Cisco Security Summit 2026 Tokyo

AI エージェント時代のセキュリティ戦略

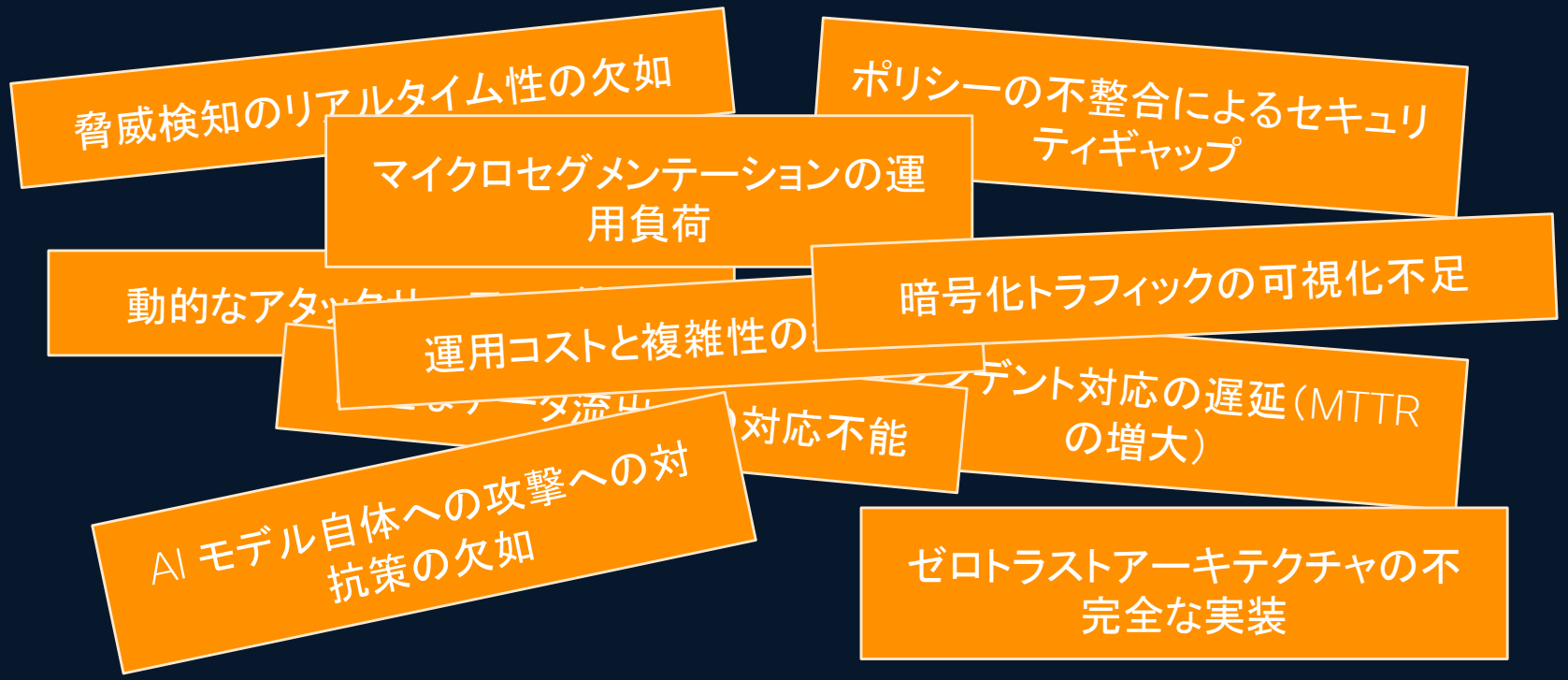
AI エージェント時代のネットワーク戦略：LAN・SASE を融合したゼロトラスト環境で実現する次世代ネットワークセキュリティ

シスコシステムズ合同会社

セキュリティ事業　クラウドセキュリティ製品担当　福留 康修

2026年7月10日

ネットワークとセキュリティの分断がもたらす致命的なリスク



セキュリティのあり方を変えつつある 3 つの要因

Mythos モーメント

防御態勢の強化

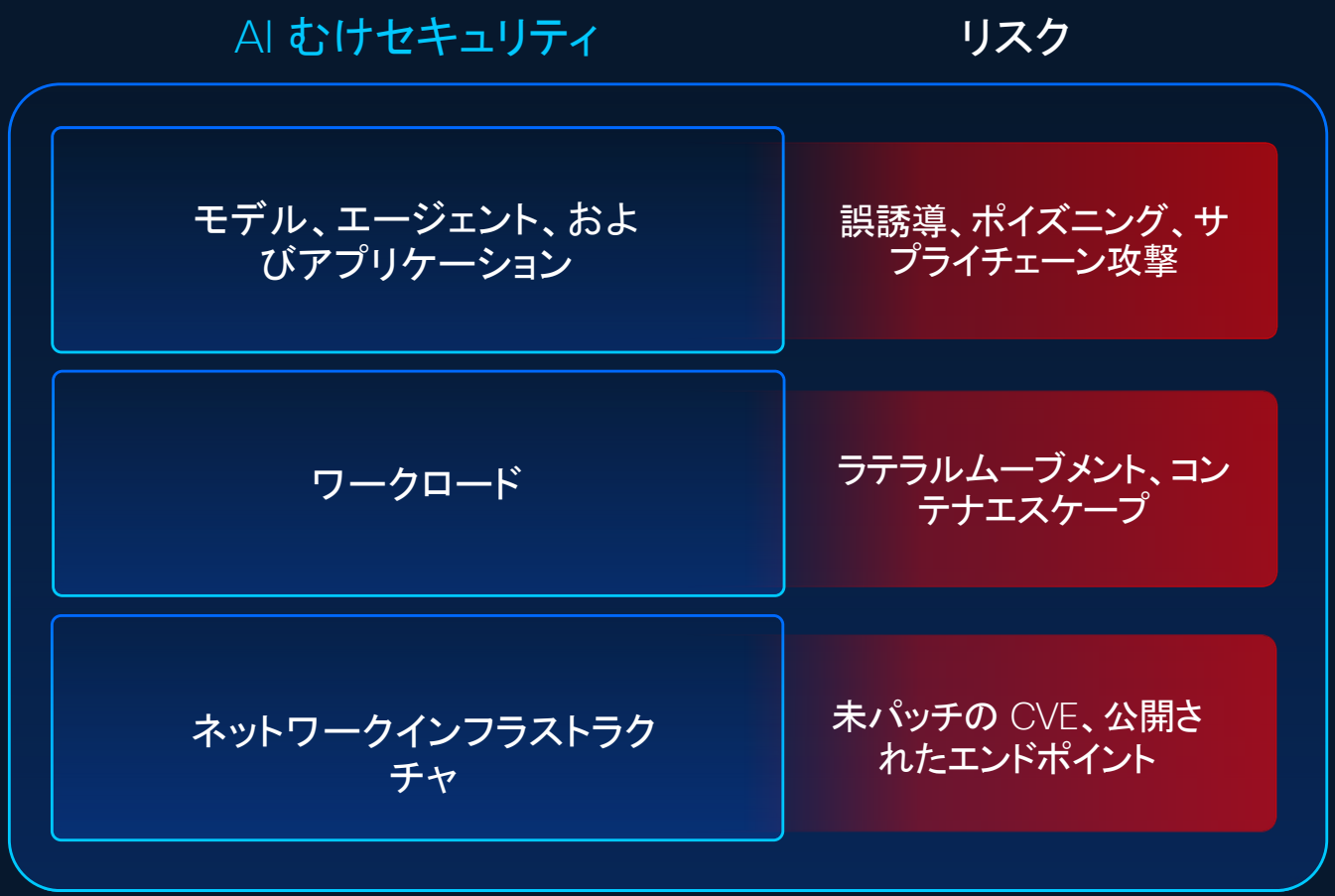
OpenClaw モーメント

エージェントのためのセキュリティ

スピードのニーズ

エージェントを使用したセキュリティ

AI のためのフルスタック セキュリティ ファブリック



防御態勢の強化 – Shields up

AI 活用型攻撃の時代における防御のためのガイダンス

基本対策の強化

フィッシング耐性のある MFA（多要素認証）、ゼロトラスト、最小権限（AI エージェントを含む）、規律あるパッチ管理、包括的なアセットの可視化

構造的リスクの排除

サポート終了システムの排除、メモリ安全性およびエクスプロイト対策を備えた最新プラットフォームへの置き換え、継続的なアップグレードを前提とした設計

マシンスピードでの自動化

検出、トリアージ、封じ込めの自動化への投資（AI 活用型攻撃速度への対応）

アクティブ防御の組み込み

ワークロード、デバイス、トラフィック経路への防御機能の組み込み（eBPF によるランタイム制御、インライン適用、個別にアップデート可能なエクスプロイト対策など）

防御のための AI 活用

脅威ハンティング、適合性テスト、デジタルツイン、検証に AI を活用（展開サイクルを数か月から数日へと短縮）

基本的な管理策と適応型のリアルタイム防御能力のバランスを両立

https://www.cisco.com/c/m/ja_jp/about/doing_business/trust-center/cisco-defending-against-ai-attacks-guidance.html

防御の最前線はファイアウォール

暗号化された脅威の早期検出

シスコ暗号化可視性エンジン

インラインでゼロデイ脅威を検知

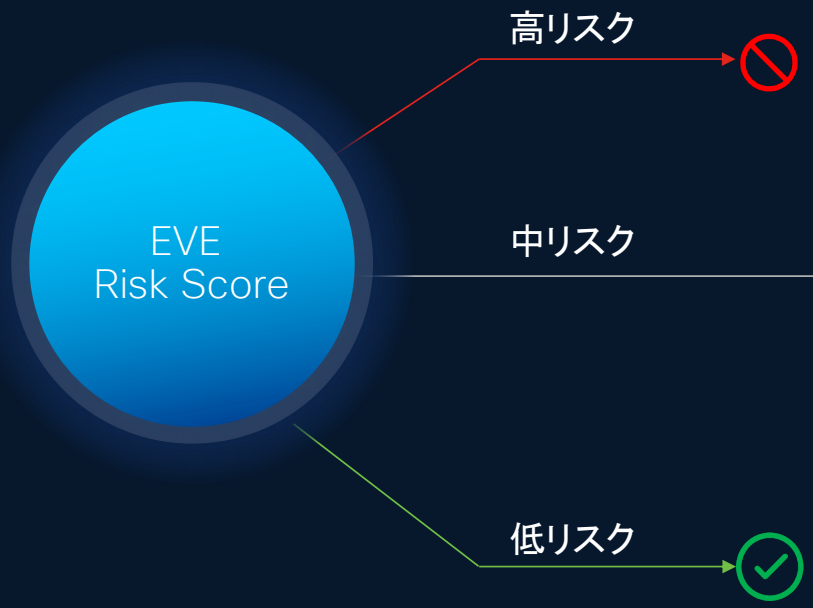
脅威インテリジェンス

インテリジェントな　セグメンテーション

ネイティブな統合

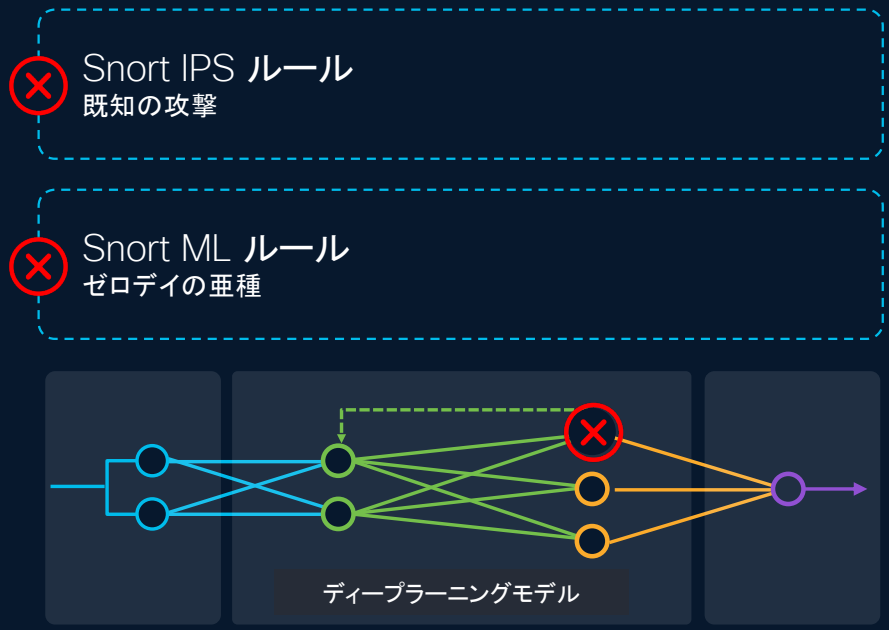
次世代型トラフィック検査と防御

暗号化されたトラフィック内の悪意のあるフローを、復号することなく可視化



Cisco Encrypted Visibility Engine (EVE)

一般的な攻撃の未知の亜種に対しても IDPS の保護機能を拡張



Powered by TALOS Intelligence

Kubernetes で動作する AI

プロセスの非表示
ログイン情報の収集
特権昇格
コンテナエスケープ
カーネルのエクスプロイト
ファイルの改ざん
サイドカーインジェクション
シェルインジェクション
ネットワークスキャン
リバースシェル

セグメンテーション

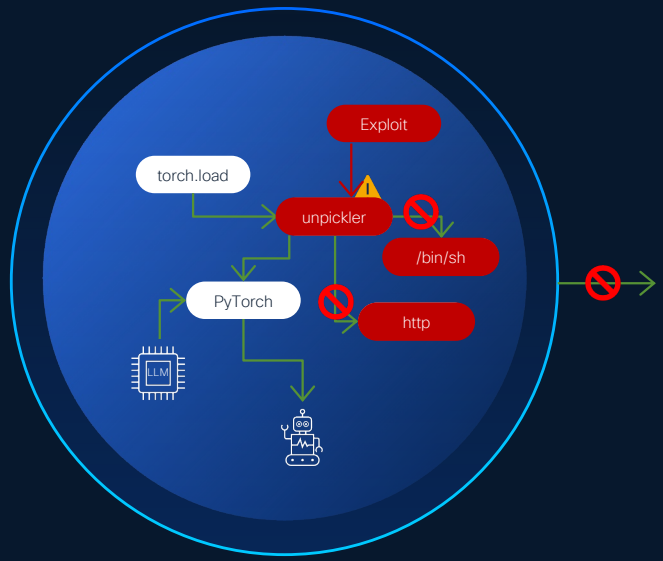
ランタイムシールド

ホストファイルシステムへのアクセス
サービスの発見の悪用
API サーバーのプロービング
トークンの窃取
Init コンテナの悪用
DNS トンネリング
逆シリアル化
未認証のサービス
ランタイムソケットの露出
コマンドインジェクション

プロセスレベルの可視性

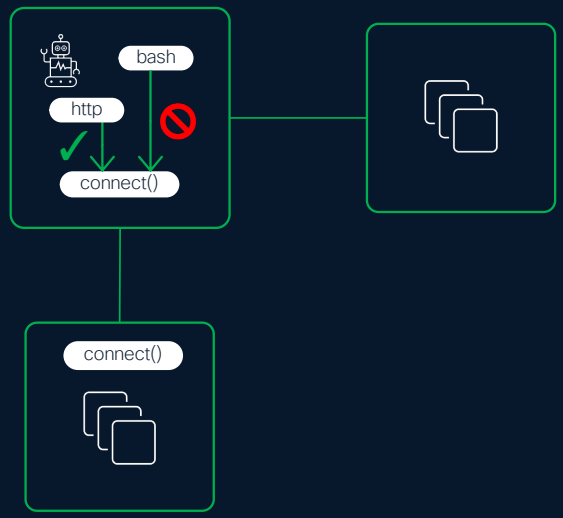
あらゆるレベルでのセグメンテーション

プロセスの挙動監視によって脅威をブロック



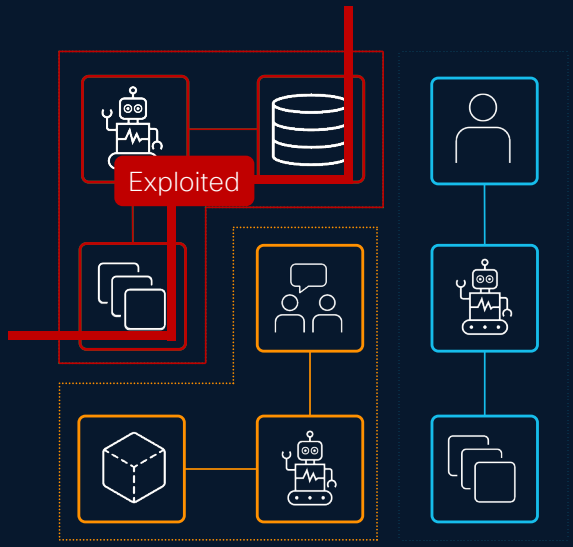
エクスプロイト阻止

きめ細かなマイクロセグメンテーション



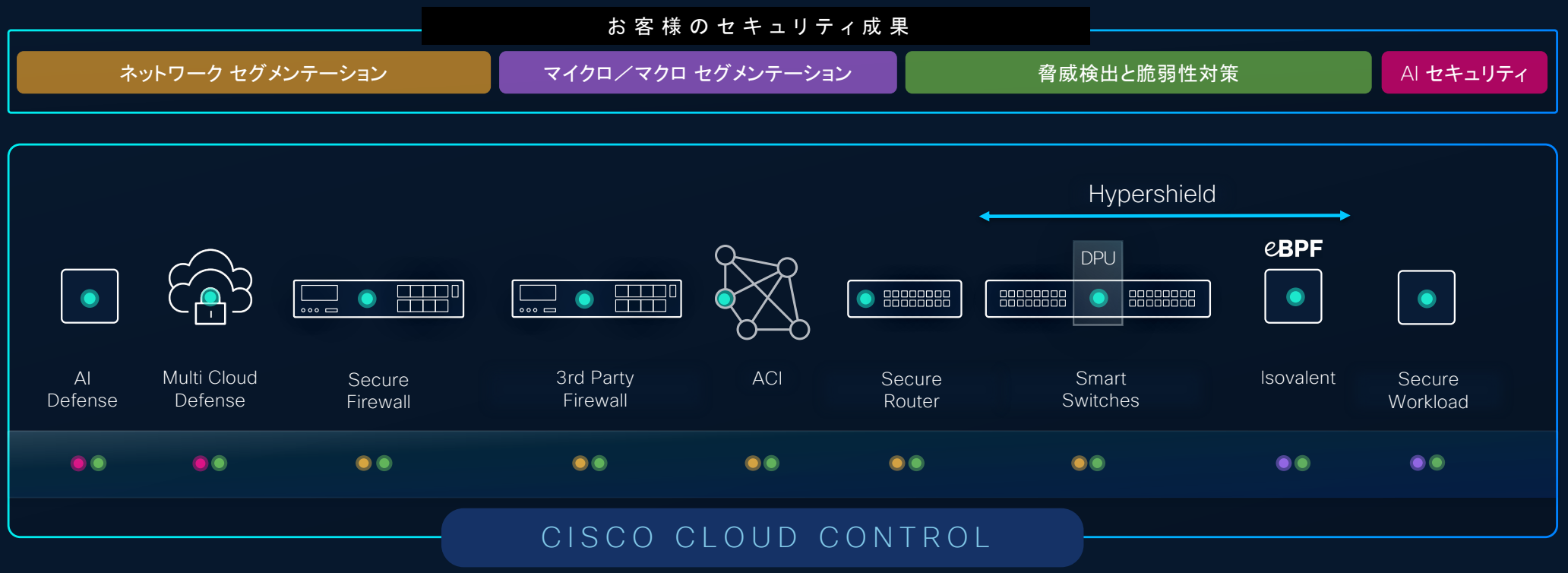
プロセス セグメンテーション

ゾーンベースのセグメンテーションにより、影響範囲を限定



ネットワーク セグメンテーション

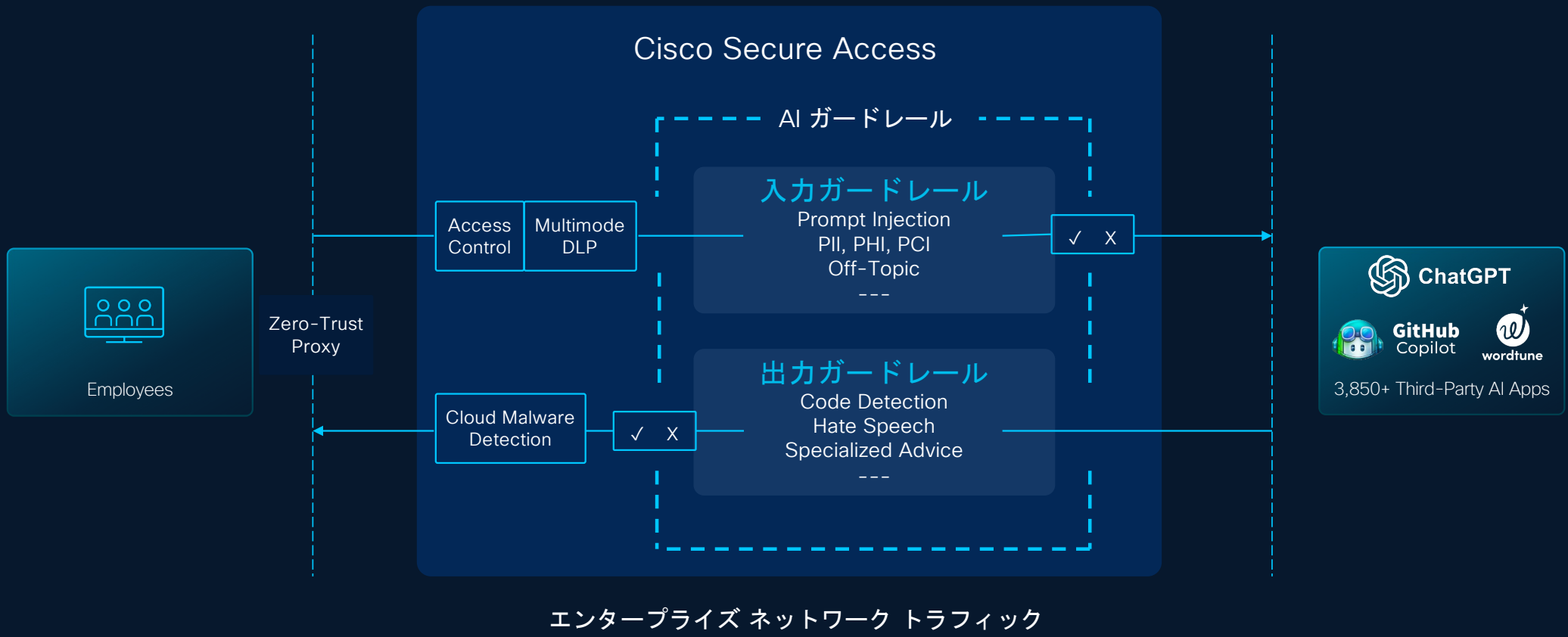
Cisco Hybrid Mesh Firewall



一度作成したポリシーをメッシュ全体に適用

Secure Access の機能

サードパーティ AI App 保護 – AI Access ポリシー



エンタープライズ ネットワーク トラフィック

エージェントにもゼロトラストを提供する Cisco SASE

Duo ＋ MCP Gateway 機能 セマンティック インスペクション

きめ細かな権限設定

セキュアな AI エージェント開発への 3 段階のフレームワーク

検出

モデル、エージェント、データセットなどの AI 資産を特定

検証

AI リスク、脆弱性、攻撃への耐性をテスト

保護

データを保護するガードレールを定義し、ランタイムの脅威から防御

Cisco Security Cloud Control による一元管理

カスタムエージェントと AI アプリケーションの保護

Cisco AI Defense

検出

新機能

適応型レッドチーミングと
カスタムガードレール

検証

新機能

エージェントのサプライ
チェーン全体を保護

保護

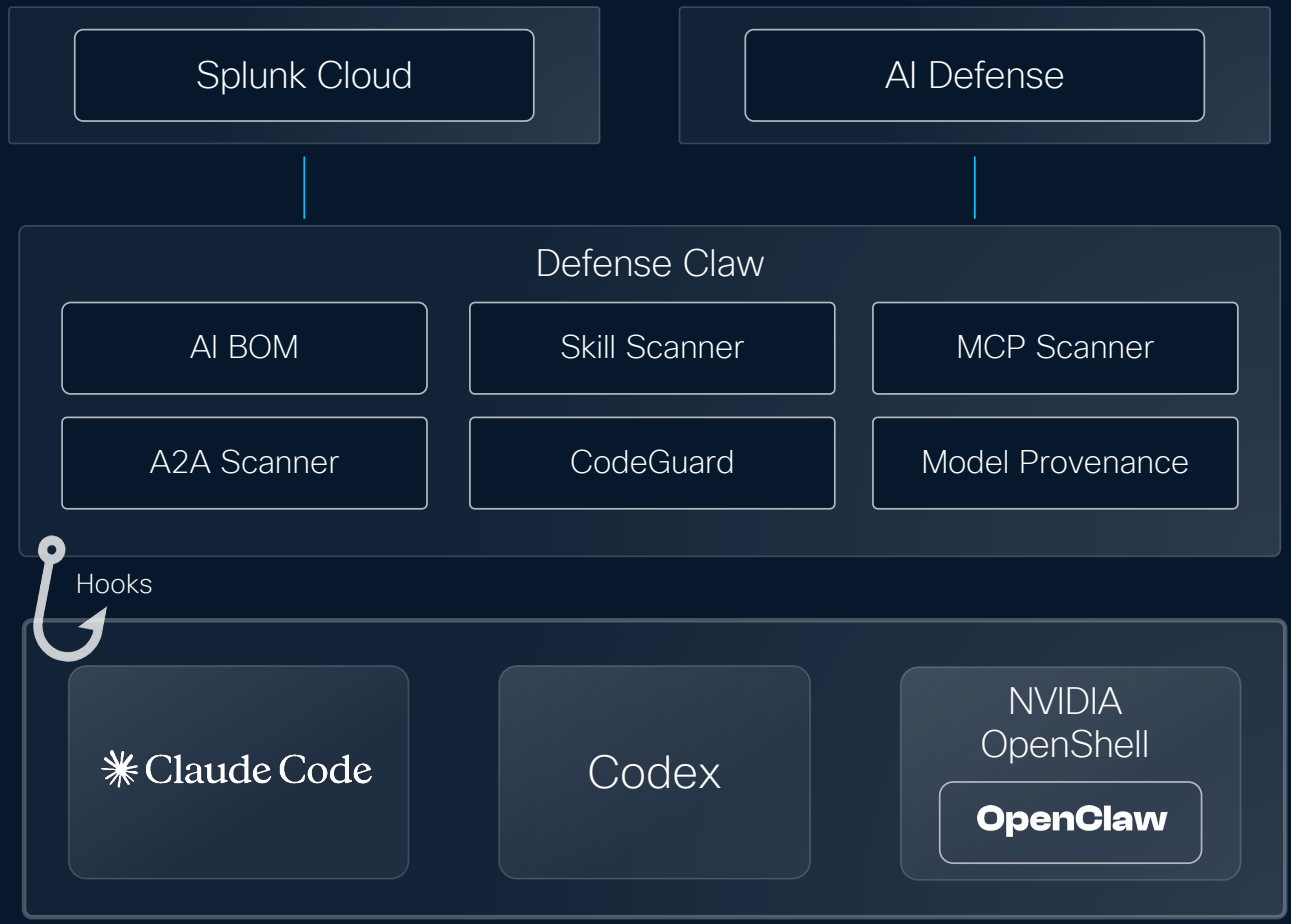
新機能

あらゆるクラウド、
あらゆる GPU に対応
するエコシステム

AI エージェントの保護：DefenseClaw

- エンタープライズのエージェント ガバナンス
- 堅牢なワークフロー検証
- エージェンティック・セキュリティ・オブザーバビリティ

- OpenClaw、Claude Code、Codex に対応
- エンタープライズ ガバナンスレイヤ
- オープンソースとして利用可能
- 近日 Cisco Secure Client の一部として提供予定



エージェントはさまざまな方法で導入

まとめ

- AI を意識したネットワーク (AI-Aware Network)
- ネットワーク セグメンテーションの必要性
- Cisco Cloud Control によるネットワークとセキュリティ運用統合
- AI エージェント時代のリスクとフルスタック防御の重要性
- 分散化した環境を SASE を含むメッシュ型セキュリティでフルカバー
- AI エージェントのライフサイクル保護 (Cisco AI Defense 他)


CISCO