

Cisco **Security**

Cisco Security Summit Tokyo 2025

企業の境界線を再定義する

新たな防御ライン *Cisco Hybrid Mesh Firewall*



セキュリティ事業 SE本部長

中村 光宏

Aug 5, 2025

Agenda

1. 業界の動向：ハイブリッドセキュリティの進化
2. Hybrid Mesh Firewall：ビジョンと基盤
3. Hybrid Mesh Firewall：アーキテクチャ
4. Hybrid Mesh Firewall：各機能（抜粋）
 - ① 最新の脅威からの保護
 - ② ラテラルムーブメントを阻止
 - ③ 脆弱性のギャップを解消
 - ④ シンプルな統合管理
 - ⑤ AIトランスフォーメーションを保護
5. Hybrid Mesh Firewall：ユースケース
6. まとめ

本日のテーマ

今日の脅威に対処するためにファイアウォールを進化させる必要がある理由

スマートスイッチによる
セグメンテーションの簡素化戦略

AIアプリケーション保護戦略

ネットワークの攻撃サーフェスはますます拡大している...

拡大



複雑

不透明



顧客の課題を解決する

- 従来のファイアウォールでは、最新のクラウドベースのアプリケーションやネットワークを保護できない
- ゼロトラストは管理の複雑さを増大させる
- ラテラルムーブメントを防ぐ為のセグメンテーションが難しい
- 攻撃者はパッチ適用よりも早く脆弱性を悪用する
- AIモデルとアプリケーションが新たなセキュリティの盲点を生む

業界の動向：

ハイブリッドセキュリティの進化

ハイブリッドセキュリティ = Hybrid Mesh Firewall

ハイブリッド メッシュ ファイアウォールは、ハイブリッド環境向けに設計された中央集約型のクラウドベース管理機能を備えたマルチデプロイメント ファイアウォール プラットフォームです。CI/CD パイプラインとの統合、クラウドネイティブ機能のサポート、IoT や DNS ベースの脅威を含む多様なユースケースにおける高度な脅威保護を提供します。

Hybrid Mesh Firewall – なぜ必要か？



ネットワーク



プライベート
DC



クラウド



クラウド
ネイティブ

組織的な課題



NetSec Admin



Server/VM Admin



Cloud Architect



DevSecOps

複数のチーム、組織、
および環境



環境間で一貫性のな
いポリシー制御の山



Gartner – Hybrid Mesh Firewall

コア機能とオプション機能

Gartner

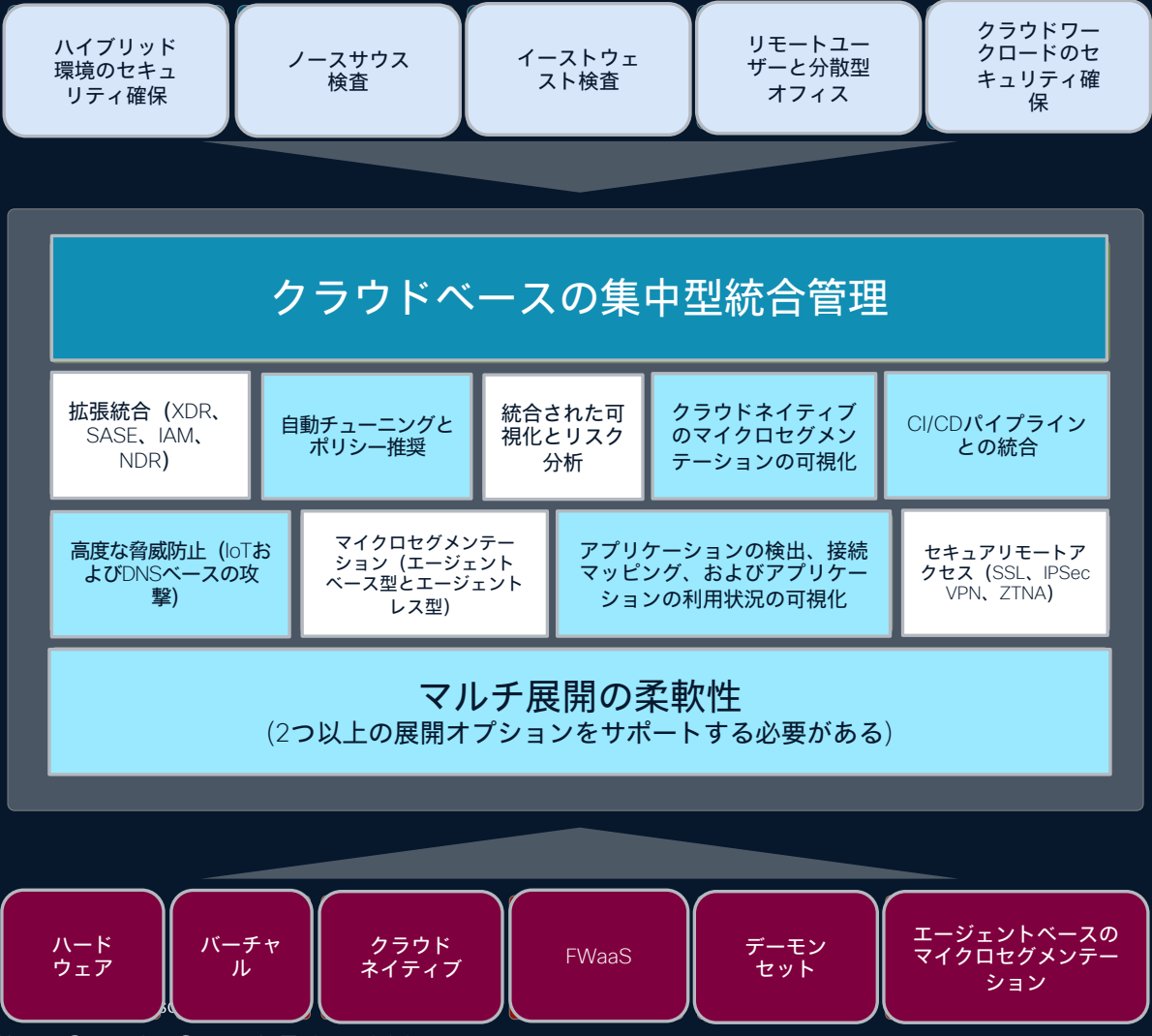
Gartner

Market Guide for Hybrid Mesh Firewall Platforms

Published 16 January 2024 - ID G00794201 - 15 min read

By Analyst(s): Rajpreet Kaur, Adam Hills

Initiatives: [Infrastructure Security](#); [Build and Optimize Cybersecurity Programs](#)



Cisco Hybrid Mesh Firewall :

ビジョンと基盤

シスコのビジョン – Hybrid Mesh Firewall

Our North Star

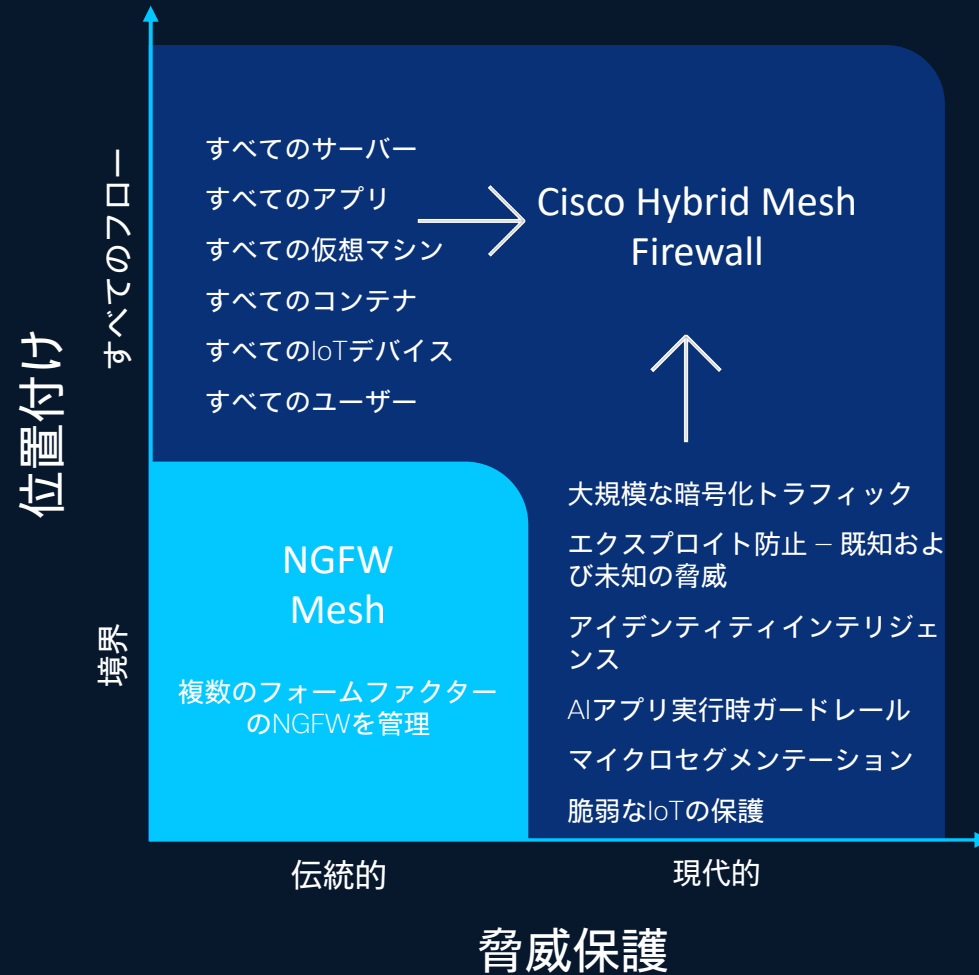
組織が簡単に利用できるように

Reduce アタックサーフェス

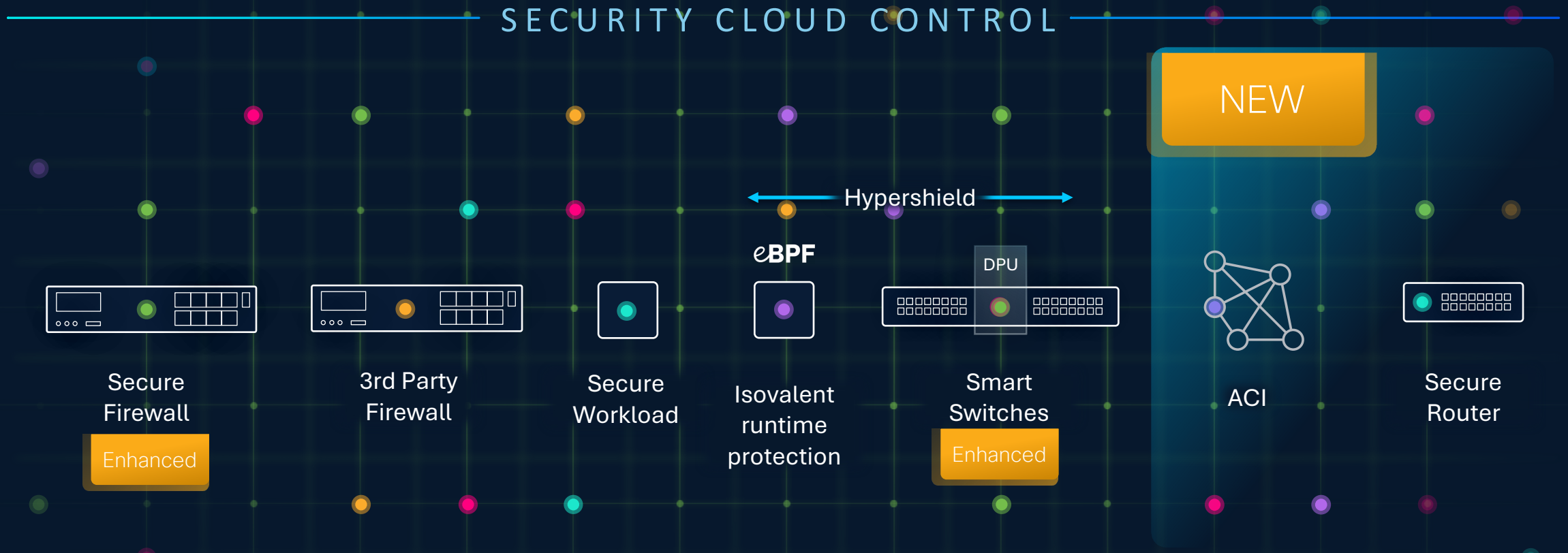
Prevent 侵害

Stop ラテラルムーブメント

現代のデータセンター、クラウド、キャンパス、および工場において



Cisco Hybrid Mesh Firewall



一度ポリシーを書けば、メッシュ全体に一気に適用

NEW

シンプルで将来性のあるライセンス体系

Cloud protection suite

Gateways

Workloads

Secure
Firewall

Multicloud
Defense

Secure
Workload

Isovalent
Enterprise

Hypershield

Security Cloud Control

一度ポリシーを書けば、メッシュ全体で一気に適用

Cisco Firewalling

AI Defense

3rd Party Firewalls

Secure Firewall | Secure Workload | Hypershield
Secure Access (FW as a service) | Secure Router NGFW



Unified AI Assistant:
ポリシー管理を最大70%簡素化

NEW

Security Cloud Control

マルチベンダー対応のインテントベースポリシーの導入



既存のルールを吸収し
最適化

ポリシーではなく
適用ポイントを変更

リプレイス不要

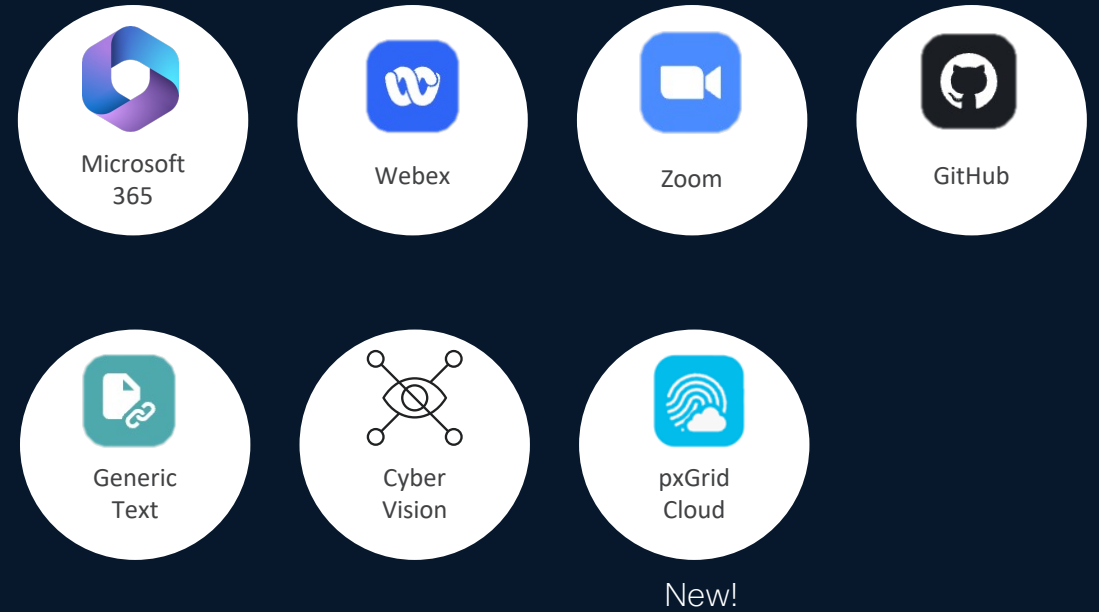
Cisco Hybrid Mesh Firewall : アーキテクチャ

Cisco Secure Dynamic Attribute Connectors

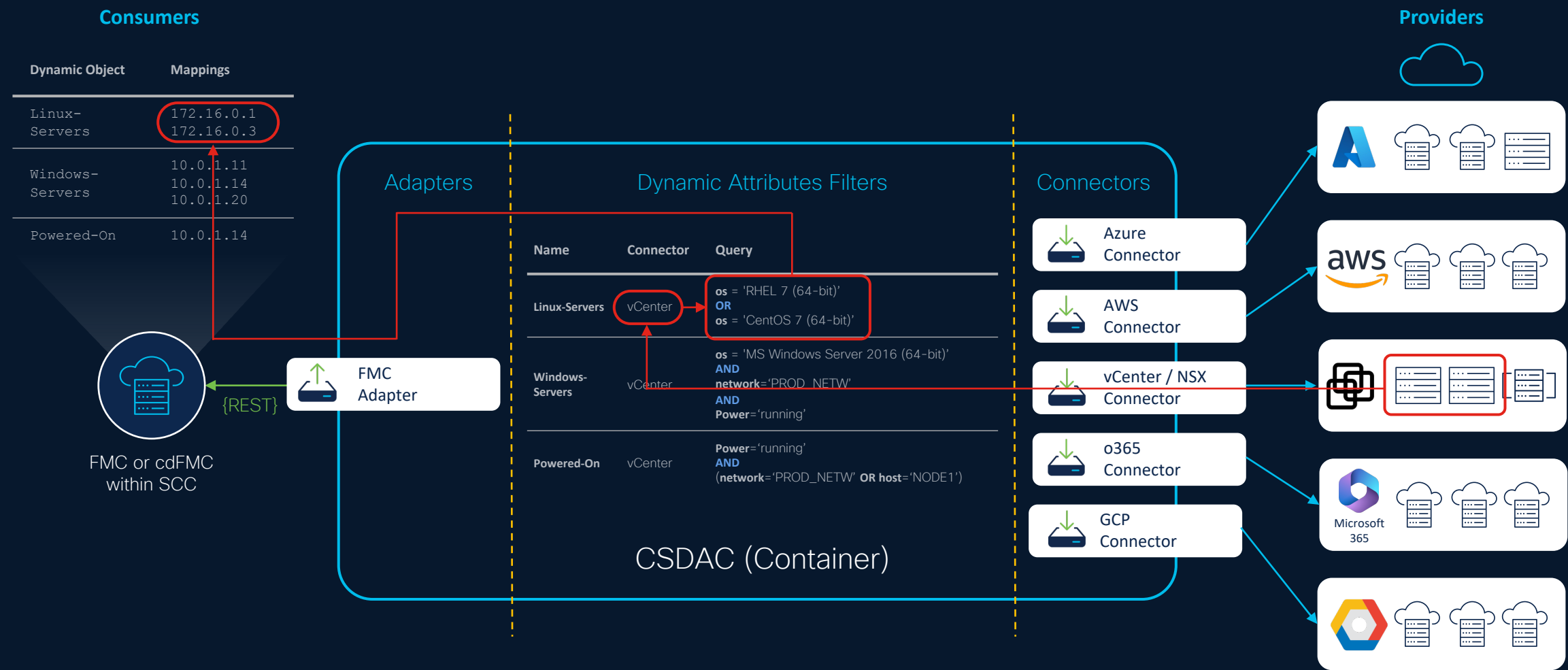
クラウドコネクタ



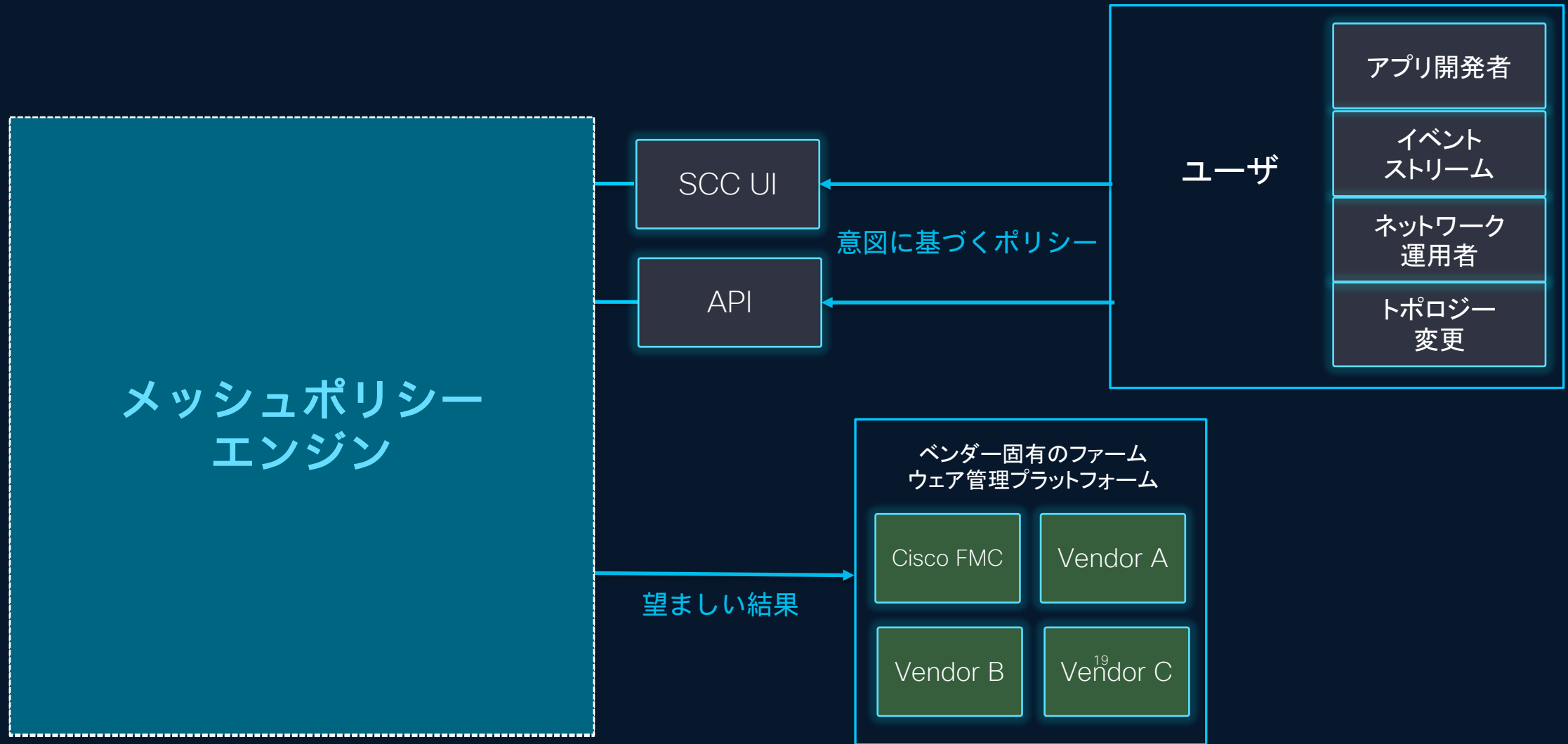
公開フィードと外部コネクタ



Dynamic Attribute Connector – アーキテクチャ



ポリシー ワークフロー & アーキテクチャ



Cisco Hybrid Mesh Firewall :

各機能（抜粋）

- ① 最新の脅威からの保護
- ② ラテラルムーブメントを阻止
- ③ 脆弱性のギャップを解消
- ④ シンプルな統合管理
- ⑤ AIトランスフォーメーションを保護

① 最新の脅威からの保護

現代に最適化されたファイアウォール

Secure Firewall Capabilities

ディープパケットインスペクションを超える優れた可視性



Security
Intelligence



Encrypted
Visibility Engine



Snort 3
with SnortML



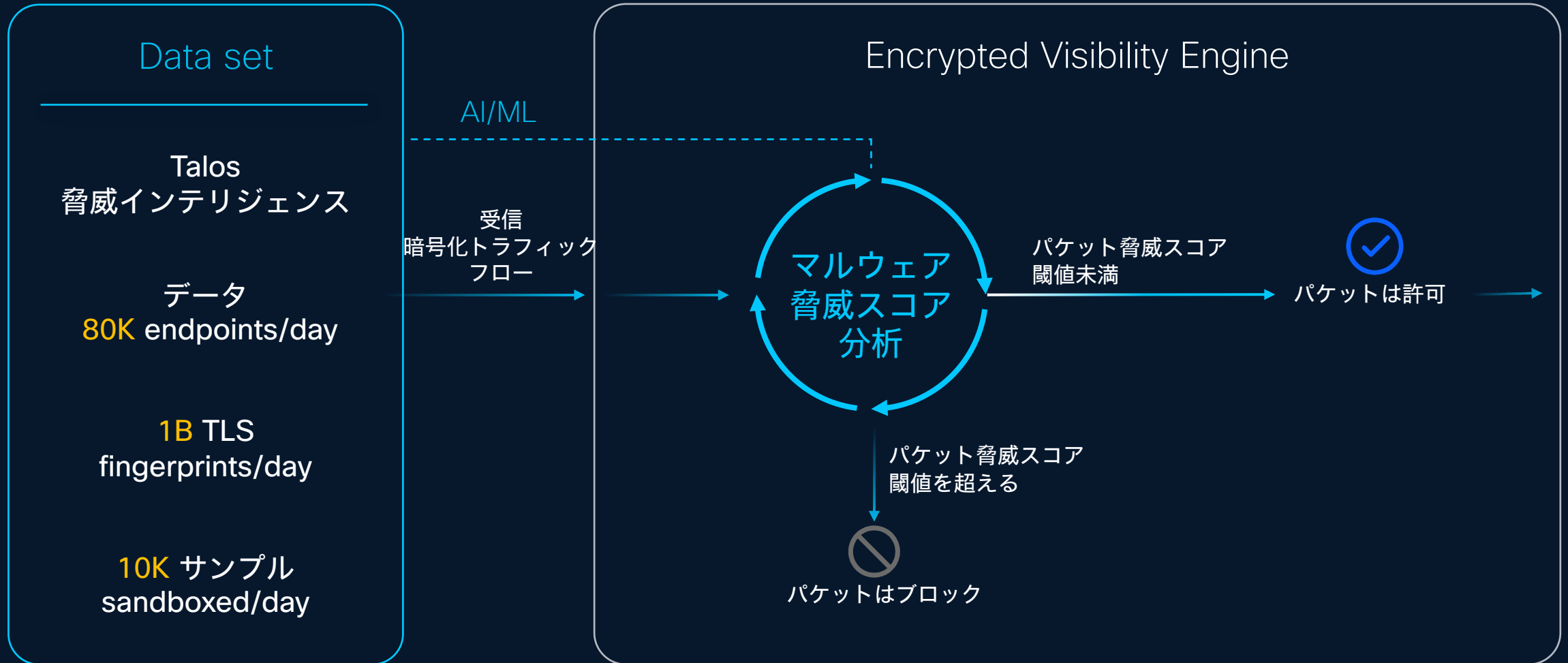
QUIC
Decryption



Advanced
Malware
Protection

Secure Firewall Capabilities

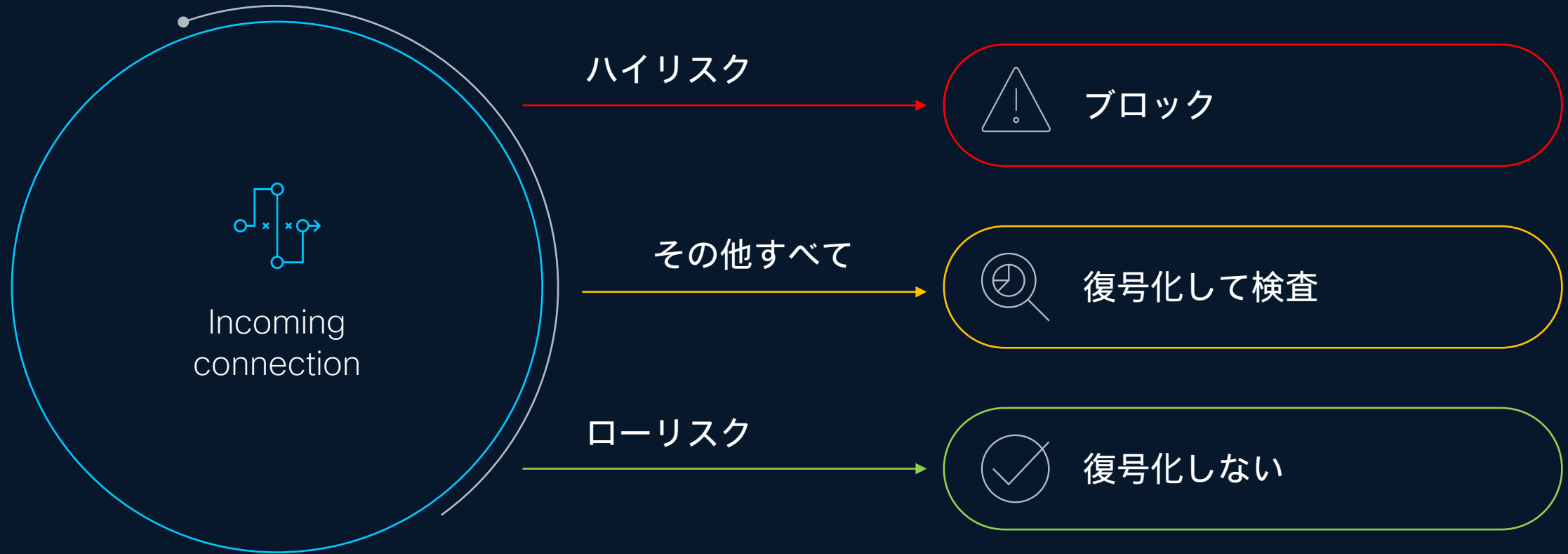
Encrypted Visibility Engine (EVE) -暗号化された現在のトラフィックに対応した最適化



Secure Firewall Capabilities

Intelligent Selective Decryption

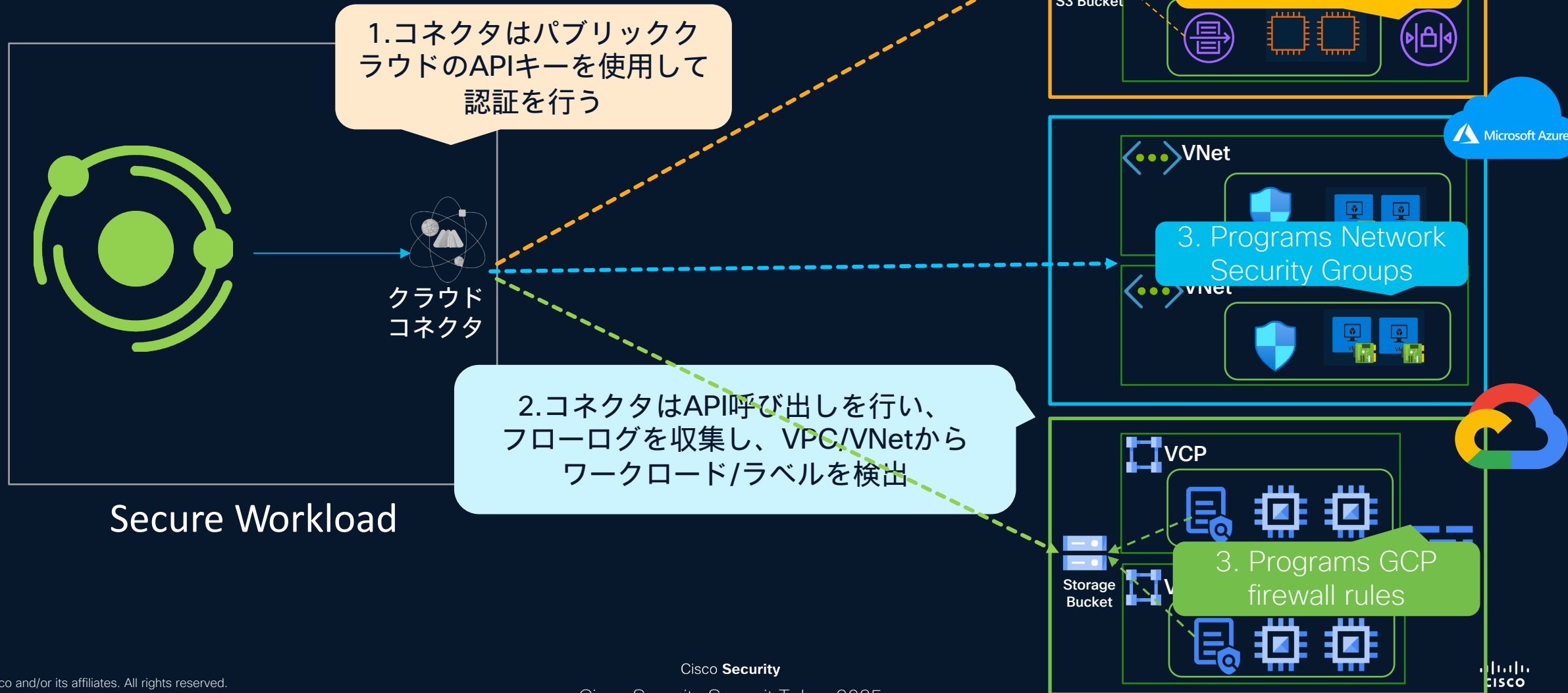
リスクベースのインテリジェントな暗号解読バイパス機能、EVEとTalosサーバーレピュテーション技術を搭載



② ラテラルムーブメントを阻止 ネットワークにセキュリティを統合する (マイクロセグメンテーション)

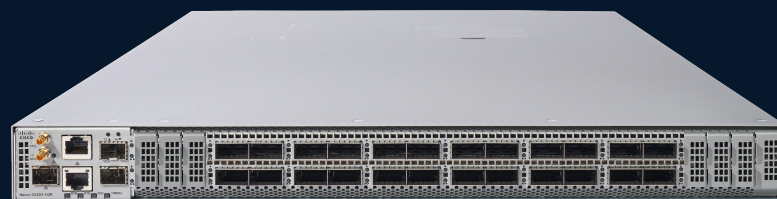
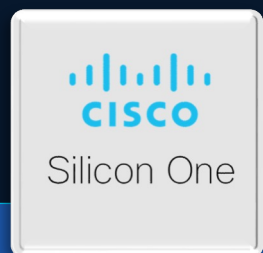
Secure Workload Capabilities

クラウドネイティブ ファイアウォール 統合 (SGs, NSGs, GFWs)

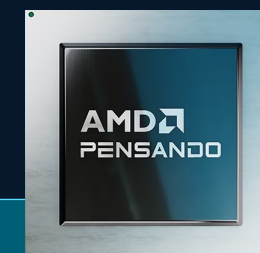


Hypershield Capabilities

ネットワーキングとセグメンテーションを1台のスイッチで実現



Cisco Nexus 9000 Smart Switch



- 豊富なNX-OS機能とサービス
- 高速接続とスケーラブルなパフォーマンス
- 遅延と電力効率を最適化



Routing
Switching



EVPN/MPLS/
VXLAN/SR



Rich
Telemetry



Line-rate
Encryption



Power
Efficiency

- ソフトウェア定義型ステートフルサービス
- すべてのレイヤーでプログラム可能：ハードウェアの変更なしで新しいサービスを追加可能
- スケールアウトサービスでワイヤーレート性能を実現
- 使用しない場合はDPUを電源オフ



Large-Scale
NAT



IPSEC
Encryption



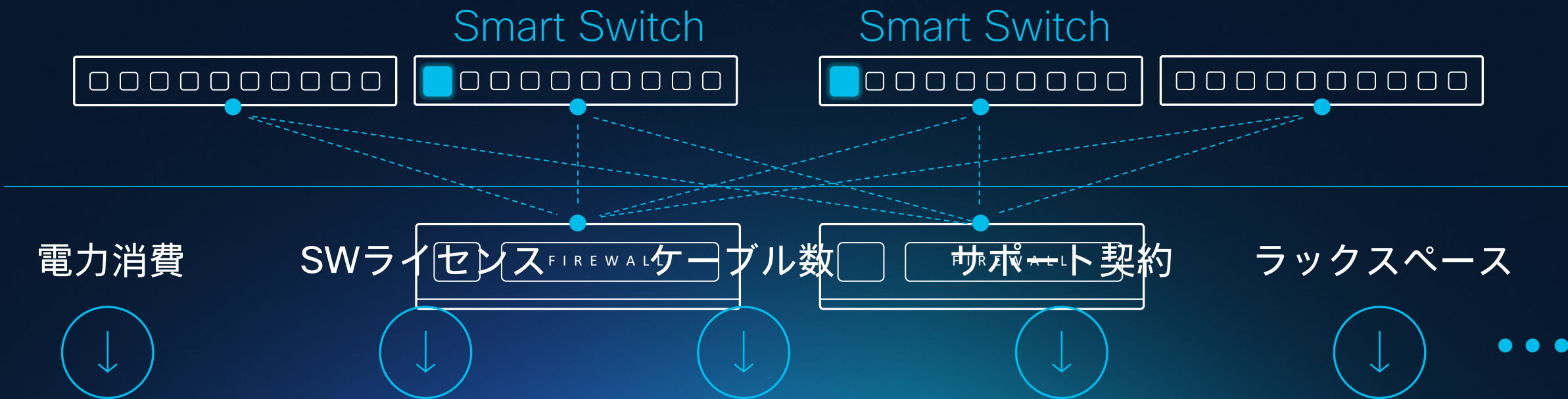
Distributed
Firewall



Event-Based Telemetry

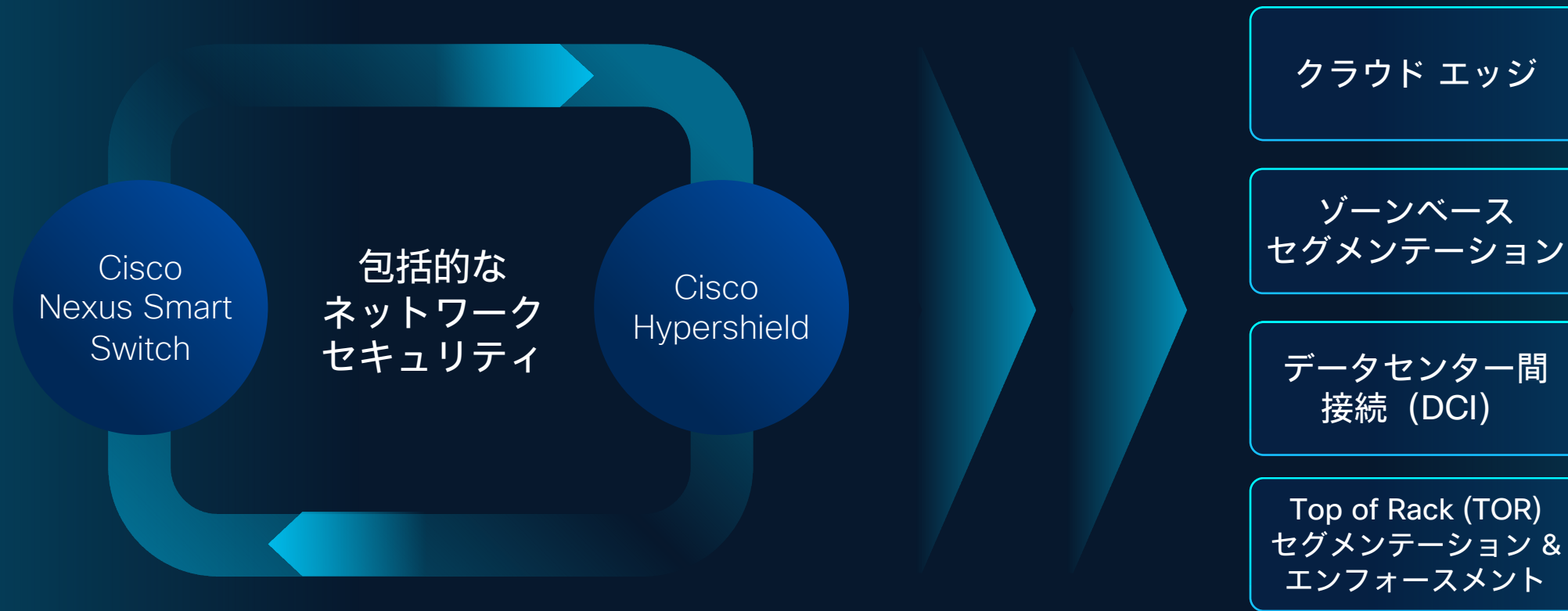


DoS
Protection



Hypershield Capabilities

ネットワークのある場所のどこにでもセキュリティを組み込み、セグメンテーションを実現



③ 脆弱性のギャップを解消 分散型エクسプロイト保護

Hypershield Capabilities

AI ネイティブのルールエンジンが脆弱性を優先順位付けし、アプリケーションを稼働させ続ける

公開グローバルデータソース

- CVE リポジトリ
- CWE情報
- MITRE
- Kenna
- TALOS
- ...

エクスプロイトからの保護を数ヵ月ではなく数分で実現

Hypershield AI

各CVE用のシールド

分散型
エクスプロイト保護

プライベートローカルデータソース

詳細な可視性

- 何
- どこ
- バージョン
- ライブラリ

Local Graph

Hypershield
AI

Global Graph

Qualys

RedSeal

Tenable

WIZ

リスクエンジン

- HIGH CVE - 2024 - 53757
- MED CVE - 2024 - 5664
- MED CVE - 2021 - 28810
- LOW CVE - 2023 - 4522

メモリ上で実行されているか？

実環境で悪用されているか？

それは高価値資産か？

AI

Compensating Control

BLOCK

Process "java"

Load file

`"/opt/teamcity/temp/uploadedPlugin"`

☐ View Compensating Controls in map

CI/CD Tooling Auth Bypass CVE-2024-27198

CVSS 2 Score 9.8

CVSS 2 Score

Compensating control
removed

Virtual Machine	Cloud Platform	Status	External ID	Internet Exposure	Operating Sys.
test-fdsek	Google Cloud	Active	2313482482374	Yes	Linux

完璧なフィット感

実トラフィックでテスト実施済み

最適な配置

④ シンプルな統合管理

ハイブリッド環境に一貫したポリシー導入

Cisco Mesh Policy Engine

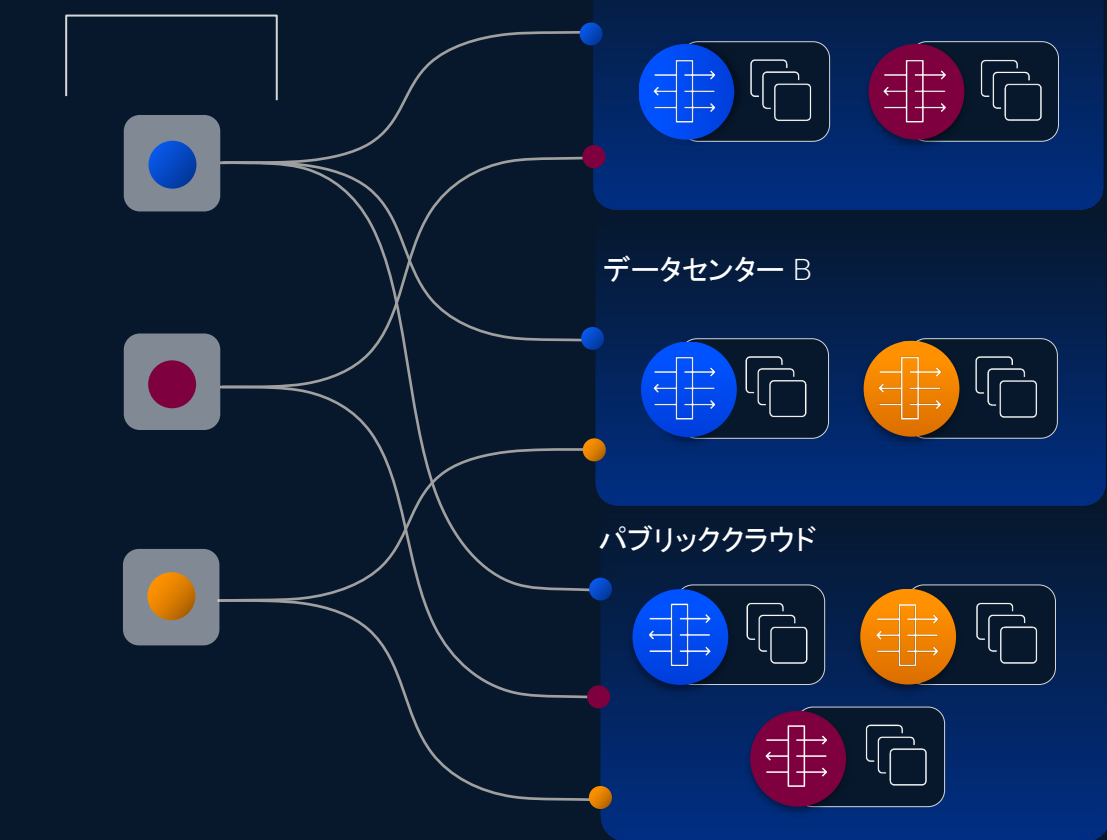
現在、ファイアウォールポリシーの管理は分散化されている

伝統的なポリシー管理

- ポリシー設定はデバイスごとに個別に行われる
- 複数のベンダーにわたって1つのインテントを複数のポリシーに翻訳するには時間がかかり、エラーが発生しやすい
- 時間をかけてファイアウォールデバイスを追加していくと、問題は指数関数的に悪化する

これらの課題解決には
異なるアプローチが必要

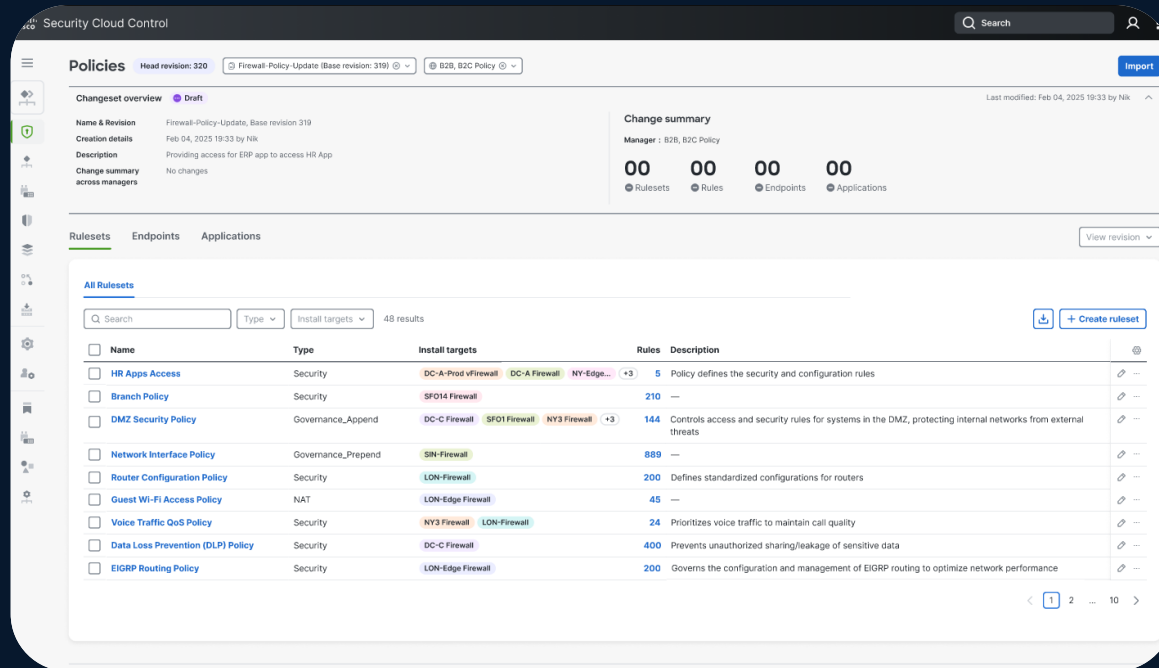
複数のベンダー
ユーザインターフェース



Cisco Mesh Policy Engine

シスコは、非シスコ製FWにポリシーを拡張する唯一のエンタープライズFWベンダーです

- ポリシーマネージャー
(デバイスマネージャーやポリシーコンバーターでは無い)
- ポリシーの「何」と「どこ」を維持し、その「なぜ」を明確にする
- ポリシーではなく、変更の適用ポイントを変更する
- シスコを含む他のエンタープライズ向けFWベンダー



Cisco Security Cloud Control

データセンター A



データセンター B



パブリッククラウド



Cisco Mesh Policy Engine

一度ポリシーを書けば、メッシュ全体に一気に適用

Security Cloud Control

← Policies

Create rule **Draft** Firewall-Policy-Update (Base revision: 319) B2B, B2C Policy HR Apps Access

Ticket ID: [Link ticket](#)

☒ Rule is enabled

Name * ERP-to-HR app Order * 01 Description (optional) Controls traffic flowing from ERP to HR Application

☒ Specify Access Specify which users and endpoints can access which resources. [Help](#)

2 Review Deployment and impact Review rule impact and reachability across different segments of the network.

+ Add install targets **Topology** List

Public Cloud ^

ERP Cloud Edge Firewall

Data Center_A ^

DC-A Firewall

App Zone ^

DC-A-App vFirewall HR App

Delete [Revert changes](#) [Back](#) [Save](#)

メッシュ ポリシーエンジンは、ネットワークのトポロジをインテリジェントに分析し、関連するFWに最も効果的なポリシーを適用します

1. ルール名と目的を説明
2. ユーザーとエンドポイントへのアクセスを定義
3. ネットワークトポロジー全体に展開

⑤ AIトランスフォーメーションを保護

AIモデル/アプリへの新たな脅威を保護

AI applications are different

Presentation

|

App

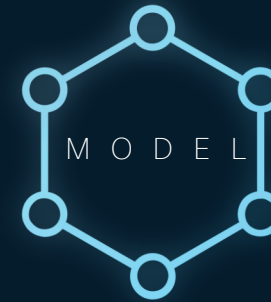
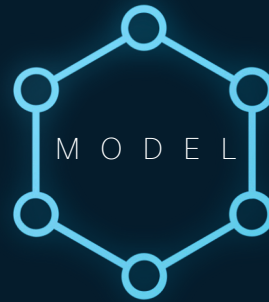
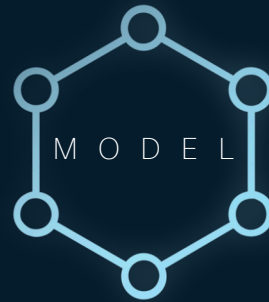
|

Data

Presentation

App

Non-deterministic



New risk vectors

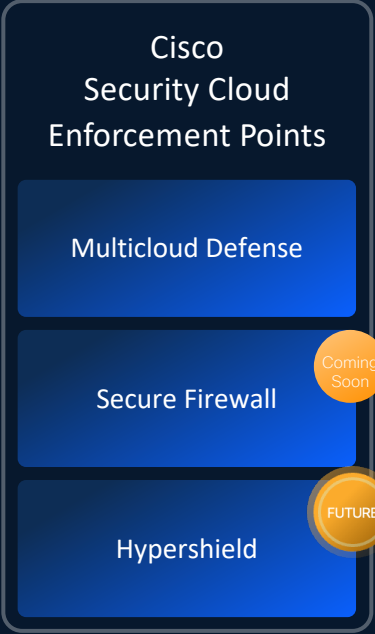
Data

AI Defense Capabilities



AI Defense Capabilities

AIモデル/アプリへの新たな脅威に対してエンフォースメントポイントを広げて面に対応



Cisco Hybrid Mesh Firewall : ユースケース

ユースケース – 問題の定義

ラテラルムーブメントを阻止するためにマイクロセグメンテーションを導入したい。一方でクラウドシフトが各事業部門で進んでいて、会社全体での安全性が誰も管理出来ず不明な状態

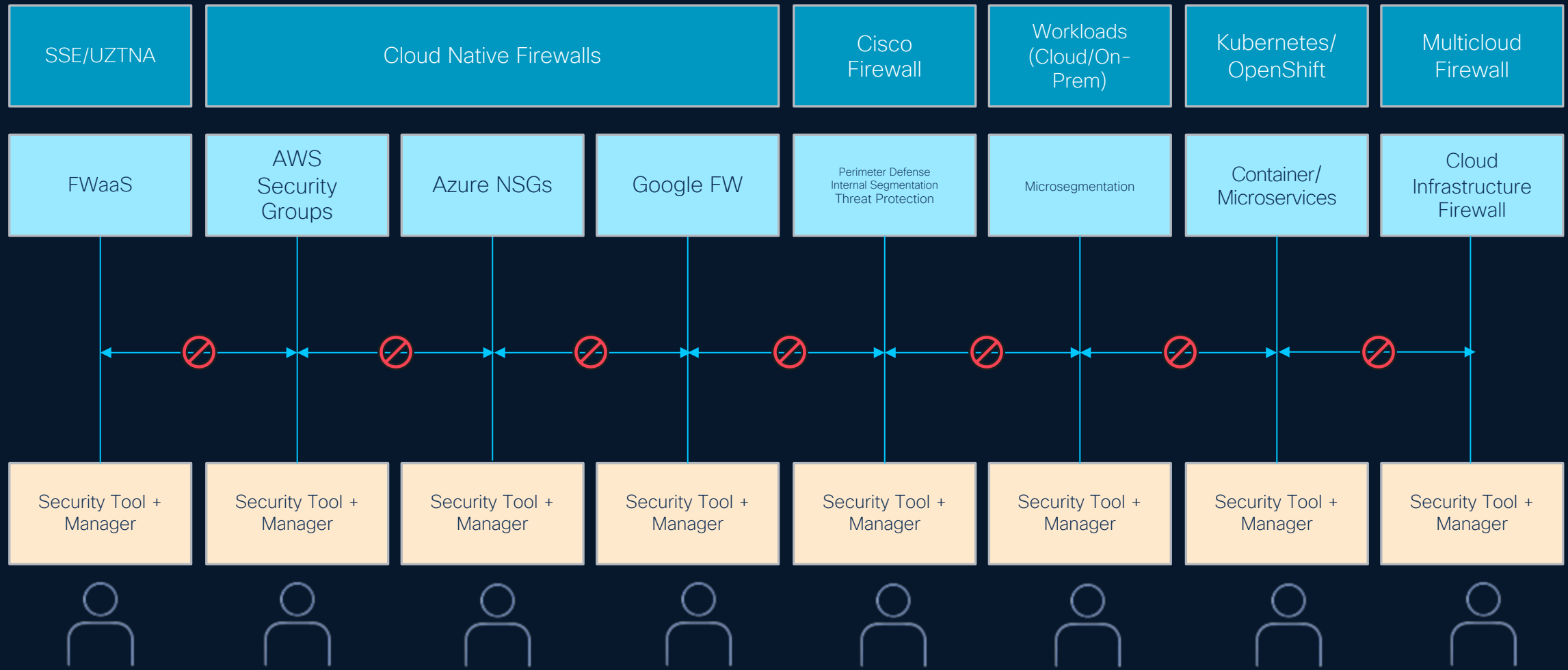
クラウド移行の加速: 迅速に重要なワークロードをGoogle Cloud Platform (GCP) に移行し、俊敏性とスケーラビリティの要件に対応

セグメンテーション互換性ギャップ: 既存のオンプレミス型セグメンテーションソリューションはGCPと互換性がなく、一貫したセキュリティの適用が妨げられている

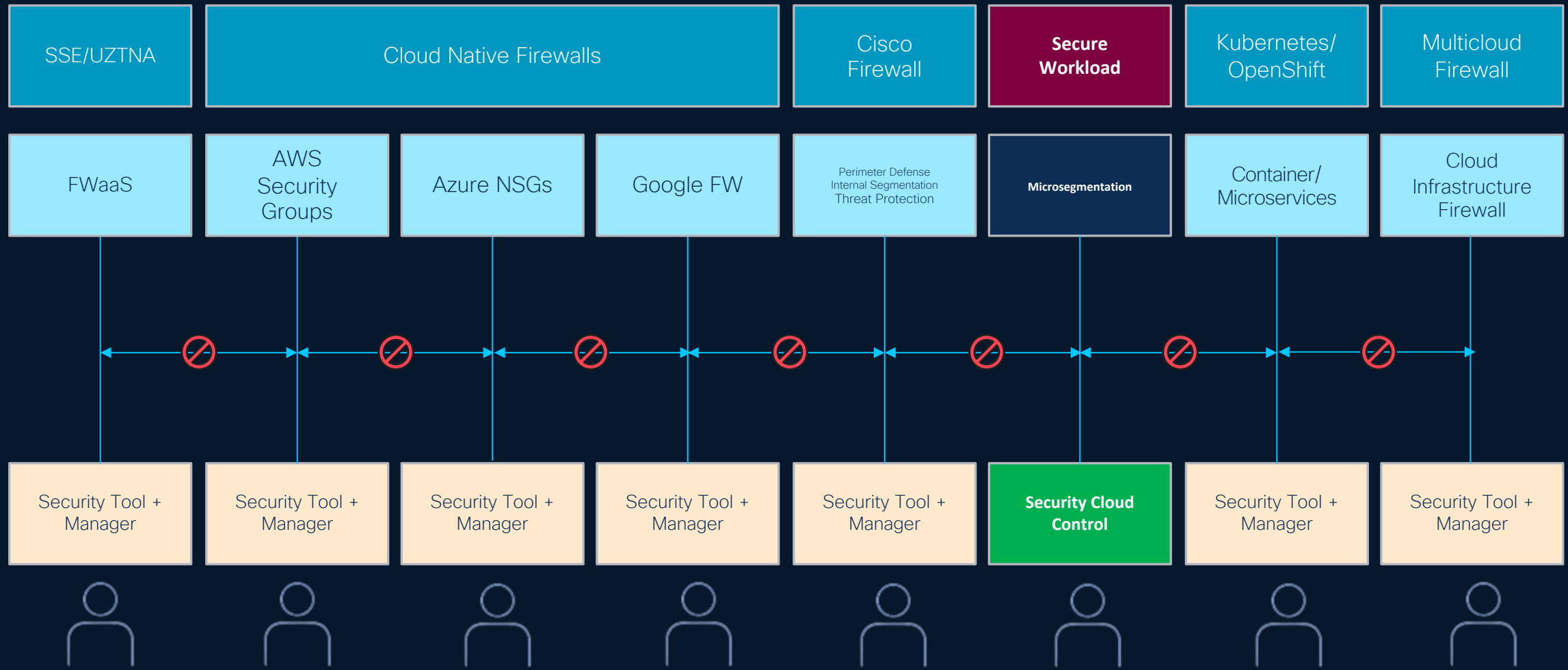
コンプライアンスリスク: この乖離は、ハイブリッドインフラストラクチャ全体でポリシーを統一的に適用できないため、重大なコンプライアンスリスクを引き起こす

統一されたポリシー管理の必要性: 直近の要件は、GCPに移行するワークロードのコンプライアンス要件を満たすこと、および将来を見据えた統一されたポリシー管理を実施すること

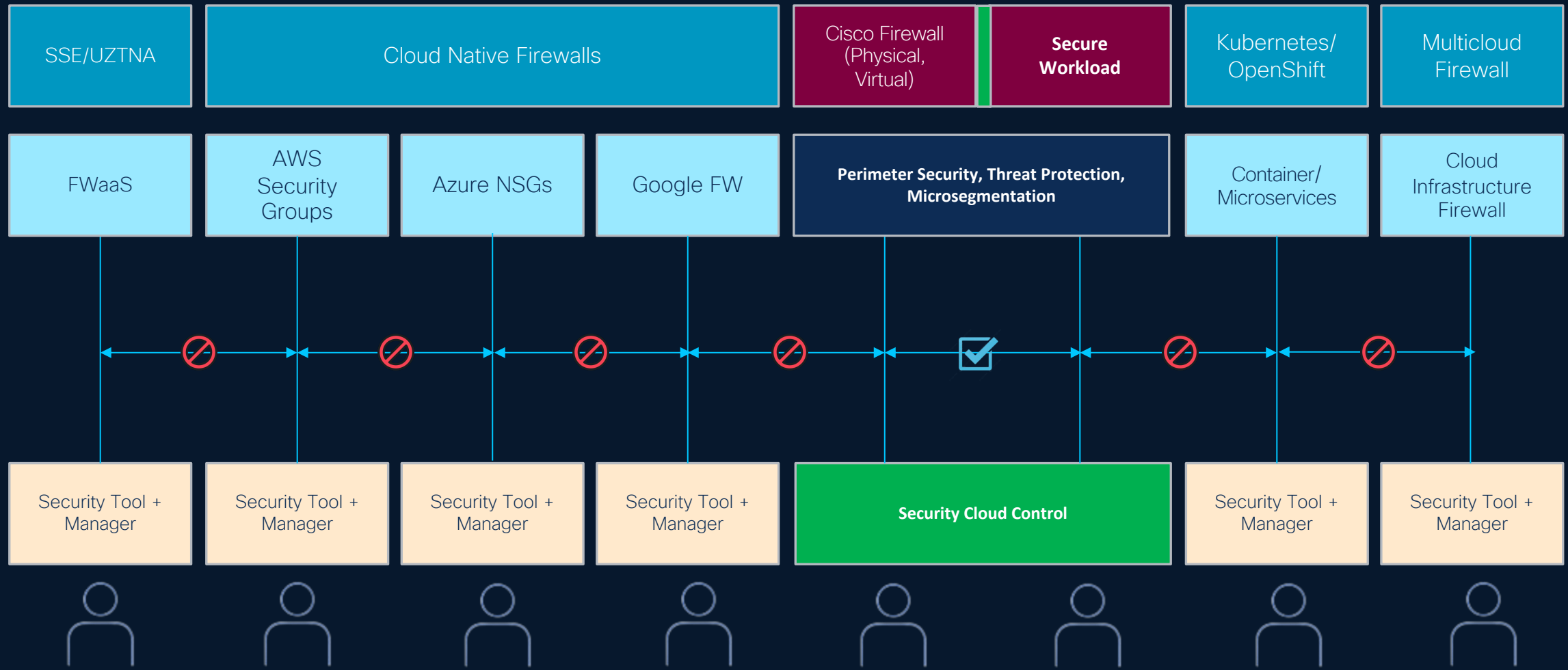
ユースケース - 現状



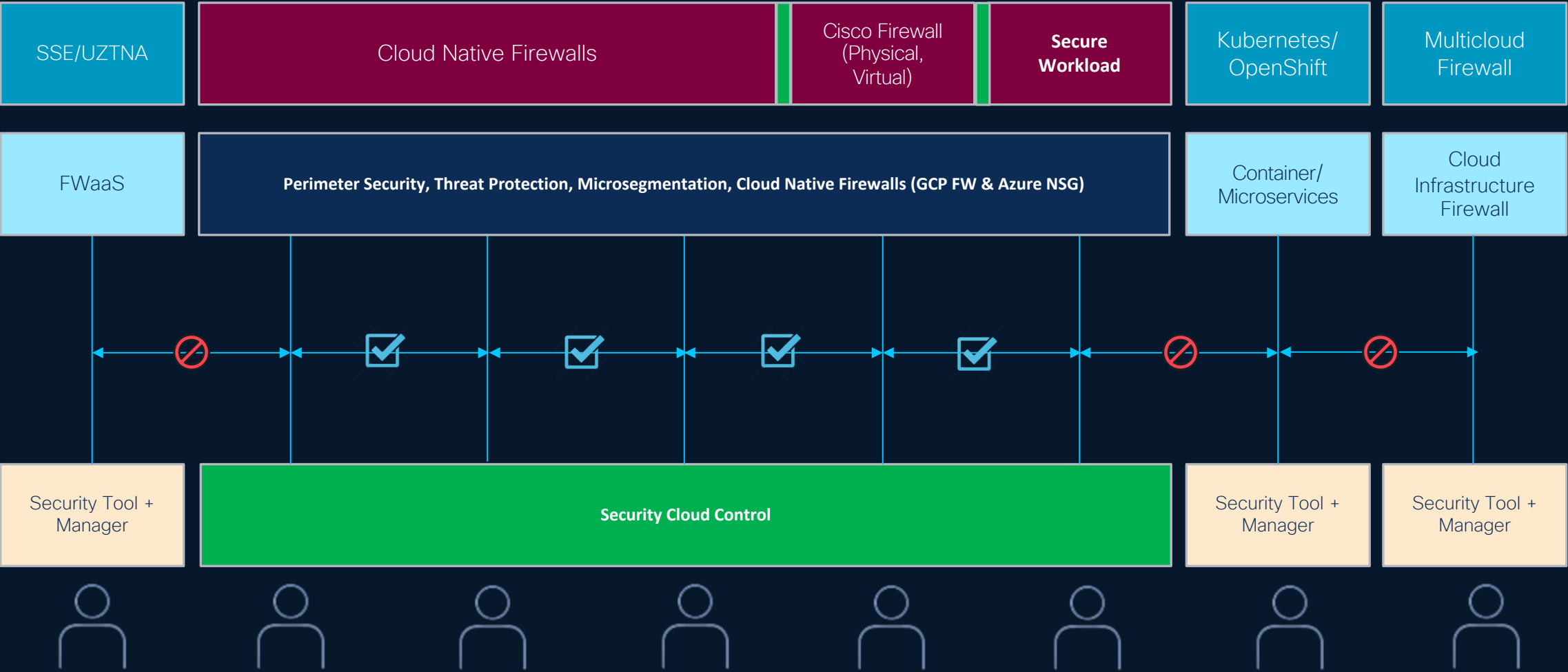
ユースケース



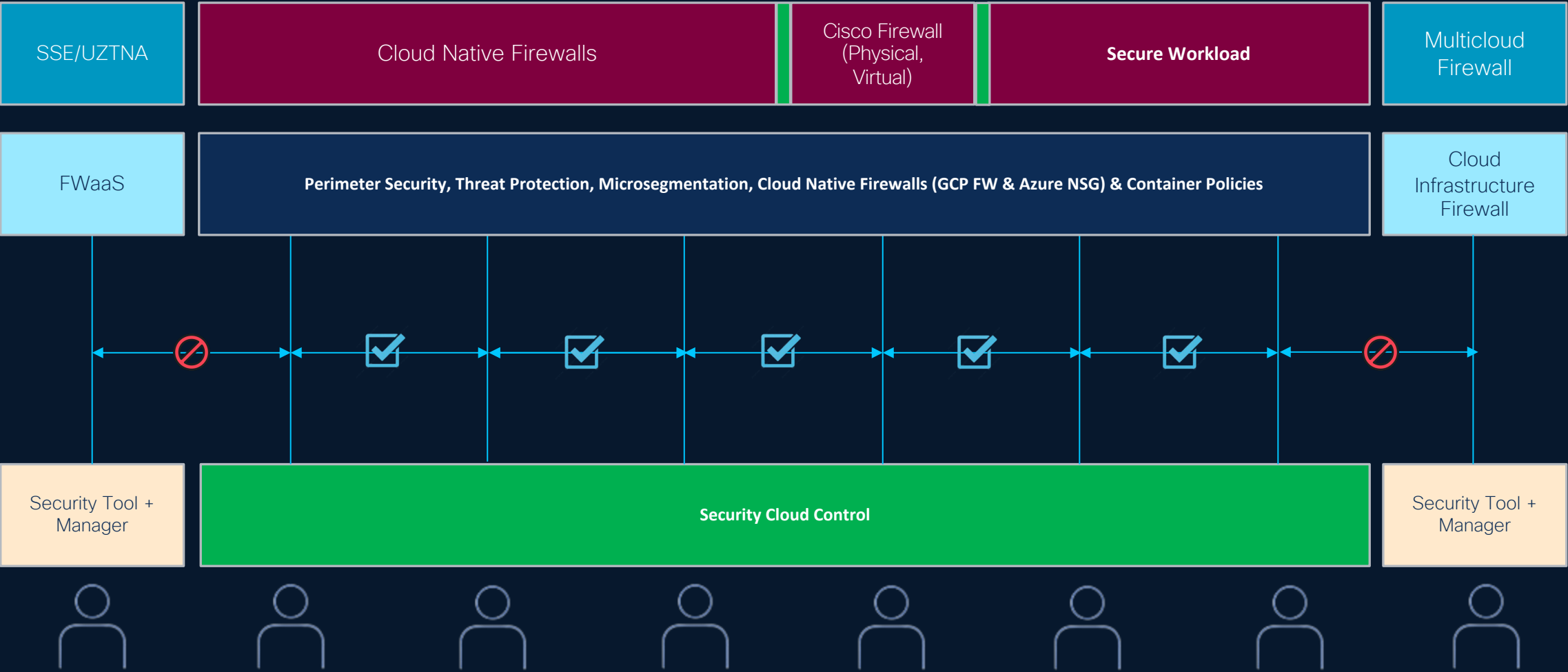
ユースケース



ユースケース



ユースケース



まとめ : Cisco Hybrid Mesh Firewall

ハイブリッド環境向けにシンプルな統合管理で多様なユースケースにおける高度な脅威保護を提供

- 統合管理

SECURITY CLOUD CONTROL

Hypershield

eBPF

DPU



Secure Firewall



3rd Party Firewall



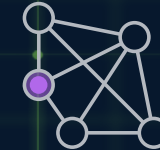
Secure Workload



Isovalent runtime protection



Smart Switches



ACI



Secure Router

- エンフォースメントポイント

一度ポリシーを書けば、メッシュ全体に一気に適用

Cisco **Security**

Cisco Security Summit Tokyo 2025

Thank you

