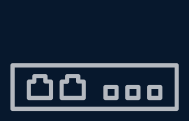
マネジメント

API | 統合

アシュアランス

インテリジェンス

ハードウェア



スマート
スイッチ

セキュア
ルータ

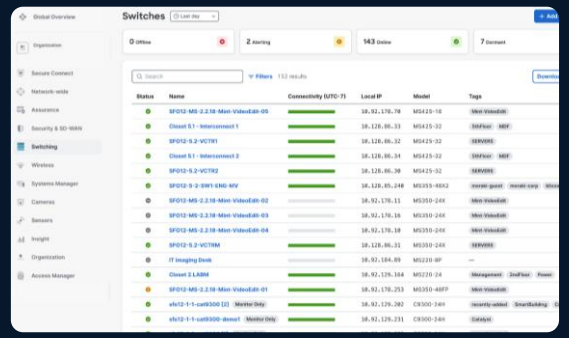
ワイヤレス

産業向け
IoT

cisco

統合プラットフォームの開発ステータス

統合された
マネジメント



CatalystとMerakiとの統合管理 –
クラウド・オンプレミス・ハイブリッド

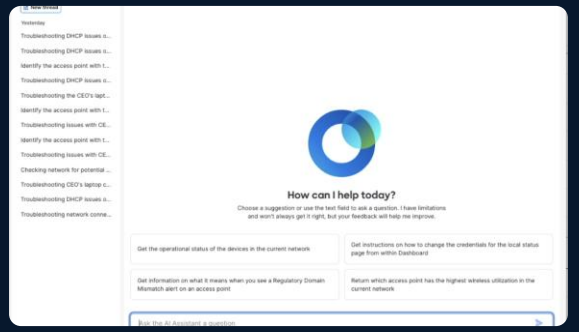
正式版 | 6月

マルチレイヤの
アシュアランス

企業ネットワーク、クラウド、
エンドポイントをより深く可視化 –
Splunkとの統合も可能

正式版 | 6月以降

AI
アシスタント



自然言語で質問・検索・アクション –
設定変更とスイッチ更改のための
自動化されたワークフロー

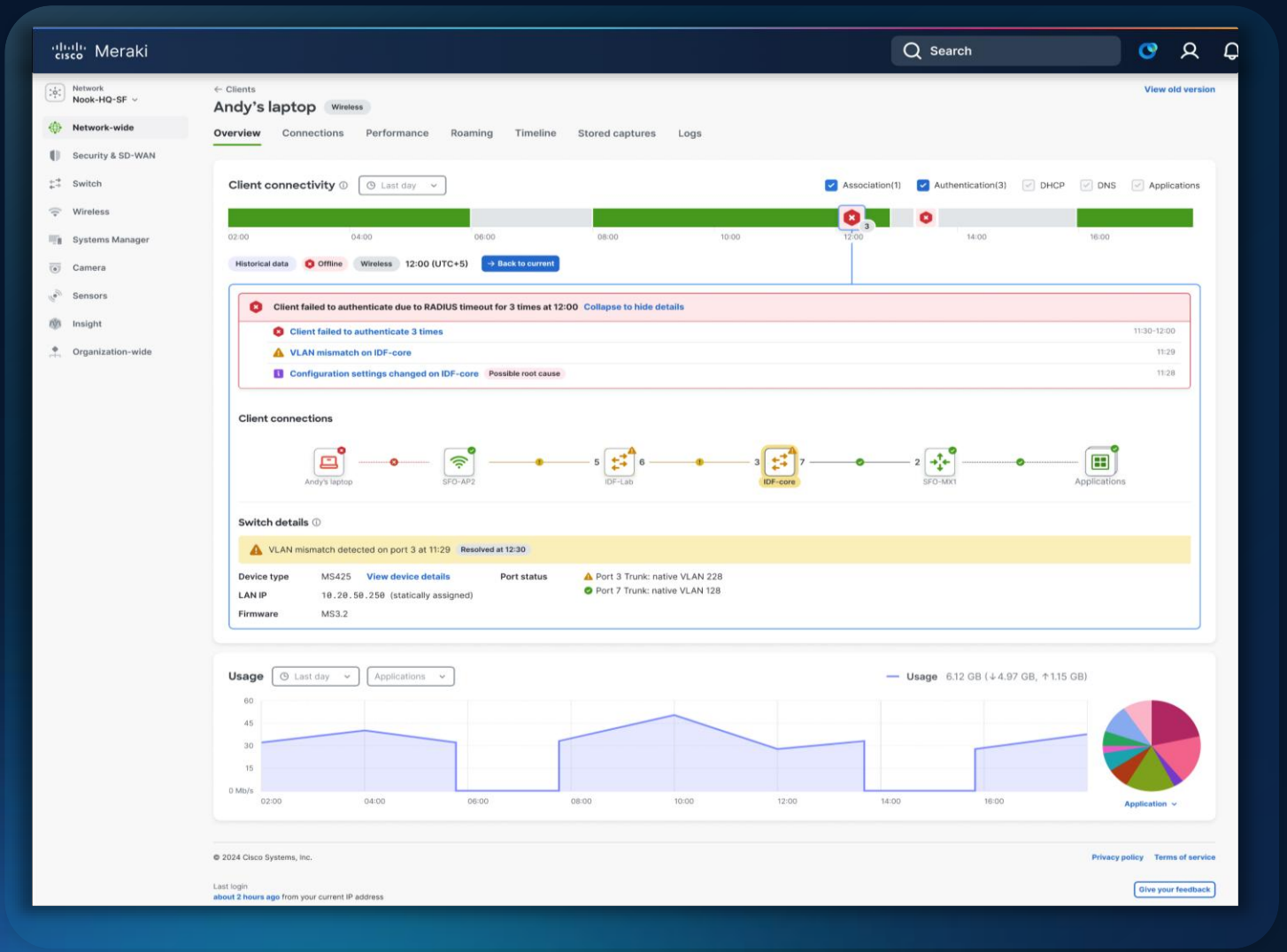
ベータ版 | 6月

AVAILABLE | NOW

マルチレイヤ アシュアランス

～ThousandsEyesの統合～

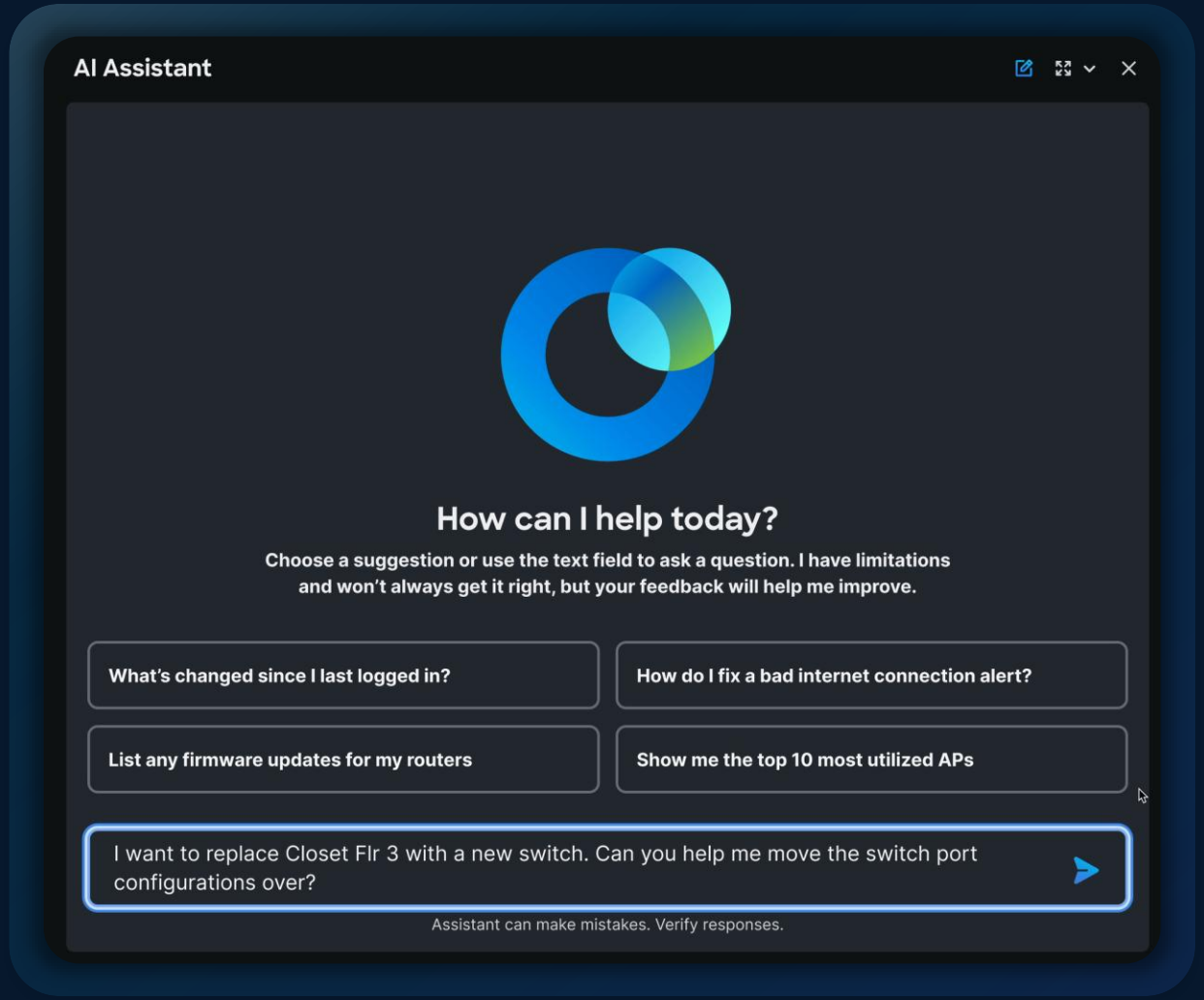
- 自社および外部ネットワークの両方に対する深い可視性
- AIがユーザーに影響を及ぼす問題を即座に検出・提示
- 問題を検知から修復まで自動で完結させるワークフロー
- AIにより、エンドツーエンドの原因分析がスピードアップ



BETA | JUNE

Introducing
AI Assistant

- 自然言葉で確認、検索、Actionする
- 設定変更・スイッチ移行のための新しい自動ワークフロー
- 新しい統合型アシュアランス機能

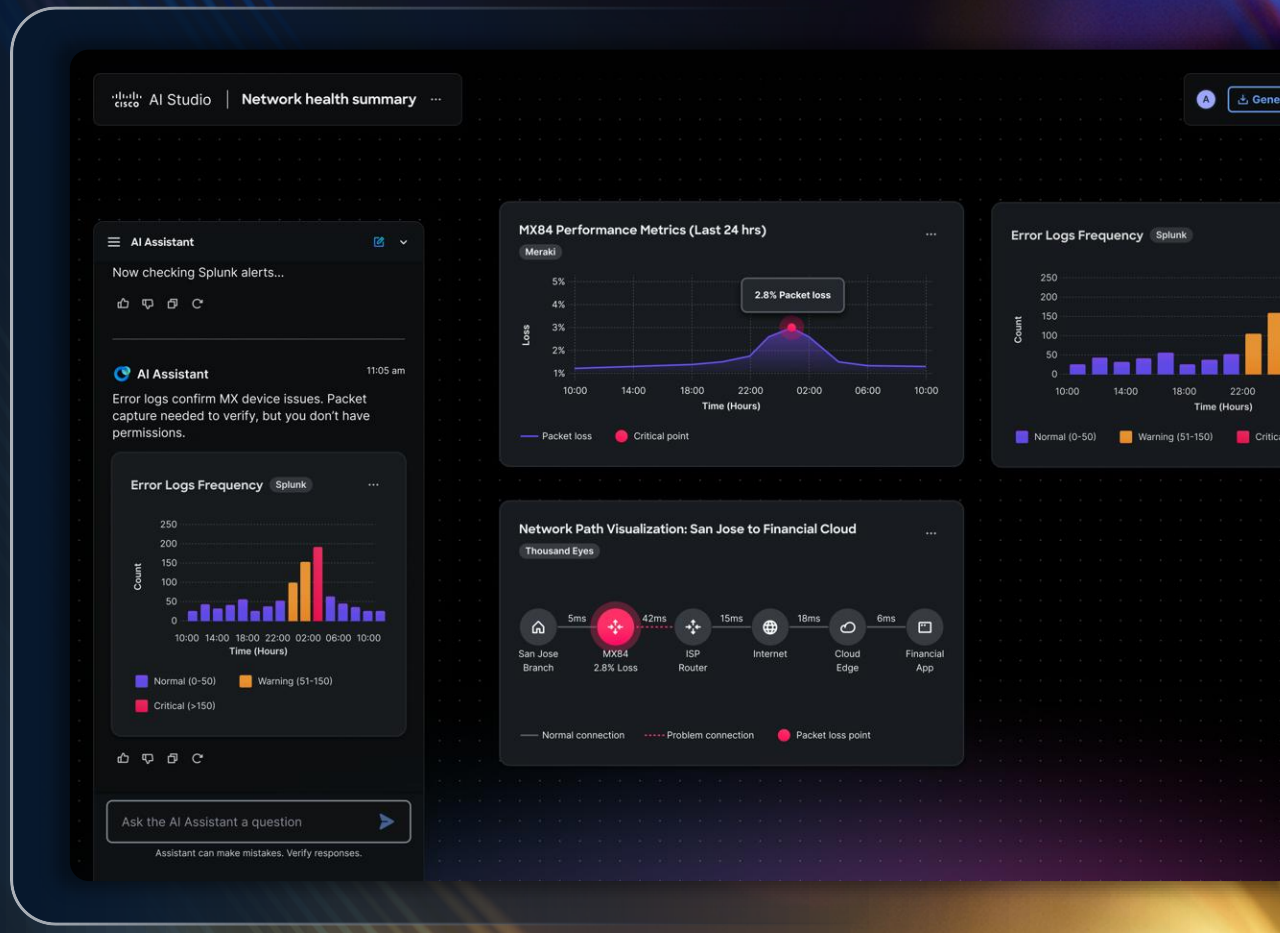


Introducing

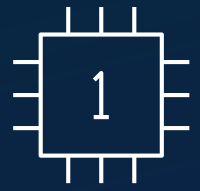
AI Canvas

一緒に確認して、
解決するための
一つのキャンバス

- 動的で文脈に沿う生成UI
- NetOps, SecOps, エグゼクティブのための共有ワークスペース
- AIアシスタンス機能の強化



拡張可能なデバイス
ready for AI



Smart Switches

Secure Routers

Campus Gateway

Large Venue Wi-Fi 7

Scale OT for AI

Introducing

新しいネットワークのための
新しいラインナップ

cisco

Introducing

Smart Switches for the AI-powered campus

高性能・低遅延

Cisco Silicon Oneと
セキュリティ・
AIのための
Co-Processor

ポスト量子
セキュア

インテリジェント
なエネルギー効率

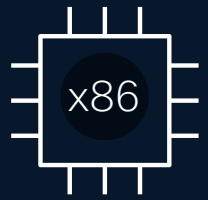
2025年7月

Cisco C9350 & C9610 Smart Switches

AI時代のためのハードウェア

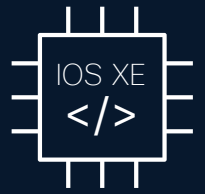
Silicon

- Massive packet bandwidth
- High forwarding performance
- Large forwarding info base
- P4 programmable for future protocols



System

- Integrated application hosting
- AI-driven visibility
- Programmable open ecosystem
- Power Efficient



OS

- Pervasive programmability
- Deep observability
- Highly scalable
- Near-zero downtime architecture

Sustainable

Smart Power, PoE Assurance and Energy dashboard

データセンタへの
トラフィック増加
に対応するための
スループット向上

セキュアな
SD-WANとSASE
のための高度な
ルーティングと
ファイアウォール

ポスト量子
セキュア

Introducing

Secure Routers for the AI-powered unified branch

2025年6月

Cisco C8000 Secure Routers

将来のAIワークロード向けに新たなハードウェアの実装

Secure Networking Processor

64-bit Multi-threaded Parallel Processing

Embedded Security Engine

Hardware Accelerated Dataplane

Greater IO

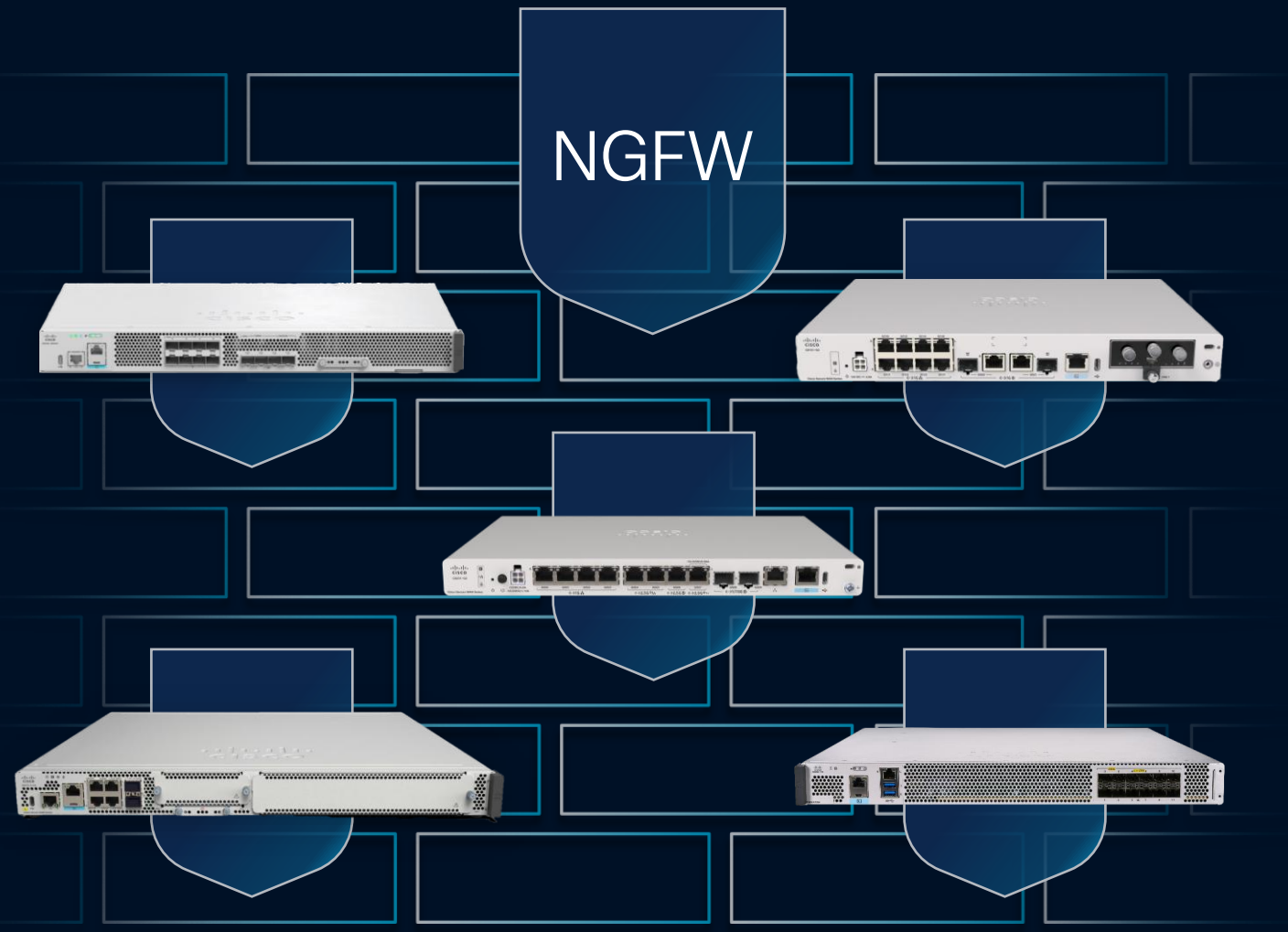
10GE Interfaces in Branch

25GE Interfaces for Campus

40GE/100GE Interfaces for DC

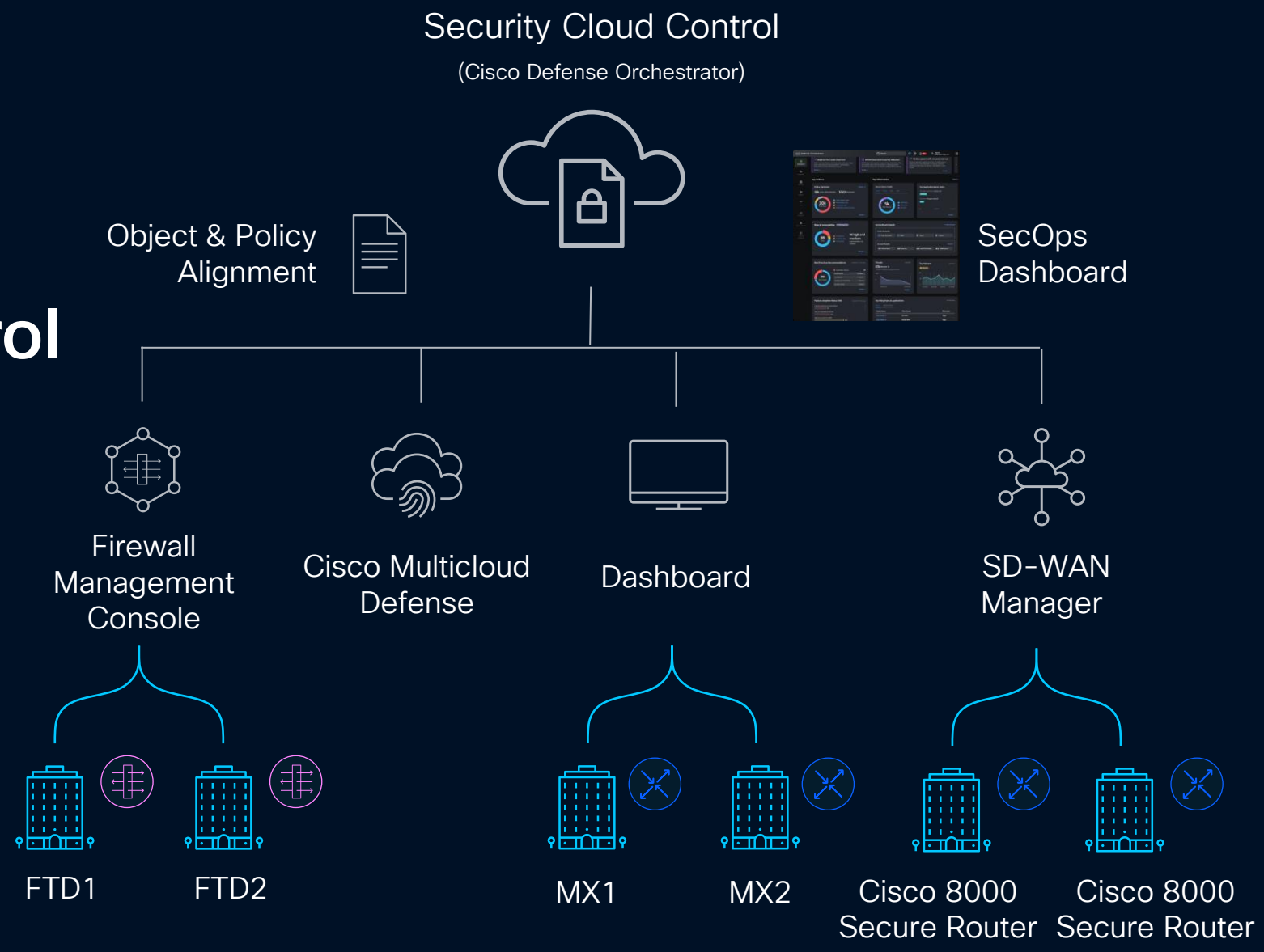
Advanced Security

- **Embedded NFGW stack** with native support in IOS-XE, backed by Talos
- **3x greater threat protection** throughput than previous generation Catalyst 8000
- Physical Security with **Tamper detection**



Security Cloud Control

SecOps管理者に、ポリシー最適化・脆弱性管理・ベストプラクティスの推奨を含む、包括的かつ集中管理型の管理機能を提供します。



それぞれの運用規模に対応可能なWi-Fi 7

CW9172

6 空間ストリーム

全方向性アンテナ

天井取付型と壁面取付型
ラインナップ

CW9176I

12 空間ストリーム

全方向性アンテナ

10Gbps, GPS, UWB

CW9176D1

12 空間ストリーム

指向性アンテナ

10Gbps, GPS, UWB

CW9178

16 空間ストリーム

全方向性アンテナ

2x 10Gbps, GPS, UWB

NEW

CW9179

16 空間ストリーム

ソフトウェア定義型ラジオ

2x 10Gbps, GPS

Wi-Fi 7 | グローバル展開可能なアクセスポイント | 統合ライセンス | 最適化されたAI

cisco

Introducing

The New Campus Gateway

5,000AP、50,000
クライアントまで
拡張可能

既存のLAN
コントローラ・
アーキテクチャ
への移行が容易

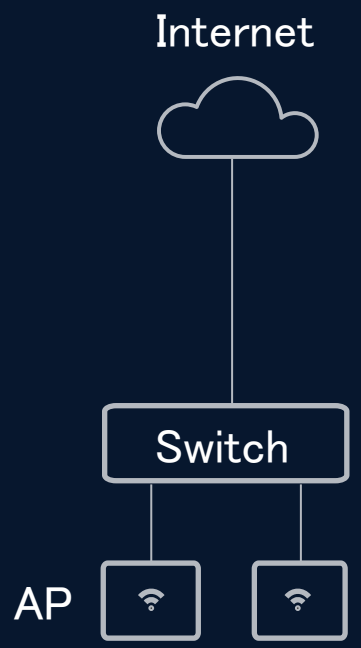
ケーブルの再敷設、
VLANの変更、
運用の中断が不要

2025年8月

Cisco Campus Gateway

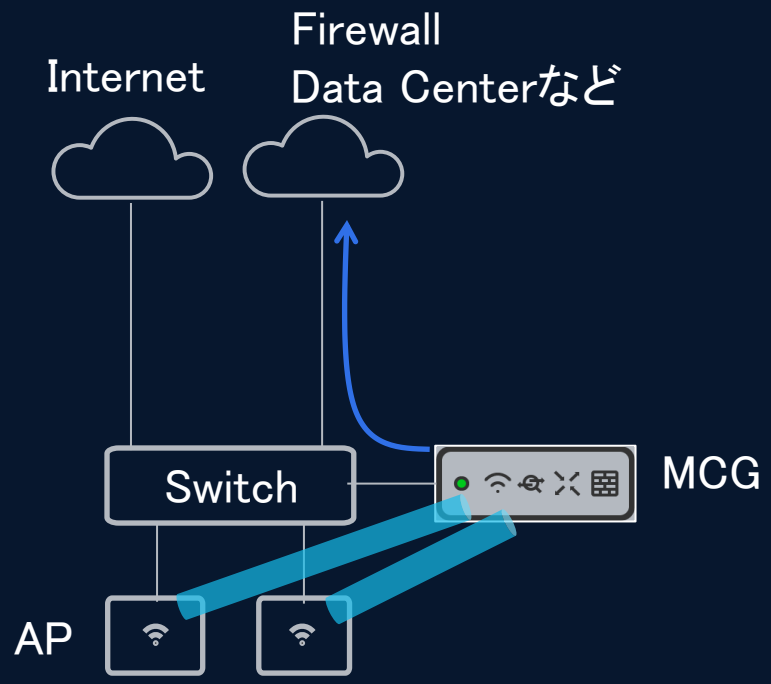
Campus Gateway(CG)

[今まで]



- スイッチの AP 接続ポートに Tagging 設定で運用に手間がかかる
- AP でローミングテーブル保持

[CG ある場合]



- AP と MCG でトンネルを張ることでスイッチのポート設定が Access VLAN となり運用が楽
- MCG でローミングテーブル保持することで、L3 ローミングが向上
- 特定の SSID のトラフィックを Firewall やデータセンター経由に変更が可能
- 最大5万台のクライアント端末および5,000台のアクセスポイントをサポート

[統一ハードウェア]

CW9800H1 ⟷ MCG

変換可能

R31.2 以上
対応 AP : Meraki Wi-Fi 6 AP以上,
共通 Wi-Fi 6E AP 以上 で
サポート予定

Introducing

Wi-Fi + Ultra-Reliable Wireless Backhaul

エンドユーザと
産業向けAIをつなぐ
単一のアクセス
ポイント

高度な耐障害性と
常時接続性

超低遅延と
高信頼性

2025年7月

Cisco IW9165 | Cisco IW9167

Introducing

All New Industrial Ethernet Portfolio

19のフォーム
ファクターに対応

54Gbpsの
スループット

スイッチあたり
720W

セキュリティが
組み込まれた
Cyber Vision

2025年7月

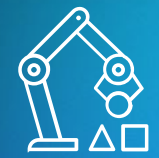
Cisco IE3100/H | Cisco IE3500/H | Cisco IE9300

セキュリティ
fused into the network

セキュリティ
fused into the network

Securing users, things, and agents

Securing network access



Securing network connectivity

Device Security

cisco

セキュリティ fused into the network

Securing users, things & agents

Common policy, distributed enforcement

- UZTNA
- SASE

Securing network access

Policy attached to every packet traversing the network

- Scalable segmentation
- Software-Defined Access
- Security Group Tags
- AI device classification
- Common policy
- Hypershield-ready

Securing network connectivity

Safeguarding and optimizing network connections

- Quantum-resistant encryption for data in transit:
  - MACsec
  - IPsec
  - WAN MACsec

Securing the device

Protecting and ensuring compliance of devices

- Quantum-resistant secure boot
- Compensating controls with Cisco Live Protect

cisco

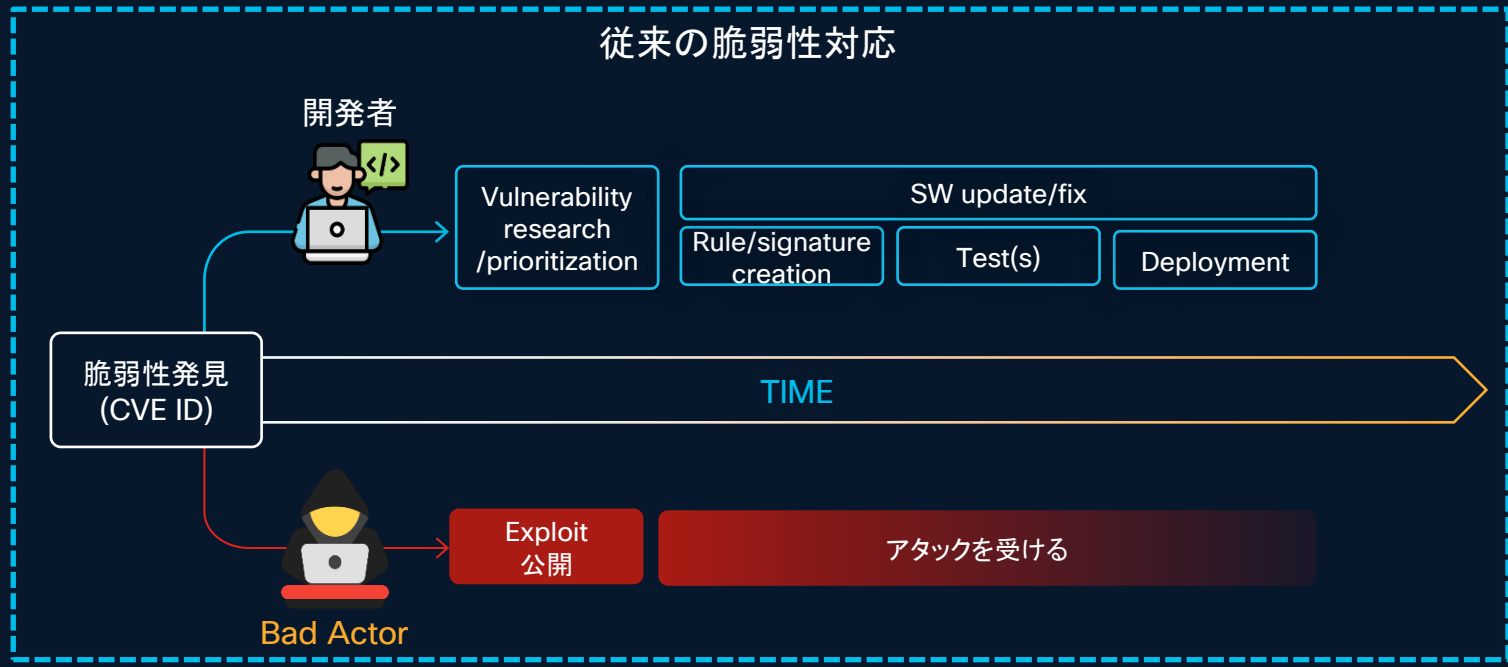
Device Security

Secure from hardware to software, from boot time to runtime

新たな脆弱性対応：Cisco Live Protect

*Roadmap

eBPF の力により、Tetragon はOSカーネルレベルの挙動を可視化し、セキュリティポリシーを即時に適用



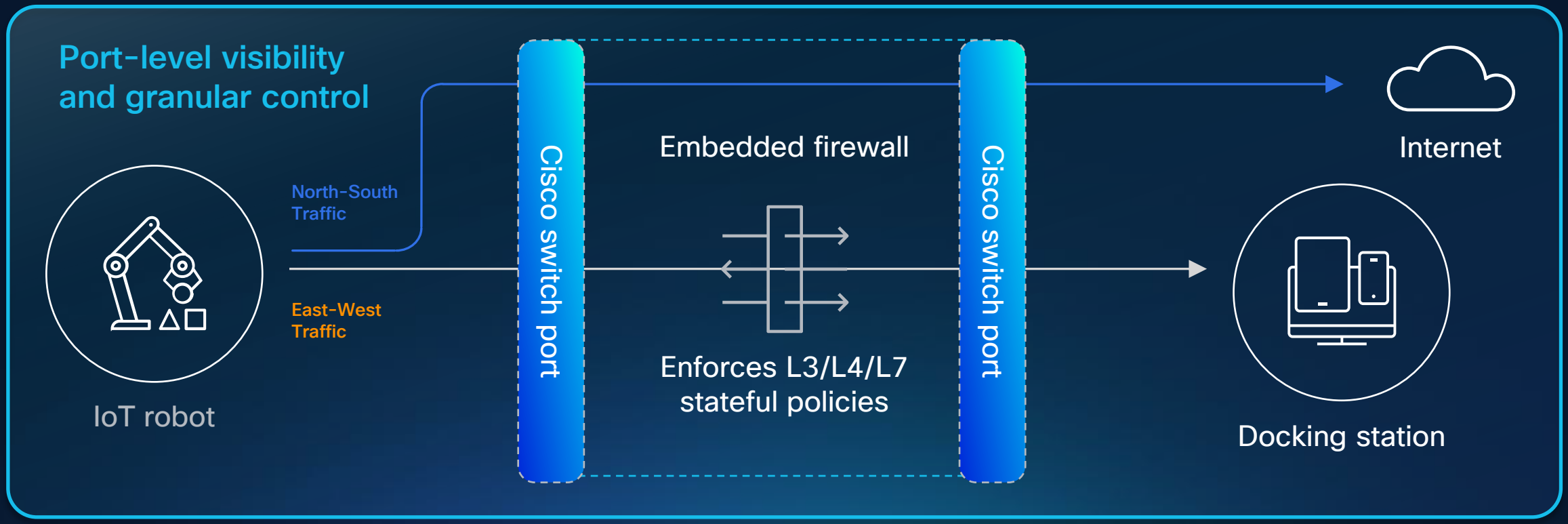
Compensating Controls

- 脆弱性を検出する自動スキャン
- 複数の補完的な対策と推奨が提供
- ソフトウェアの対策が開発される間、一部の攻撃から保護

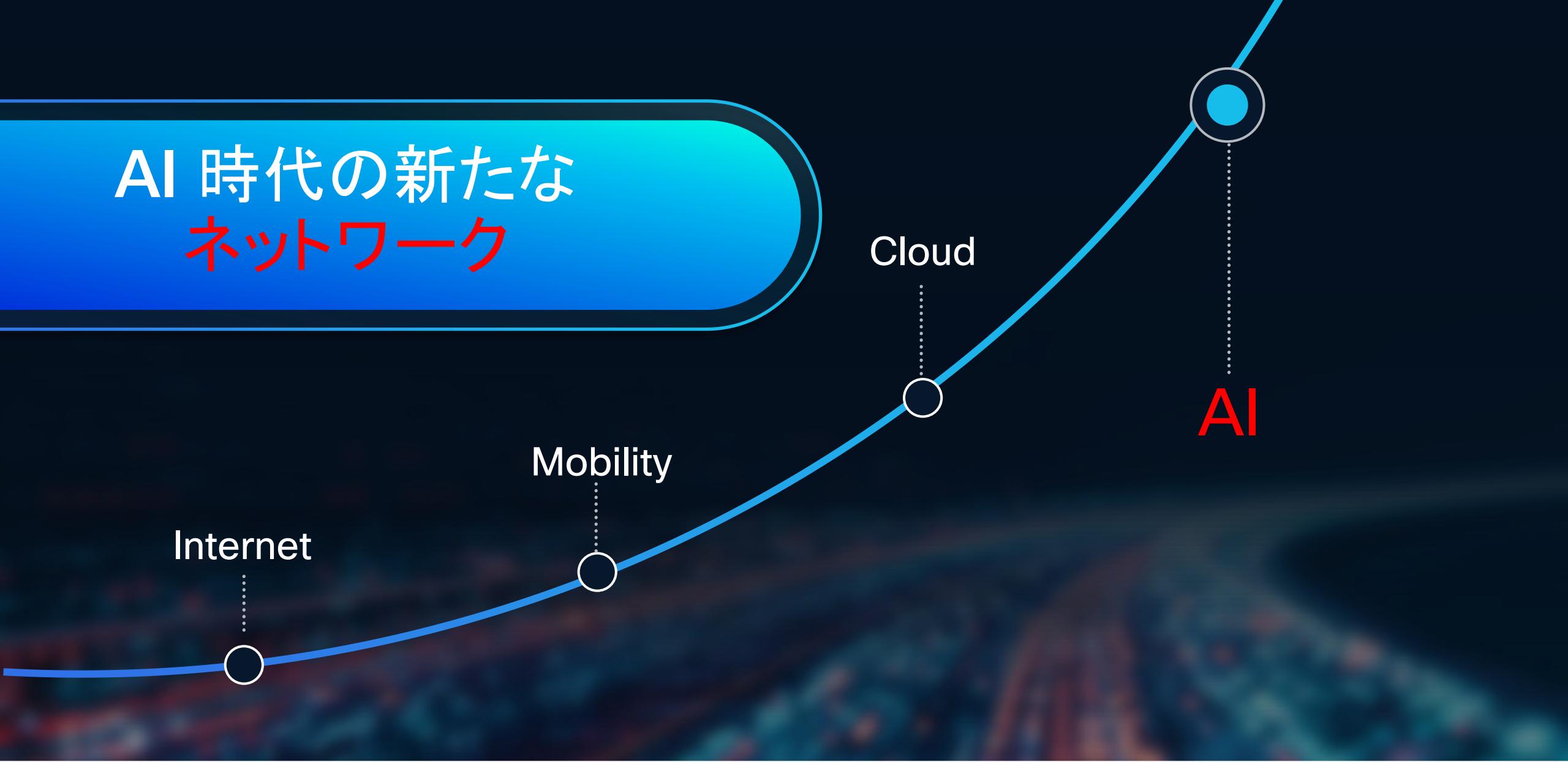
Securing network connectivity

Securing the network

Hypershield-ready: すべてのパケットに対してポリシーを



- すべてのスイッチポートがファイアウォール
- ポートレベルでのステートフルインスペクションと制御
- すべての経路でポリシーの適用を確実にする



1,000,000,000+ クライアント | 32,000,000+ デバイス

Cisco Live 2025 San Diego
AI-Ready Data Center

鈴木 康太

シスコシステムズ合同会社
クラウド・AIインフラストラクチャ事業
APJC Neocloud

2025年6月18日

Cisco powers how people and technology work together across the physical and digital worlds

AI-ready data centers

Transform data centers to power AI workloads anywhere

Future-proofed workplaces

Modernize everywhere people and technology work and serve customers

Secure global connectivity

Digital resilience

Keep the organization securely up and running in the face of any disruption

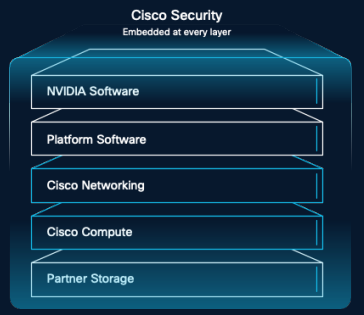
Accelerated by Cisco AI

AI Ready Data Center Announcements

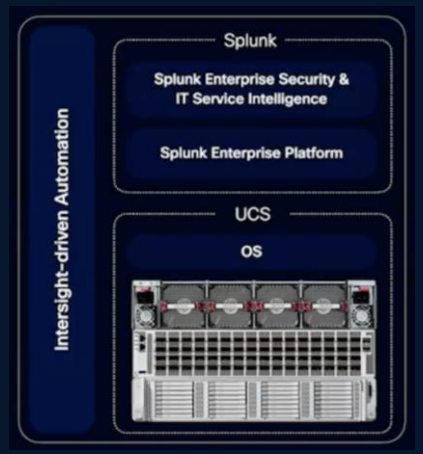
Cisco Live 2025 San Diegoでの主な発表

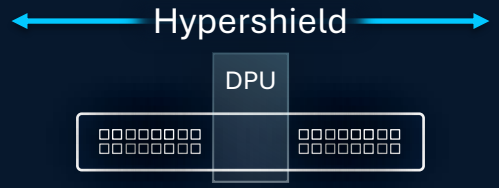
Unified Nexus Dashboard

Cisco Secure AI Factory with NVIDIA



Cross Architecture

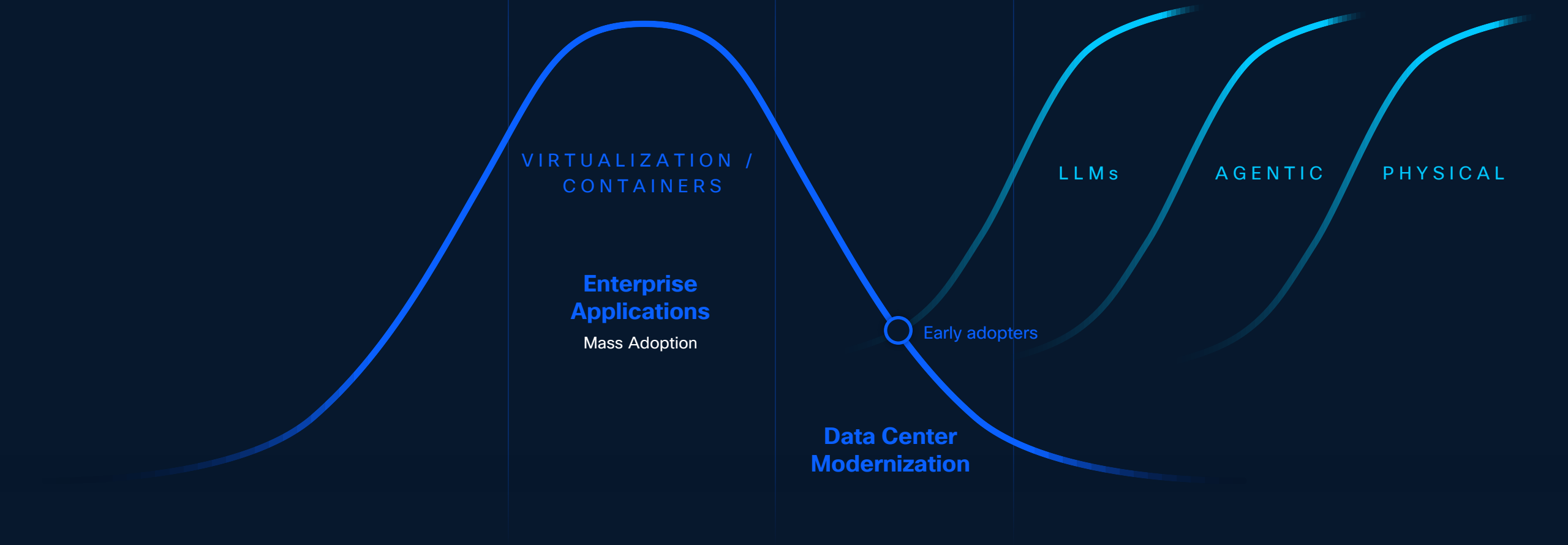




Architected for Sustainability

What we know

AI is no longer optional. The shift is inevitable.



Data Center

2010

AI-Ready Data Center

2025

AI Data Center

2030

Unified Nexus Dashboard

Announcing
Unified Nexus Dashboard

One console and common policy across NX-OS and ACI fabrics

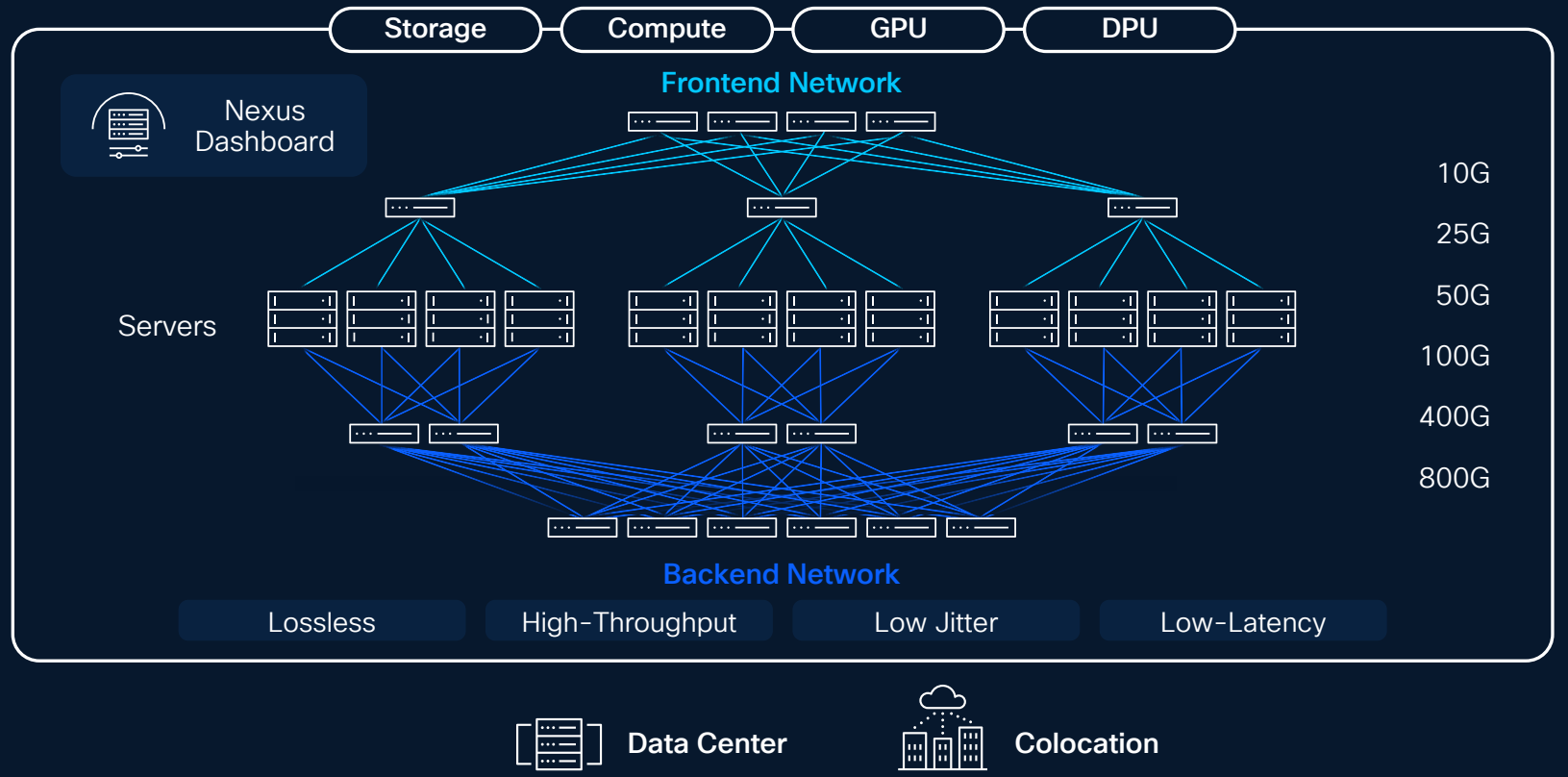
AVAILABLE JULY 2025

Unified Architecture

Powering AI Fabrics

Optimized AI/ML Fabrics with Nexus

Silicon, Systems, Software, Operations



OUTCOMES

Best performing
AI/ML networks, front-end and back-end

Managed by Nexus Dashboard
AI fabric templates, AI analytics, telemetry, congestion scores

Cisco Intelligent Packet Flow
Advanced Load Balancing features

Intelligent buffering, low latency, RoCEv2

Lower TCO

Validated designs for network and ecosystem partners

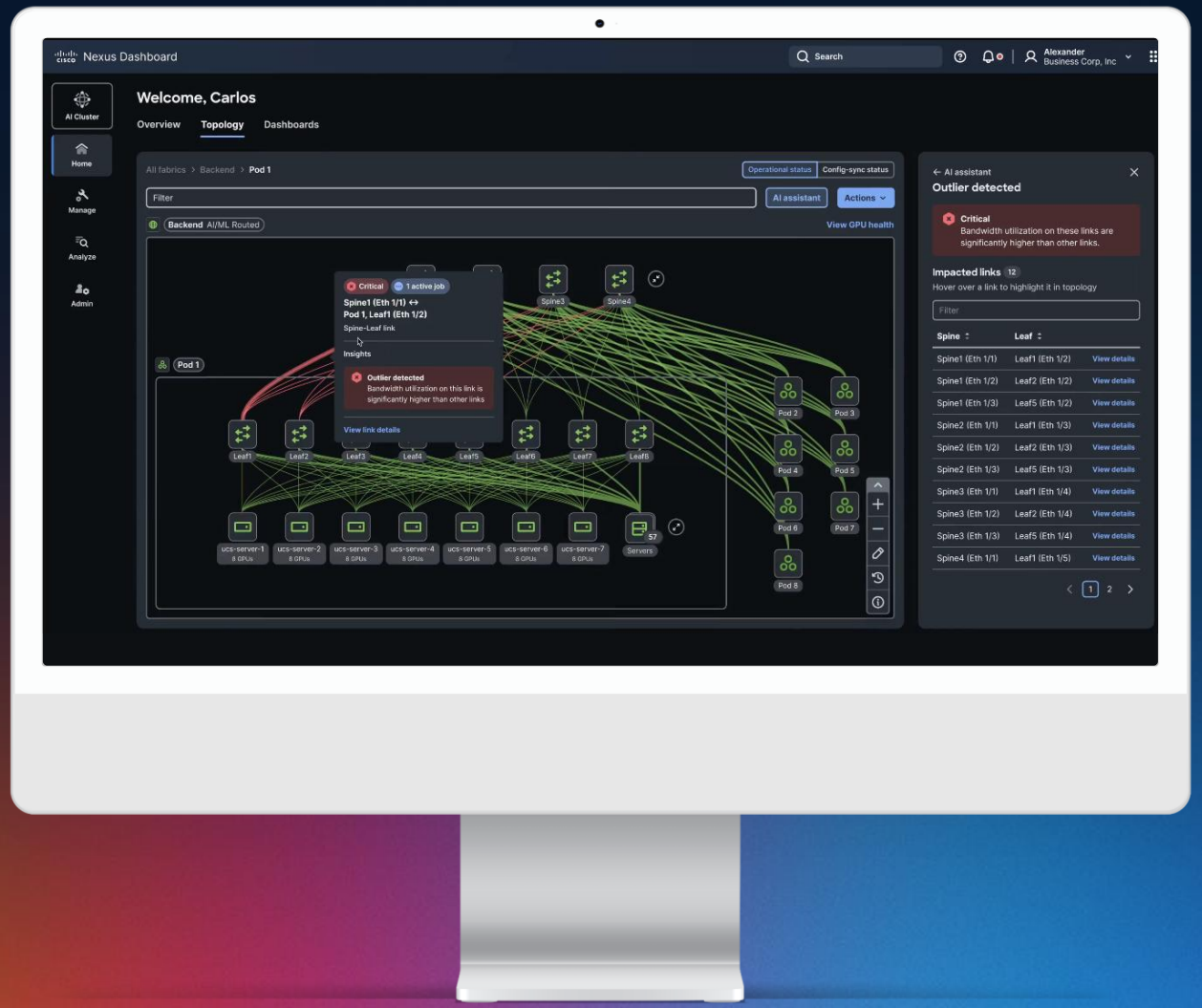
AI Job Observability

End-to-end visibility

Monitor AI workloads across the entire stack. Track network, NICs, GPUs, and distributed compute nodes.

Topology-aware visualization

Correlate network elements with hardware components. See connections between infrastructure and AI job health.



Real-time metrics

Track throughput, latency, and GPU utilization.
Get actionable insights into distributed AI workloads.

Proactive troubleshooting

Detect anomalies against historical baselines. Accelerate root-cause analysis with automated recommendations.

Cisco Secure AI Factory with NVIDIA

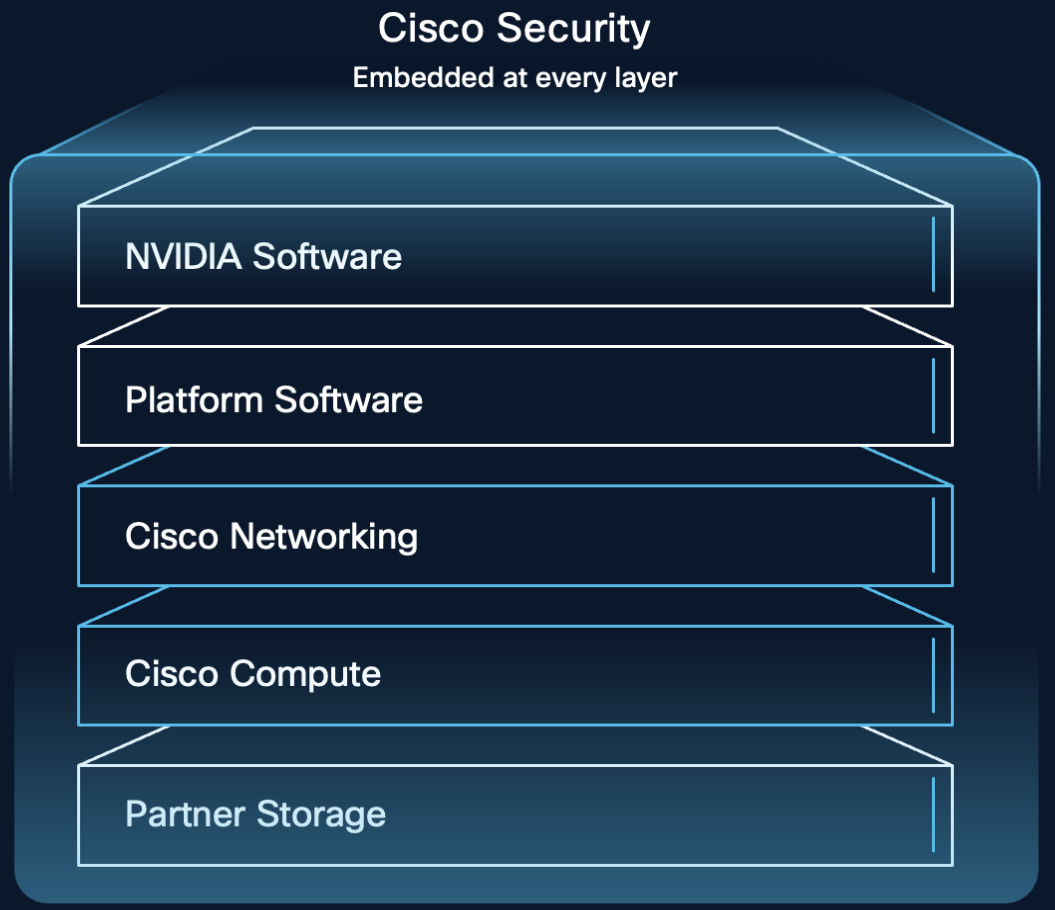
Unified Solutions

Cisco Secure AI Factory with NVIDIA

A reference design with validated architectures to **accelerate AI adoption**

Hyperfabric AI

AI PODs



Introducing

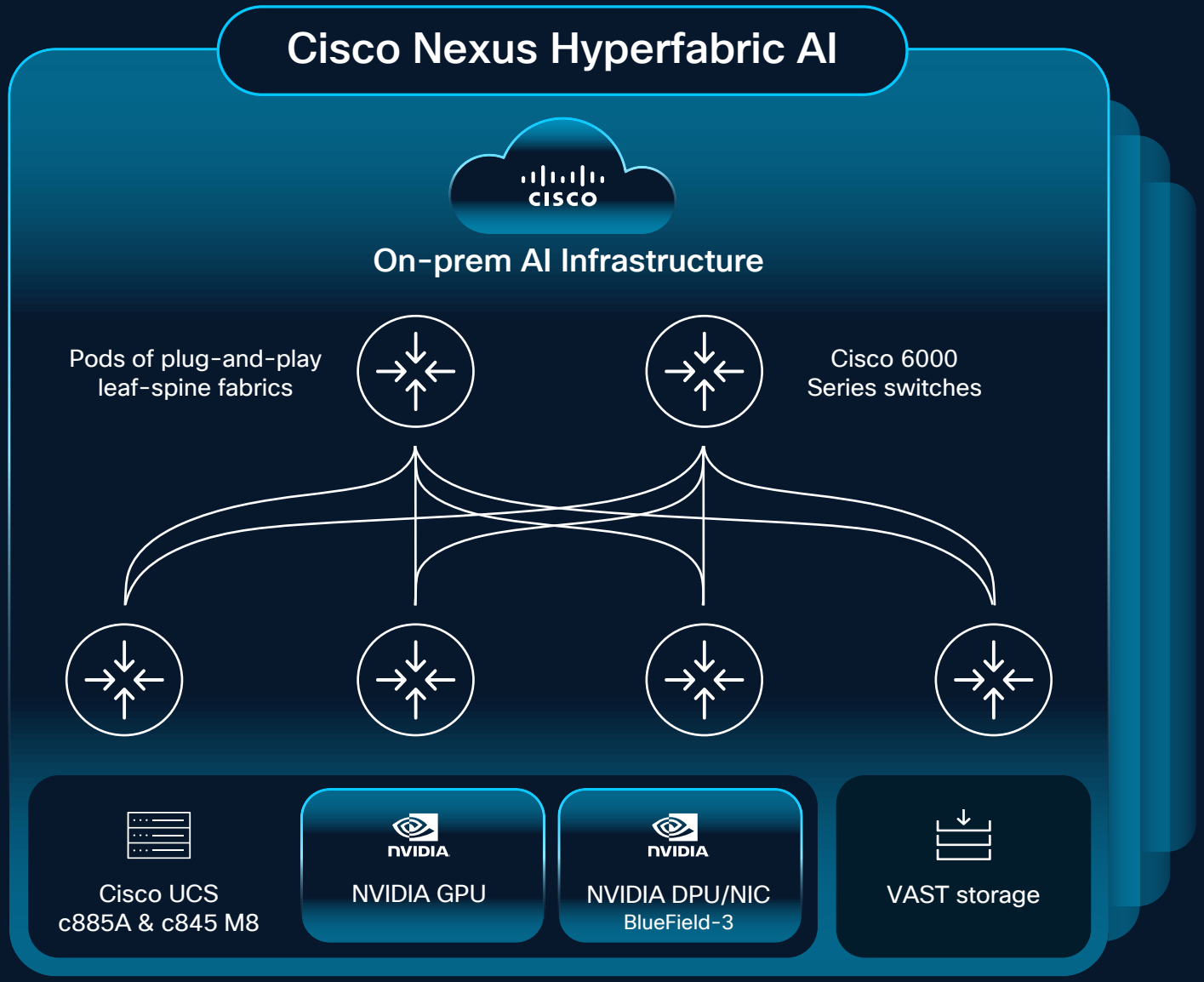
AI PODs for your entire AI lifecycle

A scalable architecture, built to support any AI workload

Orderable 2H CY25

Cisco Nexus Hyperfabric AI

- High-performance Ethernet
- Cloud-managed operations
- Unified stack, including NVAIE
- AI-native operational model
- Democratise AI infrastructure
- Visibility into full-stack AI



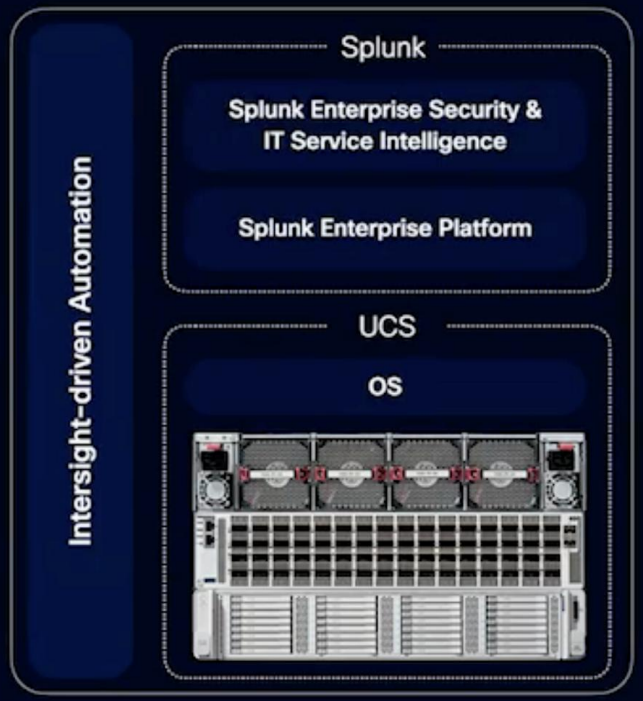
cisco

Splunk PODs

Announcing
Splunk PODs

Validated designs and simplified ordering for Splunk platform with Cisco compute

AVAILABLE JUNE 2025



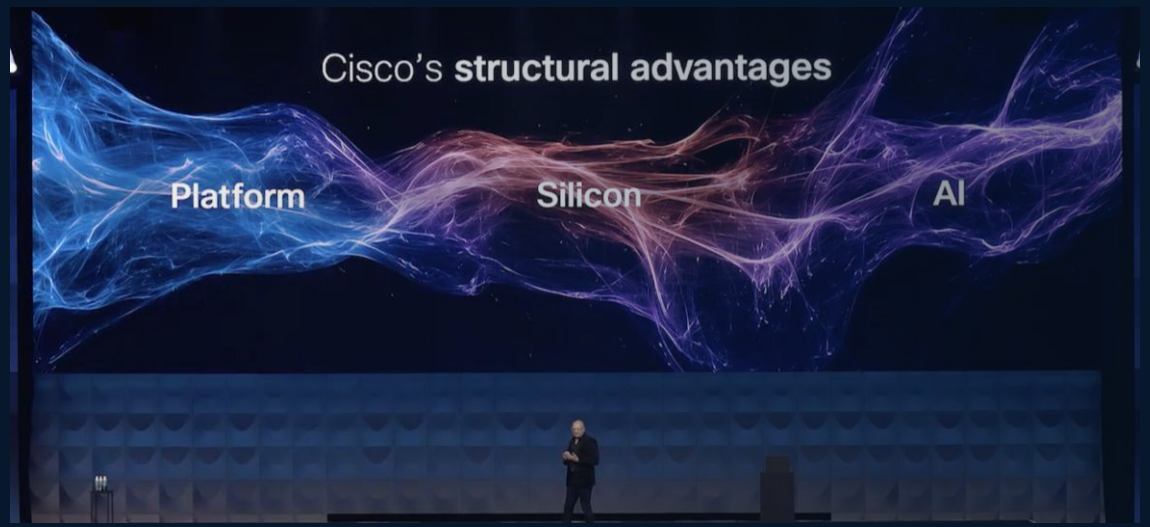
Cisco Live US 2025
Security に関する発表概要

Cisco Security

2025年6月18日

中河 靖吉（ynakagaw@cisco.com）
セキュリティ事業
シスコシステムズ合同会社

Cisco Live US 2025での主なメッセージ



AI時代の到来とその影響

- 現在のテクノロジー業界はAIによって根本的な変革期を迎えている
- 特に、単なるチャットボットから自律的にタスクを実行する「Agentic AI」への移行が、働き方やビジネスプロセスを大きく変えるという認識を共有

AIを支えるネットワークの重要性

”「The Network Foundational for AI」（ネットワークはAIの基盤である）“

- AI、特に高度なAgentic AIのワークロードには、高性能なネットワークインフラが不可欠
- 高帯域幅、低遅延、そして電力効率の高いデータセンターネットワークの必要性

AI時代におけるセキュリティの重要性と組み込み

“There is no Secure AI without Cisco」（シスコなくしてセキュアなAIはない）”

- AIの導入には、ネットワーク基盤に組み込まれた堅牢なセキュリティが不可欠
- AIが悪意のある攻撃に利用される可能性にも触れ、セキュリティがAI採用の前提条件

運用簡素化とAgenticOps

- IT運用の複雑性を解消し、効率を高めるためのAI活用
- 人間とAIエージェントが協調してネットワーク運用を行う「AgenticOps」の概念を紹介
- AIによる運用自動化や管理の統合（例: MerakiとCatalystの統合管理）がその実現に向けた取り組みとして紹介

AI時代に向けた3つの戦略的柱

- AI-Ready Data Centers（AI対応データセンター）
- Future-Proof Workplaces（将来を見据えたワークプレイス）
- Digital Resilience（デジタルレジリエンス）

Ciscoの戦略の柱

AI-Ready Data Center

Future-Proof Workplace

Secure Global Connectivity

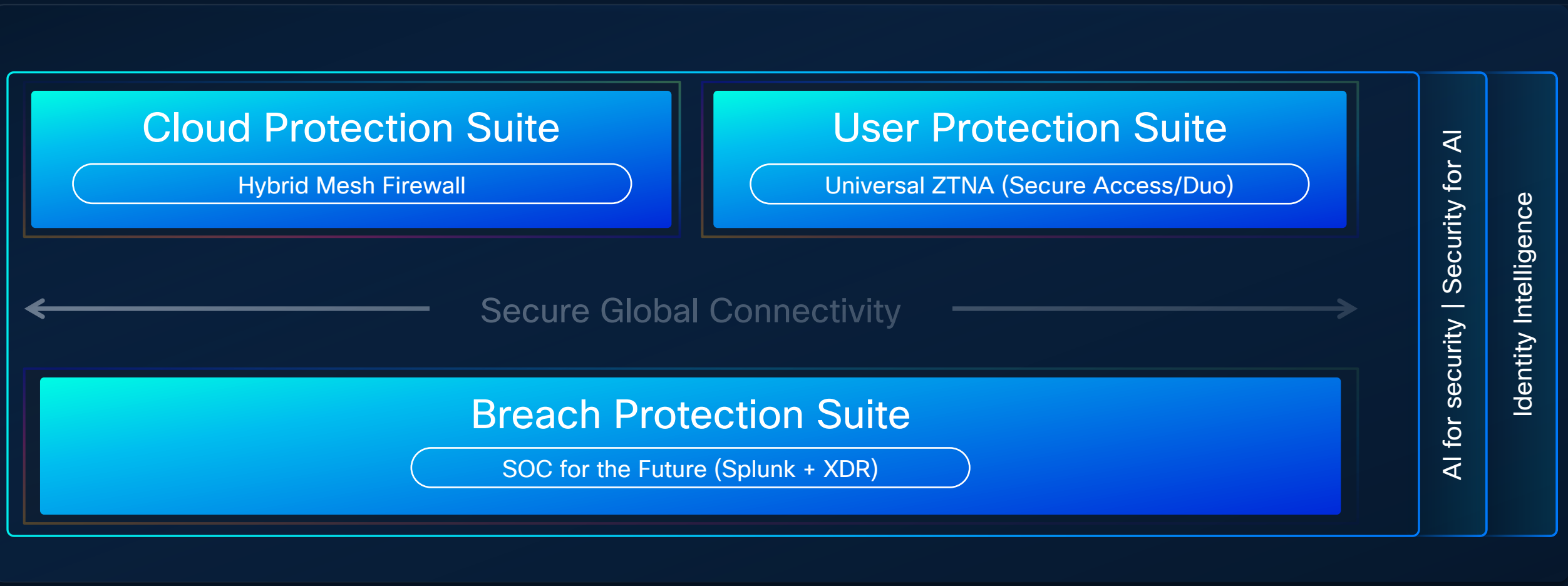
Digital Resilience

Accelerated by Cisco AI

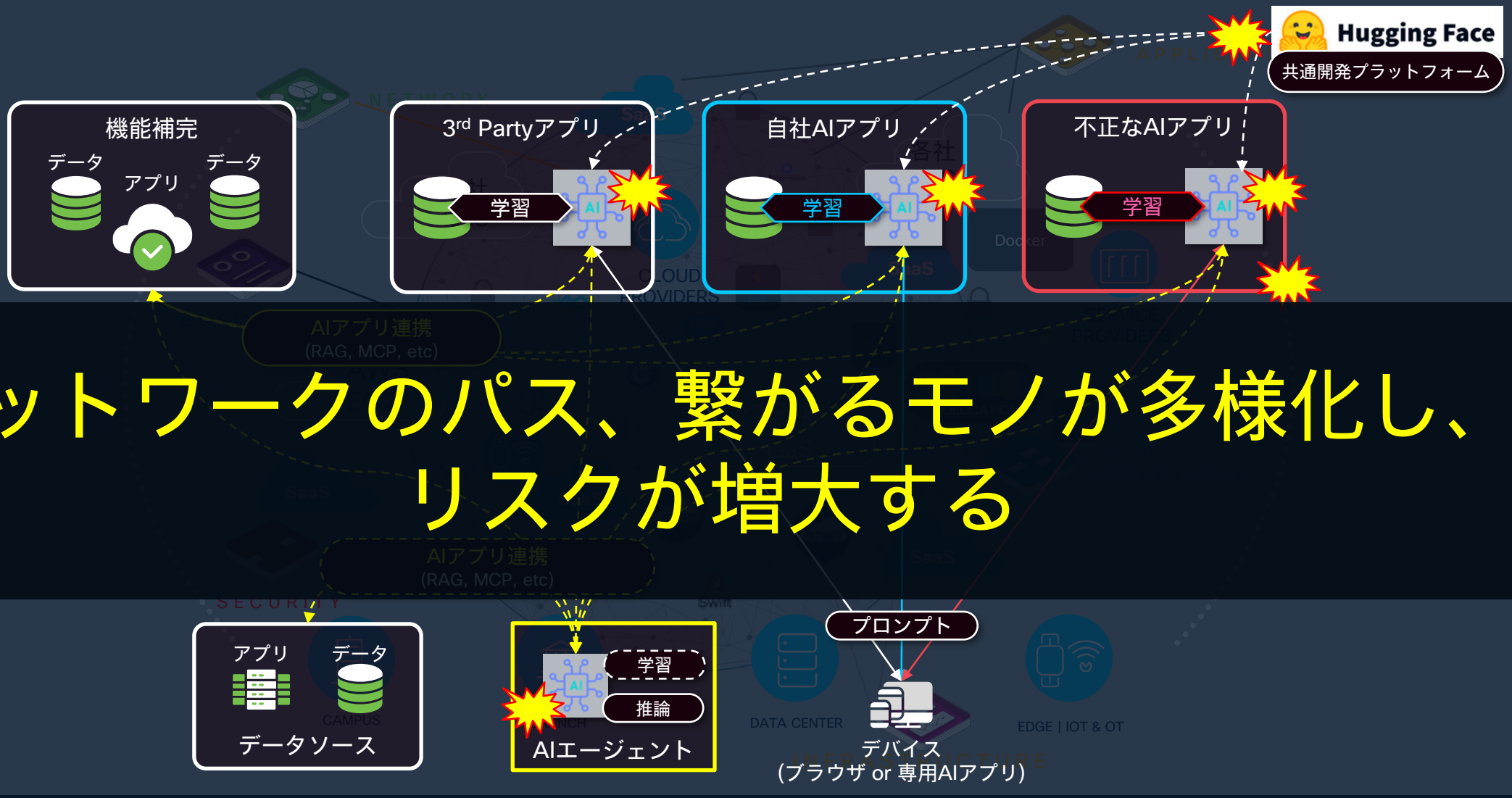
物理的な世界とデジタルの世界を超えて、
人とテクノロジーが共に働く方法を提供する

Cisco の戦略と Security のアプローチ

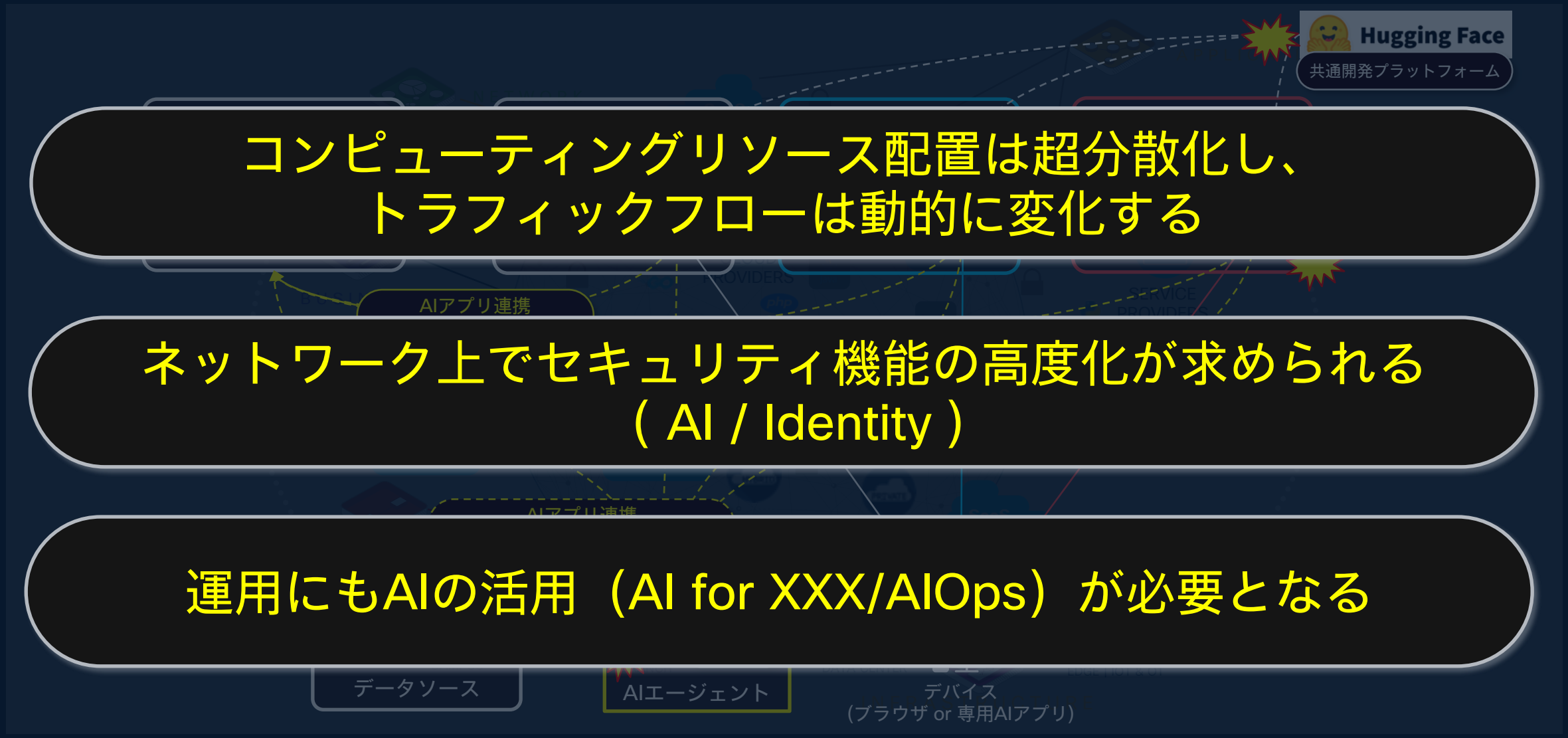
Security Suite



AIアプリケーションがあらゆる場所で利用される世界



現在～AI拡大に伴いインフラセキュリティに起きる変化

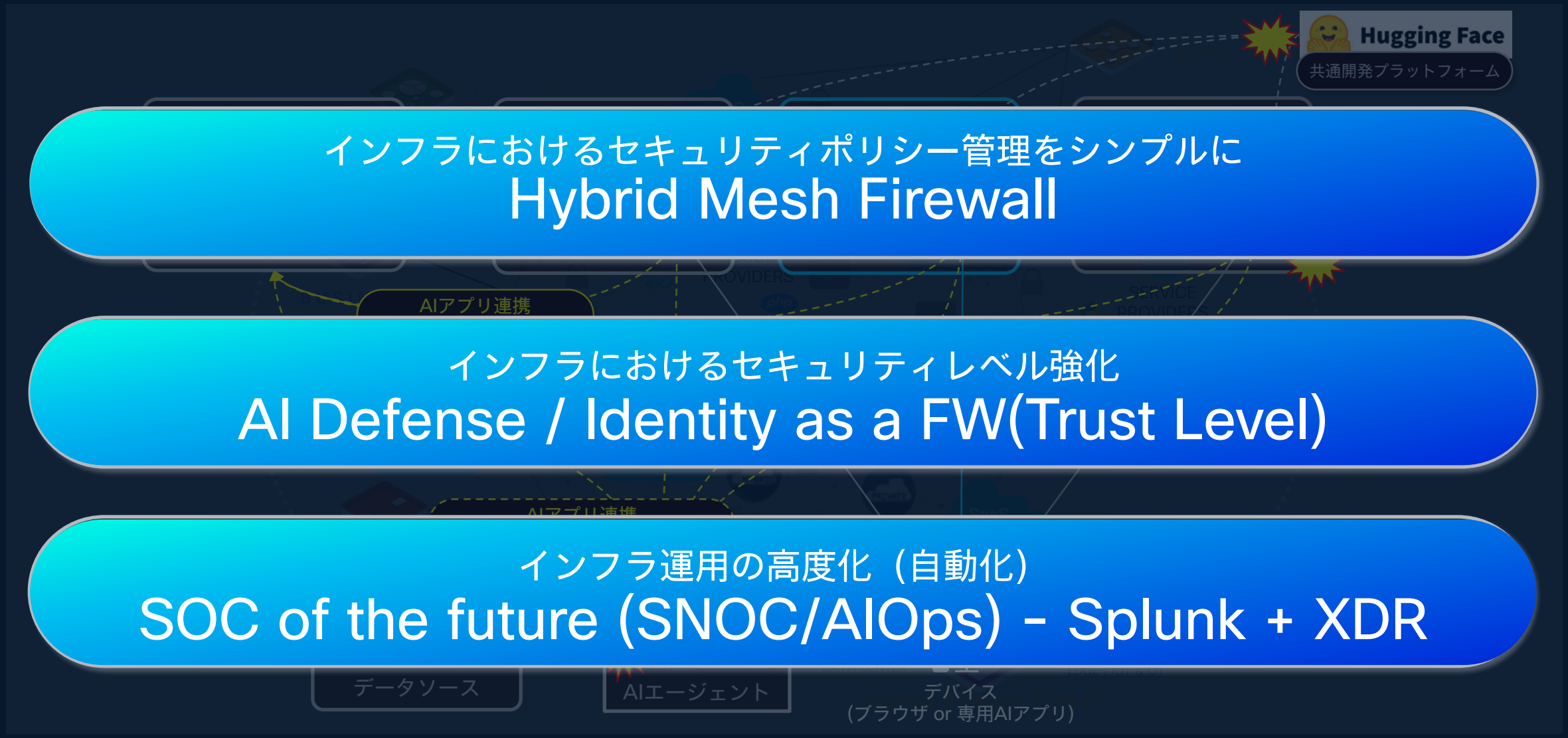


コンピューティングリソース配置は超分散化し、
トラフィックフローは動的に変化する

ネットワーク上でセキュリティ機能の高度化が求められる
（ AI / Identity ）

運用にもAIの活用（AI for XXX/AIOps）が必要となる

Ciscoのアプローチ



Cisco Live US 2025でのセキュリティ製品に関する主な発表

Hybrid Mesh Firewall の進化

Write policy once, enforce across the mesh

Hybrid Mesh Firewallの実現に向けて
対応製品と機能を拡張

Security Cloud Control対応製品の拡張

- Cisco Secure Router
- 3rd Party Firewall

ポリシー管理ポイントの拡張

- Cisco Smart Switchとの連携
  (w/Hypershield)
- ACI(APIC) とSecure Workloadの連携

Cisco Secure Firewall のラインナップ拡大

*AVAILABLE OCT 2025

Cisco Secure Firewall 6100シリーズ

- 2Uで400 Gbps
- 最大16台のクラスタリング
  -> 4 Tbps以上のパフォーマンス

*AVAILABLE DEC 2025

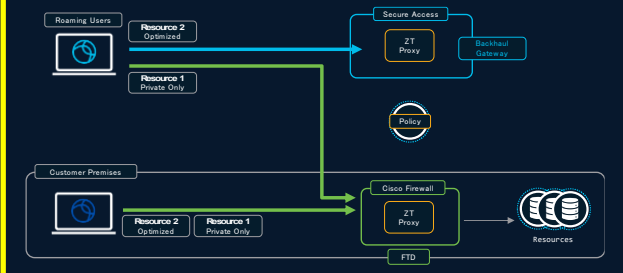
Cisco Secure Firewall 200シリーズ

- 1.5Gbpsの暗号化通信の処理性能
- 市場平均の約3倍の価格性能比

Live Protect

- ネットワーク機器の脆弱性発見から
  パッチ適用までの期間にネットワーク
  機器を保護する仕組み
- eBPFを利用し、ネットワーク機器の
  OSを保護
- 2026年10月から NX-OS(Nexus)に
  対応予定

Secure Access と Duo の機能拡張



Universal ZTNA

- Cisco Secure Firewall(FTD)との連携強化
  し、プライベートアプリケーションへの
  アクセスのポリシー管理をシンプルに
- リモート、イントラからのアクセス経路に
  関わらず１つのポリシー設定で対応

User Trust Level

- Duo/CII(ITDR)との連携により、リモート
  アクセスユーザーを評価し、可視化
- なりすましなどの不正なアクセスを
  検知し、動的にアクセスを制御可能に

Cisco Hybrid Mesh Firewall

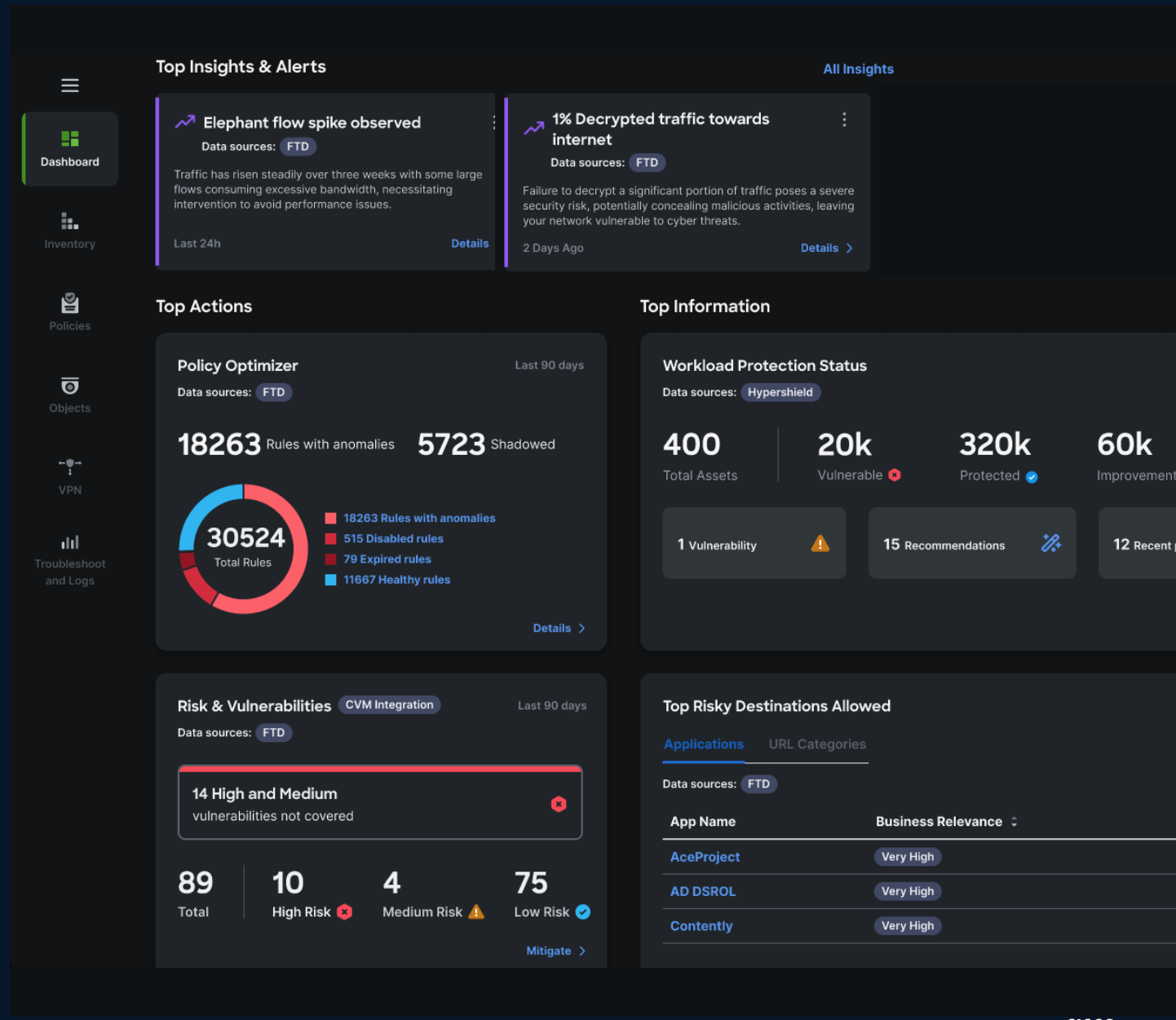
Write policy once, enforce across the mesh

新しいクラウド型統合管理

Security Cloud Control

- Cisco Security Cloud 全体を設定、管理、監視
- 各種AI Assistant機能を搭載
- ルール、ポリシー、設定の最適化、重複や設定ミスの検出、エレファントフローのような異常をAIにより検出
- サポート対象製品
  2025年6月時点
  - Secure Firewall Threat Defense / ASA
  - Multicloud Defense
  - Secure Workload
  - Hypershield
  - Secure Access
  - AI Defense

  今回の発表対象
  - Smart Switch
  - 3rd Party Firewall
  - Secure Router
  - ACI *Secure Workload連携による



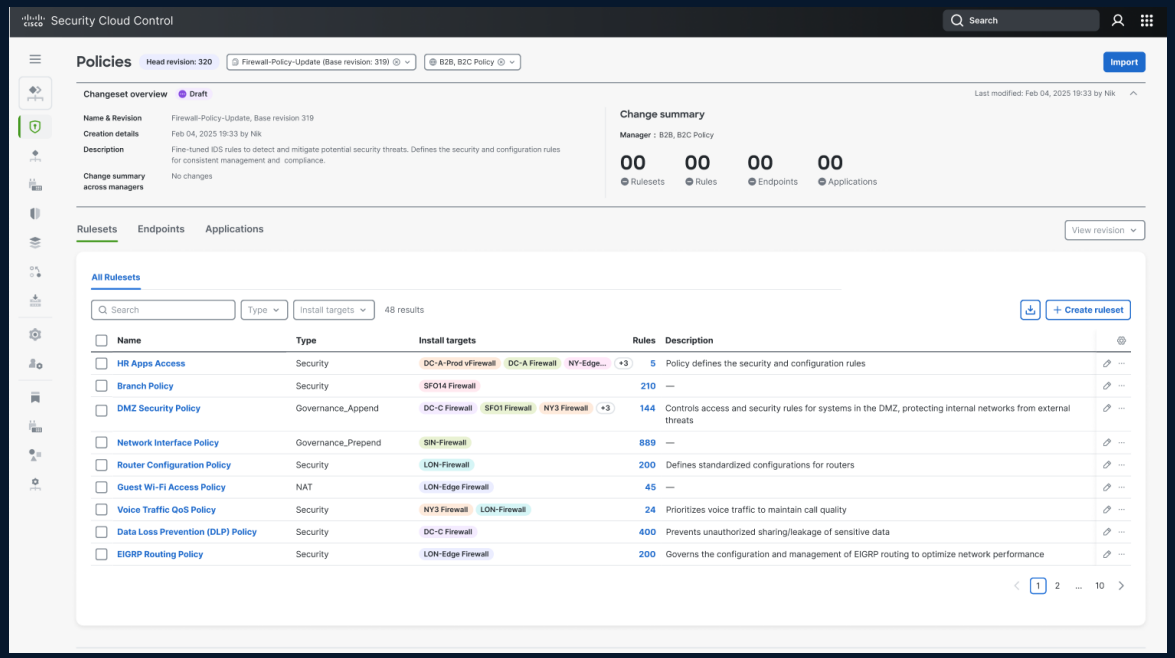
NEW

Cisco Security Cloud Control

3rd Party Firewallのポリシー制御をサポート

Mesh Policy Engine
in Security Cloud Control

- **SCCでポリシーを一度定義**
  シスコおよびサードパーティ製ファイアウォールへの展開
- **迅速なポリシー展開**
  数分でネットワーク・トポロジー全体にポリシーを展開
- **ルールとオブジェクトを自動的に最適化**
  Mesh Policy Engineでのポリシー変更を展開



*Limited availability in August 2025

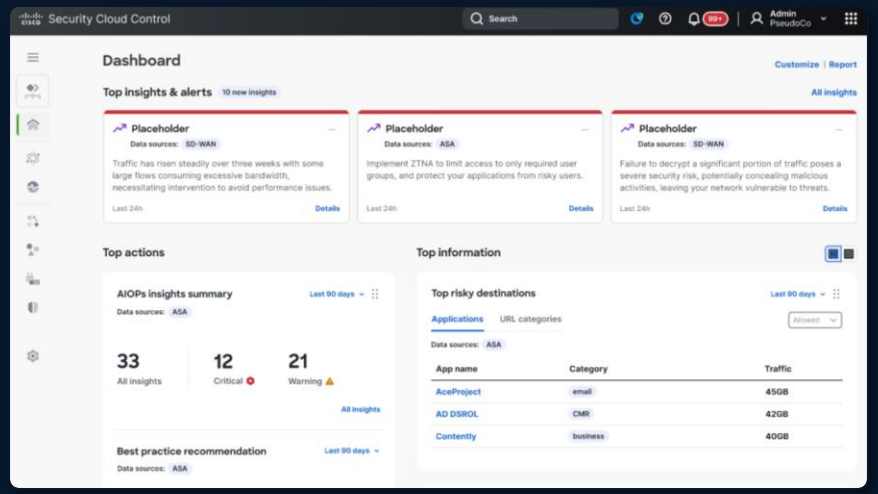
NEW

Cisco Security Cloud Control

Secure Router のポリシー制御をサポート

Cisco Secure Router
in Security Cloud Control

- オブジェクトとセキュリティ・ポリシーの作成
- 既存の Secure Router　オブジェクトの同期と管理
- 新しいセキュリティポリシーの作成
- SAL(Security Analytics and Logging)でセキュアルーターのイベントを可視化
- SD-WAN ManagerとSecurity Cloud Control 間のRBACモデルの同期



Supported models

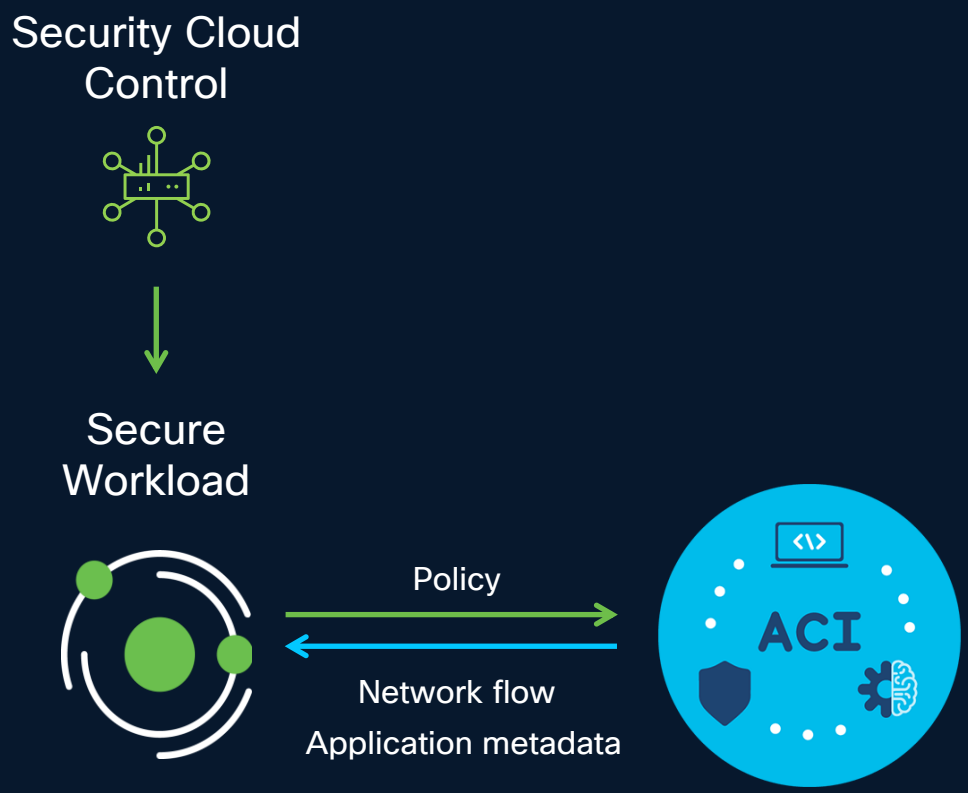
Cisco 1000 Series Integrated Services Routers
Cisco 8000 Series Secure Routers

ポリシーエンフォースメントポイントをACIに拡張

NEW

Cisco Secure Workload integration with ACI

- **セグメンテーションポリシー発見の自動化**
  AIがアプリケーションの動作と依存関係を深く可視化
- **ACIにおける最適なポリシーの適用**
  完全自動化されたスイッチングとアプリ・インフラの知見に基づくポリシーの生成
- **実装における複雑性の排除**
  コネクターによるエージェントレスの可視化とセグメンテーション
  ※可視化とポリシーの適用は段階的な実装



Hypershield と統合されたCisco Smart Switch への拡張

NEW

N9324C-SE1U

24-port 100G

- Cloud Edge, Zone-Based segmentation, DCI, Top-of-Rack
- 2.4T switch throughput, 800G services throughput
- Silicon One E100 ASIC + AMD DPUs
- Shipping now, Hypershield Target Initial Product Readiness: end of July'25

NEW

N9348Y2C6D-SE1U

48-port 25G, 6-port 400G, 2-port 100G

- DC Top-of-Rack
- 3.8T switch throughput, 800G services throughput
- Silicon One E100 + AMD DPUs
- Target Limited Orderability: July ‘25*

NEW

Cisco C9350

48/24 ports 10G/mGig, network-modules, 90W UPoE

- Campus
- 1.3T (800G stacking, 500G for switch) throughput
- Silicon One E100 + Security co-processor
- Target Orderability: June ’25*

* Hypershield capabilities are with appropriate licensing and planned for delivery over time

Hybrid Mesh Firewall

Cisco Secure Firewall
Secure Firewall 200 / 600

NEW

*AVAILABLE DEC 2025

Cisco Secure Firewall 200シリーズ

- 1.5Gbpsの暗号化通信の処理性能
- SD-WAN機能対応
- 市場平均の約3倍の価格性能比

*AVAILABLE OCT 2025

Cisco Secure Firewall 6100シリーズ

- 2Uで400 Gbps
- 最大16台のクラスタリング
  -> 4 Tbps以上のパフォーマンス

Branch		Campus	Data center		Cloud
NEW				NEW	
					
200 Series	1200 Series	3100 Series	4200 Series	6100 Series	Public/Private
1 Model	6 Models	5 Models	3 Models	2 Models	20+ cloud variants
Firewalling + IPS	Firewalling + IPS	Firewalling + IPS	Firewalling + IPS	Firewalling + IPS	
Up to 1.5 Gbps	Up to 18 Gbps	Up to 45 Gbps	Up to 140 Gbps	Up to 400 Gbps	

Hybrid Mesh Firewall

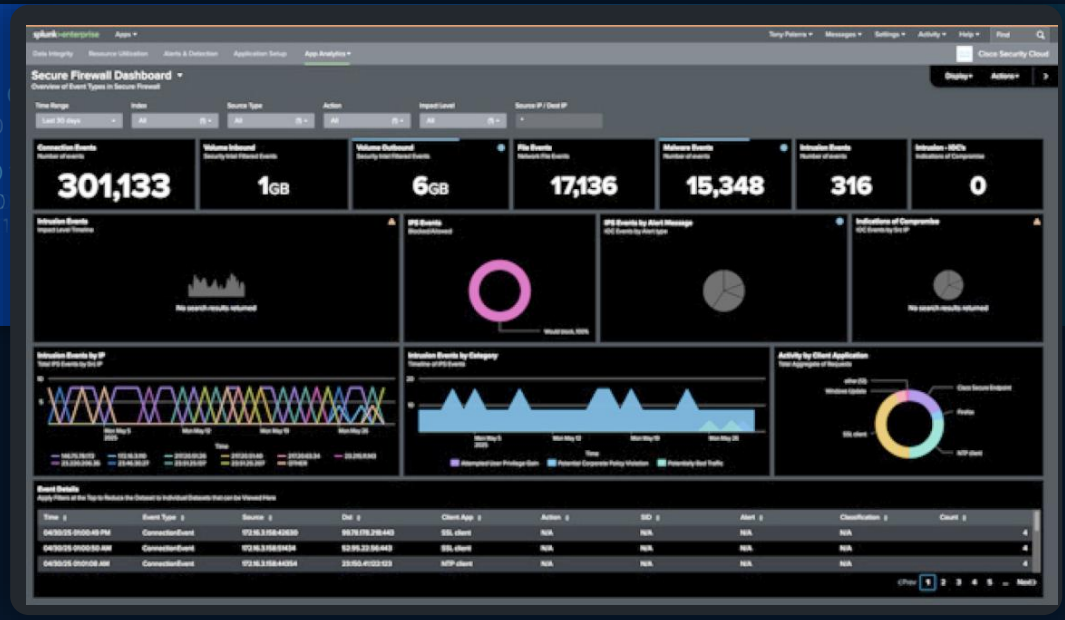
NEW

Cisco Secure Firewall

Firewall logs free in Splunk

Free log management*

AVAILABLE AUG 2025



* With active Firewall Threat Defense subscription, some limits and constraints apply

New detections | Automated response

Cisco Secure Firewall

Firewall Threat Defense 10.0

Splunk で脅威の検出を高速化

- 自動転送により、Secure Firewall から Splunk にセキュリティログデータをより簡単かつ迅速に送信

多数の FW を簡単に管理

- より多くのセキュリティイベントを毎秒処理し、より多くの履歴ログデータを保存
- 新しい FMC にて対応

高度な脅威に関する洞察を迅速に評価

- SnortMLによるコマンド・インジェクション攻撃の防御
- 1つのダッシュボードで実現

暗号化トラフィックの包括的な脅威検出

- 復号化をセカンド・プロセッサーにオフロードし、最小限のレイテンシーでQUIC暗号化トラフィックを検査

Hybrid Mesh Firewall に関連するアナウンスメントまとめ

Cisco Security Cloud Control
- サードパーティファイアウォールポリシー管理
- セキュアなルーターポリシー管理
- AIOpsによる容易なアップグレード

より迅速で容易な管理
サードパーティ製ファイアウォール、セキュアルーターのポリシーを管理し、AIOpsを介してファイアウォールのアップグレードを容易にする

Extend hybrid mesh enforcement points
- Cisco ACIによるセキュアなワークロード統合
- 新しいシスコスマートスイッチ

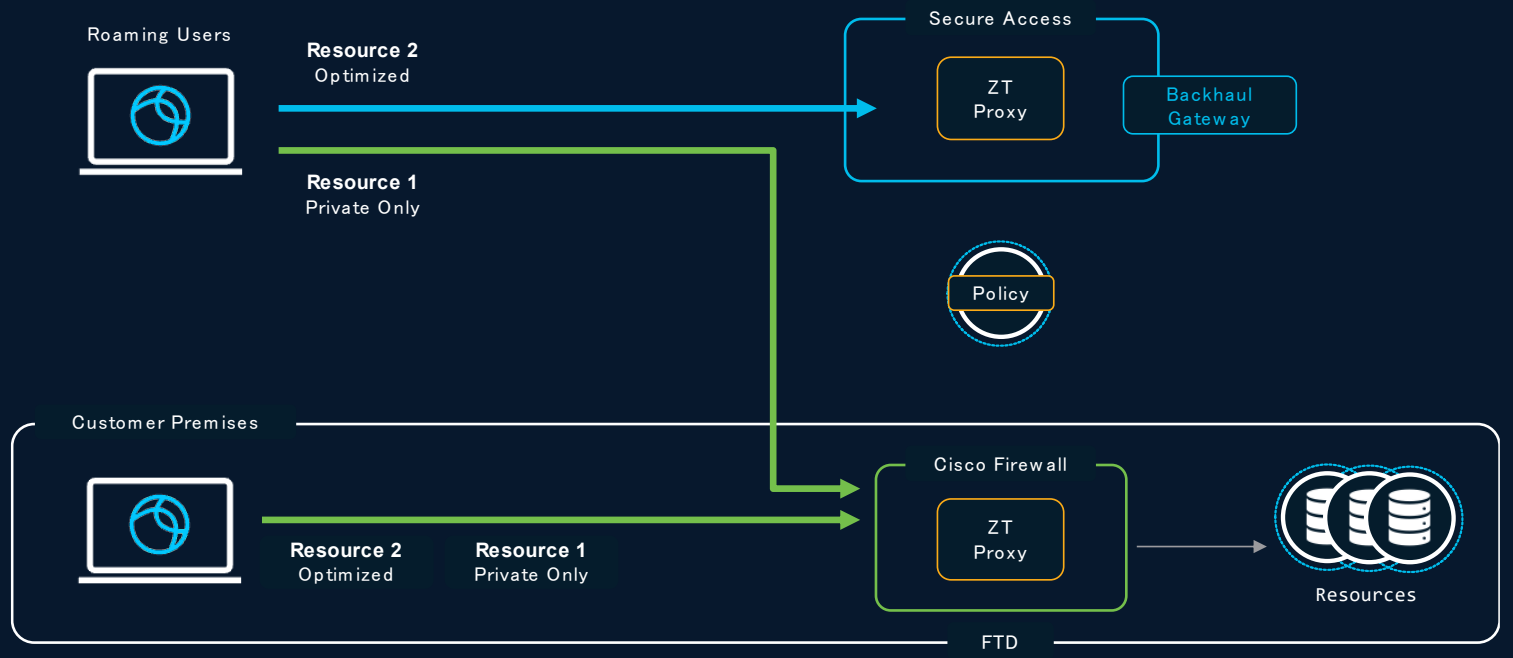
hybrid mesh firewallの拡張
Secure WorkloadによるACIファブリックのセグメンテーションポリシーの自動化、Hypershieldと統合されたスマートスイッチの導入

Cisco Secure Firewall
- Secure Firewall 200 series for branches
- Secure Firewall 6100 series for data centers
- Firewall Threat Defense (FTD) 10.0

現在のエンフォースメントポイントを強化
Firewall Threat Defense (FTD)の最新リリース10.0をプリロードした高性能ファイアウォール200および6100

一貫性のポリシーを必要な場所に適用
Universal ZTNA

PRIVATE PREVIEW



ユースケース

- ユーザーロケーションに基づく最適な接続性（ユースケース1）
- センシティブなリソースの企業プライバシー保護（ユースケース2）
- 影響度の高いクラウド停止時の回復力（将来）
- SCCによる集中管理

INTRODUCING

Duo IAM

We’ve made Duo twice as good

セキュリティファーストの
アイデンティティ

Security-First
Identity

エンドツーエンドの
フィッシング耐性

End-to-End
Phishing Resistance

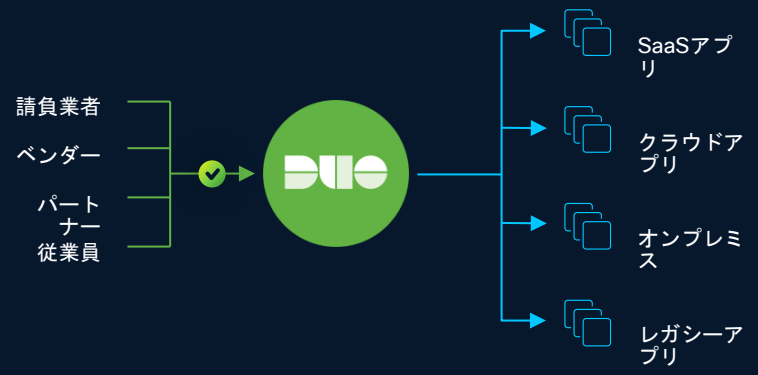
統合されたアイデンティ
ティインテリジェンス

Unified Identity
intelligence

業界最高クラスのユーザエクスペリエンス

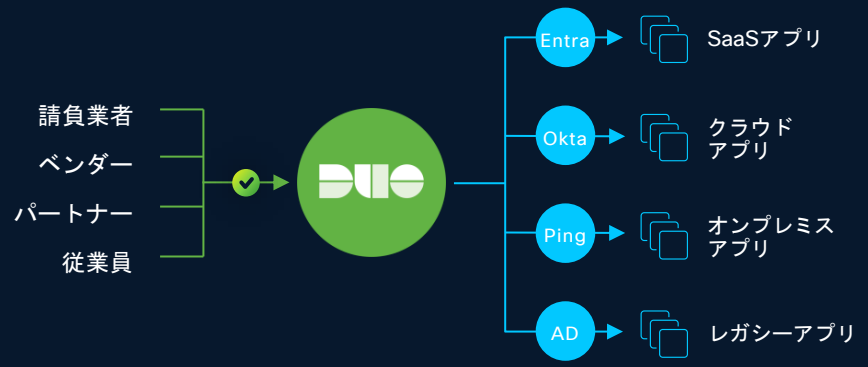
Cisco Duo IAM では主に３種類の構成が選択可能に

スタンドアロン型



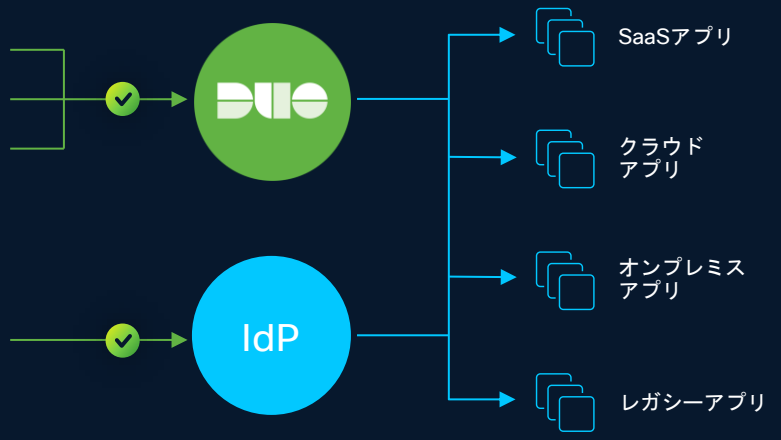
既存でIdPを持たない環境に対する新規Directoryを含めた導入

IDプローカー型



SAML IdPのプライマリと連携し、ブローカーとして動作するアプリからはDuoがIdPとして動作

代替えディレクトリ型



既存のIdPとは別の用途に対する代替のユースケースのためのディレクトリとして利用する

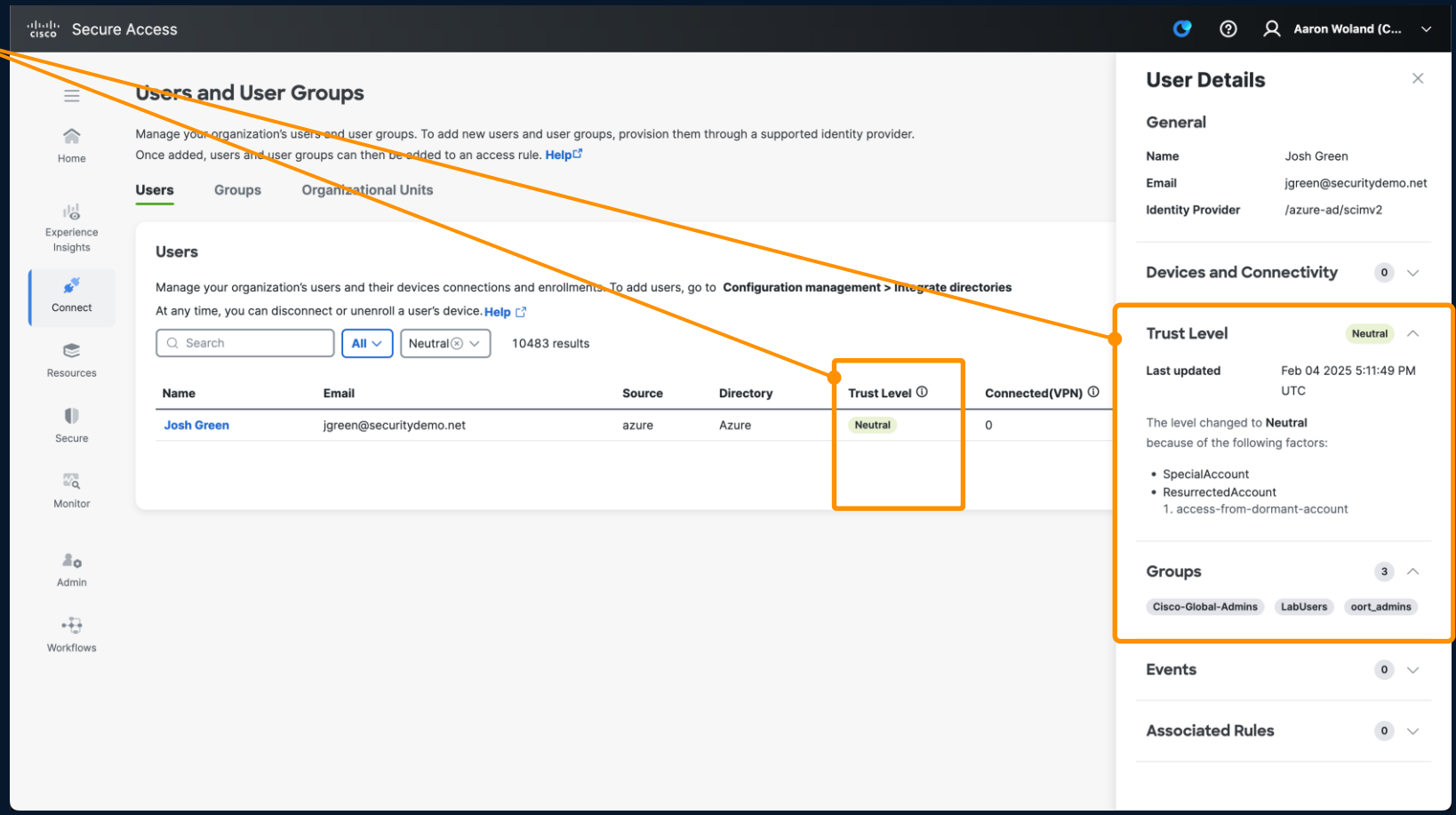
Cisco Identity Intelligence (CII) in Secure Access

Secure Accessの利用ユーザーにリスクがある場合にフラグを立てる

PRIVATE PREVIEW

User Risks

ディレクトリから Secure Access に同期されたユーザーは、CII によって発見された脅威に関連するコンテキストを持つ



Timing: In Private Preview now

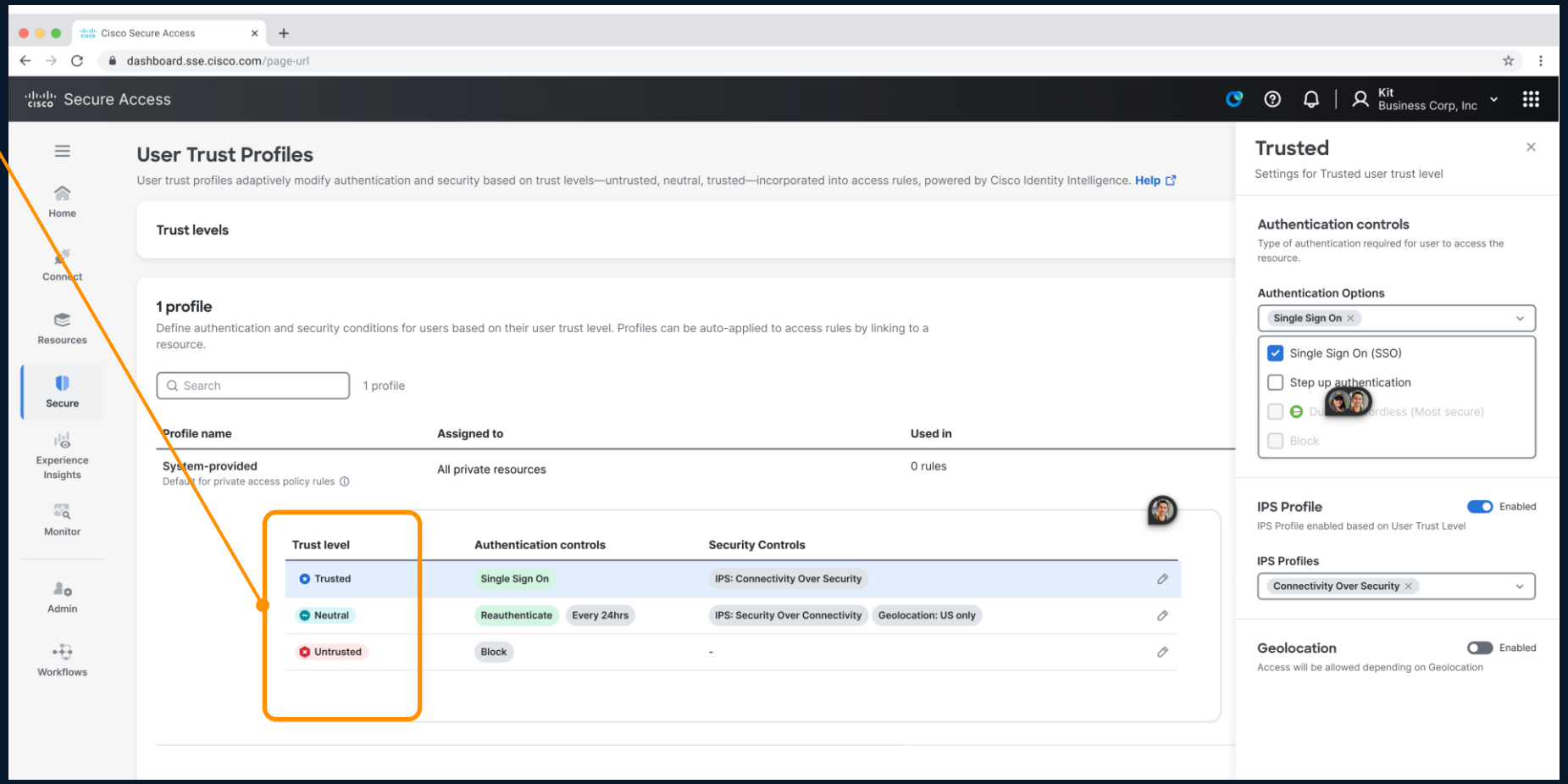
Cisco Identity Intelligence (CII) in Secure Access

リスクがあるユーザーアクセスを動的に制御 ※Phase2での対応予定

FUTURE

Trust Levels

Secure Accessは、
各ユーザーの信頼レベル
（Trust Level）により
アクセスポリシーを制御



Trust Level

セキュリティポリシーの更なる強化

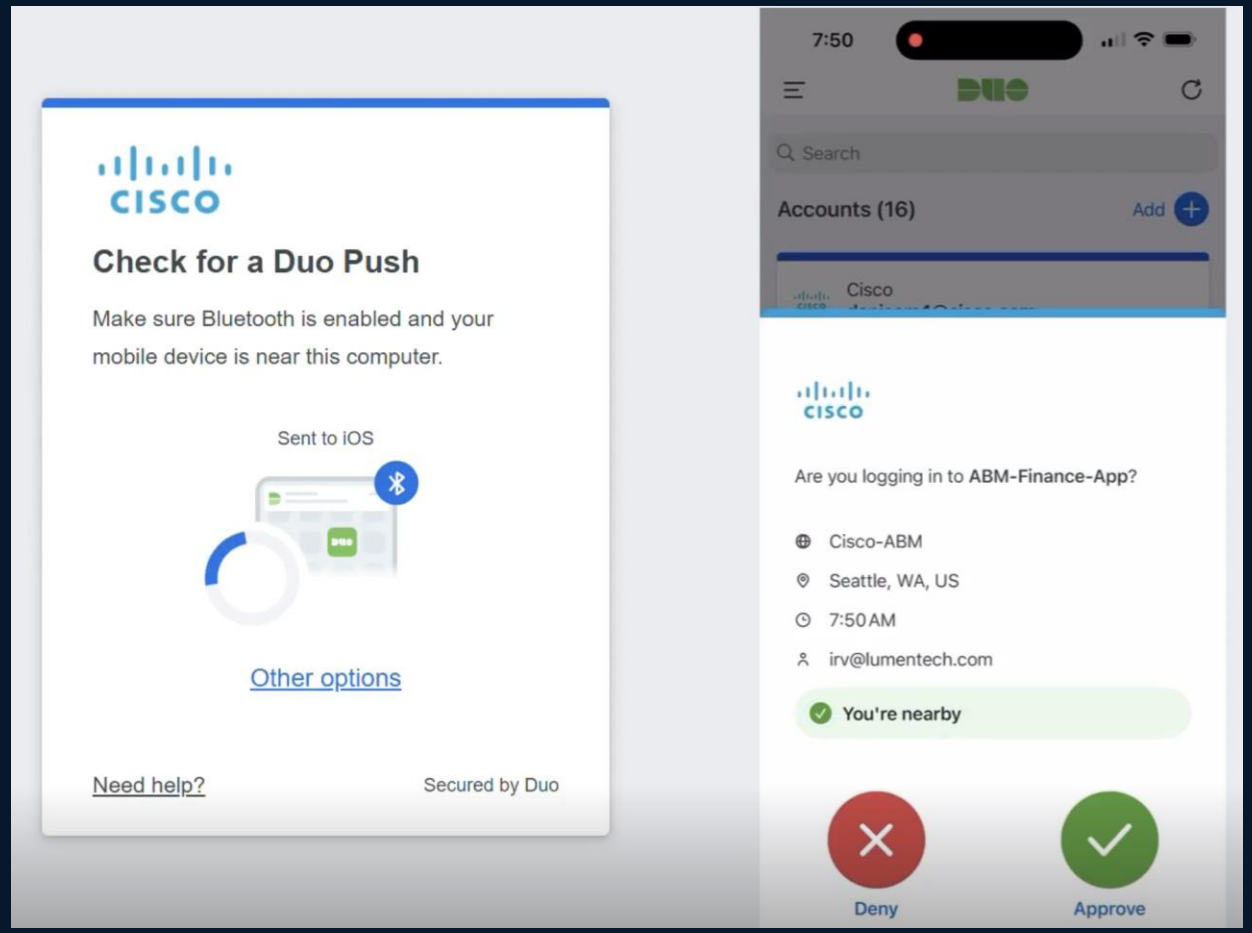
Source Criteria					Destination Criteria:			Result
IP Addr	**User / Groups**	**SGT**	**Device Trust**	**Trust Level**	**App**	**SGT**	**IPS**	**Action**
any	Executives	VIPs	Compliant	Favorable	SAP	ERP	Enabled	permit
any	any	Employees	Compliant	Untrusted	any	Ordering	-	deny

インフラアクセスにおけるポリシーの新しい基準

- ユーザーのリスクに基づいてアクセスを制御
- ユーザーの信頼レベルとTrusted Deviceコンプライアンスとの組み合わせは、インフラにおけるセキュリティレベルを向上

Proximity Based Authentication with Duo IDP + Secure Access

正当なユーザーと認証デバイスの確認



Proximity Verification

正当なユーザーアクセスと
認証デバイスが近くにあることを確認
追加のハードウェア（セキュリティキーなど）は不要

Eliminate Threats

プッシュフィッシングや中間者攻撃などのリモートMFAバイパス攻撃からの保護

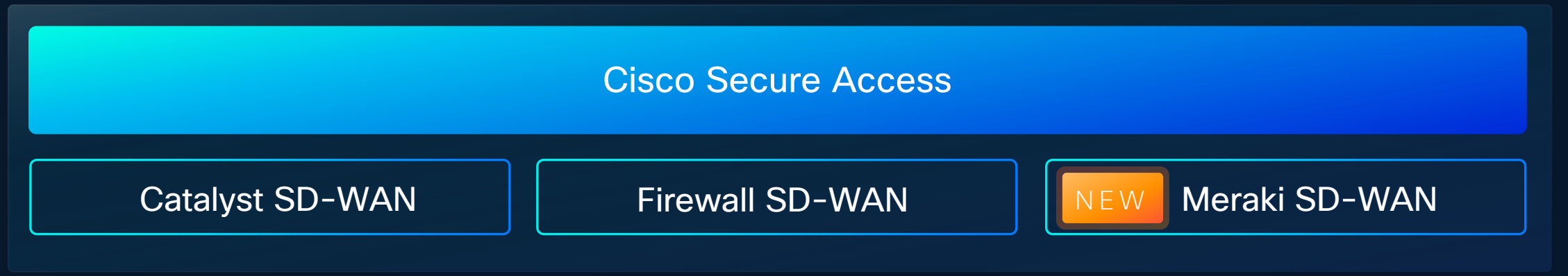
Security-first IAM

- Directory with passwordless option
- Strong MFA everywhere by default
- Device Trust out-of-the-box
- Flexible, simple deployment

NEW

Cisco SASE

Now unified on Secure Access



最適な接続を選択できる
柔軟性

Security Cloud Controlが
管理する
統合セキュリティ・ポリシー

一貫したクラウド
エンフォースメント

本日のまとめ

Network + Security

Single vendor SASE

SD-WAN
Commercial and Enterprise

+

Secure Services Edge
Cisco Secure Access

+

Identity first
ISE + Identity Intelligence

END-TO-END Segmentation | Common Policy

Cisco XDR 2.0

Clear verdict. Decisive action. AI speed.

Instant Attack Verification

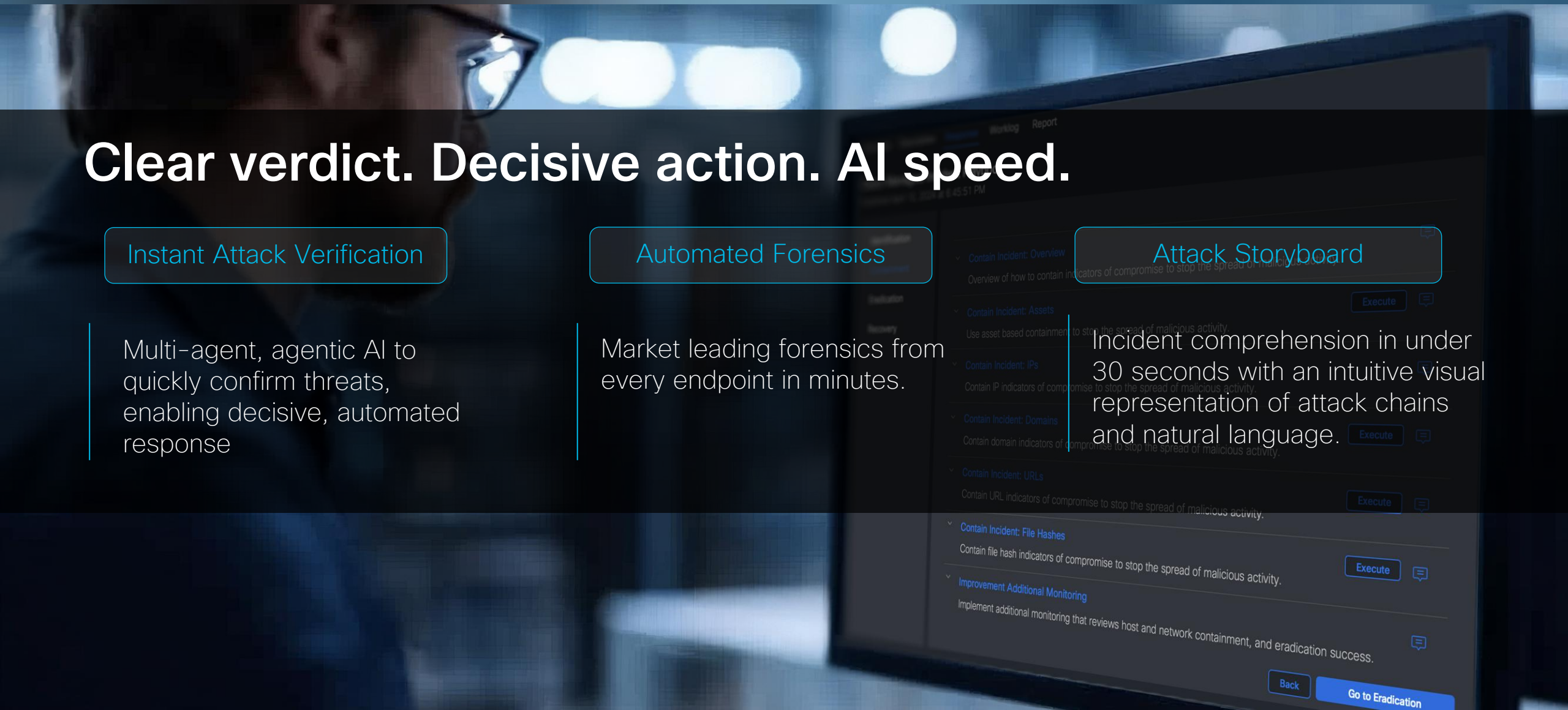
Multi-agent, agentic AI to quickly confirm threats, enabling decisive, automated response

Automated Forensics

Market leading forensics from every endpoint in minutes.

Attack Storyboard

Incident comprehension in under 30 seconds with an intuitive visual representation of attack chains and natural language.



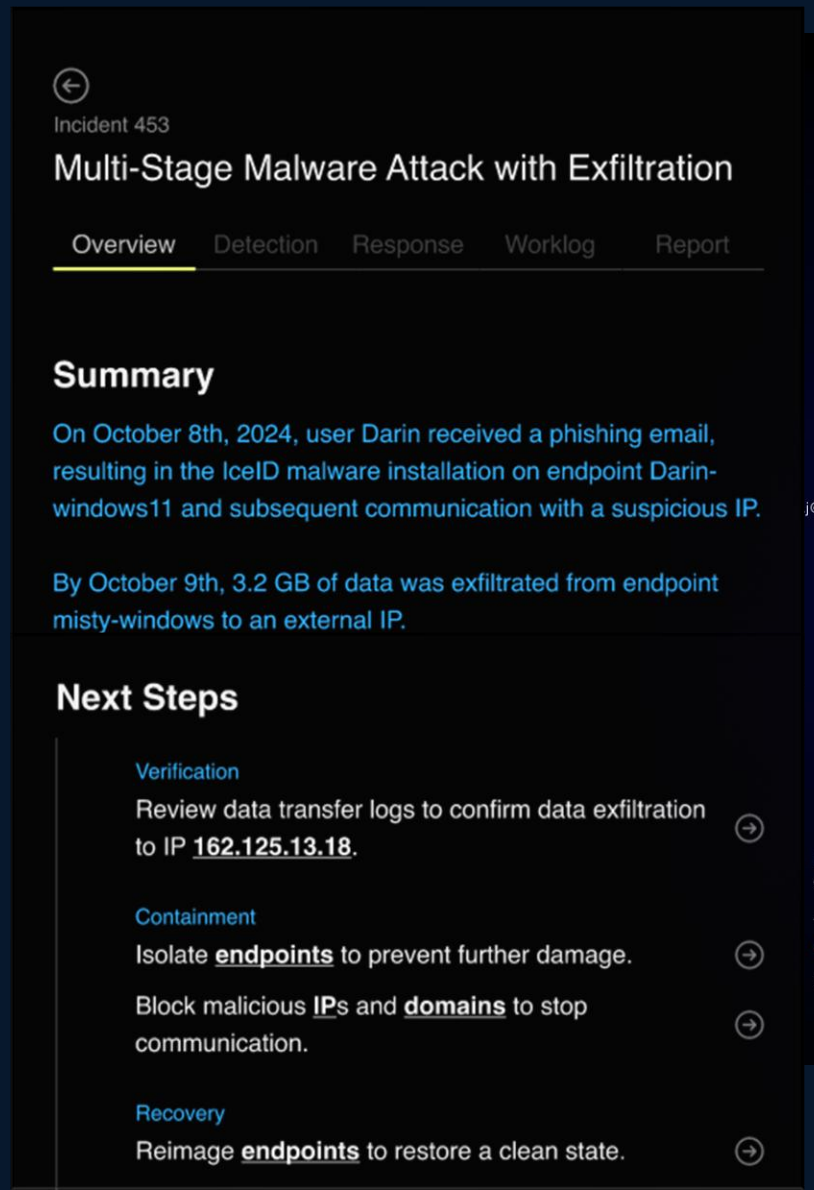
Instant Attack Verification with a clear verdict

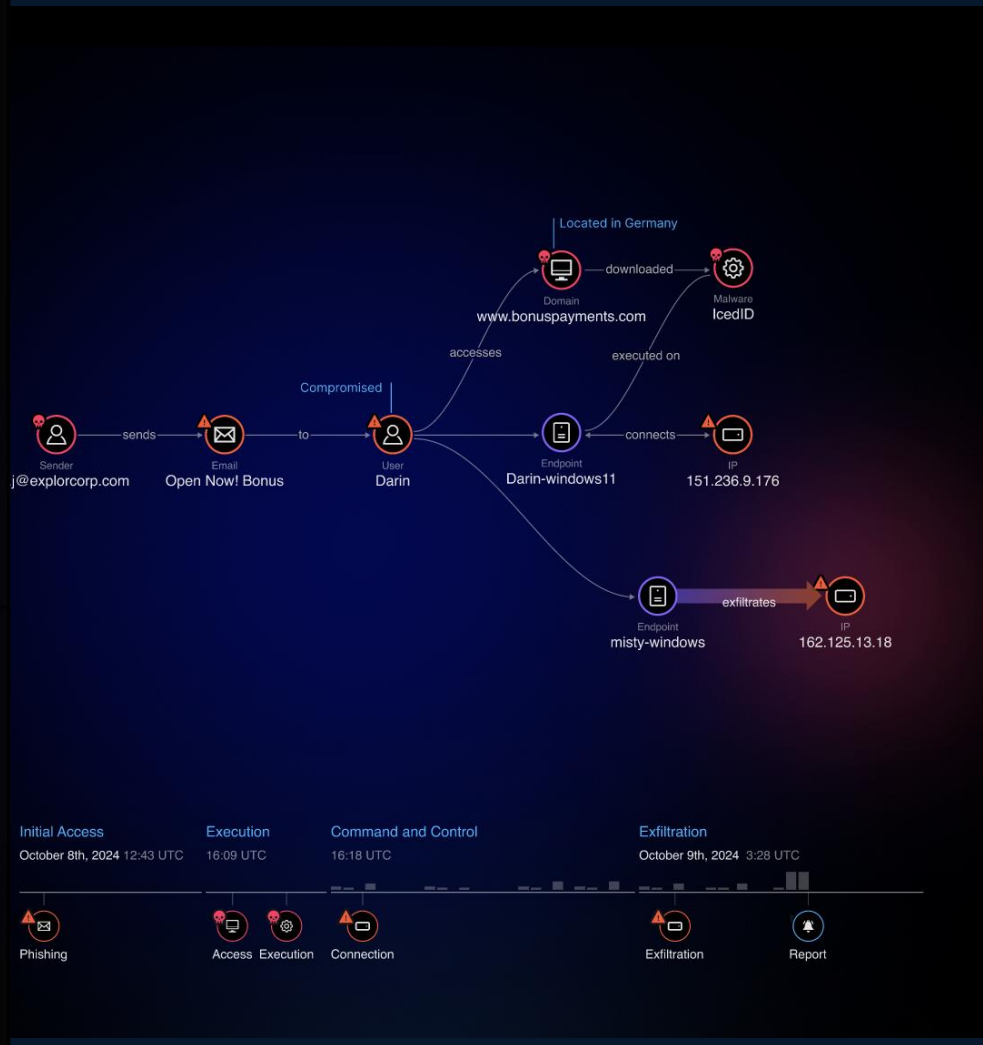
- Clear verdict. Decisive action. AI speed.

Each alert is analyzed by AI agents to eliminate false positives

Multiple AI agents launch investigation plan to verify real attack with a clear verdict

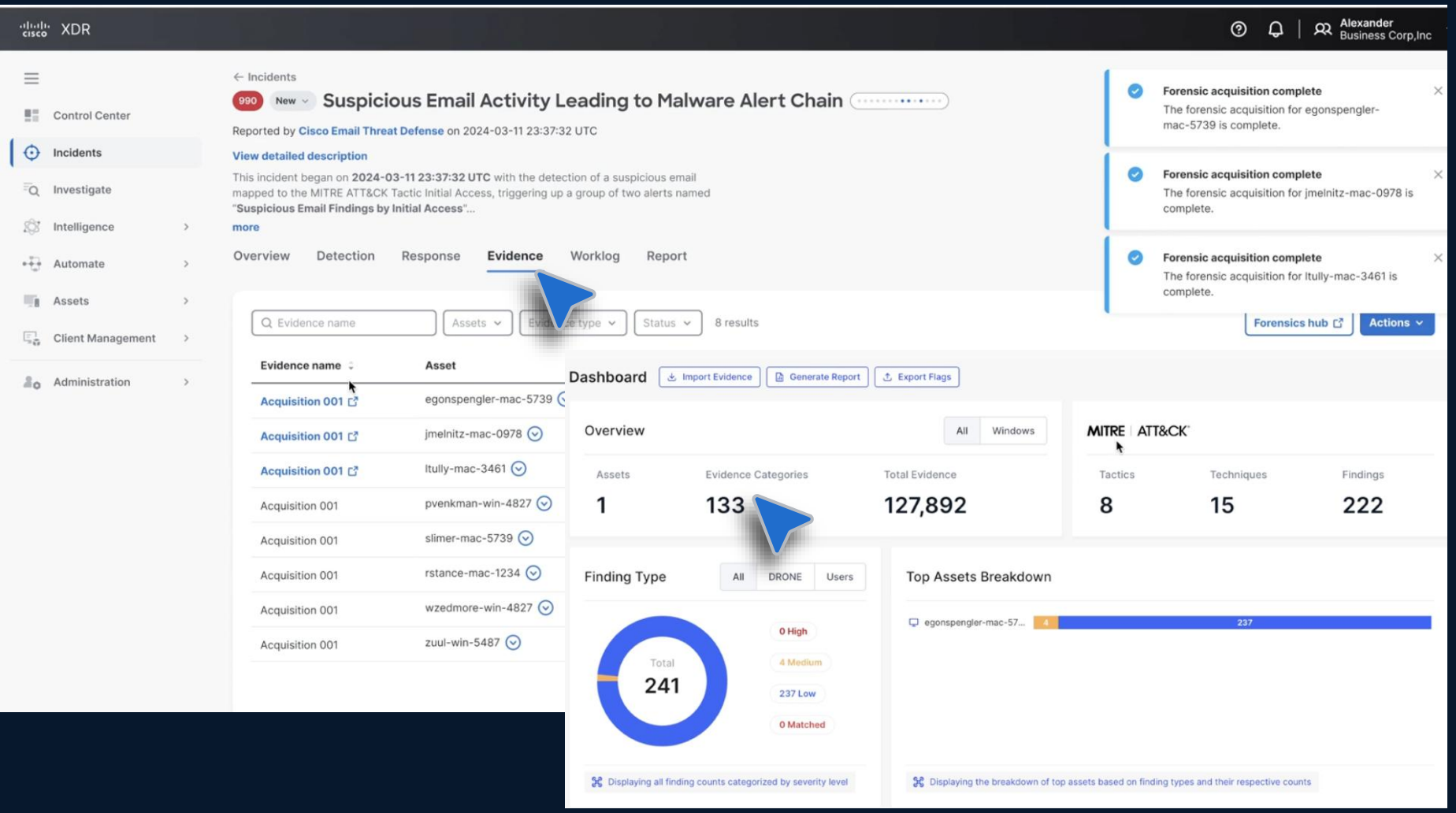
Trigger a decisive response through playbooks in XDR/ SOAR





Automated Forensics to Gather Evidence Instantly

- Clear verdict. Decisive action. AI speed.



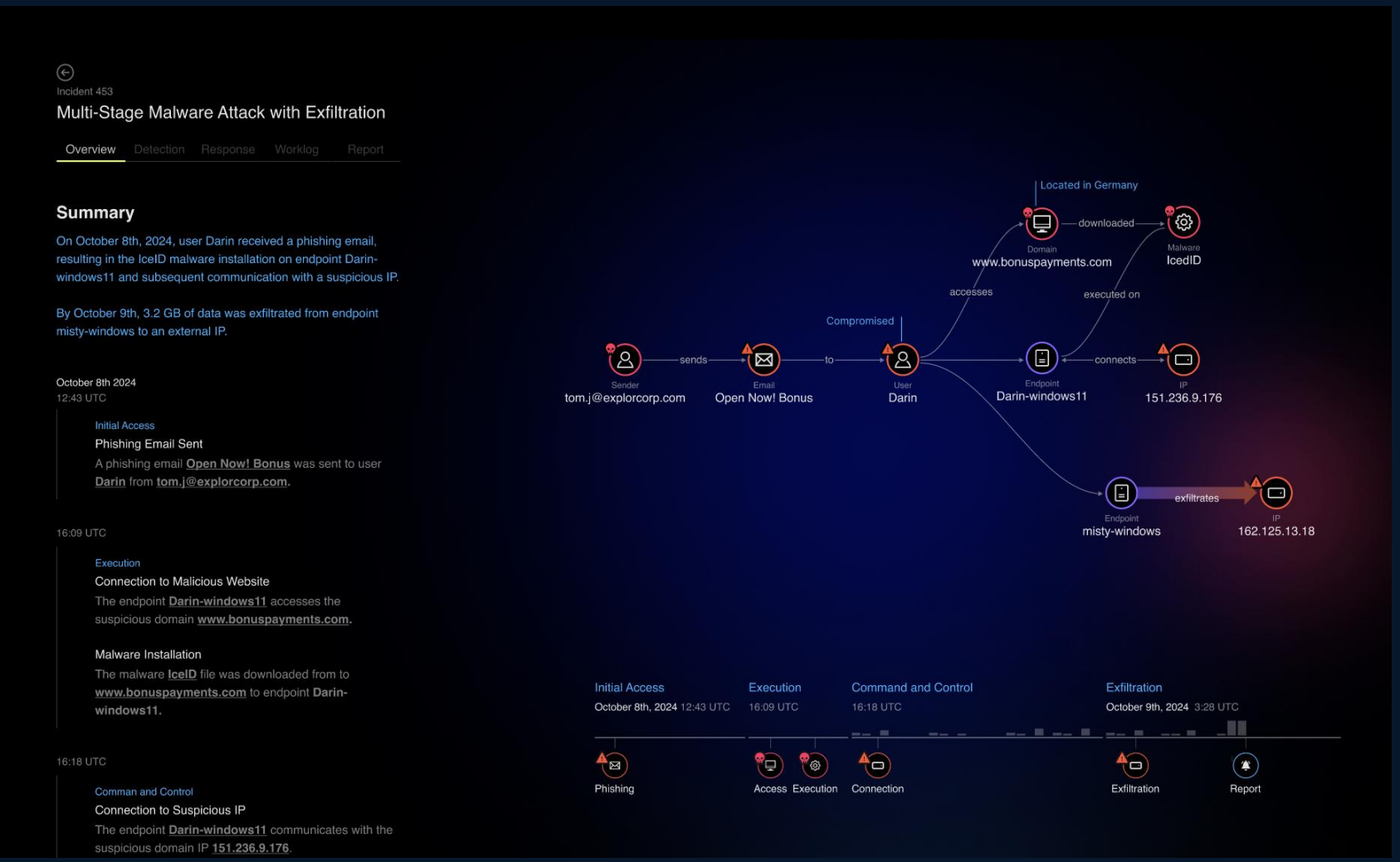
Trigger forensics before you know that you need it

100s of evidence components are captured even from compromised device

Evidence builds confidence to take decisive next steps

Attack Storyboard to Comprehend an Incident in 30 Sec

- Clear verdict. Decisive action. AI speed.



Turn complex attacks into visual narratives with explanation summary

Attack graph mapped MITRE tactics

Unified workflow from investigation to remediation with no context switching

Better together: SOC of the Future

Market leading SIEM + Innovative XDR

- Federated data management
- Advanced threat detections
- AI-accelerated investigations
- Automated response

EMBEDDED AI

CONTENT AND THREAT RESEARCH


User/Cloud/ Breach/


Networking


Third-party tools


Talos


Clouds


Devices


Data centers


Applications

Innovative XDR

XDR 2.0: Clear verdict. Decisive action. AI speed

"Storyboard" UX in XDR
Intuitive visual representation of complex attack chains, understood in under 30 secs

Instant Attack Verification in XDR
Agentic AI quickly confirms threats, enabling decisive, automated response

Automated Forensics in XDR
Collects forensics from every endpoint in minutes, not hours to enable faster response

SOC of the Future (Splunk Security + XDR)

Splunk + Cisco: better together

Automated Security Cloud Response
Splunk SOAR now contains threats faster with Cisco Secure Firewall and Cisco SMA

Instant Attack Verification w/Splunk
Splunk data fuels accurate investigation while Splunk SOAR drives decisive response

Access Isovalent Data in Splunk
Enabled by the Cisco Security Cloud App TA

Splunk: fueling SecOps efficiency

Unified TDIR Experience on-prem
Native SOAR and Threat Intelligence Management for on-prem in Splunk ES 8.1

Splunk SOAR on Azure
Native Azure implementation for scalability and ease of maintenance

Integrated FedRAMP Offering
Pair Splunk ES and SOAR to run playbooks and action Findings & Investigations

Findings-based detections in ES
Reduce alert noise, speed investigations, and improve decisions with correlated ES findings

Cisco AI PODs
Included in Cisco Secure AI Factory with NVIDIA

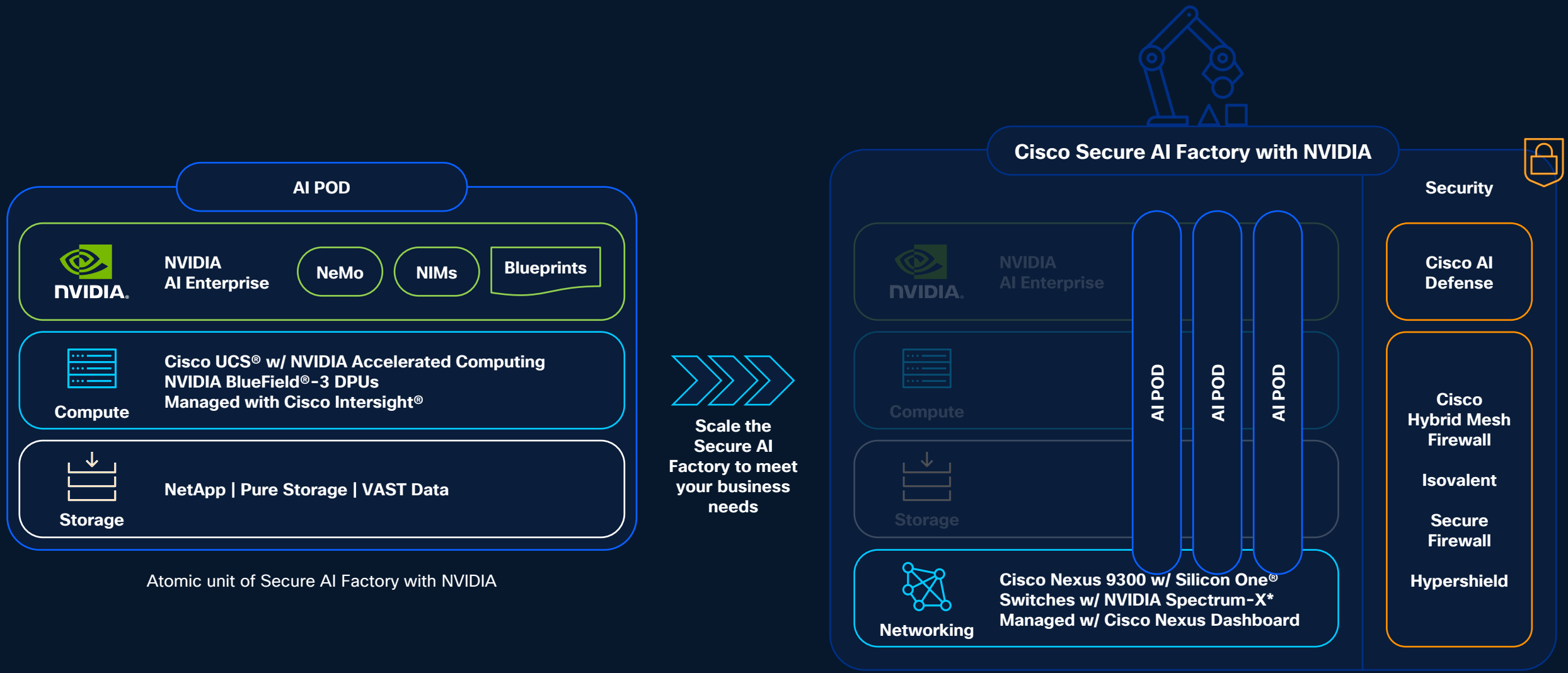
Security-first architecture enables safe enterprise AI

Unmatched performance AI infrastructure enables efficient model training, customization, and inferencing

Pre-validated AI infrastructure stack for simplified deployment drastically reduces set-up time

Cisco Secure AI Factory stack details

Modular system deployment and scaling with AI PODs



* future

Cisco Live US 2025
Observability に関する発表内容

Cisco Security

2025年6月18日

上村 徹也 | TETSUYA UEMURA

Splunk Services Japan合同会社

Observability for AI

Observability for AI

Observability CloudによるAIインフラ監視

- LLM（大規模言語モデル）、ベクトルDB、GPU基盤、およびオーケストレーションフレームワーク向けにあらかじめ構築されたダッシュボードや検出機能により、AIスタックの迅速な可視化を実現

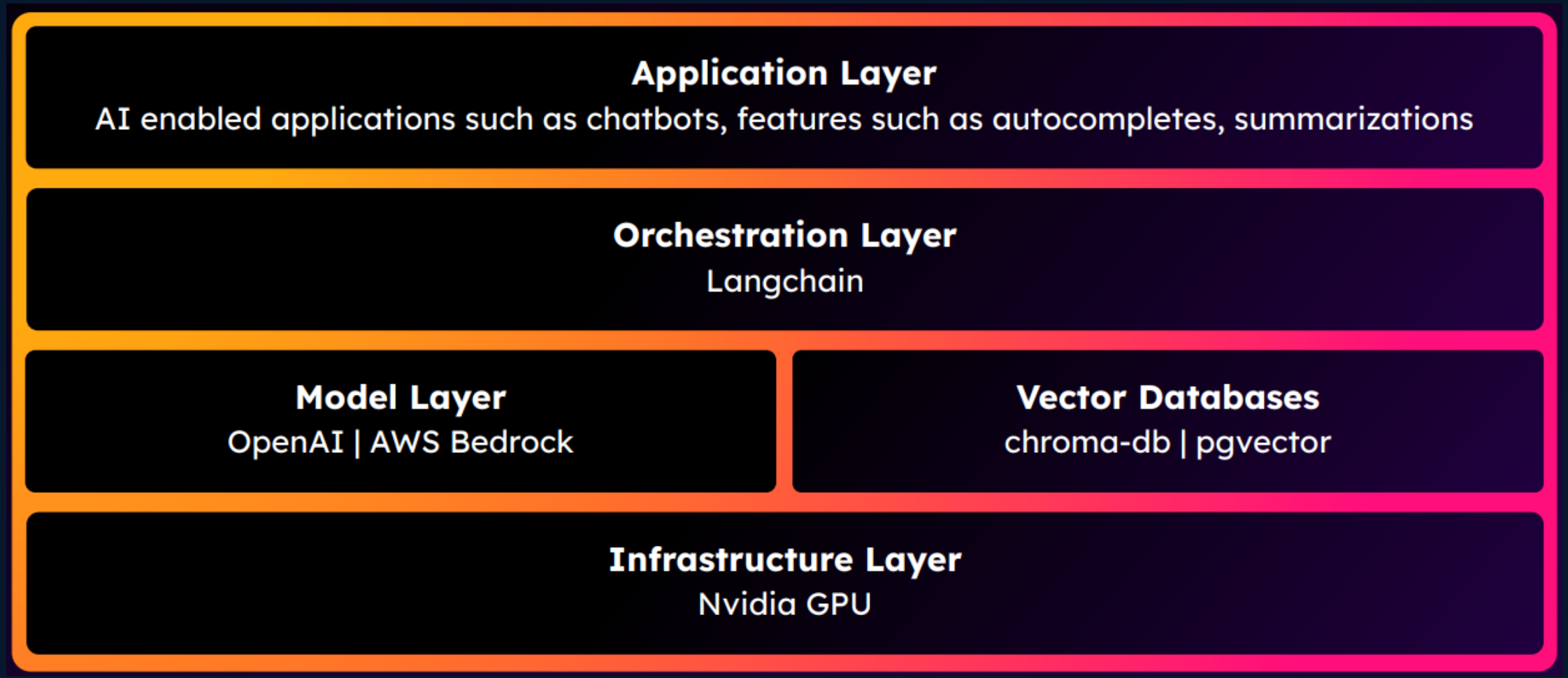
AIアプリケーションのトレースを統合

- LLMクエリ、組み込み、モデルAPIに対する深い洞察

AppDynamics LLM Monitoring

- GPU基盤、LangChainオーケストレーションレイヤー、ベクトルDBの性能監視

LLMスタックのすべてのレイヤーに対するオブザーバビリティ



AI in Observability

AI in Observability (AppDynamics)

Anomaly Detection for DB

- ビジネストランザクションに影響を与える前に、データベースの異常を自動的に検出
- チューニング可能なAI駆動型アラート機能により、ビジネスニーズに応じてモデルの感度を設定し、不要な通知を削減

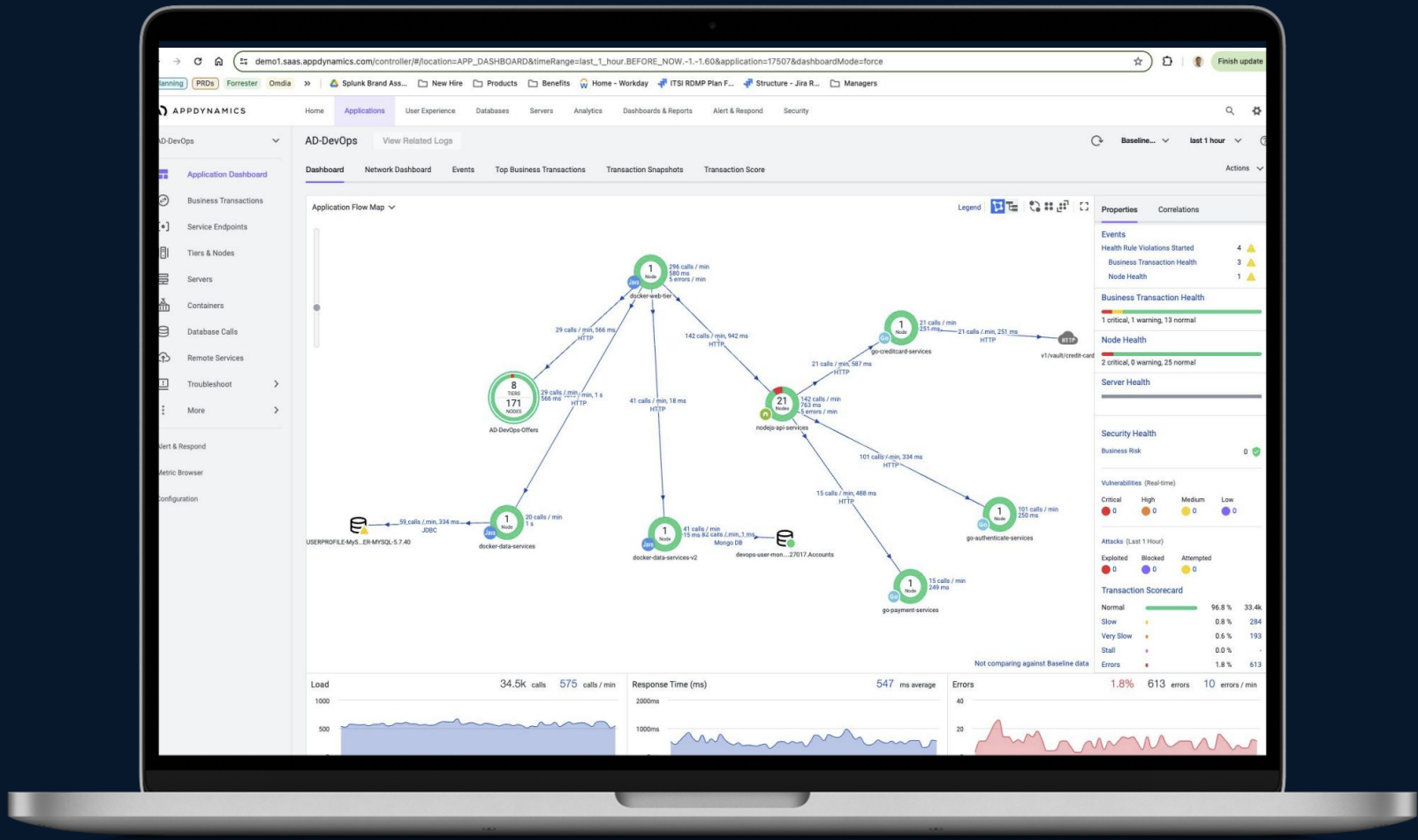
Root Cause Analysis (RCA)

for Infrastructure

- アプリケーションに影響を及ぼしているインフラの根本原因をAIが自動的に分析し特定
- レコメンデーション機能を活用してあらゆるチームメンバーがより早く問題を解決

VA Diagnostics (On-Prem)

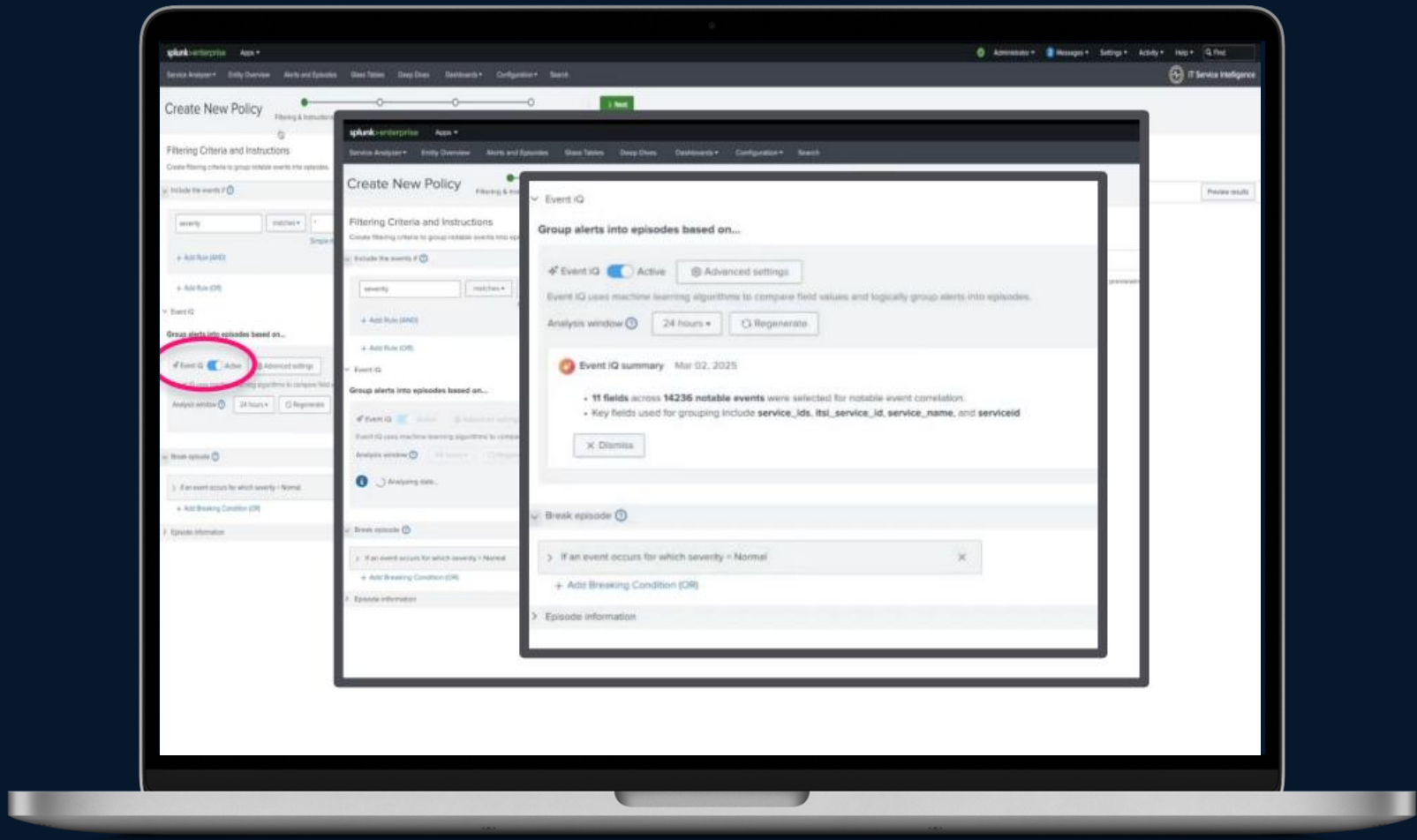
- トランザクションスナップショットのAI駆動型分析により、オンプレミスのワークロード全体でインサイトや異常な挙動を特定
- AIがパターンを自動的に検出し、複雑な問題をより自律的に対処



AI in Observability (ITSI)

EventIQ

- AI駆動型のアラートグループ化により、手動でのポリシー調整なしでアラートデータのパターンを自動的に特定
- ルール設定不要でインシデントを優先度づけ
- ThousandEyes、Catalyst、Merakiなどのネットワークドメインを含むシステム全体の相関
- 根本原因の特定とサービス復旧を支援



Cisco/Splunk Integration

Splunk ITSI Content Pack追加

Catalyst＋Meraki

- CatalystとMerakiのメトリクスおよびイベントをITSIのイベントインテリジェンスに統合し、アラートのノイズを削減し、MTTR（平均復旧時間）を短縮
- Catalystデバイスやインターフェースの状態をビジネスメトリクスと関連付け、ネットワーク関連のサービス劣化を優先的に対応
- Merakiで管理されるインフラストラクチャ（ゲートウェイ、スイッチ、APなど）の可視性を拡張し、デバイスをビジネスサービスにマッピングすることで、ネットワーク問題の影響をより的確に把握

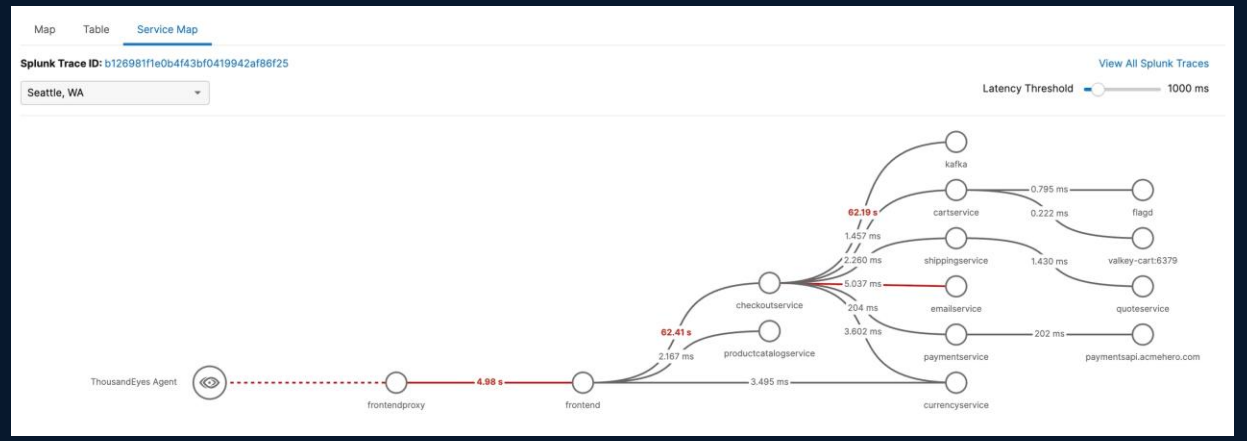
ThousandEyes

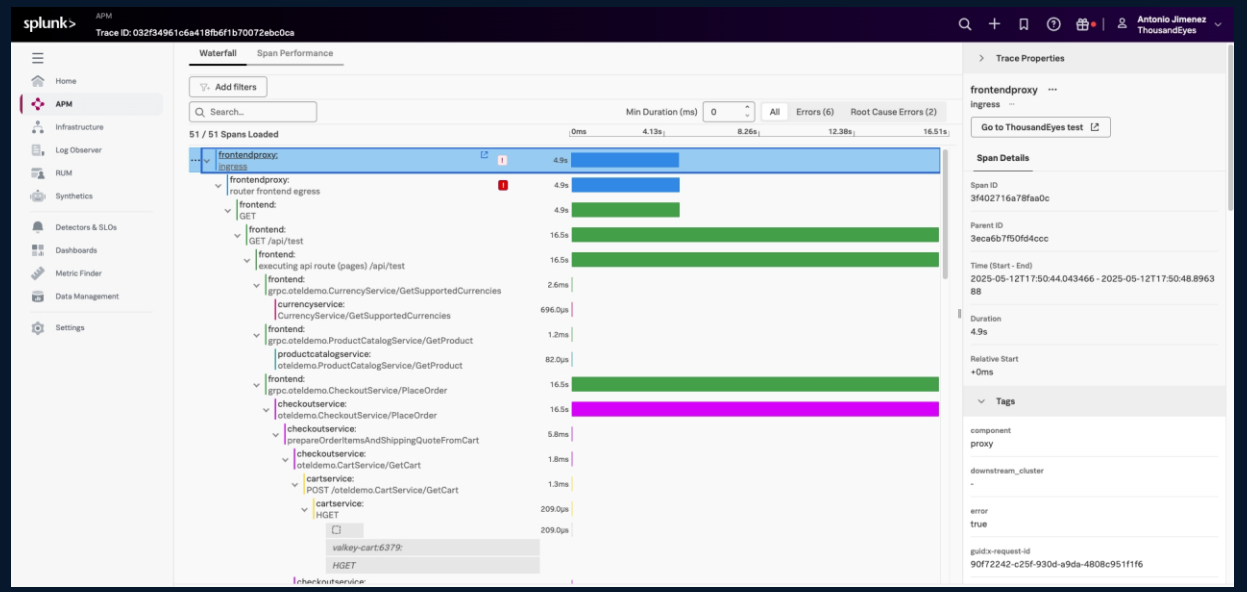
- ThousandEyesのイベントをITSIのイベントインテリジェンスに統合し、アラートのノイズを削減し、MTTR（平均復旧時間）を短縮
- ThousandEyesからネットワークパフォーマンスおよびビジネスメトリクスをITSIに取り込み、影響に基づく迅速なトラブルシューティングを実現
- ThousandEyesや他のCiscoソリューション全体からネットワークのテレメトリデータとインシデント対応を一元化

Splunk Observability + ThousandEyes

ThousandEyes連携

- ThousandEyesテストの失敗を迅速に診断
- ネットワーク層またはアプリケーション層のどちらに遅延の原因があるかを把握
- ThousandEyesテストの文脈でトレーストポロジーや主要なサービス間メトリクスを確認
- ThousandEyesのUIからSplunk Observability Cloudで計測されたサービス向けのテストを簡単に設定





Cisco Live US
コラボレーションアップデート

Collaboration Launch 2025

June 5, 2025

Cisco Live 2025

June 8–12, 2025 – San Diego

Cisco Live US Sandiego 2025 コラボレーションソリューションアップデート

1 働き方に合わせて設計された ワークスペースインテリジェンス

- Zoom Meetings for Cisco Rooms (Cisco Live 外でアナウンス)
- AI搭載のRoom Vision Pan Tilt Zoom カメラ
- ゼロタッチデバイスプロビジョニング
- Agentforce および Jira インテグレーション
- AI アシスタント ミーティングスケジューラ
- Webex Calling カスタマーアシスト
- Webex Calling AI レセプショニスト
- 9800 Desk Phone と Cisco Smart Switch 連携

2 AI による革新と柔軟性で 顧客のニーズに寄り添う

- オンプレミスでのAI機能: Contact Center Enterprise
- オンプレミスでのAI機能：Meetings and Calling
- Cloud Meetings 顧客へのサイトサバイバリティ
- オンプレミスプライベート会議、暗号鍵、録画

3 AIを活用した カスタマーエクスペリエンス

- Webex AI Agent の活用
- AI Agent でのテンプレートの活用とLLMエンジンの拡大
- Cisco AI Assistant 機能の拡張

4 IT管理者向けに 統合管理と分析

- AI 分析と管理 in Control Hub
- カスタム Role-based access control (RBAC) in Control Hub
- Webex Calling および Merakiネットワークの可視性

2025年末リリース予定

Zoom Meetings for Cisco Rooms

会議中の体験をフル機能でサポート

Zoomご利用のお客様が使い慣れた機能に、Ciscoが提供する高画質・シネマティックな会議体験が融合

zoom Meetings

with Android™

RoomOS 11は、ネットワークから隔離されたセキュアなコンテナ内でAndroidを実行

1

働き方に合わせて設計されたワークスペースインテリジェンス

没入型のワークプレース体験を提供する
AI搭載 Room Vision Pan Tilt Zoom カメラ

デバイスオンボーディングのさらなる簡易化を実現する
ゼロタッチデバイスプロビジョニング

ネットワークとコラボ機器の運用を連携し
省エネ管理もスマートに
9800 Desk Phone とCisco Smart Switch 連携

オフィスの電話業務をよりスマートに
Webex Calling カスタマーアシストとAI レセプショニスト

AI アシスタントを利用したシームレスなワークフローを実現
ミーティングスケジューラおよび Agentforce, Jira 連携

https://youtu.be/zlKXRoFkfaU

2025年6月より
段階的に販売予定

NEW

AI搭載 Room Vision Pan Tilt Zoomカメラ

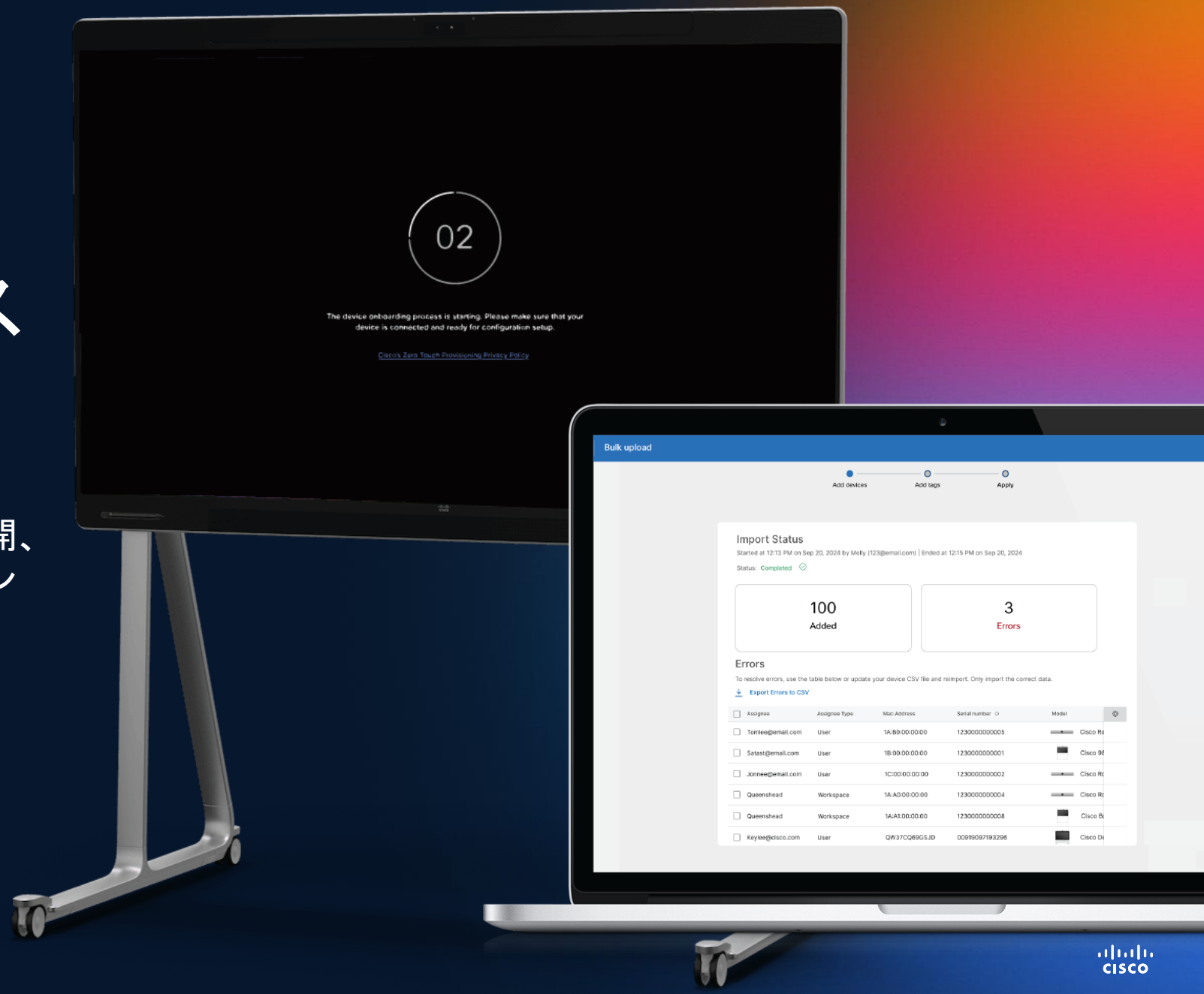
- 柔軟に拡張できるマルチカメラ体験
- AIが人物を正確に自動追尾
- ケーブル1本で簡単設置（Ethernet対応）
- 誰でも簡単に使えるPresenterTrack設定

https://youtu.be/wfYIdA0teuI

2025年6月より
限定提供開始

ゼロタッチデバイス プロビジョニング

プラグ＆プレイのセットアップ、自動展開、集中管理により、大規模なデバイスのオンボーディングを簡素化



C9350 Smart Switch + Cisco Desk Phone 9800 Series

よりスケーラブルな運用、より優れたエネルギー管理

2025年7月ベータ

スケーラビリティとサステナビリティの革新

- **ネットワーク＆コラボ機器全体でスケーラブルな運用を実現**
- **集中管理によるエネルギーの可視化と包括的な指標**
- **エネルギー管理の最適化に加え、診断・トラブル対応も強化**

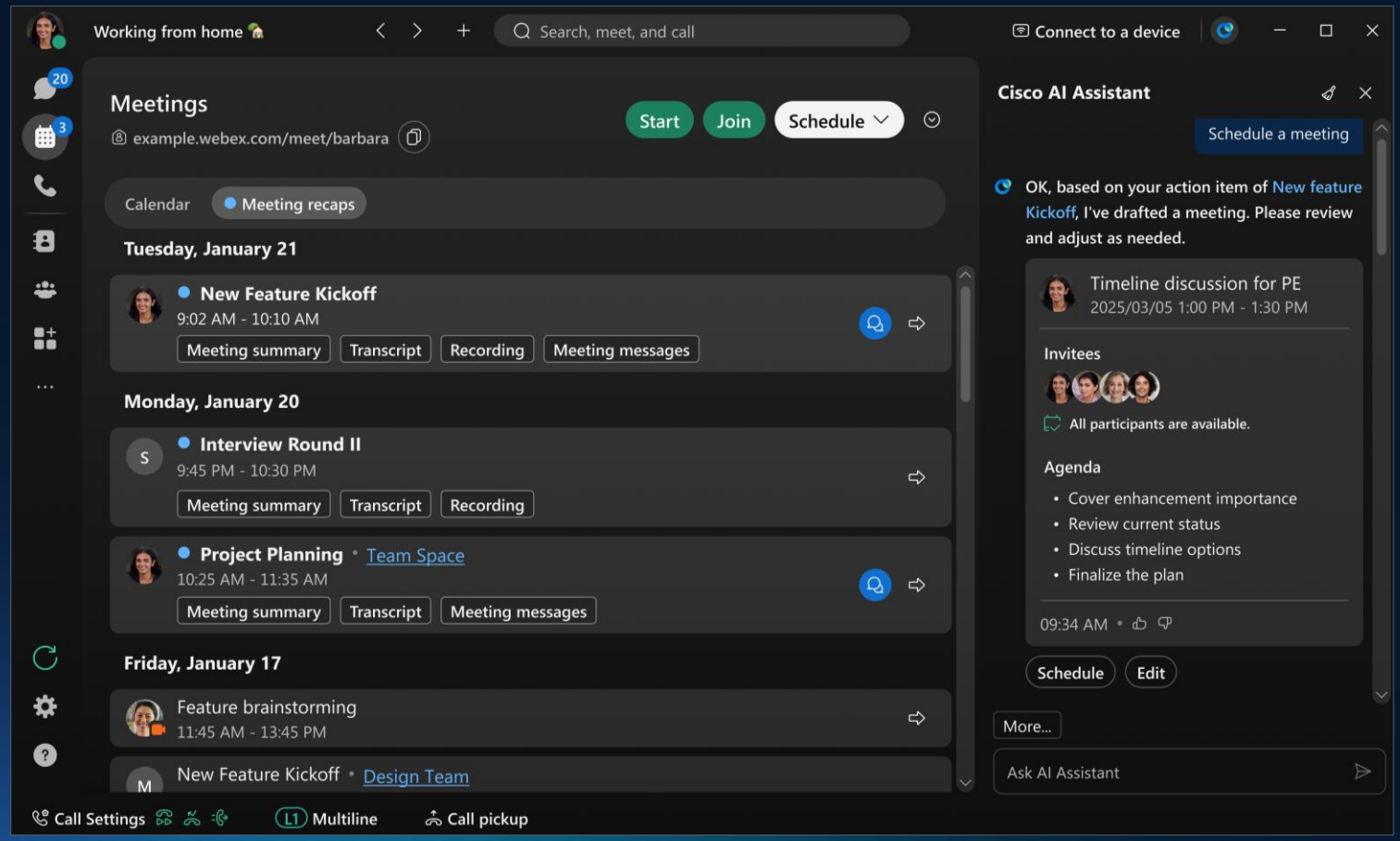
2025年第3四半期
ベータ予定

AI アシスタントミーティングスケジューラ

Cisco AI アシスタント

プロセスではなく人を中心としたコラボレーション

コンテキスト、コミュニケーション、アクションを統合し、チームの働き方に最適なシームレスなワークフローを実現



Webex ワークフロー統合

普段使いのアプリから、そのまま利用が可能

2025年第4四半期
ベータ

Webexのワークフローの中で、
Jiraチケットをその場で作成・
更新・管理

2025年6月
リリース予定

Webexの高品質なミーティングを
Agentforceでもシームレスに

従業員と顧客を支援するAI

https://youtu.be/DZWwEKVARFU

リリース済

Cloud Calling

AIを活用するクラウド型
コーリングサービス

柔軟な働き方を支える
安全で信頼性の高い
クラウドコーリング

リリース済

カスタマーアシスト

フロント業務を支える
スマートなツール

テキストキュー*、感情分析、
要約機能を活用した高度な通話管理
(*ベータ：2025年第3四半期予定)

2025年後半
ベータ

アドオン

AI レセプショニスト

24時間365日
AIが対応

問い合わせ、予約、転送も対応
可能な仮想通話受付

2

AI による革新と柔軟性で顧客のニーズに寄り添う

Contact Center Enterprise 顧客が利用可能な
オンプレミスebex AI Agent 及び AI Assistant

オンプレミス会議、電話利用時でも
AIを利用した音声とビデオ体験を提供

シームレスな会議体験を継続提供する
クラウド会議利用のサイトサバイバビリティ

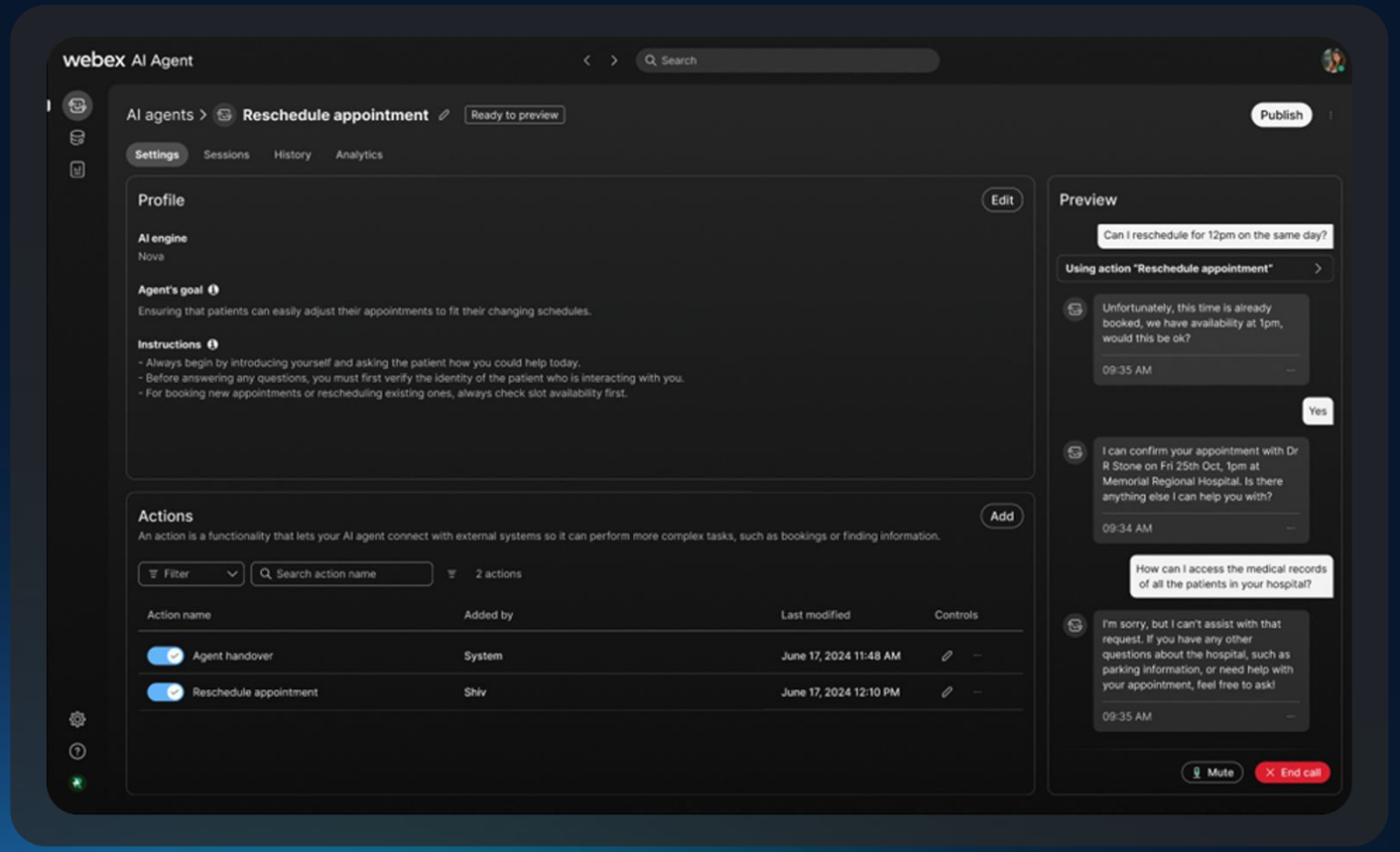
オンプレミス会議の強化による
規制要件への対応とデータ管理の強化

2025年5月
リリース

CCE Release 15

Contact Center Enterprise AI機能

- デジタル機能を強化した新たなプラットフォーム
- AI Agent & AI Assistant
- BYO 仮想エージェント

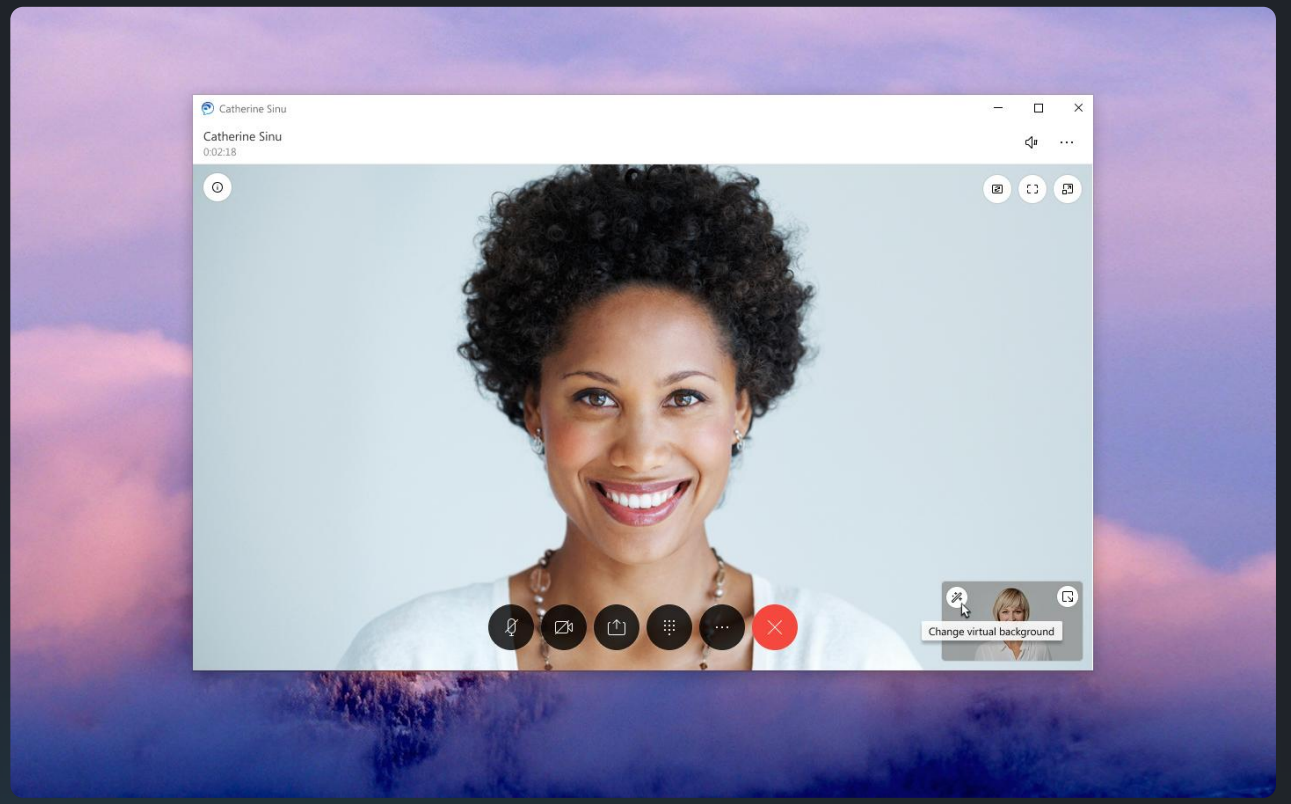


2025年後半
ベータ

AI機能拡張 オンプレミス Meetings and Calling

業務の中断を抑え、生産性を高める

- 背景雑音の除去
- 文字起こしと翻訳
- 背景ぼかし



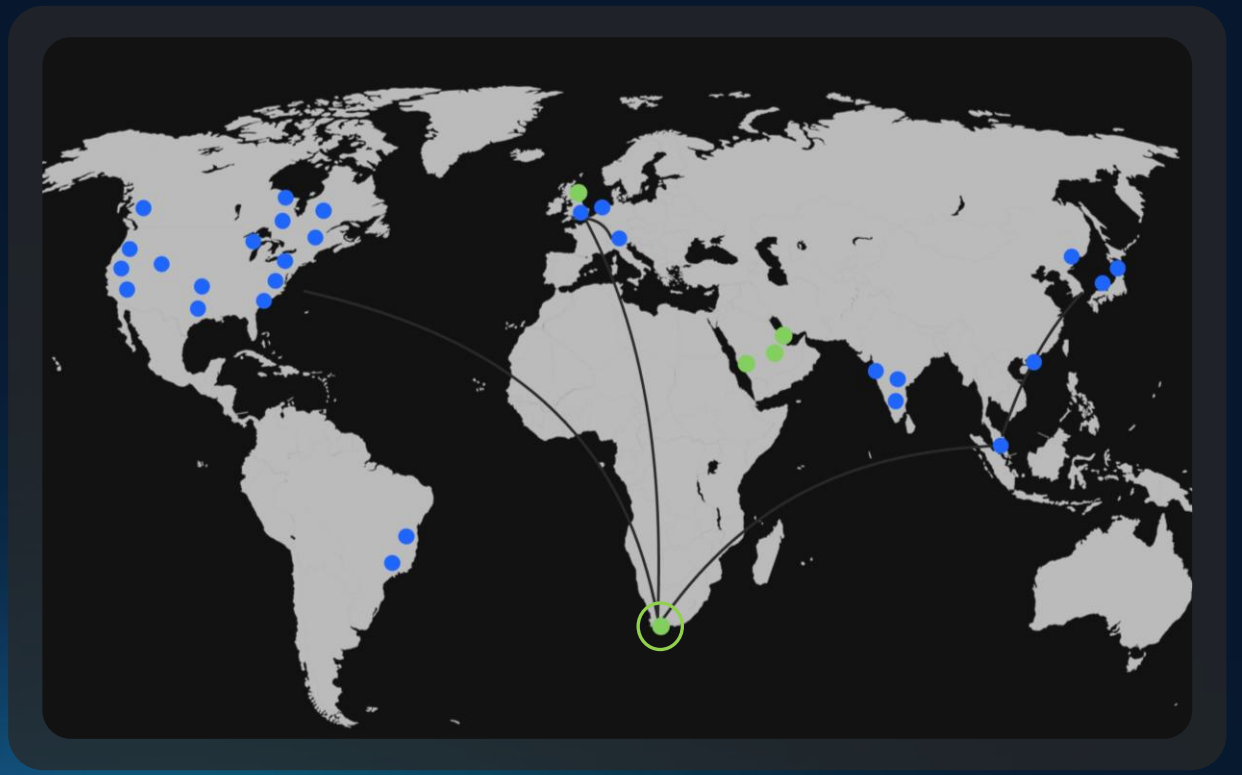
Meeting Server | Jabber | CUCM

2025年第4四半期
リリース予定

アドオン

規制に対応した高度な会議管理

- ローカルでの会議録画、暗号化キー管理オプションにより、さらなるデータ管理を実現
- オフィス内、社内の参加者のみが利用可能なプライベート会議機能

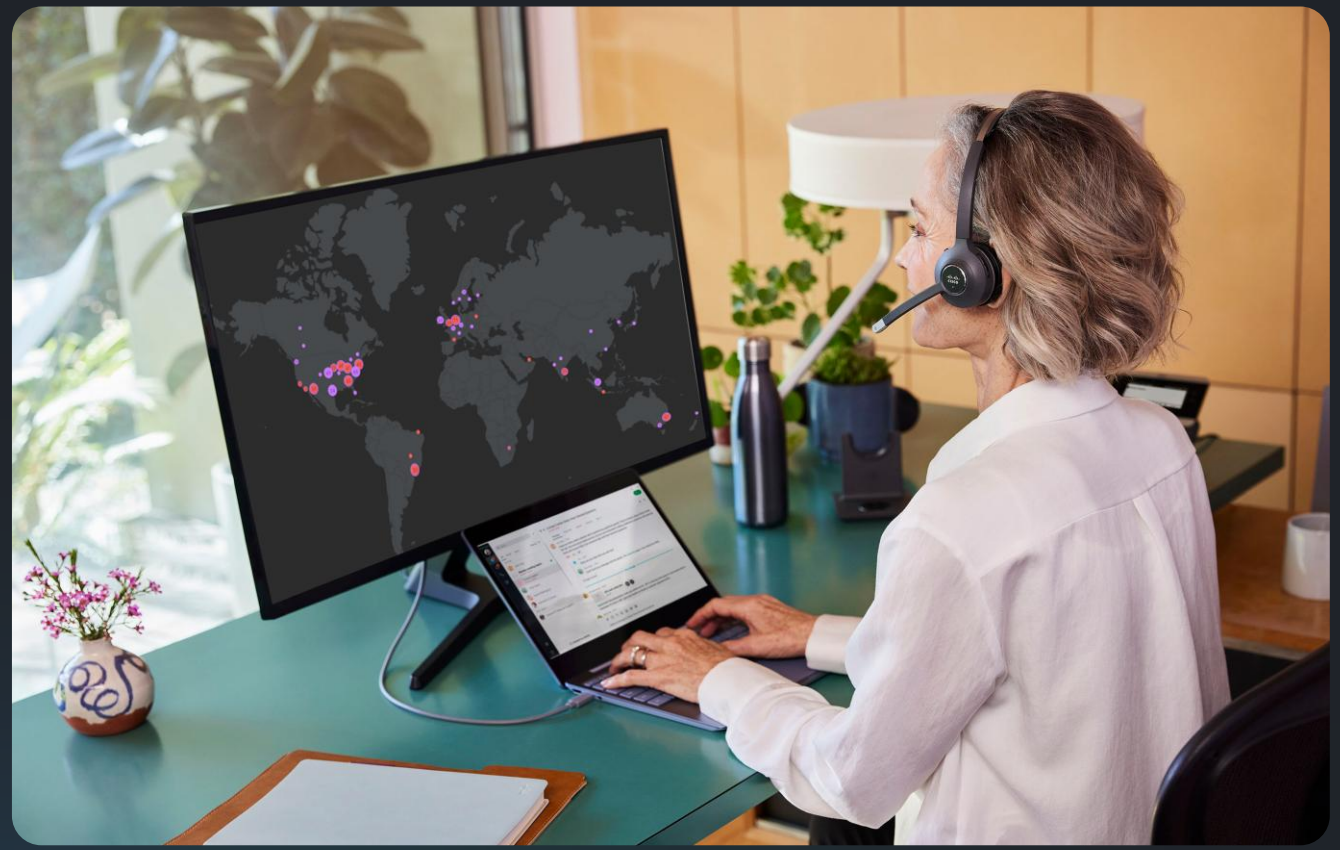


2025年第4四半期
リリース予定

ADD-ON

重要な局面でコミュニケーションを継続

障害や自然災害によるインターネットの中断時でもサイトサバイバビリティ（Meetings 向け）により途切れのないコラボレーションを実現



3

AIを活用した カスタマーエクスペリエンス

- Webex AI Agent により、音声・デジタルの両方で人間のような対話を実現
- 事前構築されたテンプレートと拡張されたLLMエンジンを活用してAI Agent を構築
- Cisco AI Assistantの活用で、エージェントの業務を最大限にサポート

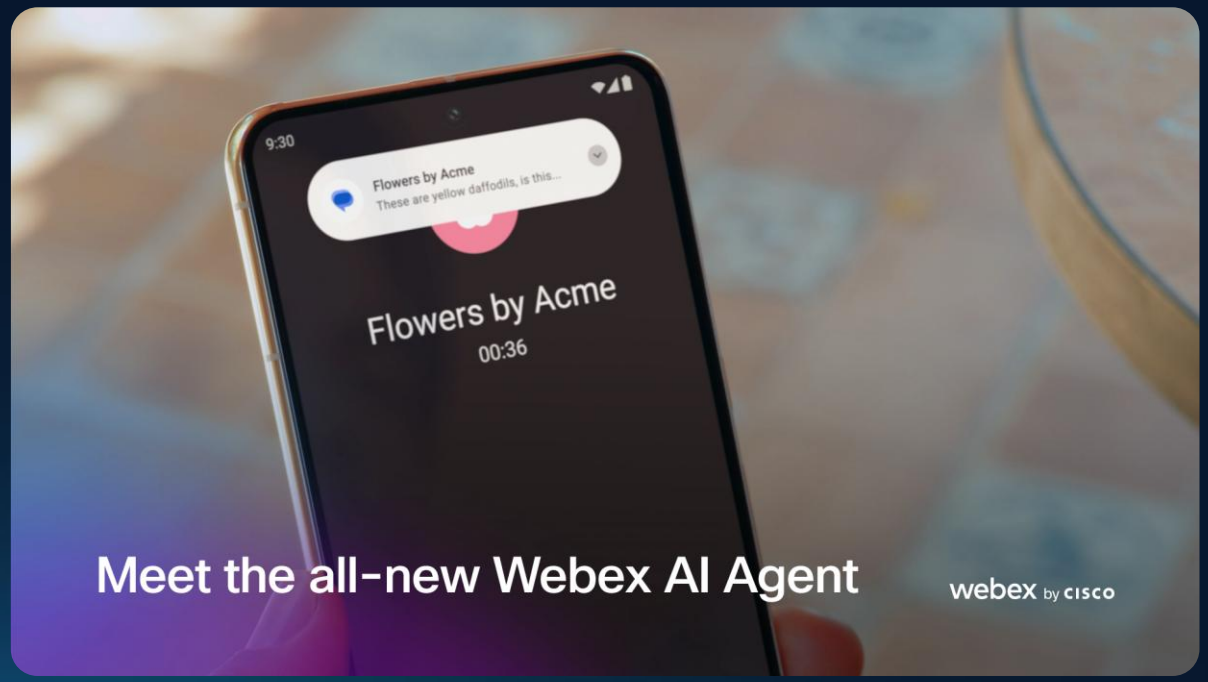
リリース済

https://youtu.be/x1vGZBSSPvs

Webex AI Agent

音声・デジタルの両方で人間のような対話を実現

- オムニチャネル・多言語対応 AI agents
- リアルタイムで顧客意図の実現
- コンタクトセンターとの統合
- 9 言語サポート

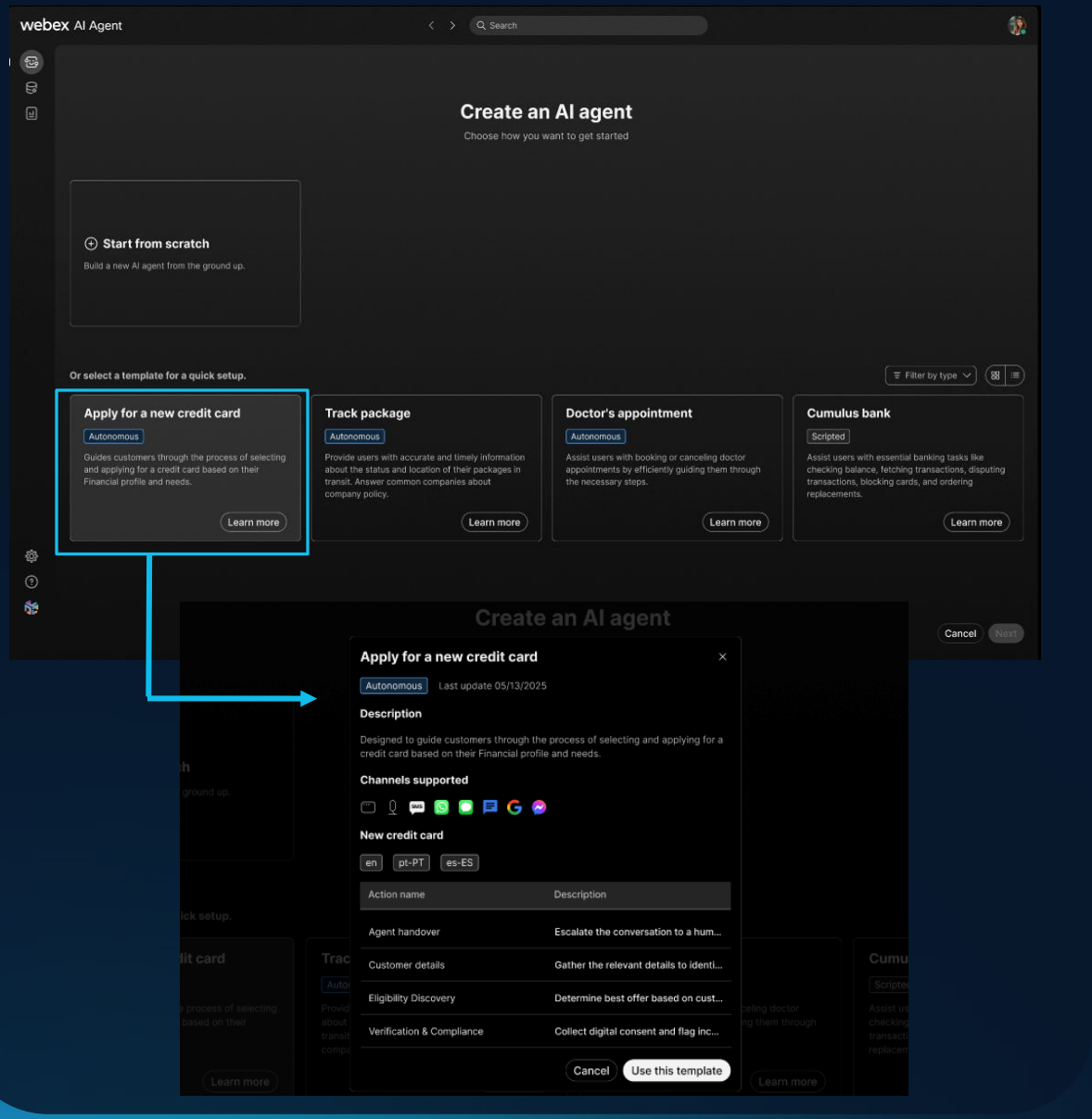


Contact Center | HR | IT | Sales | Finance | Healthcare

2025年6月
ベータ

AI Agent 作成用の柔軟なAIツール

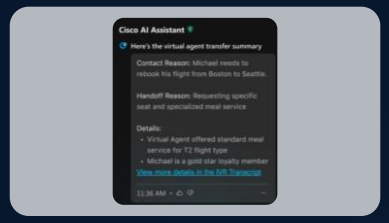
業界別ユースケース向けに拡張されたAIエンジンサポートと事前テンプレートにより、AIエージェントの構築がさらに容易に



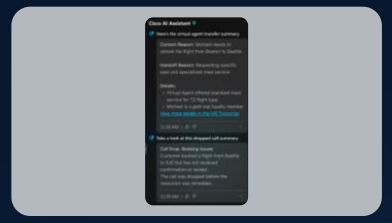
Cisco AI Assistant

継続的な機能のリリース

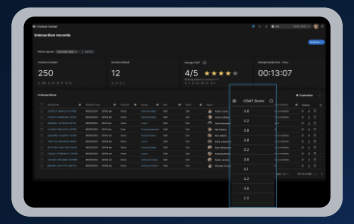
リリース済



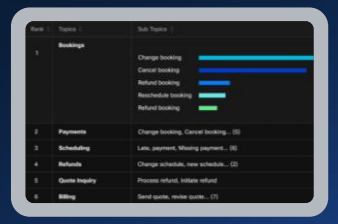
仮想エージェントの
対応引き継ぎ要約



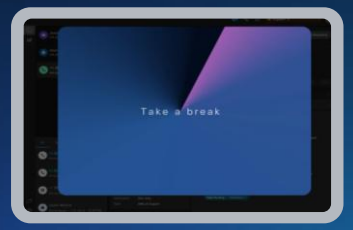
通話切断サマリー



自動
CSAT

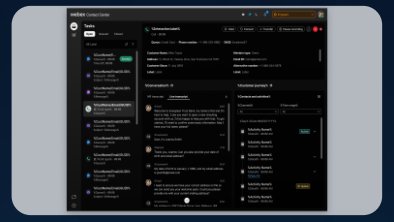


トピック分析

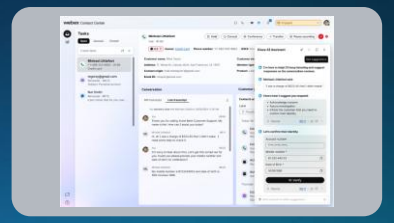


エージェント
ウェルビーイング

ベータ

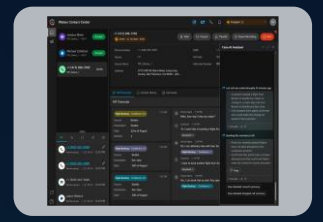


リアルタイム文字起こし
2025年第2四半期予定

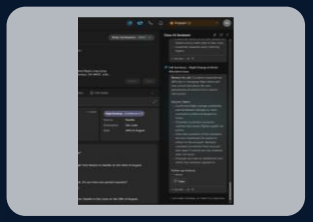


応答提案機能
2025年第3四半期予定

ベータ



転送時の要約機能
2025年第３四半期予定



ラップアップ
サマリー
2025年第3四半期予定

12 追加言語のサポート

- Dutch
- French
- German
- Italian
- Spanish
- Hindi
- Japanese
- Korean
- Polish
- Portuguese
- Chinese, Mandarin (simplified)
- Chinese, Mandarin (traditional)

2025年第３四半期予定

4

IT管理者向けに統合管理と分析

Control HubのAI管理・分析機能により、AIアシスタントの設定、利用状況の把握、傾向分析が可能に

Webex Calling と Meraki の統合により、

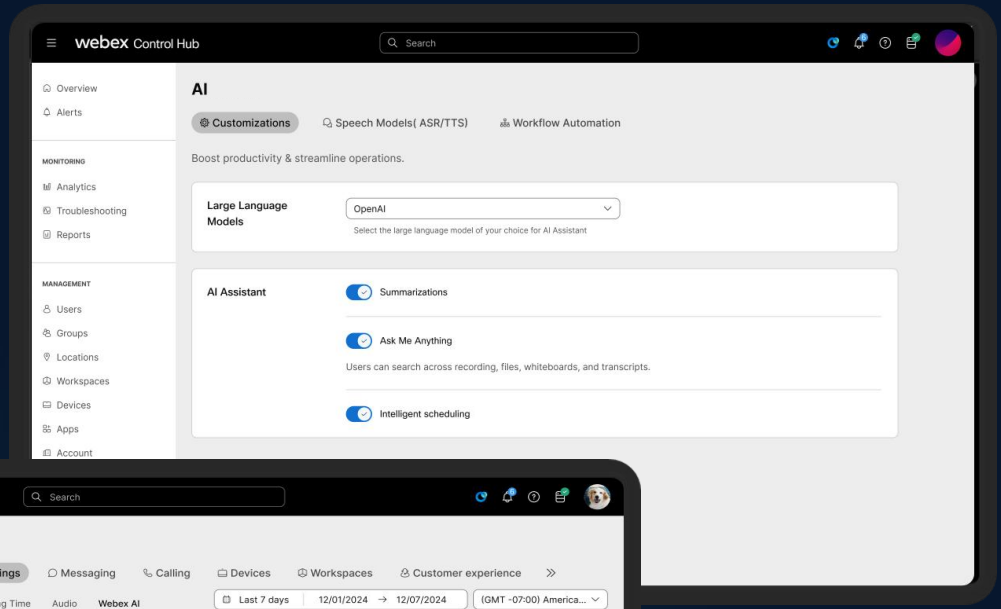
ITチームは統合プラットフォームでネットワークを効率的に一元管理・監視可能に

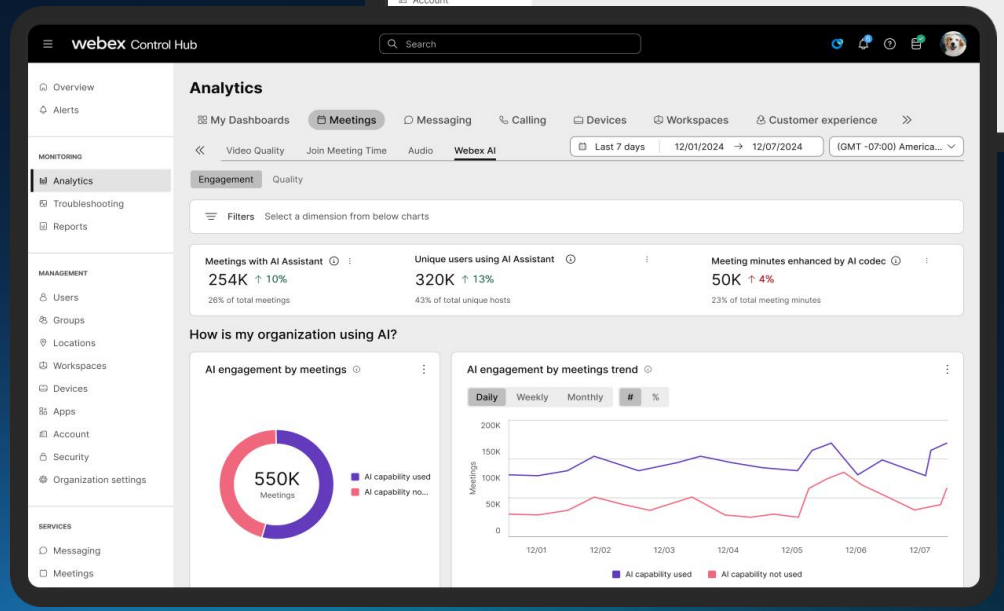
Role-based access control (RBAC)により、アクセス管理・役割の割り当て・適切な権限設定を実現

2025年第3四半期
ベータ

AI 管理と監視

Control HubのAI管理・監視機能により、
複雑なものをわかりやすく整理することで、
アクションへとつなげる

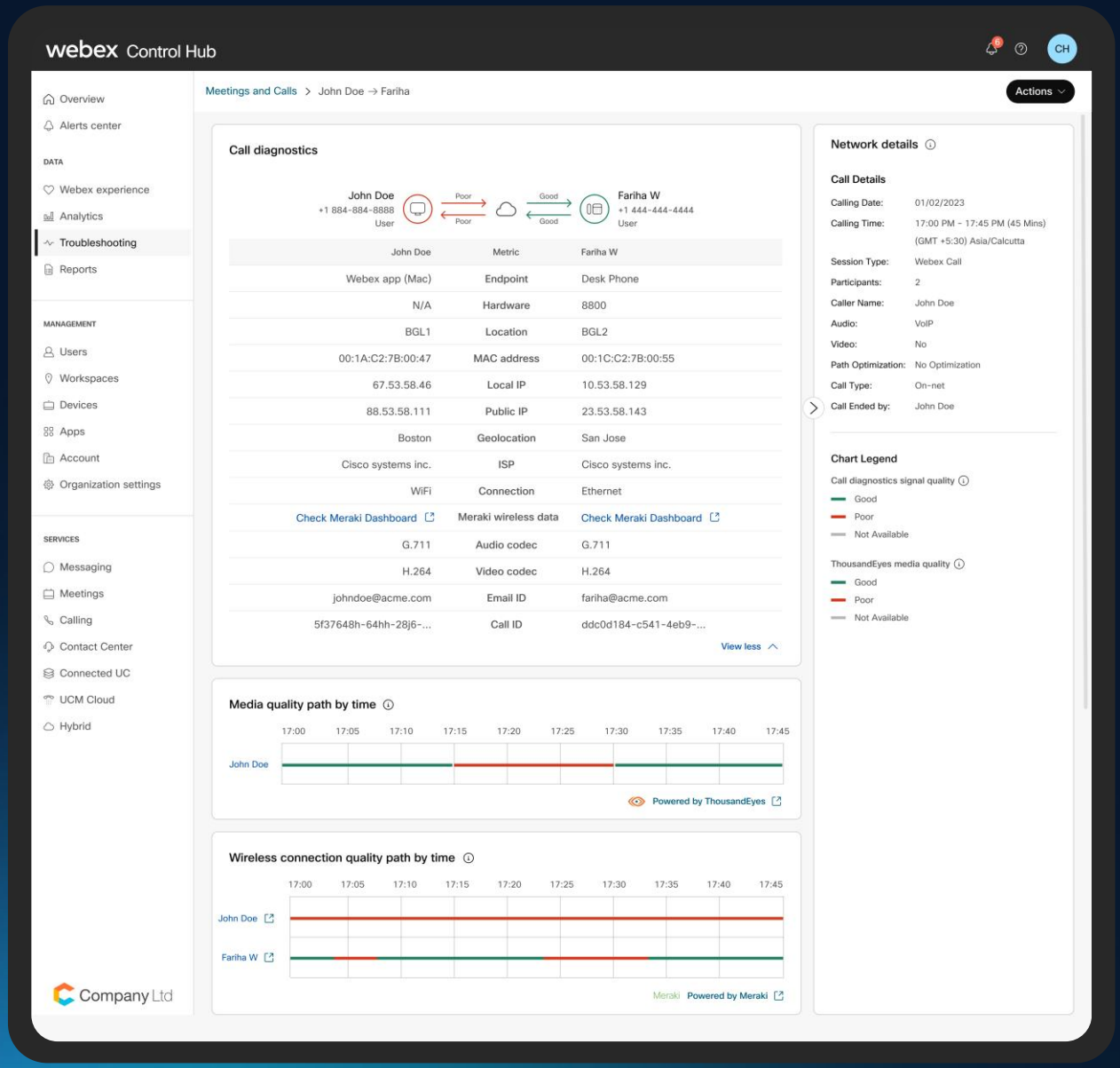




2025年6月
リリース予定

MerakiによるWebex Calling ネットワークの監視

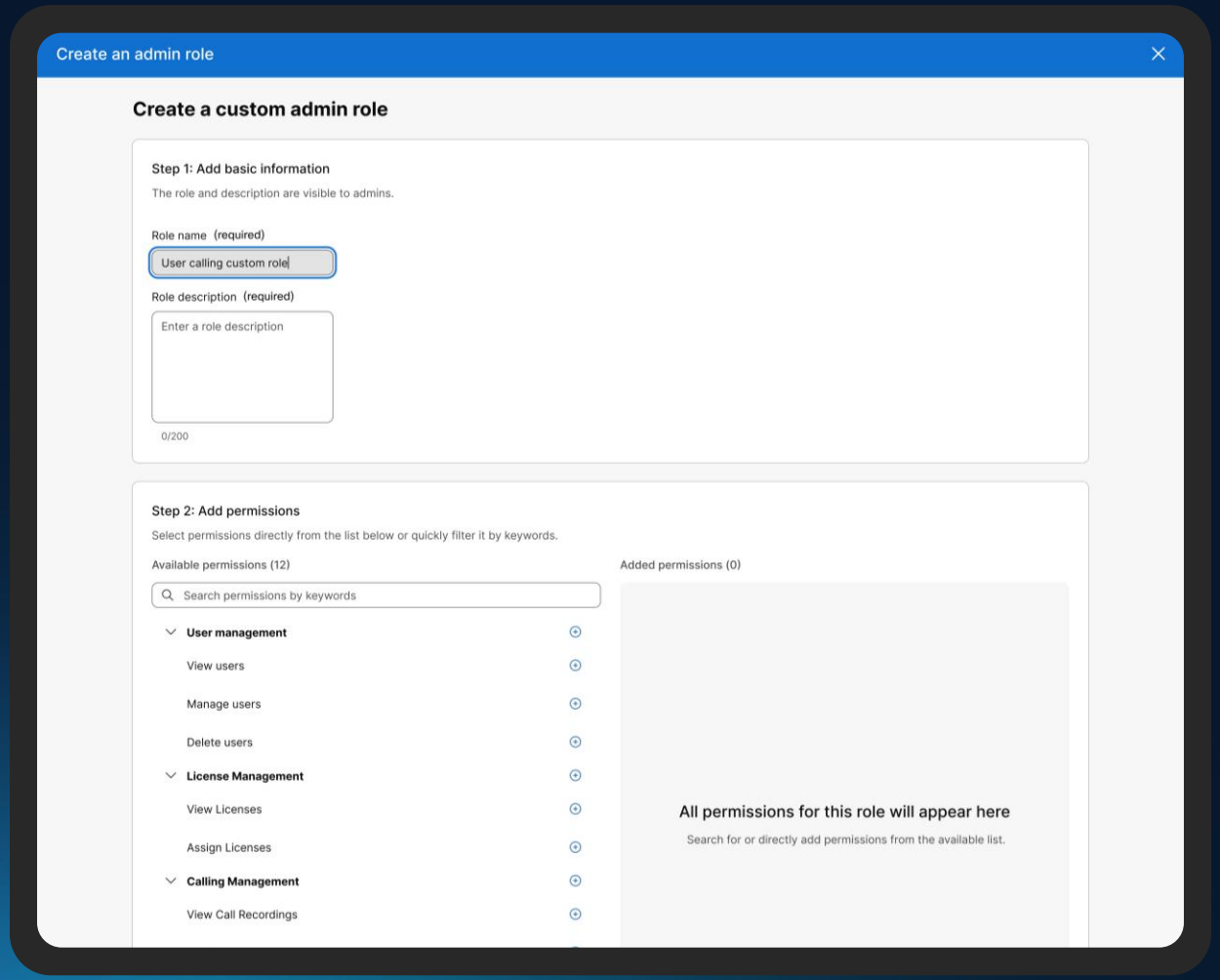
Merakiとの統合が拡張され、ITチームはControl HubからWebex Callingのネットワーク問題を効率的に診断・解決し、パフォーマンス最適化と高い信頼性を実現可能に



2025年6月
リリース予定

Control Hubでの Role Based Access Control

ビジネスのニーズに応じて、アクセス管理・役割割り当て・権限設定を簡単に実現。Webex Suite、デバイス、コンタクトセンター*で利用可能



*コンタクトセンターは2025年9月のリリース予定

Thank you