

One Cisco : エージェント時代を守るセキュリティ

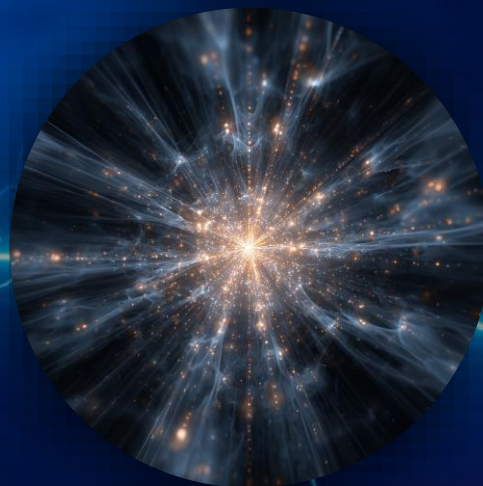


Dave West、SVP（グローバルスペシャリスト）

私たちは今、**きわめて重要な局面**に立っています



チャットボット
生産性向上ツール



エージェント
デジタル同僚



物理
ロボットとセンサー

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

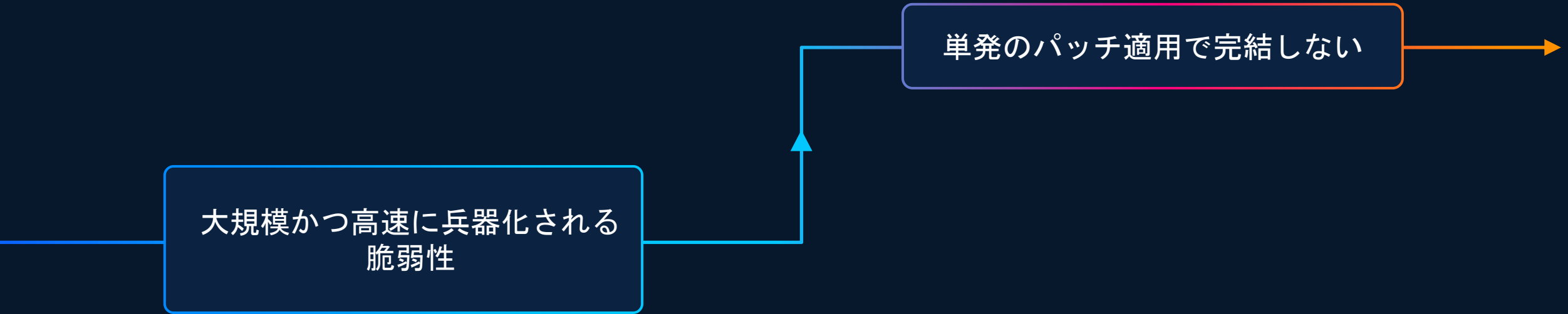
求められる スピード

→ エージェントを使用したセキュリティ

防御態勢の強化

パッチ適用だけでは不十分。

フロンティアAIモデルがもたらす新たな次元のリスク



脆弱性の悪用までの平均時間

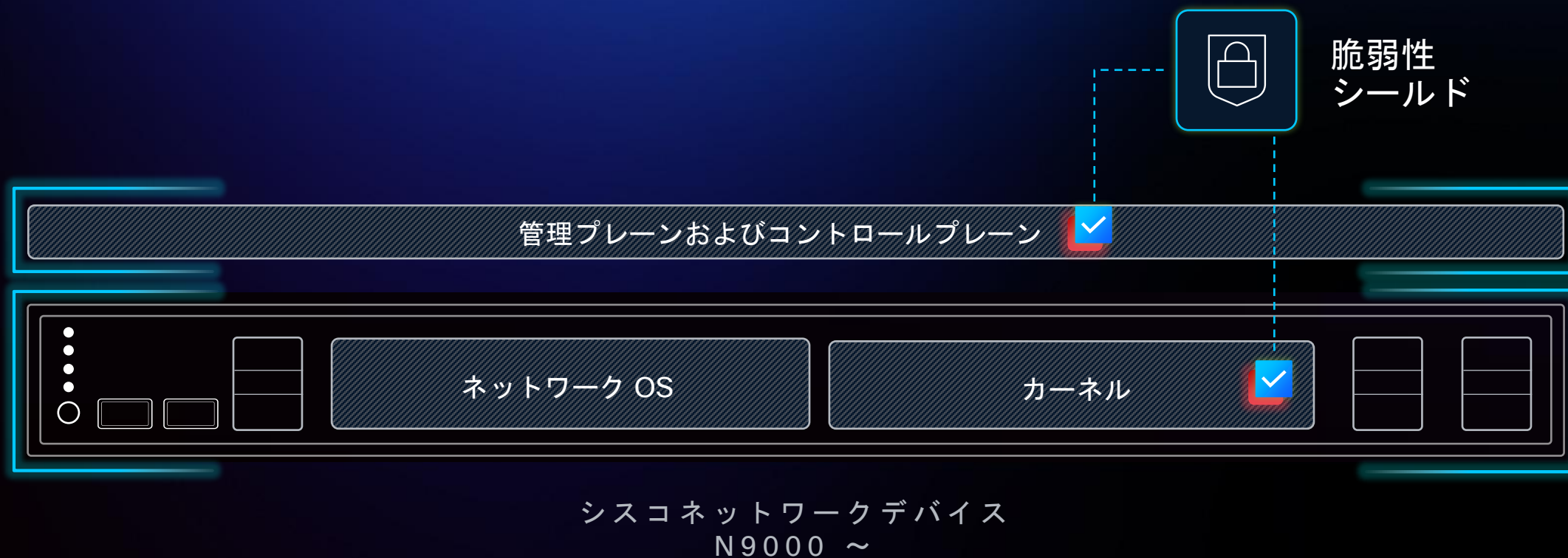
2018
2.3 年

2023
4.2 ヶ月

2025
21.5 日

2026
8 時間

Live Protect



実稼働システムへの
ポリシー適用

即時保護、パッチ適用は
計画期間内

ダウンタイムや
スイッチの再起動なし

継続的な
再検証

セキュリティ態勢の強化

課題: 悪用ウィンドウの数時間以下への短縮 不要なアクセスによる脆弱なシステムと横展開経路の露呈 隠れたIDの脆弱性による侵害の拡大 アナリストの対応を上回る攻撃スピード

解決策:  脆弱性の特定とシールド  分散型セグメンテーションと封じ込め  IDの可視化とセキュリティ  エージェント型セキュリティ運用（SOC）

- シスコの支援:
- | | | | |
|---|---|--|--|
| <ul style="list-style-type: none">• Live Protect• Snort IPS• Splunk Exposure Analytics• Cisco IQ | <ul style="list-style-type: none">• Identity Services Engine• Smart Switches• Hybrid Mesh Firewall• Zero Trust Network Access (SASE) | <ul style="list-style-type: none">• Identity Intelligence• Duo IAM• Identity Services Engine• Splunk Exposure Analytics | <ul style="list-style-type: none">• Cisco Data Fabric• Splunk Enterprise Security• Talos threat intelligence |
|---|---|--|--|

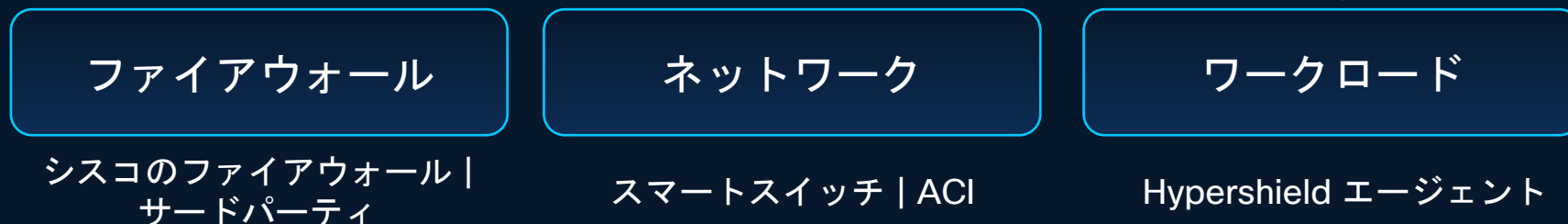
← Cisco Cloud Control と AgenticOps による運用効率化 →

AI を含む、アプリケーションとインフラストラクチャの保護

Cisco Cloud Control



メッシュ



エージェントのためのセキュリティ

エージェントはあらゆる場所に存在し、あらゆるものにアクセスする。そして、エージェント自体が新たな攻撃対象となる。

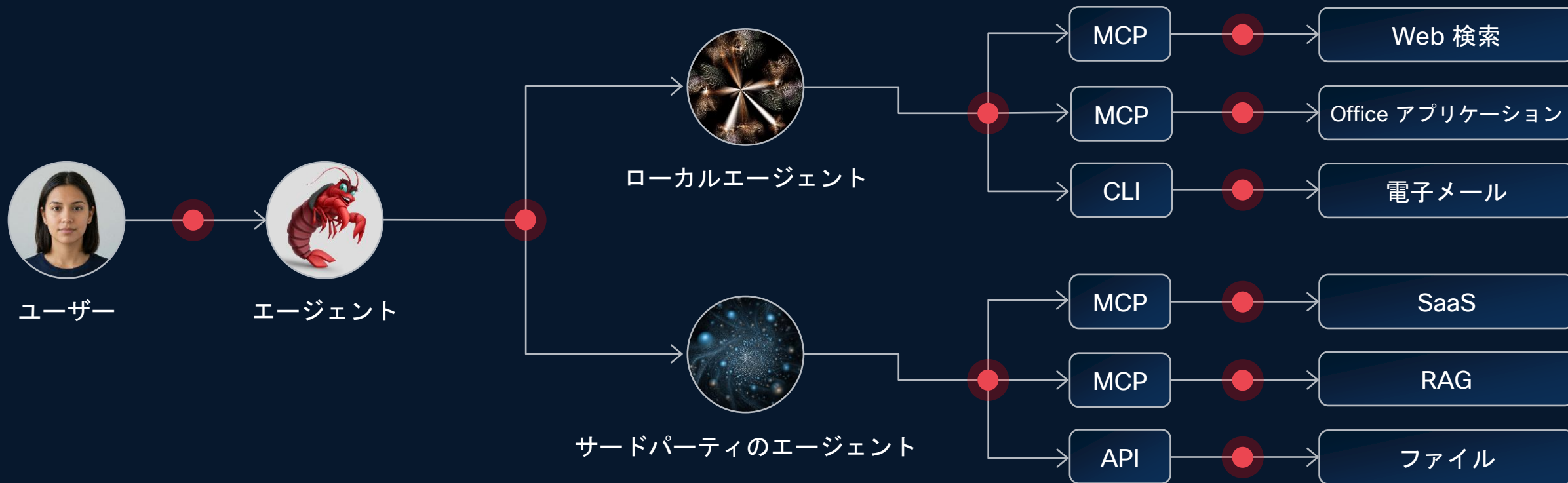
エージェントのためのセキュリティ

世界から
エージェントを守る



エージェントから
世界を守る

マシンスピードでの
検出と対応



エージェントのためのセキュリティ：世界からエージェントを守る

エージェントのためのランタイム保護



Zero Trustの進化



人

アクセス

PROVE IDENTITY.
TRUST THE USER.



エージェント

アクション

VERIFY BEHAVIOR.
CONTROL THE AGENT.

主要な買収による成長の加速



Non-human and agent identity



Agent observability & trust

求められるスピード

攻撃者はマシンスピードで行動するため、
手動対応では追いつかない。

求められるスピード

リスクを把握し、迅速に対処



脆弱性



マシンスピードで
行われる攻撃



フィッシングおよび
組織内に潜む脅威

Splunk ソリューション



リスク分析と
リスクポスチャ



エージェント型 SOC



フィッシング脅威の
自動修復



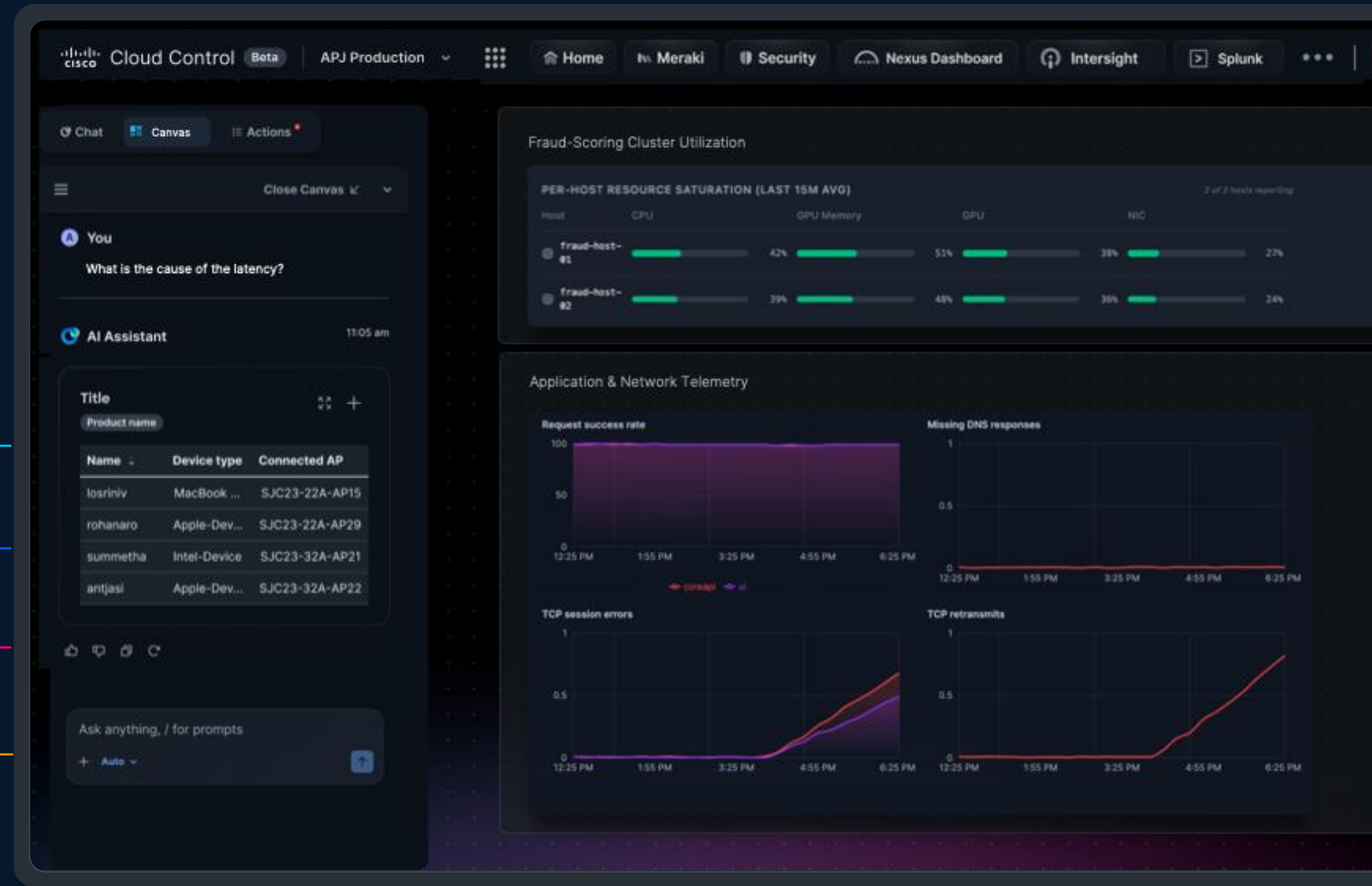
日常業務の効率化

ネットワーク

セキュリティ

アイデンティティ

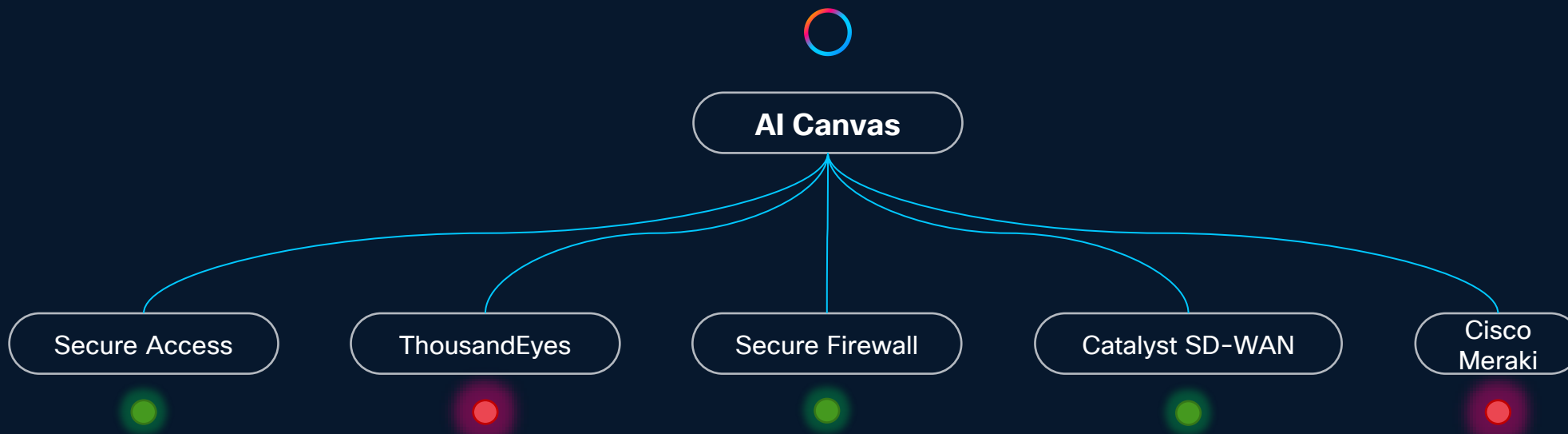
Splunk



1 回の調査で、すべてのドメインを網羅

Salesforce のユーザー体験が遅い理由は何ですか？

+ 自動 ▾



SECURE NETWORKING

AIスケールの運用には、
AIスケールのセキュリティと可視性が
不可欠です。

ネットワークは 結合組織

セキュリティ

Secure Networking：ネットワークに融合したセキュリティ



復元力の高い
インフラストラクチャ



アイデンティティ



セグメンテーションと
ステアリング



保護



可視性と
インサイト

シスコのセキュリティ



ありがとうございました

