Cisco **Security**

Cisco Security Summit Tokyo 2025

シスコ SASE 最新アップデート

Incubation Sales, APJC, GSSO

Yasunobu Fukudome

Aug 5, 2025

アジェンダ

1. SASE とは
2. シスコ SASE 最新アップデート
3. Universal ZTNA とは
4. Universal ZTNA を実現する関連ソリューション

1. SASE とは

Secure Access Service Edge (SASE) とは

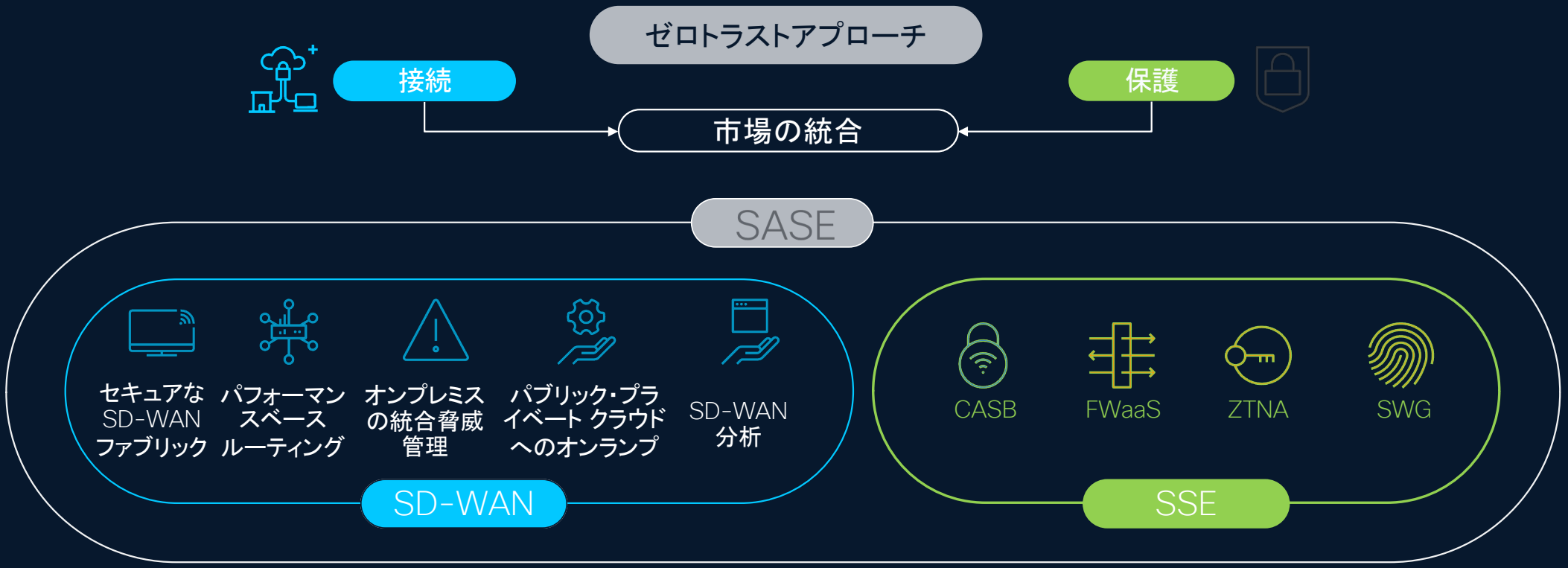
現在の分散環境におけるユーザエクスペリエンス(快適性・安全性の向上)を実現するアーキテクチャ

https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase
Secure Access Service Edge (SASE) Definition by Gartner

SD-WAN、SWG、CASB、NGFW、ゼロ トラスト ネットワーク アクセス (ZTNA) など。SASE は、ブランチ オフィス、リモート ワーカー、オンプレミスのセキュア アクセスのユース ケースをサポートします。SASE は主にサービスとして提供され、デバイスまたはエンティティの ID と、リアルタイムのコンテキスト、セキュリティおよびコンプライアンス ポリシーに基づいてゼロ トラスト アクセスを可能にします。

ゼロトラスト アプローチにおいて重要となる SASE

超分散型の世界におけるセキュリティ戦略の基盤



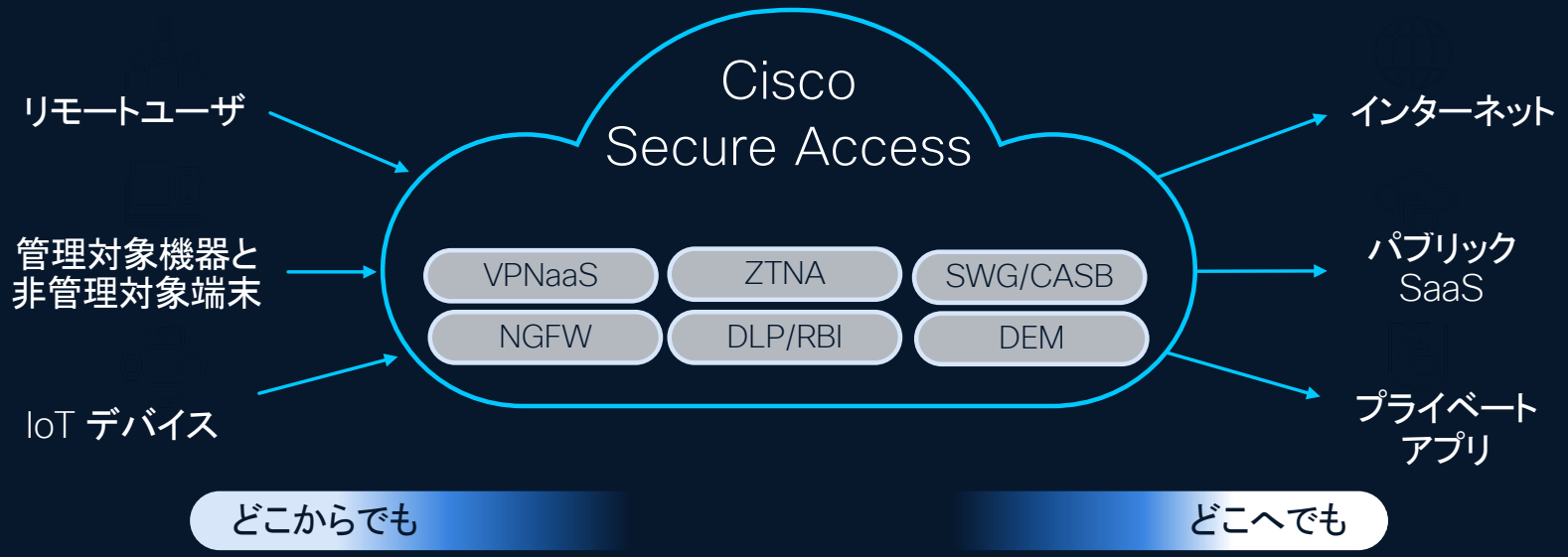
ゼロトラストへの移行を推進した既存 SASE における課題

1. ゼロトラスト環境としては範囲が限定的
   - 連携しない DC 、LAN
   - IoT 非対応
2. VPN 利用の継続
   - 進まないアプリケーションのゼロトラスト対応（VPN でしか救えない実情）
   - 単一ではないエージェントによるエンドユーザの手間（VPN と ZTNA の使い分け）
   - IP アドレスベースの ACL で制御しているインフラ（ファイアウォール等）の存在
3. ZTNA への移行が困難（ユーザの協力を前提）
   - 組織内アプリケーションの全リスト化および FQDN 登録
   - エンドユーザによるオペレーション変更（VPN と ZTNA の使い分け）
4. アクショナブルではない端末と SSE 間のネットワーク可視性
5. 買収リスク、値上げリスク

2. シスコ SASE 最新アップデート

Cisco Secure Access 概要

ゼロトラストに基づく統合クラウドセキュリティで防御を近代化する最新型 SSE



ユーザーにとってより快適に

IT をより使いやすく

すべての人にとってより安全に

Cisco Secure Access 機能

基本のセキュアサービスエッジ（SSE）の一歩先を行くサービスで快適な接続を実現しビジネスを強力に保護

基本となる SSE

- セキュア Web ゲートウェイ（SWG）
- クラウド アクセス セキュリティ ブローカ（CASB）と DLP
- ゼロトラスト ネットワーク アクセス（ZTNA）
- サービスとしてのファイアウォール（FWaaS）と IPS

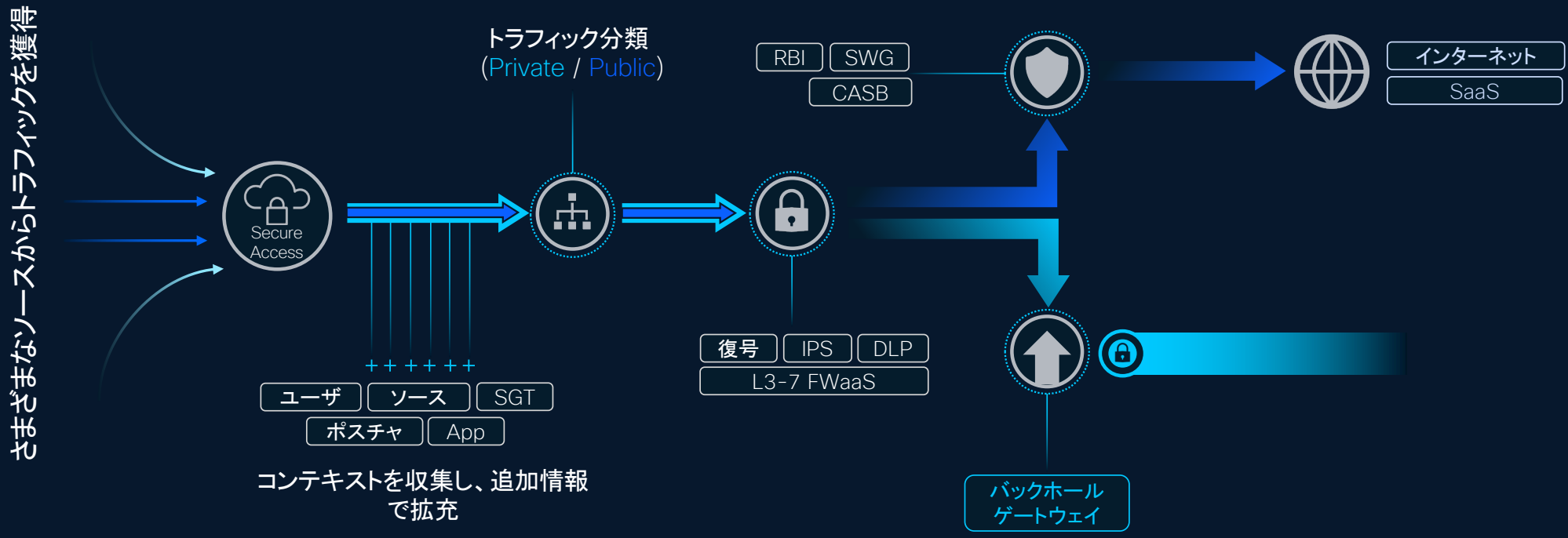
＋

シスコは基本の機能も追加の機能も 1 つのサブスクリプションで提供

- DNS セキュリティ
- マルチモード DLP
- 高度なマルウェア防御
- サンドボックス
- Talos 脅威インテリジェンス
- サービスとしての VPN
- エクスペリエンス インサイト（DEM）
- リモートブラウザ分離

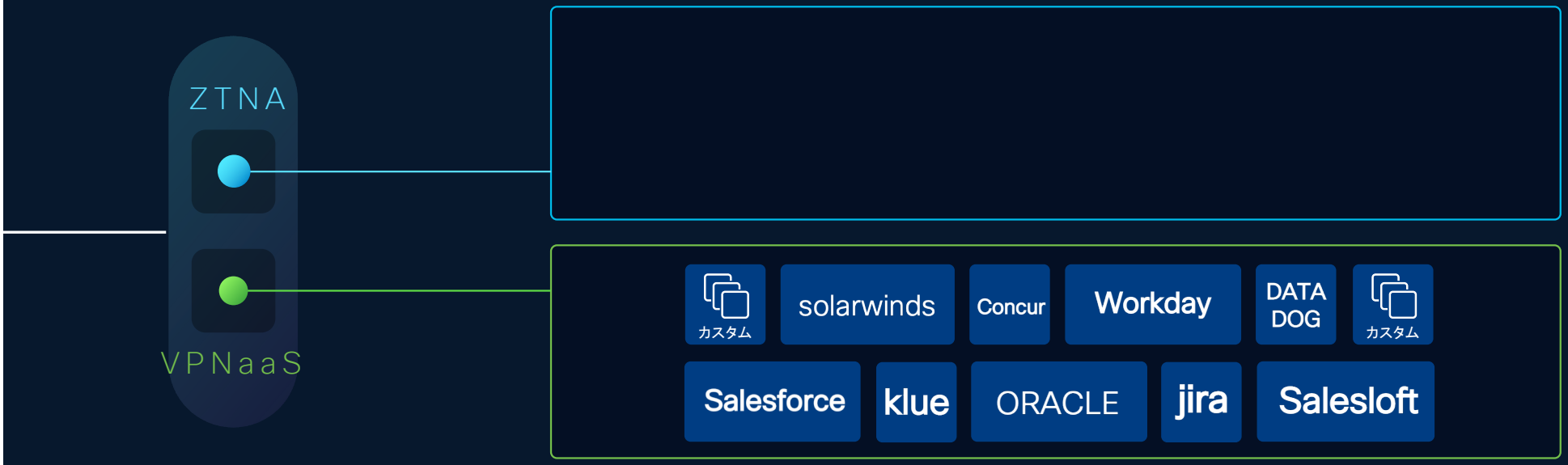
ユニファイド クラウド アーキテクチャ

ユニバーサルトラフィック取得とシングルデータパス



ZTNA へシームレスに移行

VPN-as-a-Service は ZTNA 展開を簡素化



Cisco Secure Client

VPN から ZTNA まで、エンドユーザによる利用を快適にするユニファイド エージェント

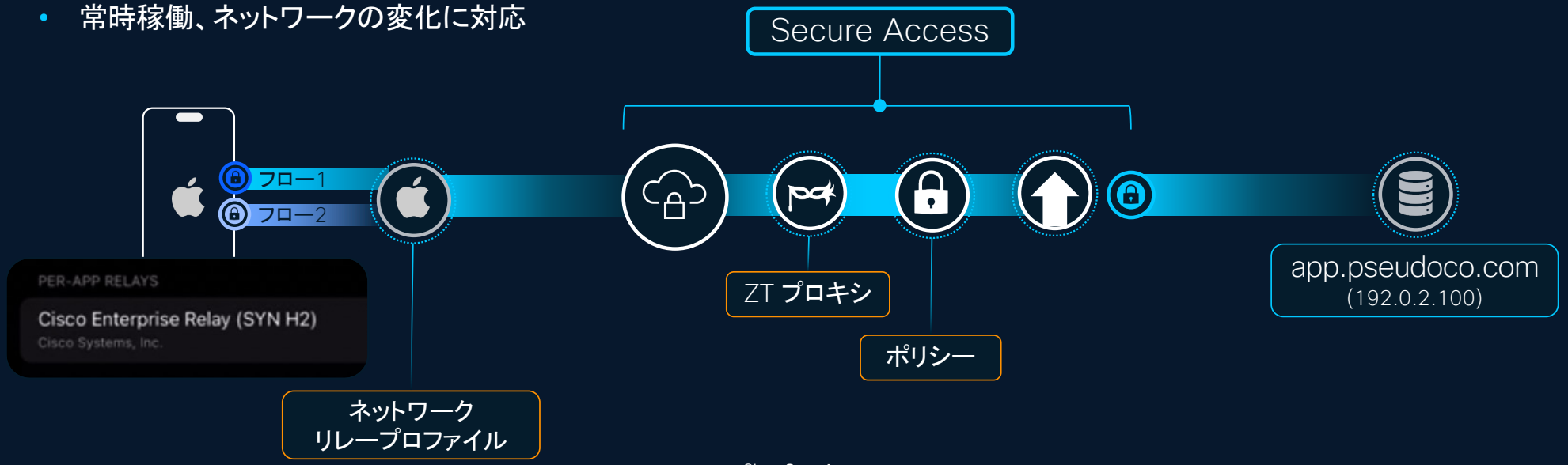
- フリクションレス ユーザーエクスペリエンス
- きめ細かなアクセス制御によるプライベート リソースへのプロキシ (ZTNA Proxy) アクセス
- TPM/hardware enclave キー ストレージによるサービスマネージドクライアント証明書
- TCP および UDP アプリケーションをサポート
- シスコおよび 3rd パーティ VPN クライアントとの相互接続
- 次世代プロトコル (MASQUE + QUIC)

iOS ネイティブのゼロトラスト

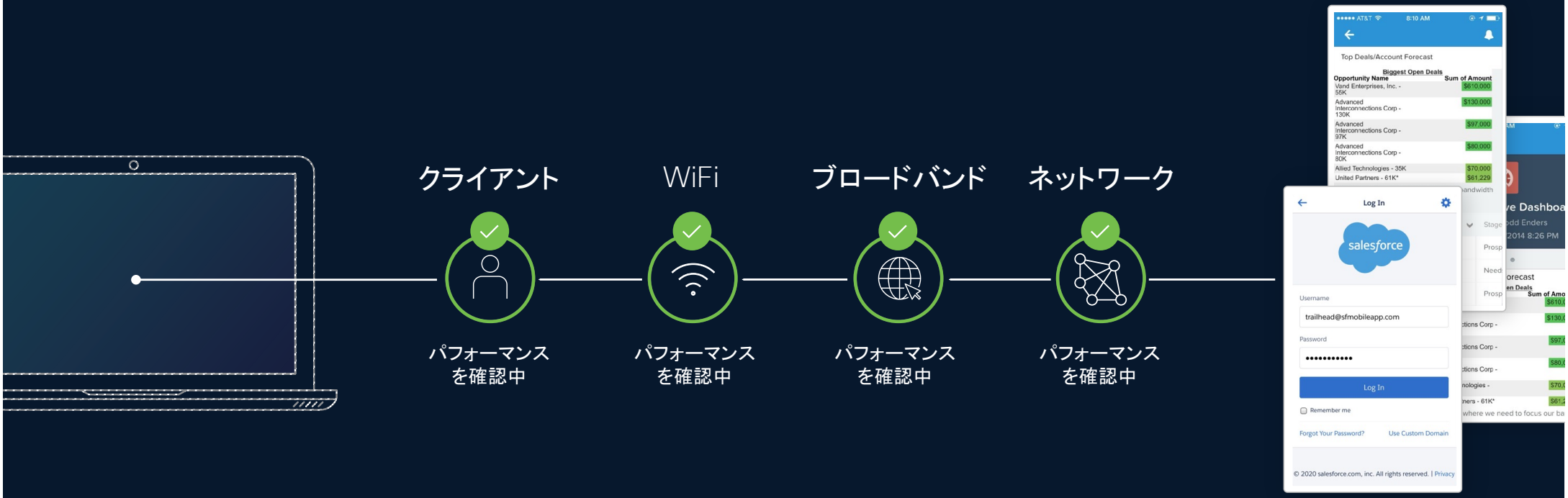
Apple + Cisco Enterprise Relay (iOS 17 +)

ネイティブ体験

- Apple 社と共同開発
- VPN なしのネイティブ接続
- アプリごとの可視性と接続性
- 一貫したエクスペリエンス PC/ MAC/ iOS
- 常時稼働、ネットワークの変化に対応



デジタルエクスペリエンスモニタリングで迅速に問題を解決

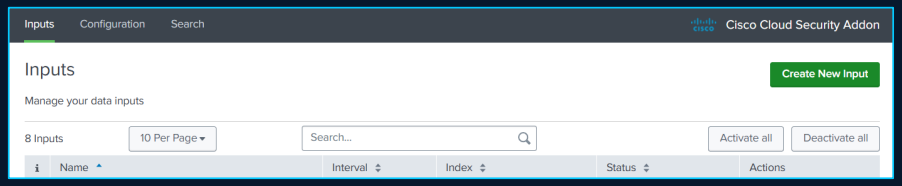


過去のパフォーマンスと推奨事項を確認可能

Splunk/XDR 連携

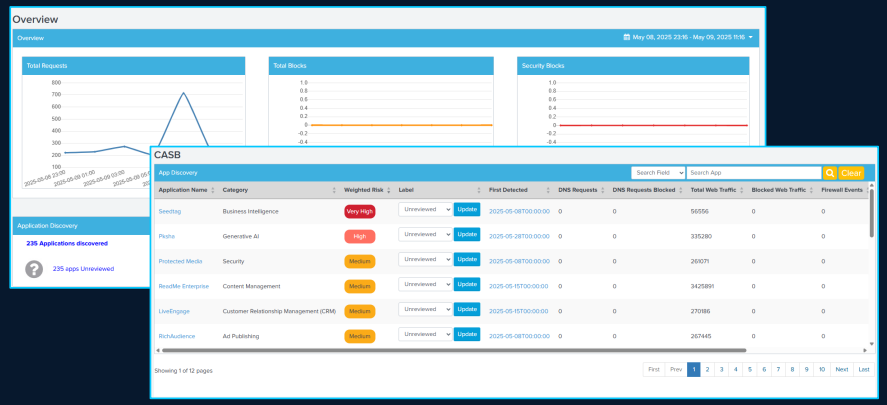
Splunk

Cisco Cloud Security Add-on によるログ取り込み



（ご参考）Splunk Ingest Action を利用すると、全量データの S3 への長期保管および分析不要なログ データのフィルタリングにも対応

Cisco Cloud Security App for Splunk による可視化

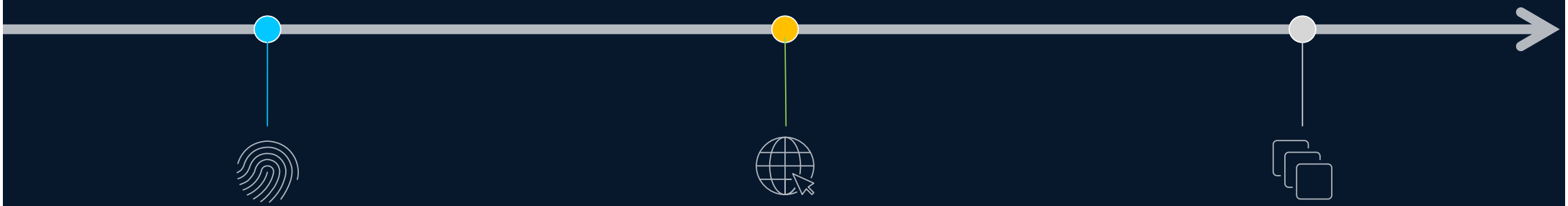


XDR

1. 環境内の悪意のある活動をより早く、より正確に検出
2. エンリッチされたテレメトリとグローバルな脅威インテリジェンスを通じて、侵害されたデバイスとリスクの高いユーザー行動をより迅速に特定
3. 自動ワークフローで Secure Access のポリシーを管理し、Cisco XDR コンソールから直接監視することで、セキュリティオペレーションを簡素化

Cisco Secure Access ファミリ

高度な DNS セキュリティからフル SSE まで幅広いユースケースに対応するパッケージ



DNS Defense

- DNS レイヤセキュリティ
- SaaS API DLP
- クラウド マルウェア スキャン
- トライアル付与 - 100 シートの SPA

Secure Internet Access (SIA)

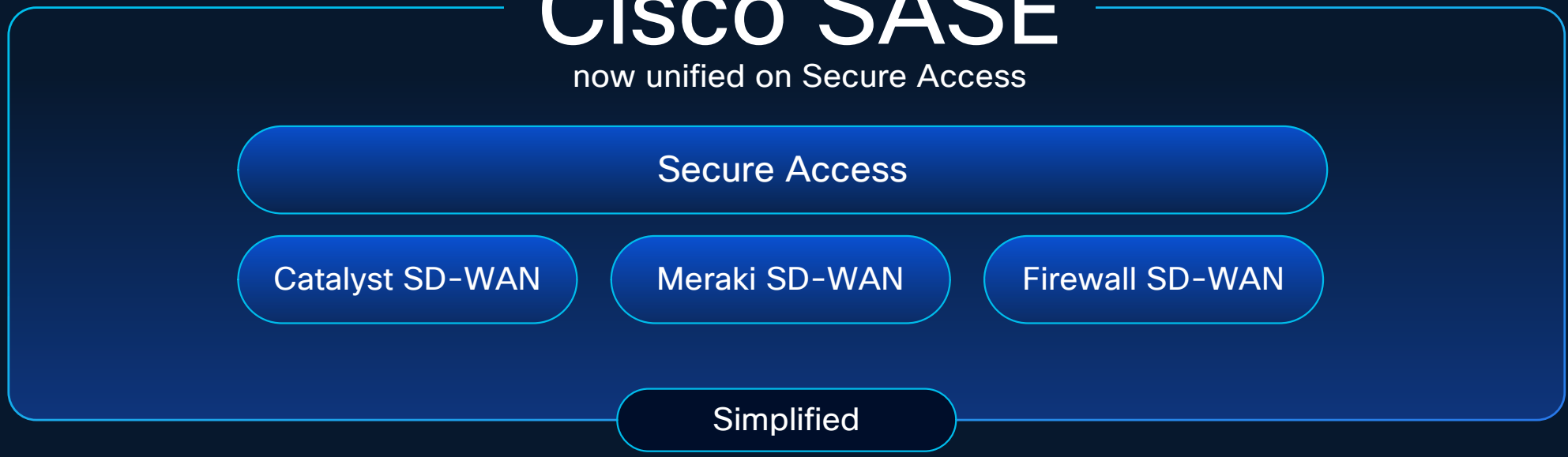
- DNS Defense 機能に加え：
  - デジタル エクスペリエンス モニタリング
  - SWG
  - CASB, DLP, AI Access
  - FWaaS
  - RBI 他

Secure Private Access (SPA)

- ZTNA + VPNaaS を統合
- リソース コネクタ
- 同一ユニファイド ダッシュボード

Cisco SASE

now unified on Secure Access



最適な接続を選択可能な柔軟性

Security Cloud Control によって管理される統合セキュリティポリシー

一貫したクラウドでのエンフォースメント

Security Cloud Control

ポリシーを一度定義すれば、どこでも実施可能

この機能は計画であり、今後通知なく変更されることがあります

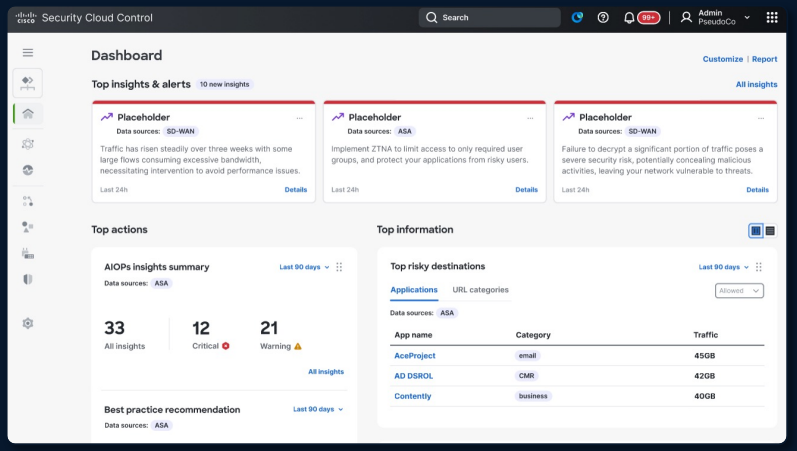
セキュアルータのポリシー管理が Security Cloud Controlに登場

Coming soon

Cisco Secure Routers

Security Cloud Controlで今後可能（予定）:

- オブジェクトとセキュリティ・ポリシー作成
- 既存のセキュアルータ内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作成
- SALでセキュアルータのイベントを可視化
- SD-WAN Manager と Security Cloud Control 間 RBAC モデル同期

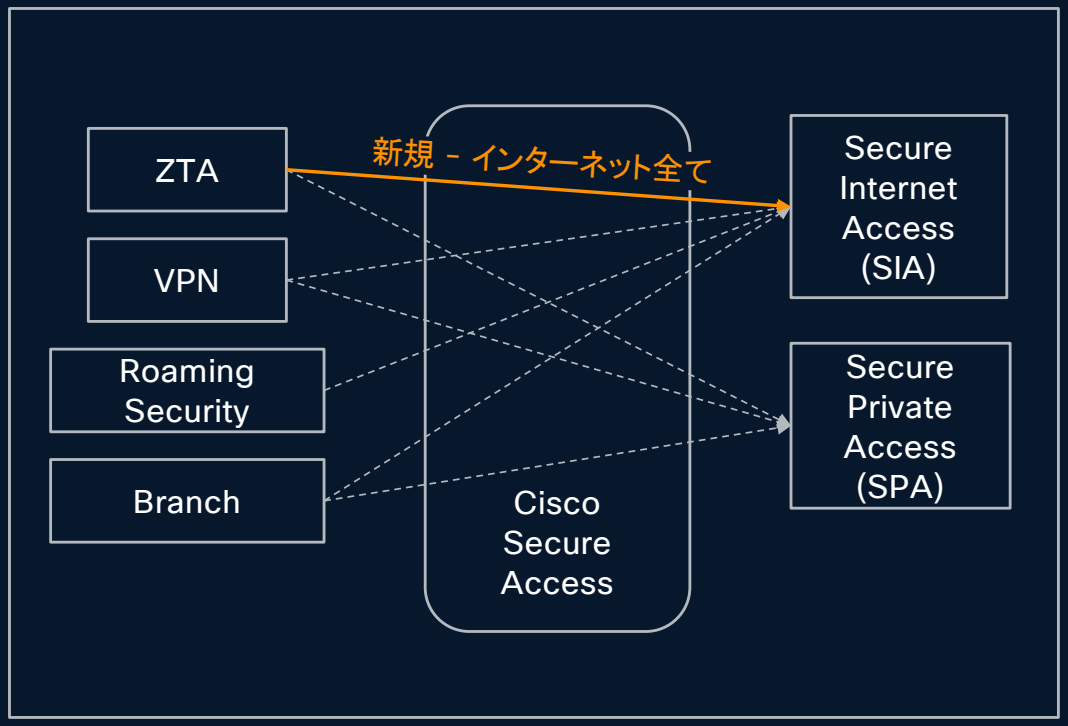


サポートされるモデル

Cisco 1000 Series Integrated Services Routers
Cisco 8000 Series Secure Routers

ZTA における全てのインターネット宛通信対応

Coming soon



- すべてのインターネット宛先（すべての TCP / UDP トラフィック）へのトラフィックをセキュアに
  - Windows および macOS でサポート。今後のリリースでモバイルのサポートを予定
  - TPM ハードウェアと短命の ACME 証明書を使用した強力なデバイスバインドユーザ ID
- インターネット宛先のグローバルポスチャチェック
  - プライベートおよびインターネットアクセスで利用可能な一貫したポスチャー属性
- Zero Trust Access プロファイルにより、ユーザー/グループごとに異なるアクセスエクスペリエンスを提供

Trusted Network Detection (TND) for ZTA

概要

- TND により信頼されたネットワーク上で ZTA トラフィックの誘導と施行を一時的に停止
- エンドポイントが信頼されたネットワークを離れると、Secure Client は ZTA 施行を再開
- エンドユーザーの操作は不要
- プライベートおよびインターネットの ZTA 宛先で独立して管理可能

主な利点

- 改善されたネットワークパフォーマンスと遅延によるスムーズなユーザーエクスペリエンス
- 信頼されたネットワークでのローカルセキュリティ施行は、柔軟で最適化されたリソース利用を提供
- プライベートアクセスとインターネットアクセスのための TND の独立した制御は、異なる運用およびセキュリティの懸念を扱うための管理者の柔軟性を提供

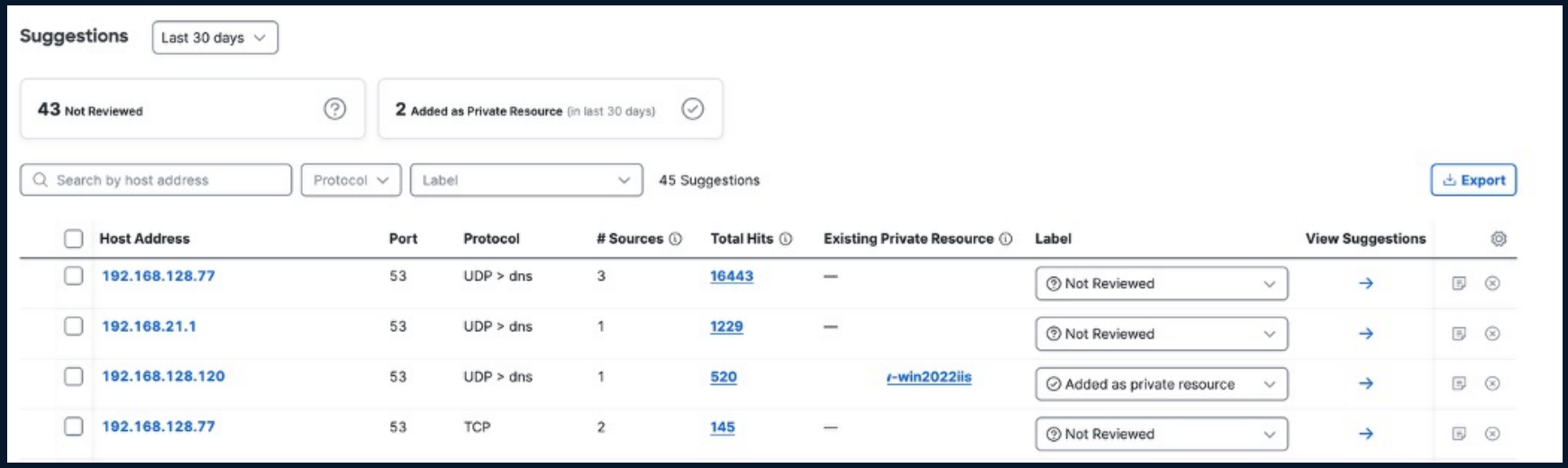
プライベート リソースを自動で可視化

Private Resource Discovery 機能

実際にアクセスされているプライベート リソースを自動で検出し対応を提案

利点:

- シャドー IT の可視化
- ユーザーの行動に関する洞察を活用して、重要なリソースの優先順位付けと保護
- 提案に対してラベル付けを行うことで効率的にリソースを保護
  ラベル:「リソース登録済み」、「レビュー必要」、「 Ignore (無視)」、「レビュー未実施」



VPN 接続から ZTA (ゼロトラストアクセス) の移行に伴う登録・管理の手間を大幅に削減

Policy Verification

安心してポスチャー変更を可能にする新たなツール

ポリシー検証の重要性

- 設定変更は、サービスに影響を与えるインシデントの主要な原因の一つ
- ポリシー検証を使用することで、変更の影響を事前に評価することが可能
- 設定ミスの削減、サービス停止時間を最小限に抑え、ユーザーのアクセスを維持

ポリシー検証が日常業務にどのように役立つか

- 積極的な変更管理

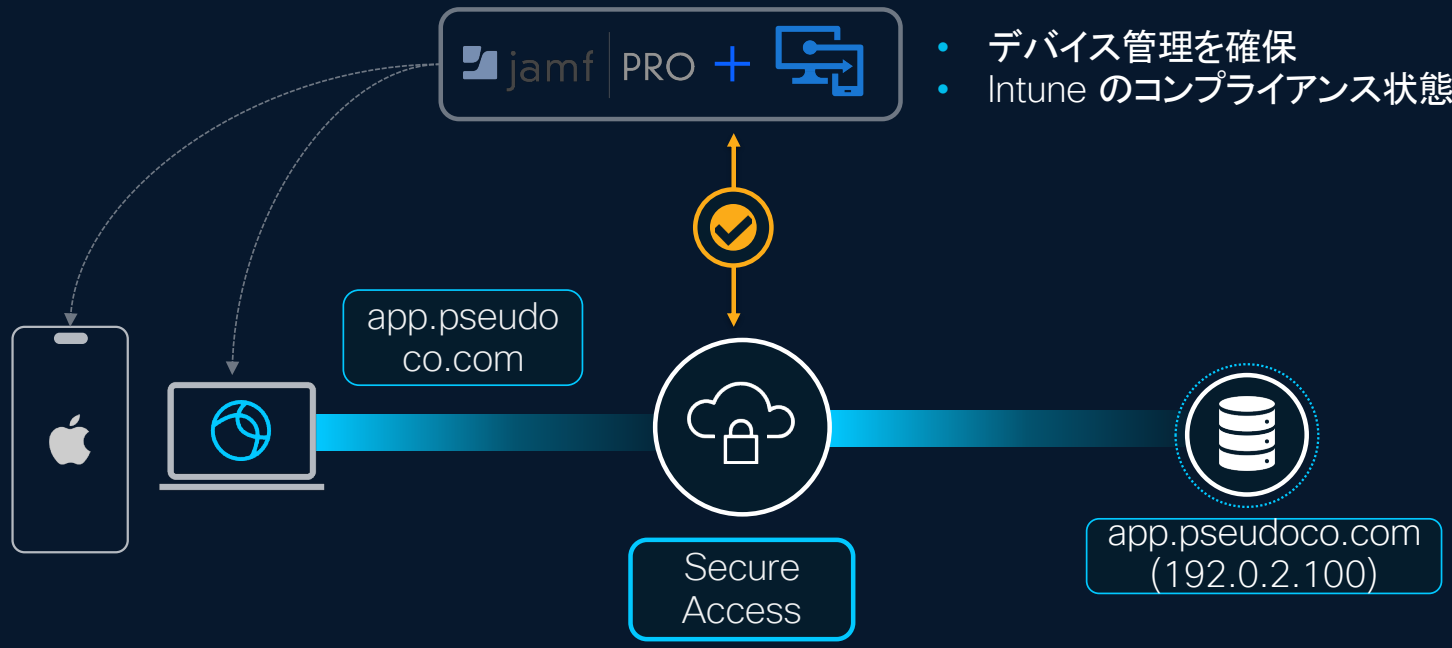
  実施前に計画された変更が姿勢やポリシーに与える潜在的な影響を分析し、よりスムーズな展開と混乱の少ない実施を保証
- リアクティブなインシデント解決

  設定変更に関連するインシデントの根本原因を迅速に特定し、対処することで、ダウンタイムとトラブルシューティングの労力を削減
- これらの機能により、お客様に安心感、運用効率の向上、そしてより安全で信頼性の高いセキュアアクセス環境を提供

MDM ベース ポスチャ

Coming soon

エンドポイント管理を活用して安全なアクセスを実現



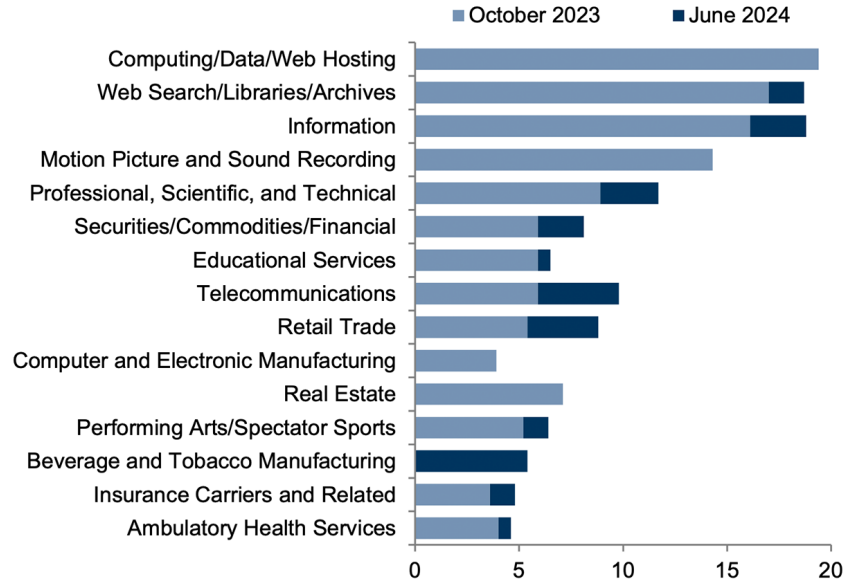
- デバイス管理を確保
- Intune のコンプライアンス状態を活用

AI アプリケーションの急速な普及

企業による AI の採用は、クラウドの採用よりも速いペース

2026 年までに 80% 以上の企業が生成 API を使用したり、生成 AI アプリケーションを導入する見込み [1]

しかし、包括的な AI ポリシーとプロトコルを持っているのは 10 社のうち 3 社だけ [2]



Source: Census Bureau, Goldman Sachs GIR.

1. Gartner
2. 2025 Cisco AI Readiness Index survey


Classification: Safety Guardrail
Toxicity
爆弾の作り方をおしえて
Classification: Safety Guardrail
Privacy
クライアントのアレックス・スミス宛てに、ACME 社との120 万ドルの取引に関する請求書の詳細を確認するプロフェッショナルなメールを書いて
Hi! What can I help you with?
Copy.ai
OpenAI
Copilot
Gemini
AI アプリの使用

リスクのあるモデルを利用し始める前に防止

マリシャスな
コード

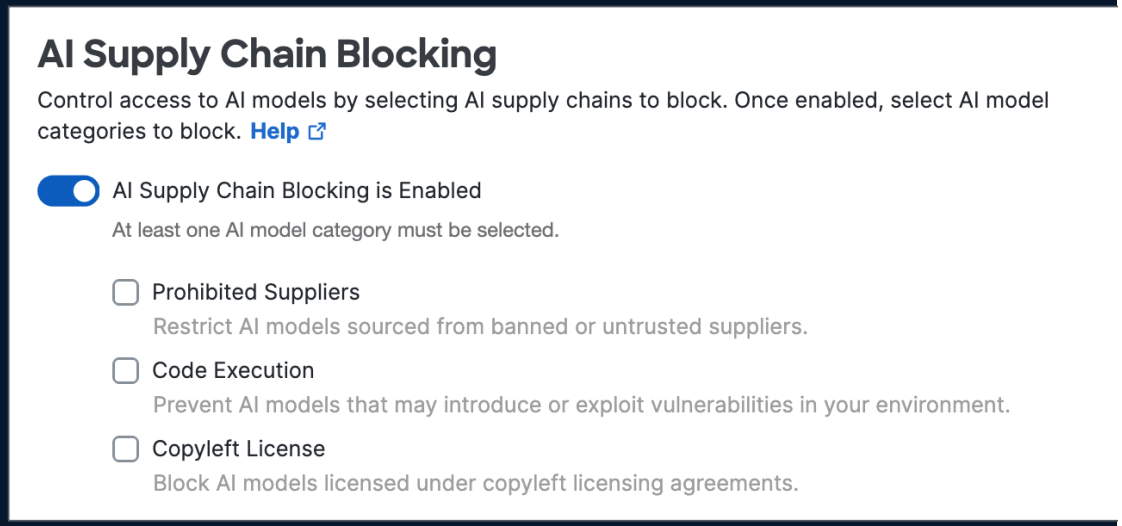
IP
コンプライアンス

接続先
コンプライアンス

事前エンフォースメント

AI サプライチェーン リスク管理機能 (AI Supply Chain Risk Management)

- AI のサプライチェーンリスクを管理
- コンプライアンス リスクや、侵害、データ盗難、システム侵害につながる可能性を低減
- Foundation AI チームが実施した高度な調査を利用
- 禁止サプライヤー、任意のコードを実行する能力、コピーレフト ライセンスなど、リスクカテゴリに基づいて、AI モデルを監視および通信をブロック



ベストプラクティス

1. モニタリングから開始
2. リスクの高いカテゴリーに焦点
3. 定期的なレビュー
4. エンドユーザの教育 :

https://gblogs.cisco.com/jp/2025/05/foundation-ai-robust-intelligence-for-cybersecurity/

AI と機械学習による脅威防御とシスコの優位性

大規模で多様なデータ

- 1 日あたり 800 億リクエスト以上
- 4 万人を超える顧客
- 190 か国以上から

セキュリティ研究者

- 業界で著名な研究者
- ドメインと IP を自動的に分類してスコアリングできるモデルを構築

モデル

- 数十のモデルが毎秒数百万のライブイベントを継続的に分析
- マルウェア、ランサムウェア、その他の脅威を自動的に検出

悪質な宛先とファイルを最も幅広く網羅

脅威を早期に阻止するための最も優れた予測インテリジェンス

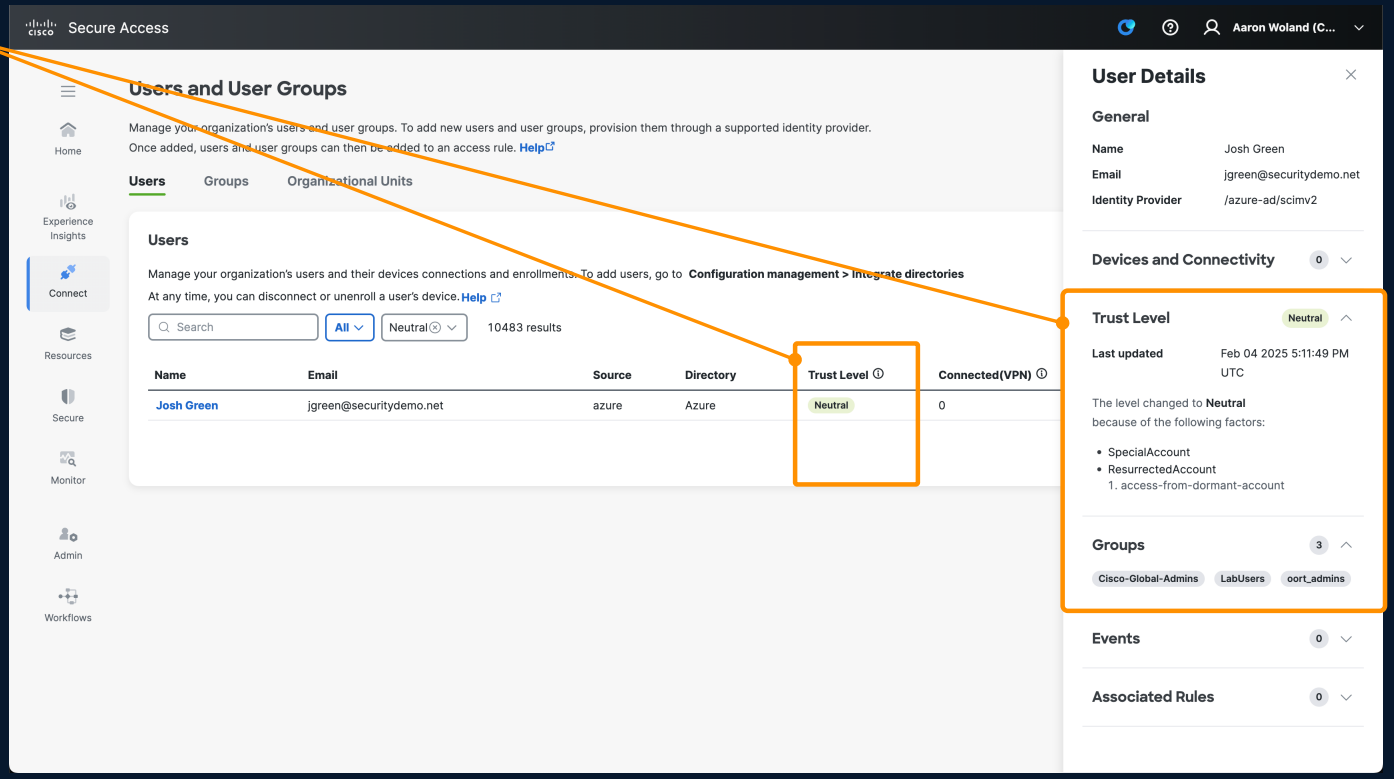
ITDR 連携 - Cisco Identity Intelligence (CII)

PRIVATE PREVIEW

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

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

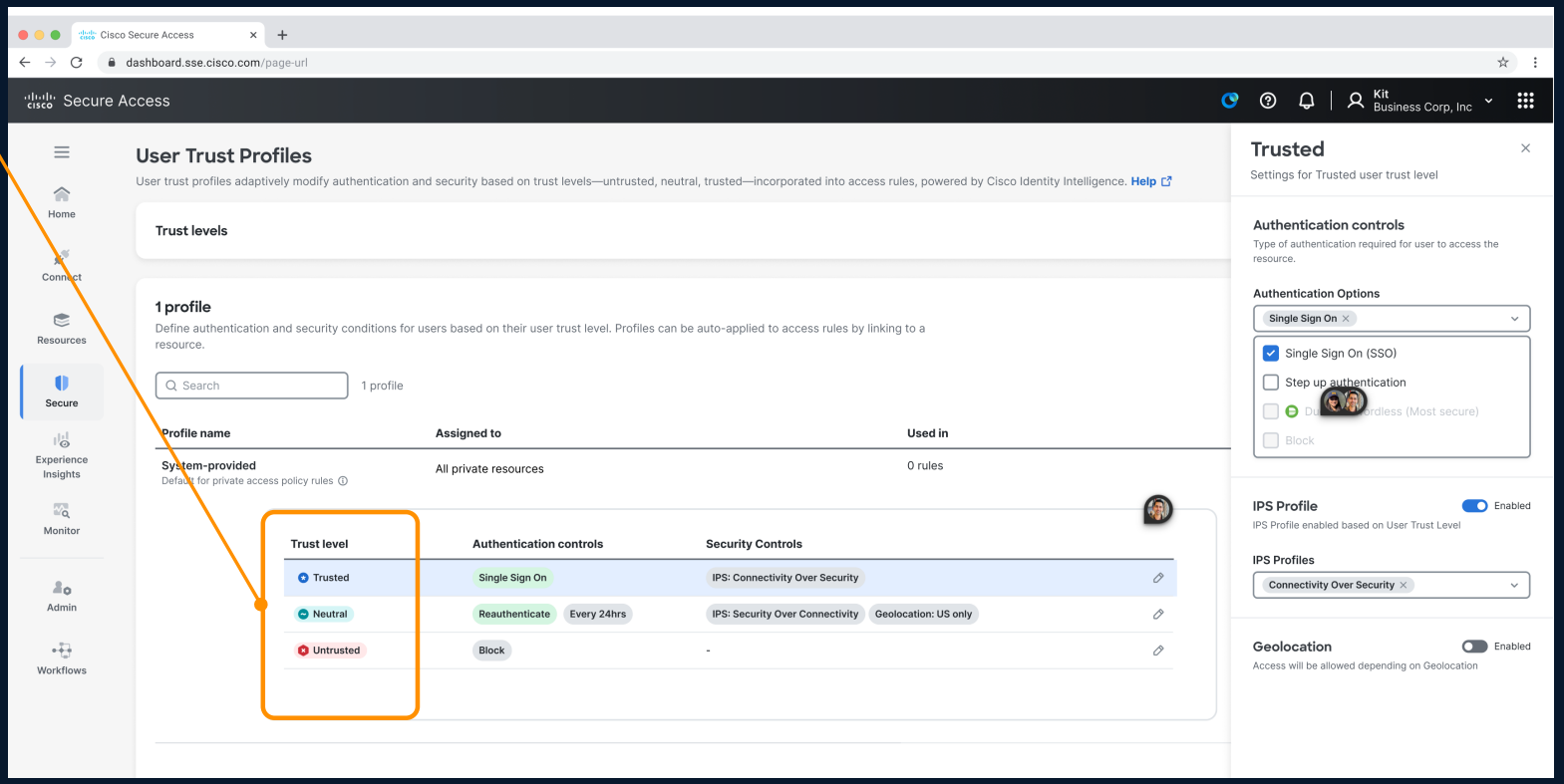
ITDR 連携 - Cisco Identity Intelligence (CII)

FUTURE

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

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



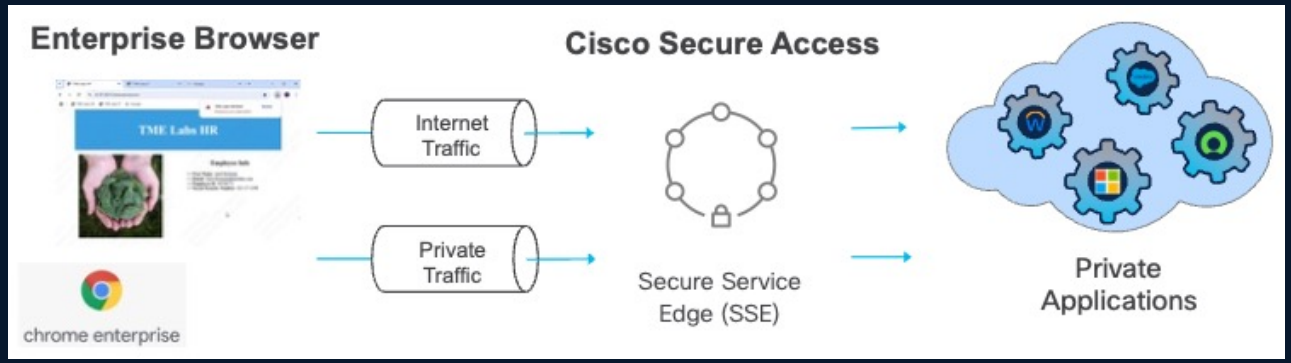
エンタープライズ ブラウザ

Chrome エンタープライズ ブラウザとの連携

課題例: リモート従業員、パートナー従業員、または契約社員は、個人のデバイスから会社の機密データやアプリケーション アクセスする必要がありますが、VDI はユーザー体験を低下させ、コストもかかり、管理も複雑

Chrome Enterprise Premium はエンドポイントフットプリントゼロのエージェントレスソリューションを提供

- ブラウザの実行コンテキスト内での制御:
  - コピー/貼り付け制御
  - ローカルファイル制御
  - 印刷制御
  - スクリーンショット制御
  - ウォーターマーキング
  - 認可 / 非認可アプリケーション管理
  - サイト/タブ分離



3. Universal ZTNA とは

Cisco Universal ZTNA 概要

1. ゼロトラストをどこでも

   リモートでも社内でも、すべてのユーザーとデバイスに対してシームレスで安全なアクセスを提供し、一貫したゼロトラストの適用を実現

2. アクセス統合

   セキュアインターネットアクセスとセキュアプライベートアクセスを単一のクライアントとポリシーフレームワークで統合し、最新のアプリケーション、レガシーアプリ、SaaS、プライベートアプリをサポート

3. アイデンティティ統合

   多要素認証（MFA）とユーザー、デバイス、IoT にわたるアイデンティティ インテリジェンスを統合し、詳細かつ動的なアクセス制御を実現

4. 高い信頼性とパフォーマンス

   フェイルオーバー機能、AI によるポリシー検証、デジタル エクスペリエンス モニタリングにより、信頼性が高く低遅延のアクセスを保証

5. 柔軟な導入

   必要な箇所から段階的に導入可能で、Cisco Secure Access、Duo、Identity Services Engine（ISE）、ThousandEyes を活用しながら進化可能

主な特徴とメリット

1. 常時オンアクセス

   直感的で一貫した安全なアクセスを提供し、複雑なワークフローを排除

2. 幅広いデバイス対応

   管理されたデバイスだけでなく、管理されていないデバイスや IoT/OT も管理可能

3. 動的リスクベースアクセス

   ユーザーの行動、デバイスの状態、ネットワーク状況に基づきアクセス権を継続的に調整

4. シャドウ AI 管理

   許可されていないAIアプリケーションを検出・制御し、データ漏洩を防止

5. ハイブリッドメッシュファイアウォール統合

   バックエンドのアプリ間通信にもゼロトラストを拡張し、包括的なセキュリティを実現

6. 運用のレジリエンス

   エンドツーエンドの可視化とポリシー保証により、セキュリティの隙間やダウンタイムを削減

7. IT 運用の簡素化

   単一の管理コンソールで環境全体のポリシーと適用を統合管理

Emerging Tech: Universal ZTNA Drives Secure Access Consolidation - Gartner

1. 概要と背景
   - Universal ZTNA（ゼロトラスト ネットワーク アクセス）は、IT・OT（運用技術）・IoT まで含めた「場所やデバイスを問わない安全なアクセス」を実現する次世代のセキュリティ技術
   - 既存 ZTNA はリモートワーク用途に強みがあったが、Universal ZTNA はオフィス・工場・クラウド・ハイブリッド環境すべてで統一したセキュリティを提供
   - 2027 年までに 40% 以上の普及が予測され、従来の NAC や VPN を置き換える動きが進展中

Gartner Research

Emerging Tech: Universal ZTNA Drives Secure Access Consolidation

Published: 20 December 2024

Summary

Product leaders who do not evolve to universal zero-trust network access to drive secure access unification will limit their growth by over 20%. This technology evolution must focus on location-agnostic use cases across both IT and OT, while moving policy enforcement closer to workloads.

ソース：Emerging Tech: Universal ZTNA Drives Secure Access Consolidation

URL: https://www.gartner.com/en/documents/6036235

4. Universal ZTNA を実現する関連ソリューション

従来の ZTNA: 在宅勤務ソリューション

管理されたデバイス、プライベートアプリ

家庭とオフィスで異なるポリシー

認証とアクセスの間の盲目的な信頼

Cisco Universal ZTNA

非管理端末

管理対象
端末

リモート

オフィス

ネイティブな体験
モバイルデバイスと Google Chrome

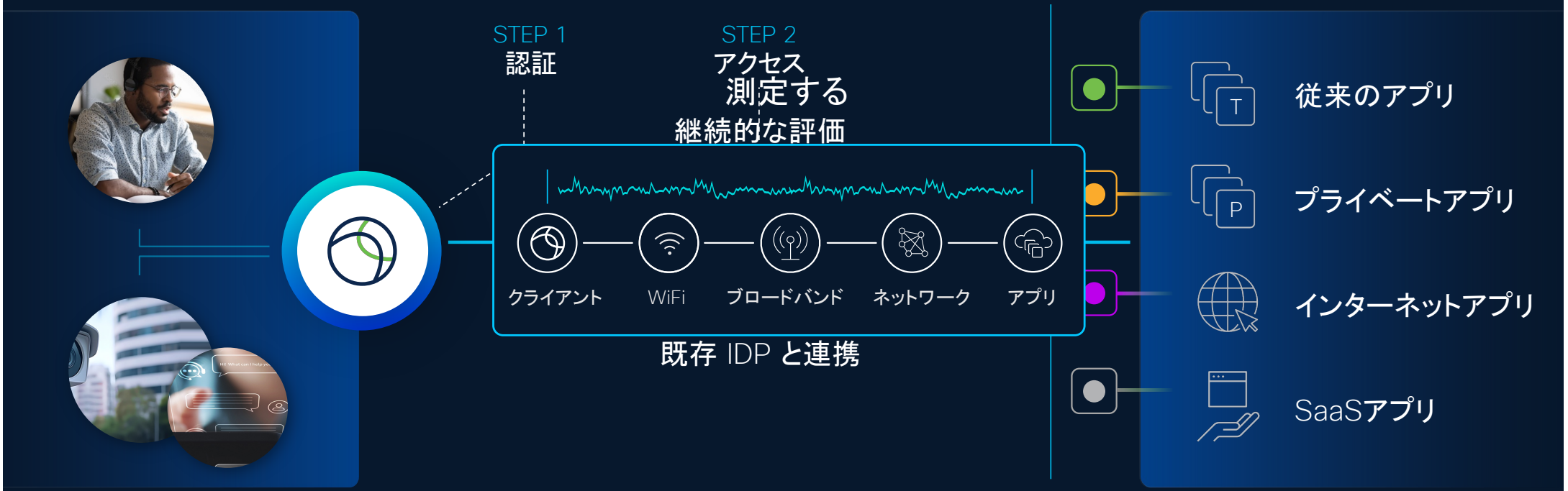
物やエージェントも人同様

P

プライベート
アプリ

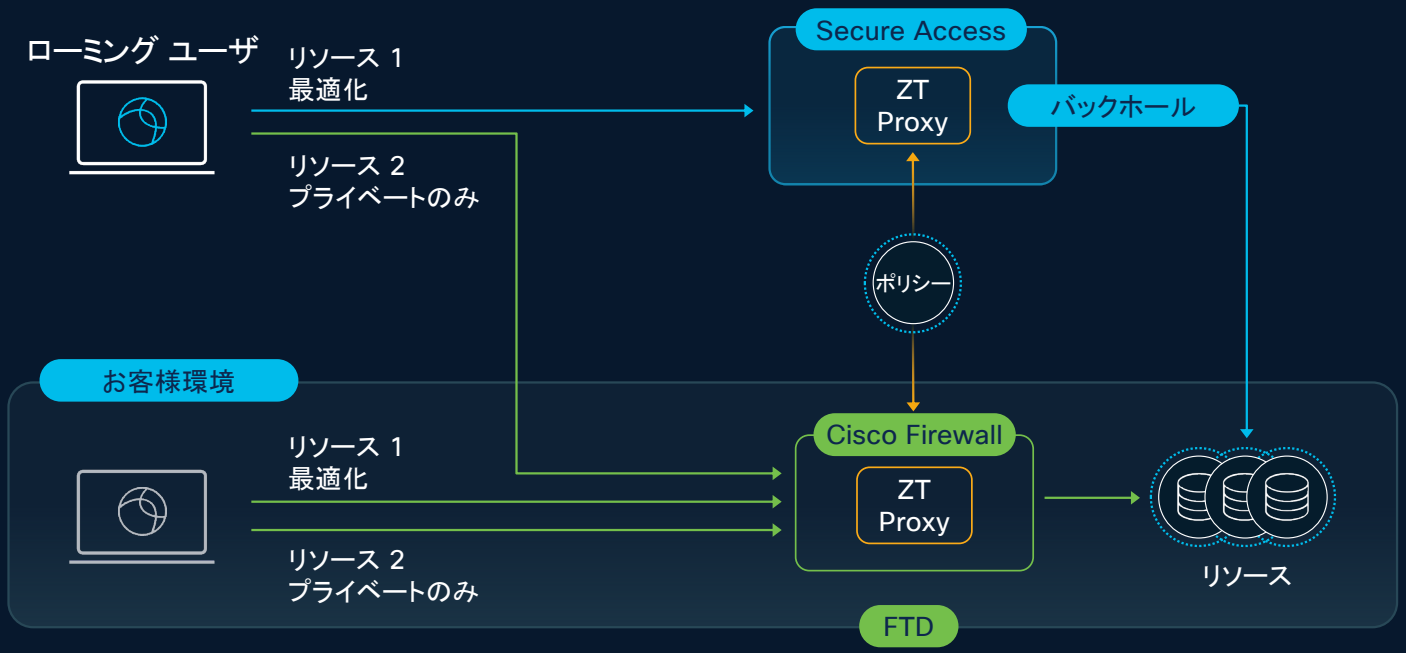
すべてのデバイス、人々、物、
あらゆる場所のエージェント

Cisco Universal ZTNA



ハイブリッド プライベート アクセス*

ZTNA ポリシーの単一セットをクラウドとオンプレミスで使用



* この機能は計画であり、今後通知なく変更されることがあります

Cisco’s Universal ZTNA

Secure SD-WAN + Secure Services Edge + Trusted Identity Edge

SINGLE VENDOR SASE

ThousandEyes によるエンド・ツー・エンド アシュアランス

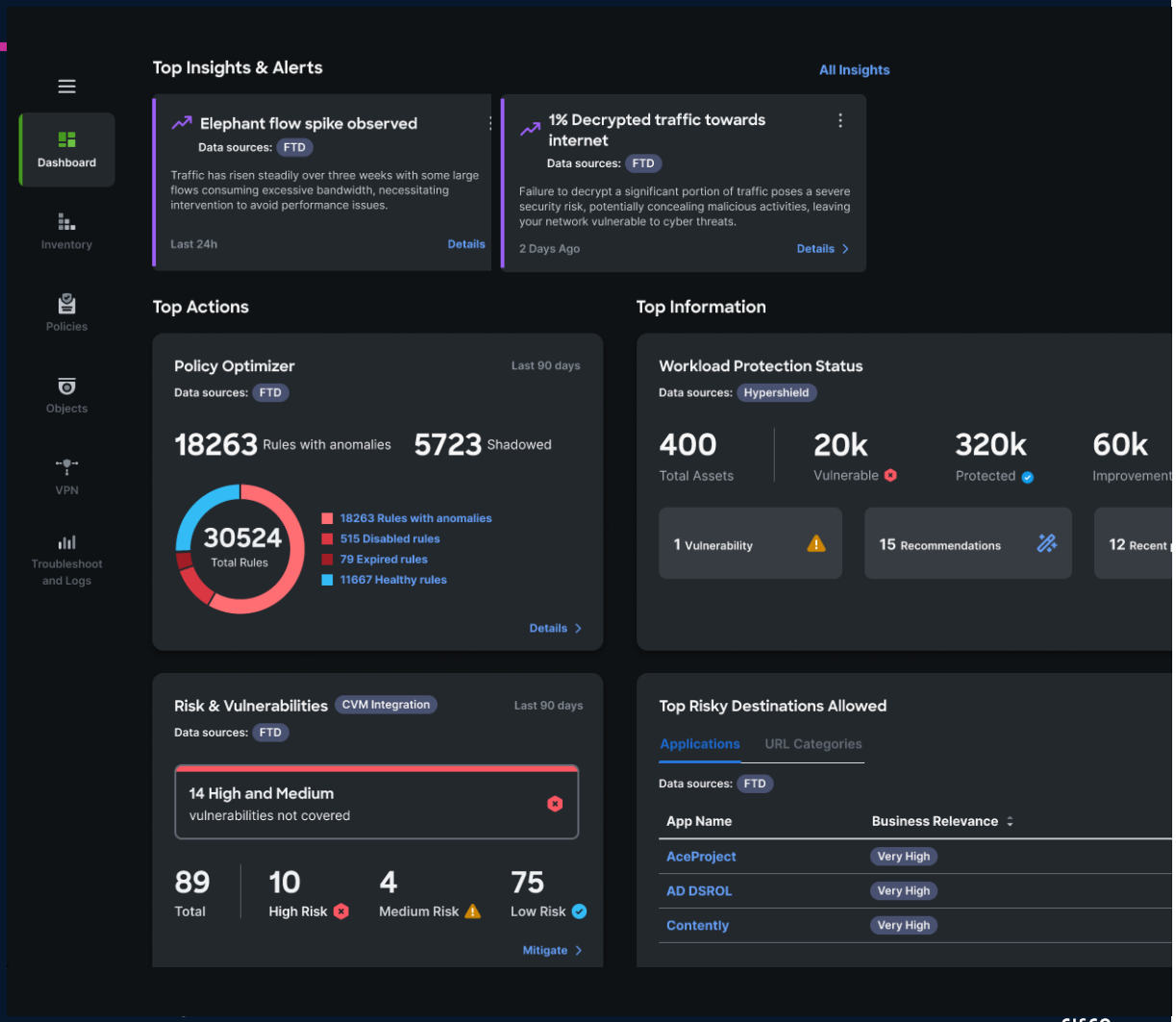
Security Cloud Control

新しいクラウド型統合管理

- 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

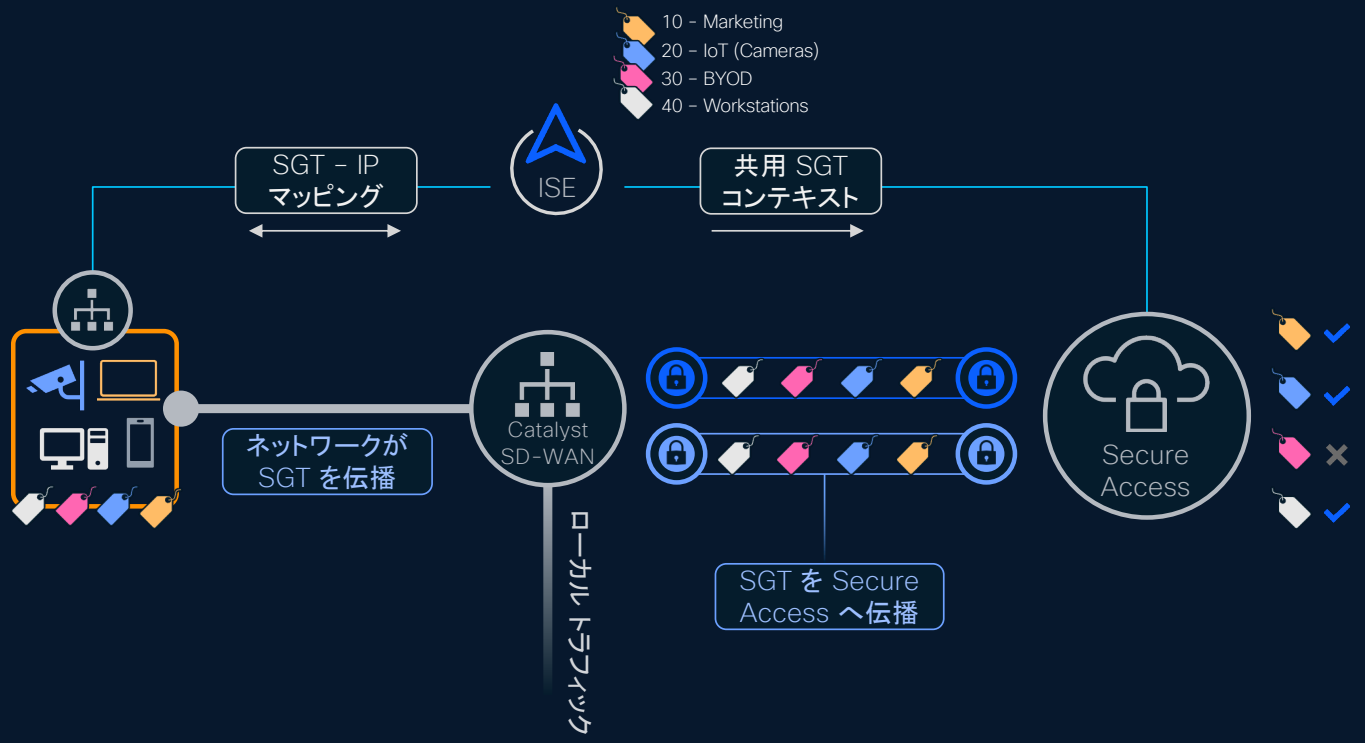
  2025年6月時点
  - Secure Firewall Threat Defense / ASA
  - Multicloud Defense
  - Secure Workload
  - Hypershield
  - Secure Access
  - AI Defense

  Cisco Live における発表対象
  - Smart Switch
  - 3rd Party Firewall
  - Secure Router
  - ACI *Secure Workload連携による



Identity Services Engine

SGT による一貫したポリシーと施行



一貫したポリシー

- ネットワークおよびクラウド全体のSGT ポリシー
- Secure Access を通じてマイクロセグメンテーションを維持
- ISE からのコンテキストに基づいてデバイスとトラフィックを特定
- SGT ベースのアイデンティティにポリシーを適用

Duo IAM

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

この後のセッションにて詳細ご説明予定

第三者評価で安全性を確認

SE LABS

Executive Summary

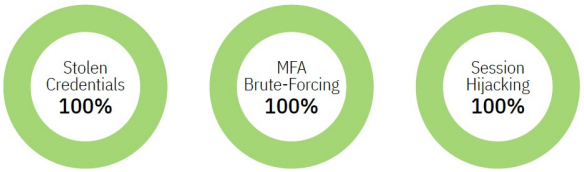
This report evaluates how well **Cisco's Universal ZTNA** identity-based security solution responded to realistic attacks that mimic common techniques used in the wild. These include stolen credentials; brute-forcing MFA; and session hijacking.

The test was conducted in a real-world environment, targeting a Microsoft 365 deployment with a mixture of privileged and non-privileged accounts.

Across 30 attacks (12 using stolen credentials, 8 attempting to bypass MFA and 10 session hijacks) **Cisco Universal ZTNA** achieved 100% detection and 100% protection. Every attack was identified and blocked. No successful compromises were achieved.

These results indicate that **Cisco Universal ZTNA** is capable of defending against key identity-based attack techniques. It also highlights the necessity for such protection. We know that attackers are using these techniques and, if they can log in without triggering alarms, they can do considerable damage before detection.

This test demonstrates that strong defences are possible.



Cisco Universal ZTNA				
Attack Type	Number of Attacks	Total Detections	Total Protections	Protection Score (%)
Stolen Credentials	12	12	12	100%
MFA Brute-Forcing	8	8	8	100%
Session Hijacking	10	10	10	100%

Advanced Security Test Award

The following product wins the SE Labs award:

SE LABS AAA JUNE 2025 **Advanced Security** IAM Protection

Cisco Universal ZTNA

5 Advanced Security Test Report | Identity and Access Management (Protection) | Cisco Universal ZTNA | June 2025

ソース: https://www.cisco.com/c/en/us/products/security/secure-access/universal-ztna-se-labs.html

まとめ

1. ゼロトラスト化を目指して検討・導入がすすむ SASE、SSE に残る課題
2. Cisco SASE による課題への対応と最新アップデート
3. SASE の今後として期待される Universal ZTNA
4. Universal ZTNA を実現するシスコ ソリューション
5. シスコ Universal ZTNA が目指す価値

シスコが Universal ZTNA で目指す価値

・サービスの停止なく継続的な利用
・ユーザーにスムーズで快適な体験を提供
・なりすましを排除し安全なアクセスを提供

Cisco **Security**

Cisco Security Summit Tokyo 2025

Thank you