Cisco Security

シスコ エンタープライズ企業向けマンスリーウェビナー

セキュリティファーストのIAMを目指して 新Duo IAMの発表

Hiroki Hata, Takashi Yamamoto

2025 年 7 月

アメリカ時間の2025年5月28日に発表

= MFA ?

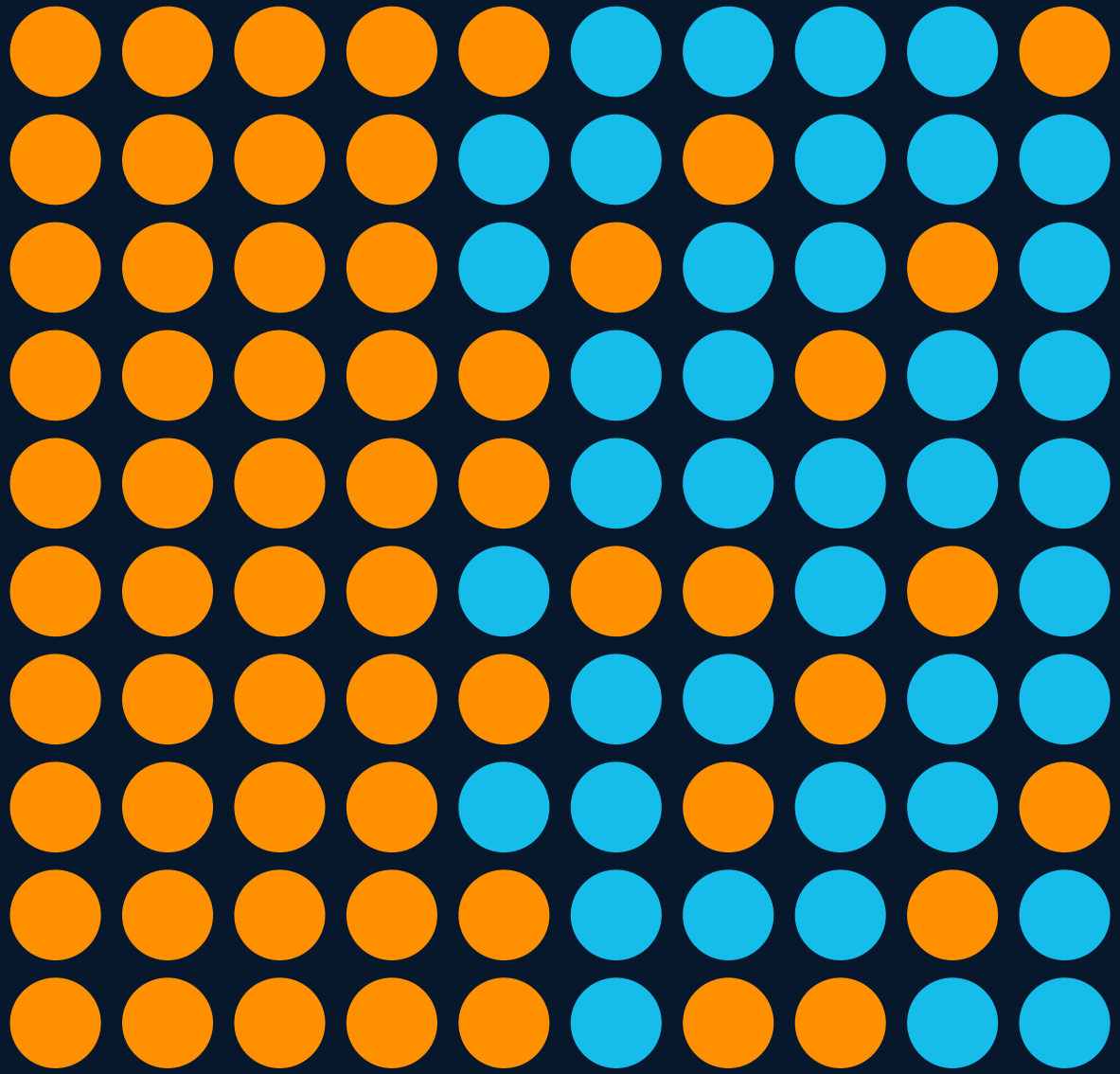
アメリカ時間の2025年5月28日に発表

= IAM

“

Duo は、アイデンティティベースの攻撃を阻止する唯一のセキュリティファーストの IAM ソリューションを発表します。

”



数年前から年々悪化している
→Identityの危機

60%

の情報漏洩はIdentityの漏洩が重要な要素になっている
（Identityがなければ起こらない）

Cisco Talos Incident Response | Year in Review 2024

これまでのIAMはIdentityを守れてきたでしょうか？

これまでのIAMは業務を開始する、生産性を向上することが主目的

セキュリティ意識の欠如

アタックサーフェスの拡大

MFAのバイパスを許容

AI がより拡大を容易に

複雑で高価な対策

セキュリティを上位Editionに

複雑なポリシー構造

設定不可能

断片化され可視化不可

Identity全体可視化不可能

限定されたホスチャ機能

脅威対策の遅延

エンドユーザーと管理者の不満増大

セキュリティか生産性かの二択 | MFA 疲労攻撃 | ヘルプデスク負荷の増大

これまでのIAMはIdentityを守れてきたでしょうか？

これまでのIAMは業務を開始する、生産性を向上することが主目的

セキュリティ意識の欠如

アタックサーフェスの拡大

MFAのバイパスを許容

AI がより拡大を容易に

複雑で高価な対策

セキュリティ≠生産性tionに

複雑なポリシー構造

設定不可能

断片化され可視化不可

Identity全体可視化不可能

限定されたホスチャ機能

脅威対策の遅延

エンドユーザーと管理者の不満増大

セキュリティか生産性かの二択 | MFA 疲労攻撃 | ヘルプデスク負荷の増大

Duo は信頼できるIdentity管理として IAMを再定義します

Cisco Duoが提供する新しい IAM（Identity & Access Management）

お客様が信頼できるIdentityを提供

NEW

セキュリティFirstのIAM

導入時点で守られている

NEW

End to Endで
フィッシング耐性のMFA

完全にフィッシングの可能性を排除

統合Identity Intelligence

継続的に信頼を検証する

世界レベルのユーザエクスペリエンスをエンドユーザーと管理者に

攻撃者を困らせ，ユーザが使いやすい

Identityの信頼を再定義

セキュリティFirstのIAM

導入時点で守られている

Duo IAM はセキュリティをデフォルトとする。
最も簡単で柔軟な方法でIdentityを守る。

提供される機能

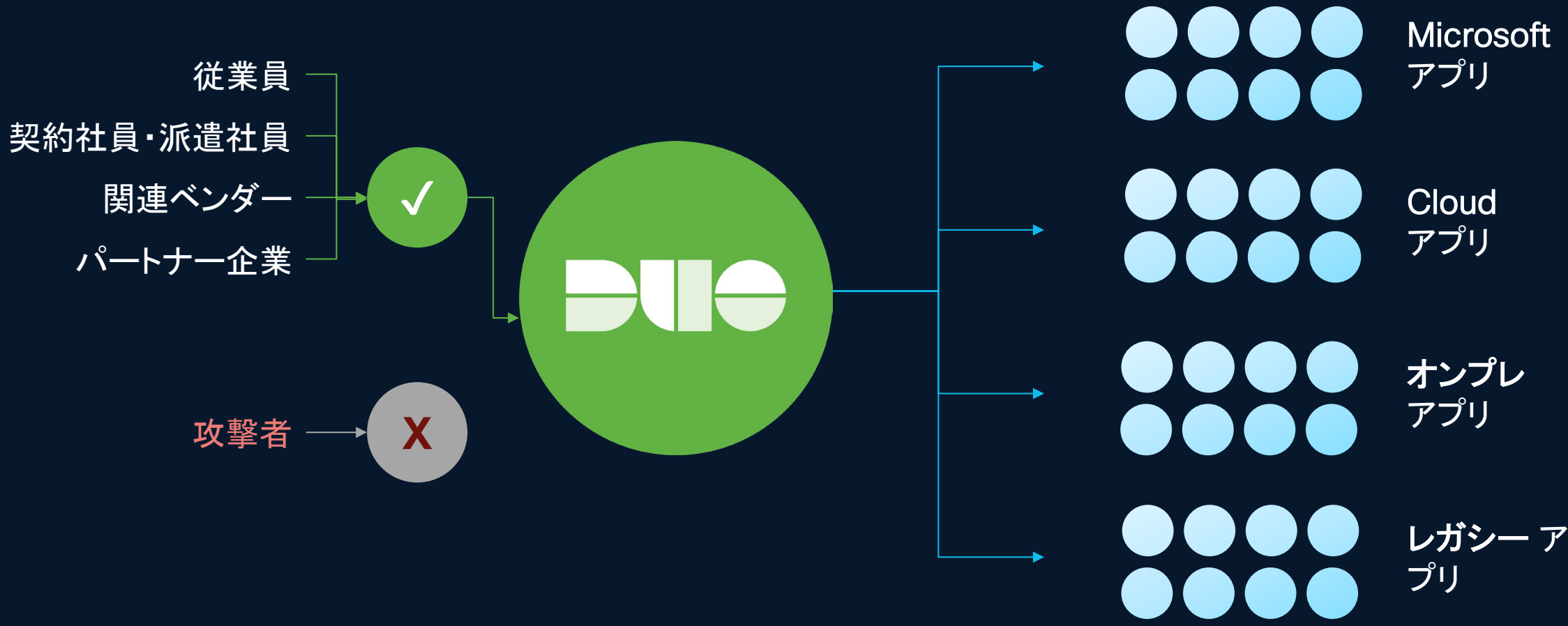
NEW 柔軟なDirectory管理

NEW 完全パスワードレス

- 強固なMFAがデフォルト
- アクセスデバイスの信頼性を確保

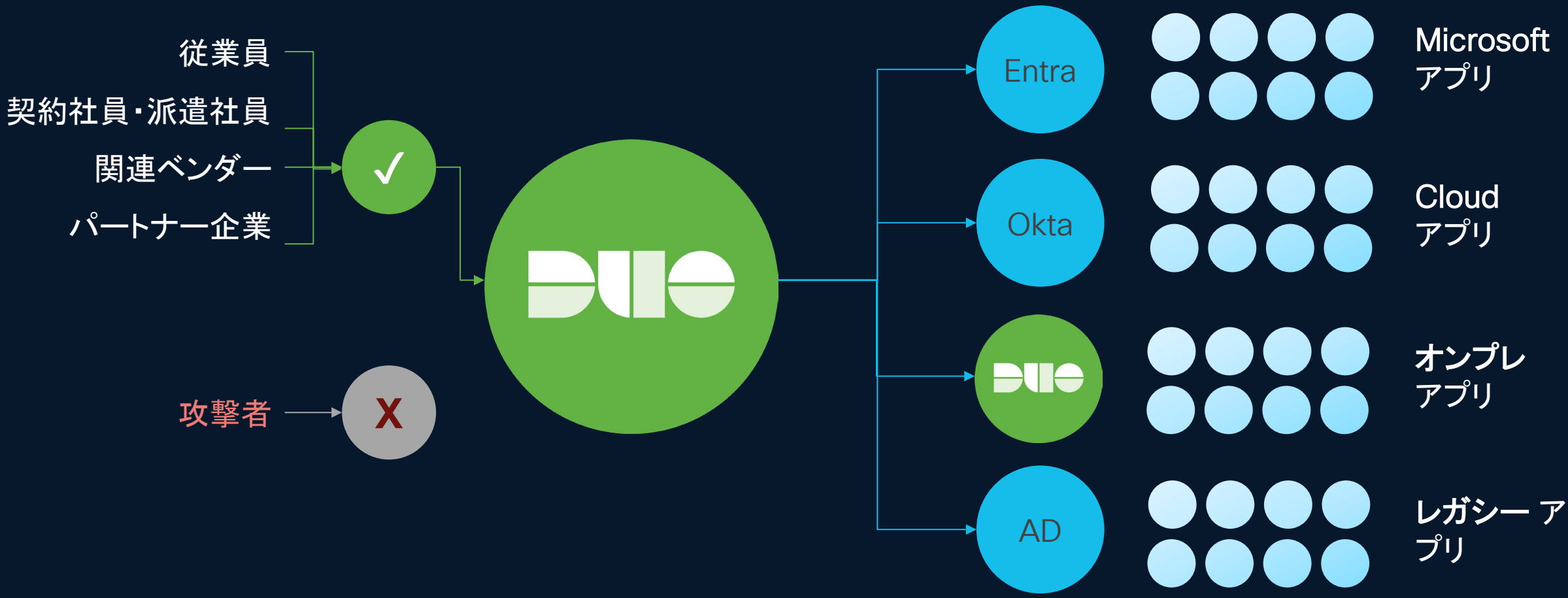
NEW 柔軟で簡単な設計・設定

Duo Directory 単体で利用可能（パスワードも保持）



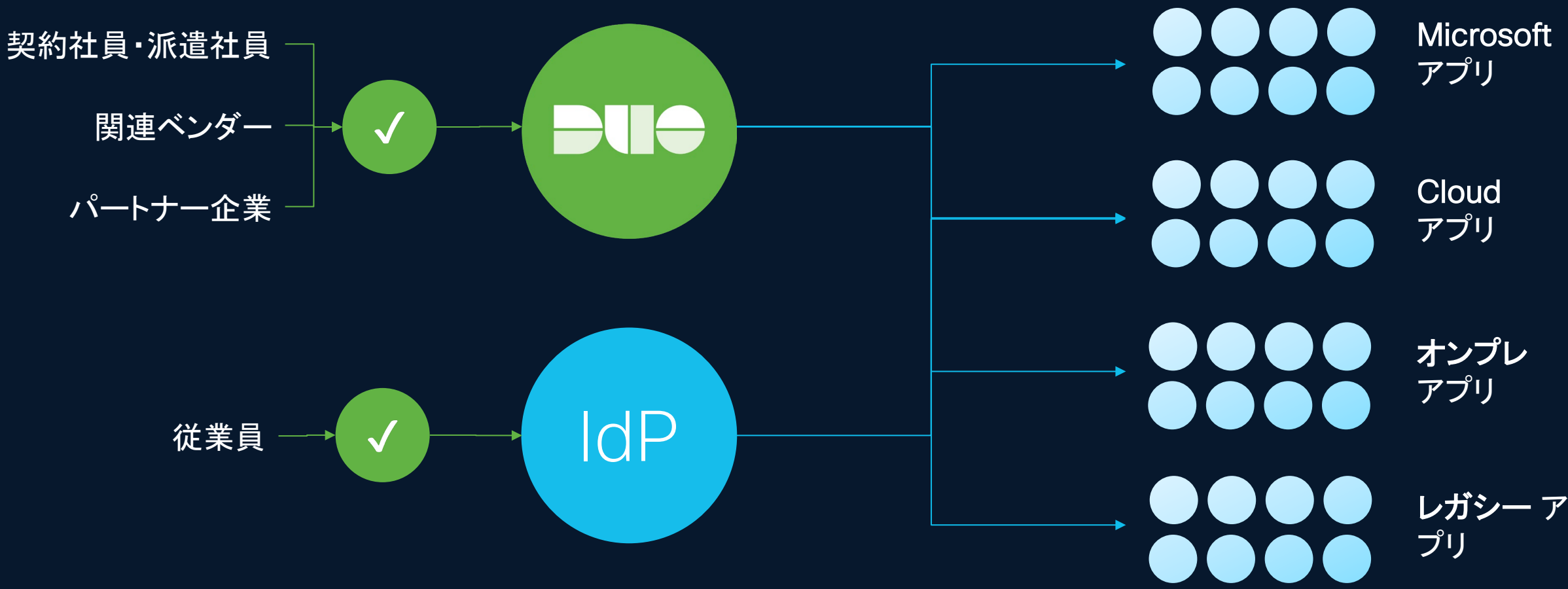
他のIDPの前面にDuoを置き、Duo Directoryを並行稼働

Duoは既存IDPの前面で、MFAを含む認証を担うことでIdentityに対する攻撃を遮断します



他のIDPを主として、Duo Directoryを並行稼働

Duoは既存IDPの前面で、MFAを含む認証を担うことでIdentityに対する攻撃を遮断します



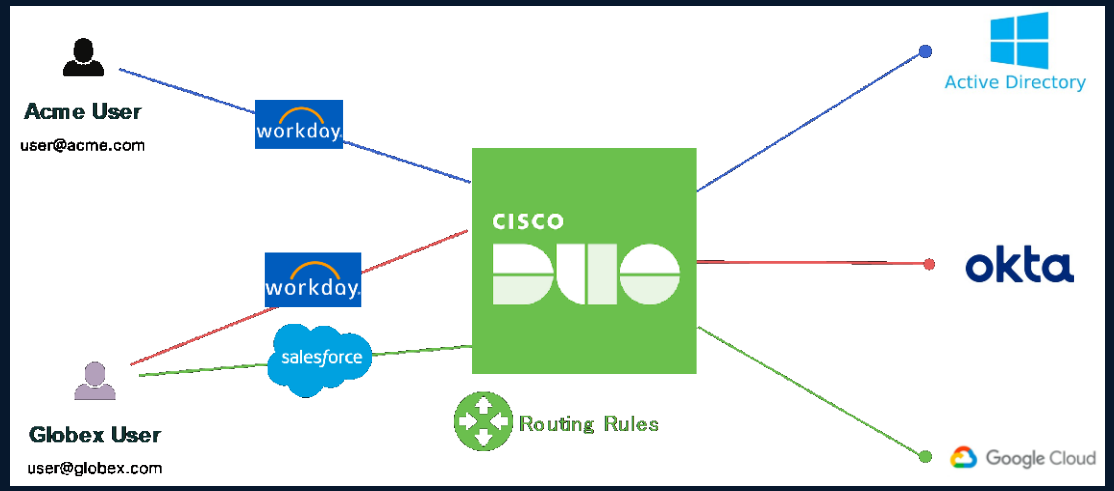
どんなIDPとも柔軟に連携

柔軟なDirectory管理

Duo SSO Routing Rules

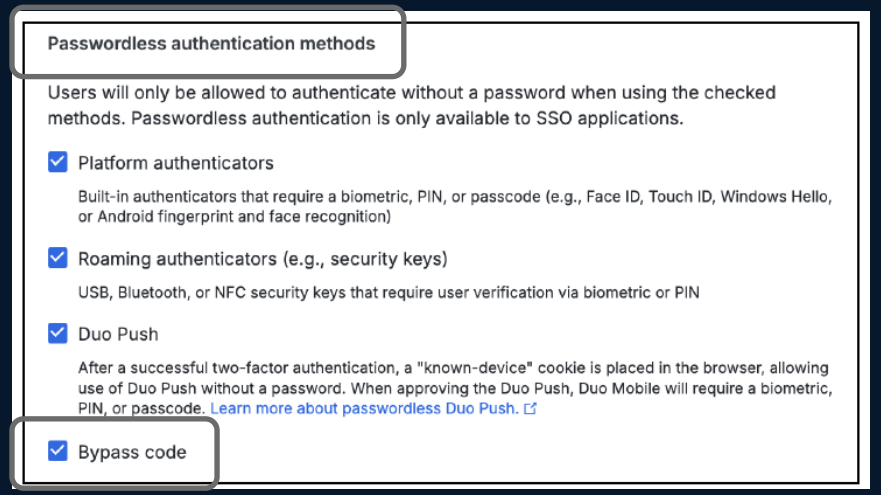
アクセス制御の統合、組織への共通ポリシーの適用を可能に。エンドユーザのU/Iもシンプルに。

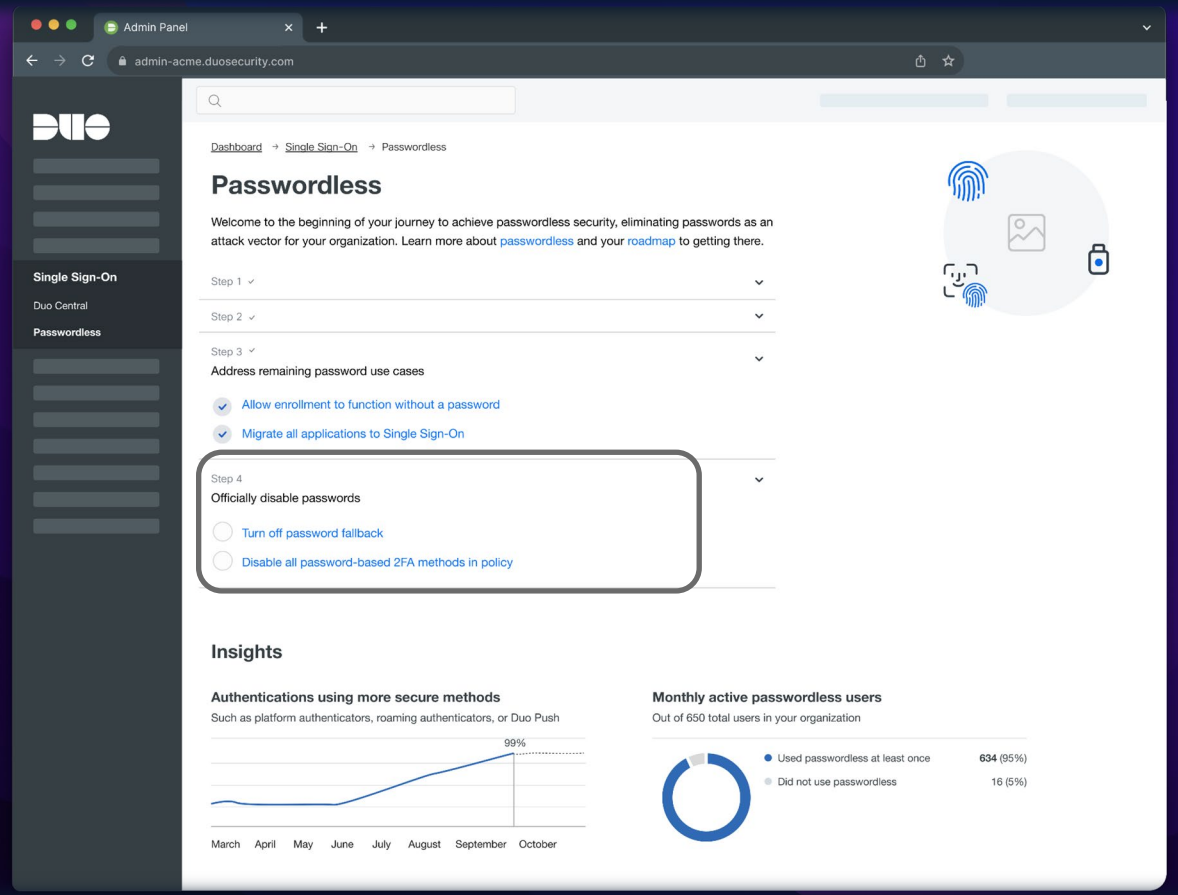
SSO Routing Rules 動作概要



完全なるパスワードレス認証の実現(Public Preview)

- パスワードへのフォールバックを禁止し、パスワードレスでの利用が可能
- パスワードレス認証がパスワードレスが動作しない緊急のケースにおいてはバイパスコードを利用可能





導入当初から使えるAIアシスタント (Private Preview)

- Duoの設定方法を単純化して、アシスト

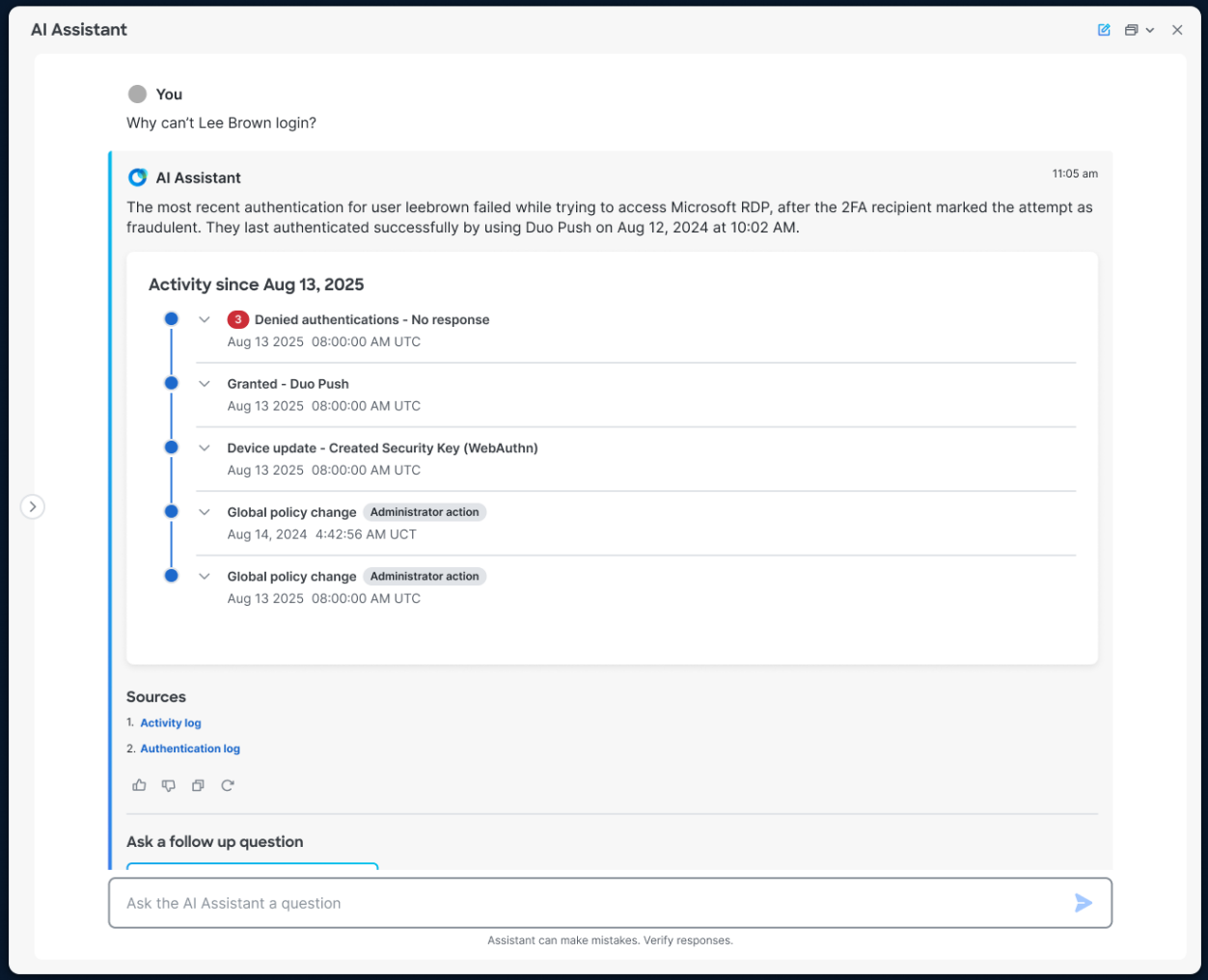
“How do I set group policy?”

→グループポリシーの設定方法をAIが単純化して管理者をアシスト

- ユーザの調査を容易に

“Why is Lee blocked?”

→ユーザの認証がなぜブロックされたのかをAIが調査して必要な情報を表示します



Duo の AI Assistant は、シームレスに認証ログ、デバイスのデータ、管理者の行動ログ、Duoのドキュメント及びナレッジベース（KB）を検索することができます。

Identityの信頼を再定義

End to Endで
フィッシング耐性のMFA

完全にフィッシングの可能性を排除

急増するIdentityに対する攻撃に対して
フィッシング耐性のMFAは最も有効

提供される機能

NEW 近接認証MFA（Proximity Verification）

- 完全パスワードレス（Complete Passwordless）
- 本人認証の検証（Identity Verification）
- セッション盗難防止（Session Theft Protection）

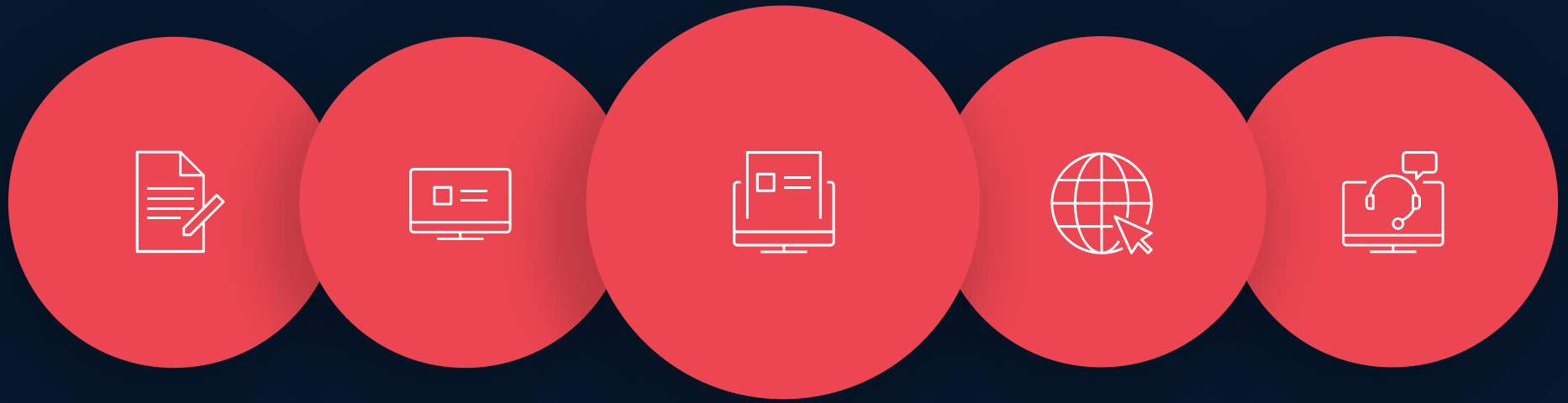
MFA だけではもはや不十分

攻撃対象は拡大しており、脅威は急速に拡大している

新しい社員に対するブルートフォース攻撃やパスワードスプレー攻撃が拡大

MFAをバイパスするため、疲労攻撃やVishing攻撃が拡大

セッションのクッキーを盗むフィッシング攻撃が急速に拡大



ID新規登録

OS ログイン

攻撃者は組織内にアクセスできるデバイスを登録しようとしている

Application ログイン

攻撃者はMFAオプションの選択で弱いMFAでの認証を狙っている

中間セッション

ヘルプデスク

攻撃者はヘルプデスクに対し、SNSの情報を利用して攻撃し、アクセス方法を確保しようとしている

Duoは end-to-end のフィッシング耐性プロセスを提供

ID新規登録

信頼できるIDのみ登録

OS ログイン

フィッシング耐性MFA

Application ログイン

フィッシング耐性MFA

中間セッション

中間者攻撃への防御

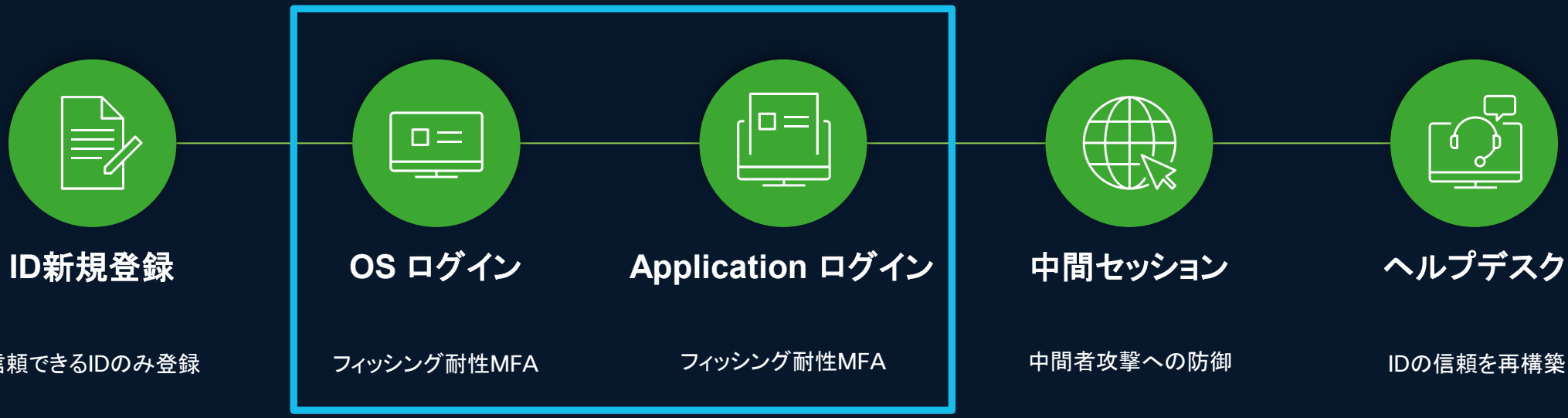
ヘルプデスク

IDの信頼を再構築

シームレスにセキュリティを確実に保護

Cisco Identity Intelligence（ITDR）にてID可視化→脅威検知と対策

Duoは end-to-end のフィッシング耐性プロセスを提供



シームレスにセキュリティを確実に保護

Cisco Identity Intelligence（ITDR）にてID可視化→脅威検知と対策

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は不要（セキュリティキーなど）

Duoは end-to-end のフィッシング耐性プロセスを提供

本人の信頼性を確実に確認

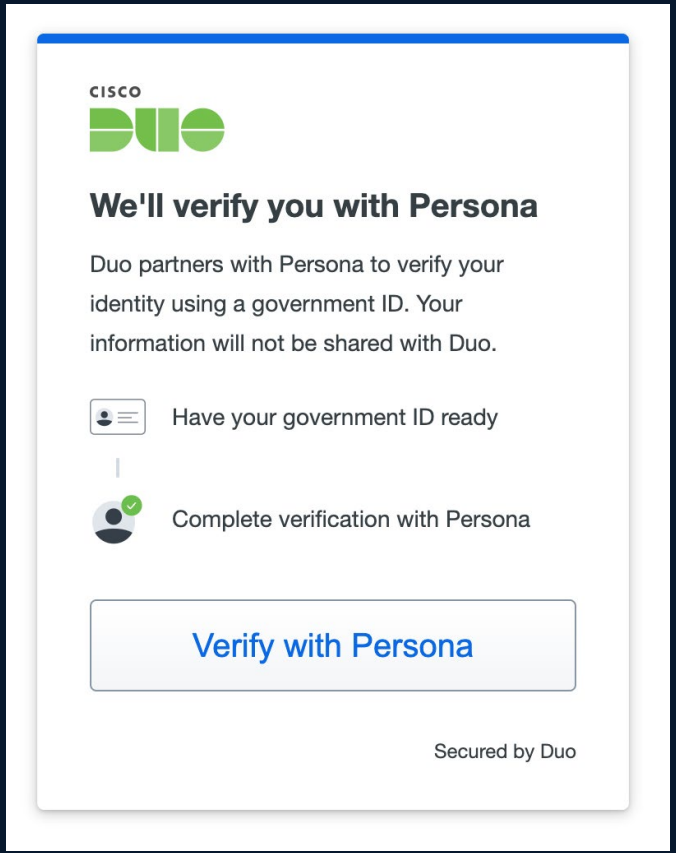
Duo Identity Verification Integration

- ユーザーのIDのライフサイクルにおける重要な場面（初期登録等）におけるIDの信頼性確認のワークフローを導入可能
- 最初の機能提供は、ペルソナ社と連携したIDの信頼性確認
  - ✓ 柔軟性と幅広いオプション
  - ✓ グローバルなサポート
  - ✓ CiscoおよびDuoとの親和性
- 主な提供予定

  ヘルプデスク検証（現在Private Preview）

  リモートオンボーディング（7月にPrivate Preview予定）

  セルフサービス



信頼を確立するために、ユーザーはDuoに保存されている情報を照合し、政府発行のIDと自撮り写真を提出しなければならない。

Duoは end-to-end のフィッシング耐性プロセスを提供

シームレスにセキュリティを確実に保護

Cisco Identity Intelligence（ITDR）にてID可視化→脅威検知と対策


実際のログインページ
ハッカーにコントロールされるプロキシページ
通常と同じように見える偽のページ

Cisco Differentiator

セッション盗難防止（Session Theft Protection）

Duo がセッション・クッキーを排除 – 特許出願中の独自技術

Cookieがないため Cookieは盗めない

攻撃者はセッション Cookie を盗んで、すでに確立されたアクセスを乗っ取ります。セッション盗難防止機能を備えた Duo Passport は、認証フローから Cookie を削除するため、攻撃者は何も盗むものがなくなります。Duo のクッキーレスソリューションは、エンドユーザーエクスペリエンスを維持しながら、セキュリティにバランスの取れたアプローチを提供します。

Identityの信頼を再定義

統合Identity Intelligence

継続的に信頼を検証する

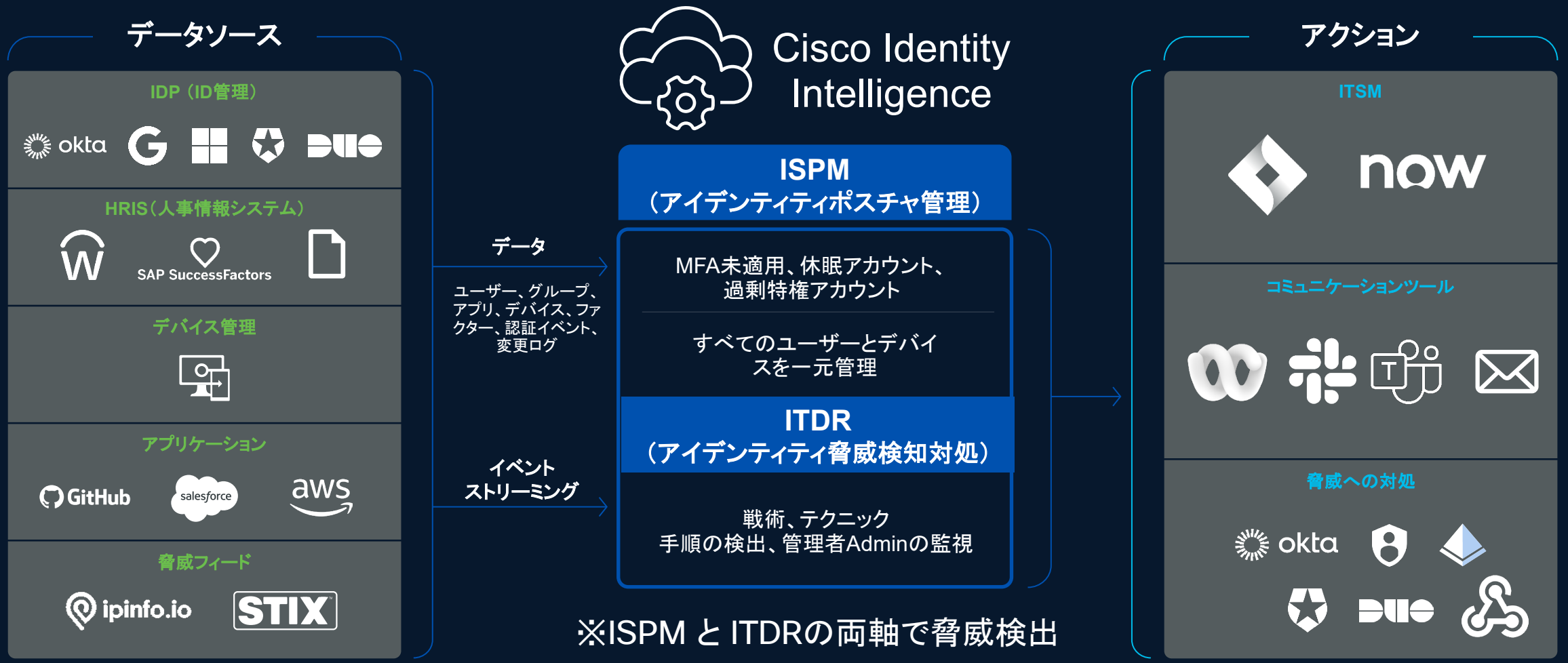
複数のIDPにまたがり広範囲でIDを可視化することにより、Identity脅威の検出と対応を強化。セキュリティを大幅に向上させることが可能。

提供される機能

- 包括的なIdentityの可視性
- ISPM と ITDRの両軸で脅威検出
- ユーザー人一人の信頼性確認
- Cisco ポートフォリオ横断でのIdentity信頼性の強化（XDR連携でスタート）

Cisco IT にて現在も継続利用

ID環境に対する可視化→ポスチャ→脅威検出→対応を強力に実現



Cisco Duo（多要素認証･デバイス認証）Advantageに搭載

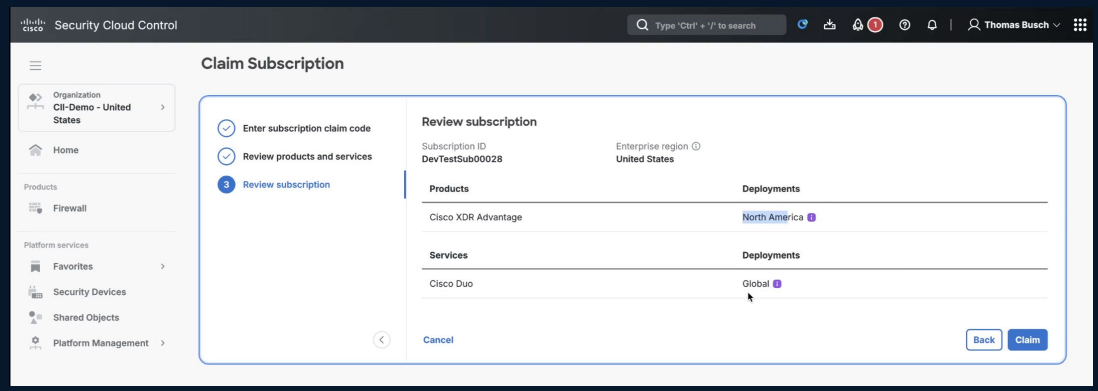
Cisco Identity Intelligence + XDR インテグレーション
(Private Preview)

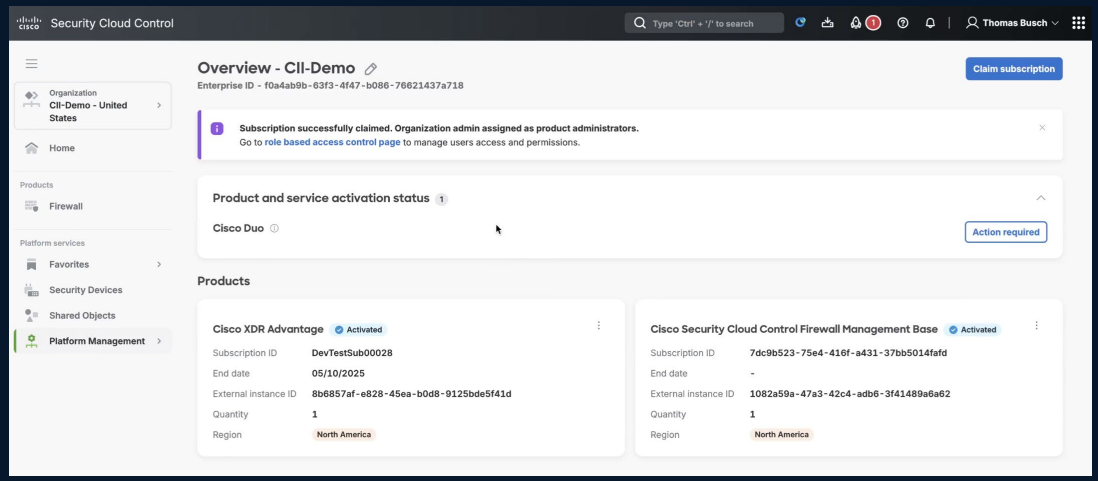
課題:

- XDRにはITDRの情報に対する機能がない。
- 漏洩の徹底的な調査には Identityに関連する情報が不可欠

Solution:

- Cisco PIAM を通じて全てのXDRのお客様はCisco Identity Intelligenceを自動プロビジョニング可能
- XDR はIdentityの情報、トラストレベル、ITDRのイベントを取り込み可能
- XDRに取り込まれたイベントにメールやユーザ名等の可視性を提供し、漏洩事故や漏洩調査の解決を協力にサポート
- セキュリティのイベントに関連するユーザの詳細を可視化可能
- スコアリングは、インシデントの優先順位付けに貢献可能
- 組織で活動しているユーザの全体像を把握するための資産インベントリを提供可能





Active Directory Defense (Private Preview前)

背景 / お客様の問題

-ほとんどの企業はオンプレAD（またはハイブリッド）が残存しており、ID情報はクラウドに同期されていない。

-オンプレADの設定不備を狙う攻撃は、不審な行動と同様に検出が難しい

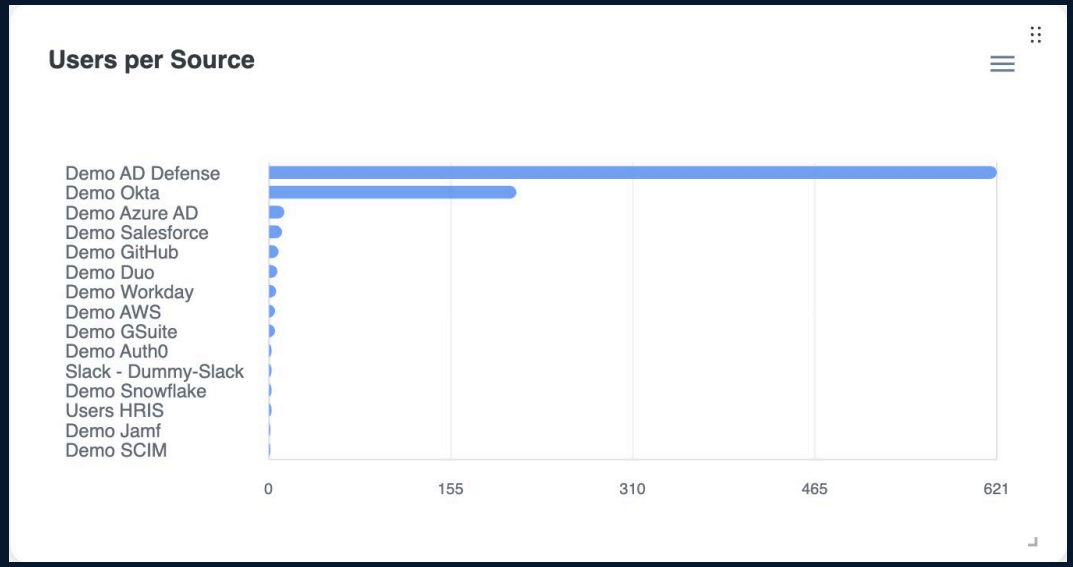
-レガシーなアプリケーションは最新のプロトコルをサポートしておらず、無防備なまま放置されている。

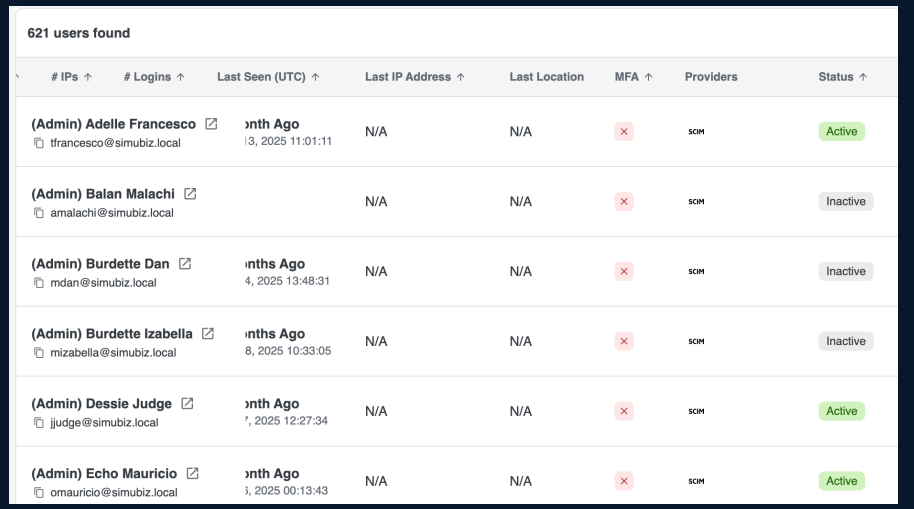
-MSがEntra IDに注力する中、ADセキュリティ市場は急成長

Active Directory Defenseプロジェクトの目標は、お客様のオンプレAD環境を保護し、ハイブリッド環境とオンプレミス環境を完全に可視化できるようにすること

最初の提供予定の機能 – Cisco Identity Intelligenceにおけるオンプレ AD情報の可視化

- ユーザーインベントリ：すべてのユーザー、アカウント（人間またはサービス）の包括的な可視性
- ポスチャと脅威検出のCheck ： ID履歴の包括的な可視化→脆弱性、不審な行動を検出するチェック
- オンプレミスとクラウド IdP 間の不整合及び包括的な分析





Identityの信頼を再定義

創業当時から追求する
ユーザエクスペリエンスを
エンドユーザーと管理者に

ユーザーと管理者は、業務生産性を低下させるセキュリティに疲弊しています。Duoは最も安全な方法です。

提供される機能

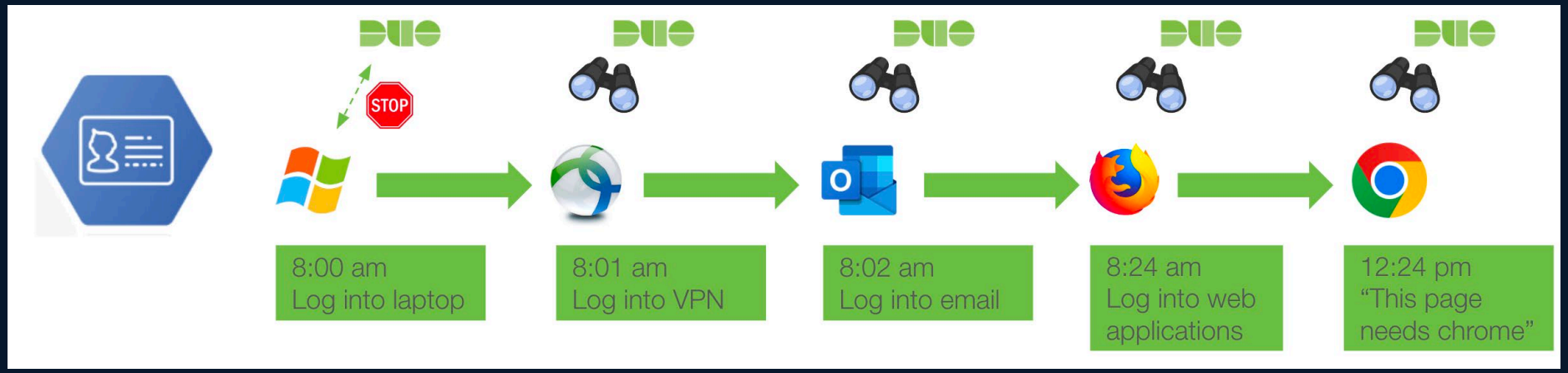
- 1日1回の唯一のログイン（Duo Passport）
- ユーザによる自己修復・管理機能が充実
- シンプルな設計と構成で短期間で導入
- 直感的で強力なポリシーエンジン

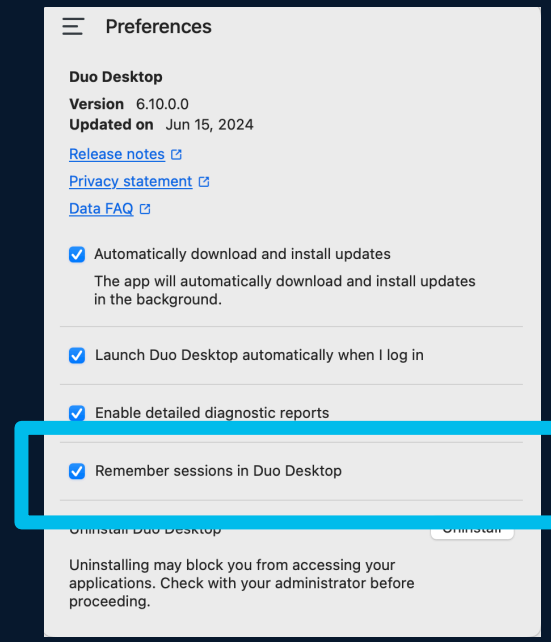
Duo Passport
Windows Logon時の１回の認証で１日認証なし業務可能（生産性向上）

エンドユーザー人ひとりの生産性が向上し、会社全体の業績向上に貢献

これまで5回の認証を必要としていた業務を1回の認証のみに

PC ログオン　VPN接続　メール参照　Webアプリ1　Webアプリ2

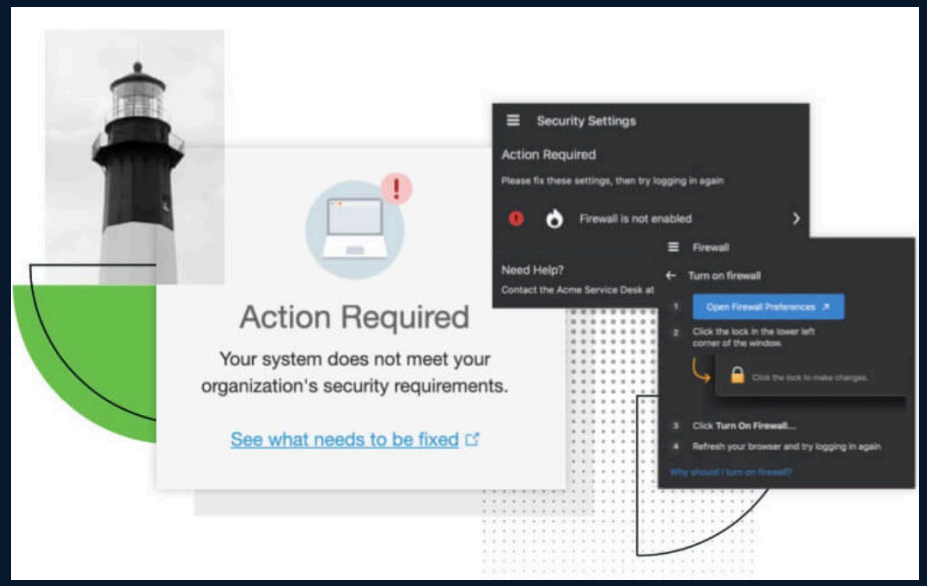




セッションをDuo Desktopにて保管して実現
危険な状態になった場合にすぐにセッション削除

Self-remediation & instant restore
ユーザ自身がデバイスの自己修復・自己管理可能

ユーザーによる自己修復を強く推進

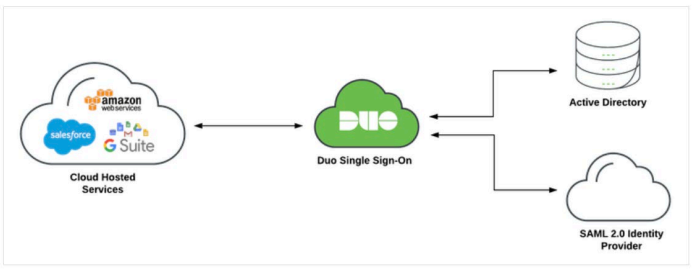


ユーザーによる簡単デバイス管理

デバイス環境変更時に、エンドユーザーと管理者業務を大幅に削減可能

シンプルな設計と構成で短期間で導入

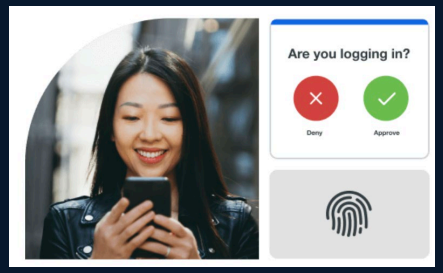
シンプルな設計と構成

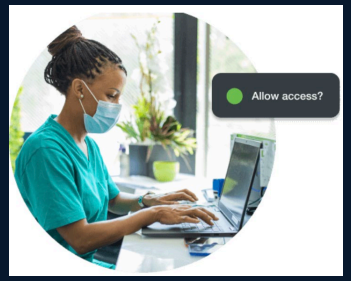


https://duo.com/docs/sso#overview

アプリケーションへのDuo構成を全てわかりやすいガイダンスや動画で解説。機能開発と同時にガイダンスも更新。
→常に最新の環境とともに最新のドキュメントを提供

創業当時から追求するユーザーエクスペリエンス





エンドユーザにわかりやすく、管理者が管理しやすい構成のため、双方にとって高い可視性を提供
→全てのDuoユーザに最高のユーザーエクスペリエンス

直感的で強力なポリシーエンジン

最も単純な方法でアプリケーション別のポリシーを設定可能

ベースが認証Deny→許可設定のみ

Group policies

O365

Edit | Replace | Unassign

This policy applies to 1 group: Staff

Enabled	Authentication policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
Enabled	User location	No action: United States. All other countries: Deny access.
Enabled	Operating systems	MacOS, Windows

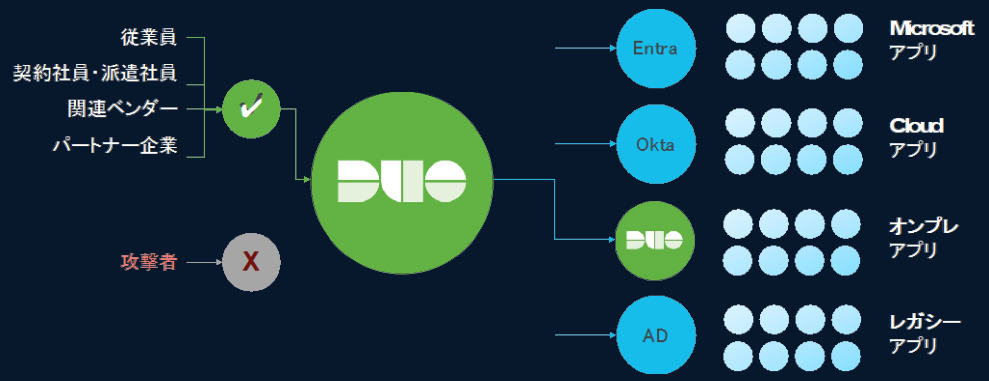
Global Policy

This policy always applies to all applications.

Enabled	New User policy	Prompt unenrolled users to enroll whenever possible.
	Authentication policy	~~Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.~~

Duoでのポリシー設計はアプリケーションごとに上記の設定のみ
（White List型のポリシー設定→許可のみをユーザ、デバイス、ロケーション別に登録が必要）
複数のアプリケーションに対するポリシー設計が容易

どのような環境でも最小の工数で設定可能



お客様の環境に適合するため、
最も少ない数のポリシーで強力なポリシーを設定可能
設定期間、設定工数を大幅に削減。

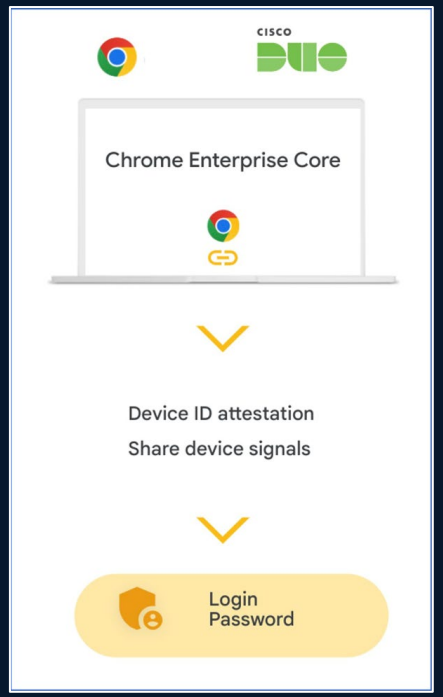
※アプリケーション別、グループ別のポリシーを簡単に設定可能

ブラウザと連携したエージェントレス デバイストラスト

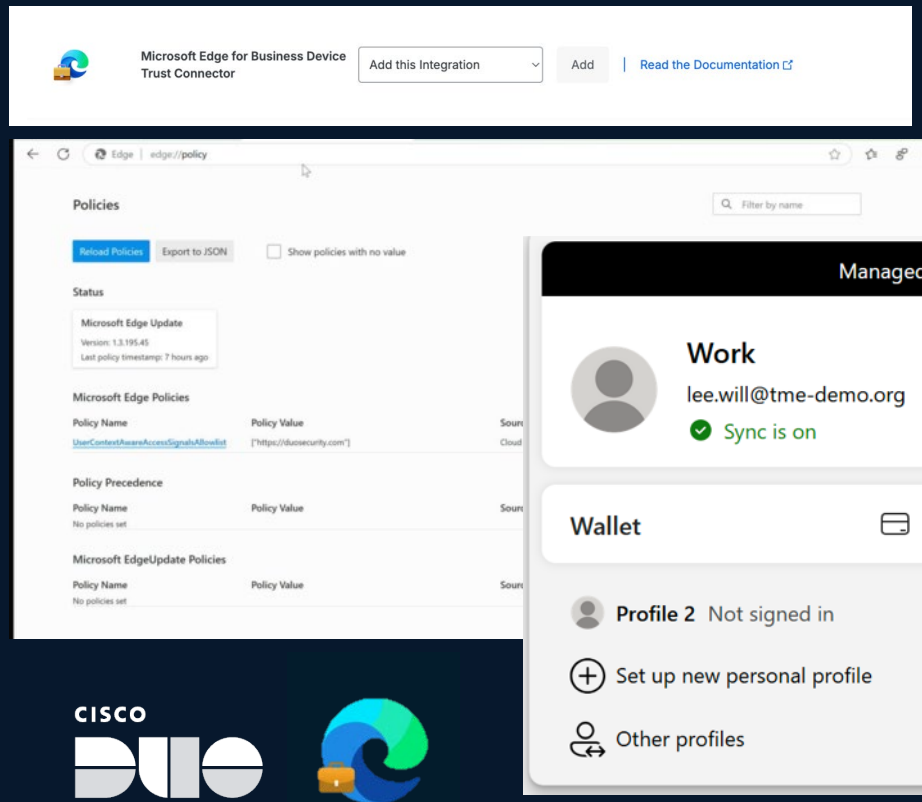
Zero Trust for Chrome Enterprise

Duo + Google Chrome Enterprise

- Device Trust Connector
- Universal Enrollment Connector



Microsoft Edge for Business Device Trust Connector



なぜDuo IAMか?

現状のIdentity環境においてDuoを利用するメリット

どのIDPともつながれる柔軟性

プライマリーIDPとして稼働

カスタム属性を作成可能

IDP間のブローカーとして利用

セキュリティファースト

強度の高いMFAがデフォルト

完全パスワードレス

強力なデバイスの信頼性確保

シンプルで容易な設定・運用

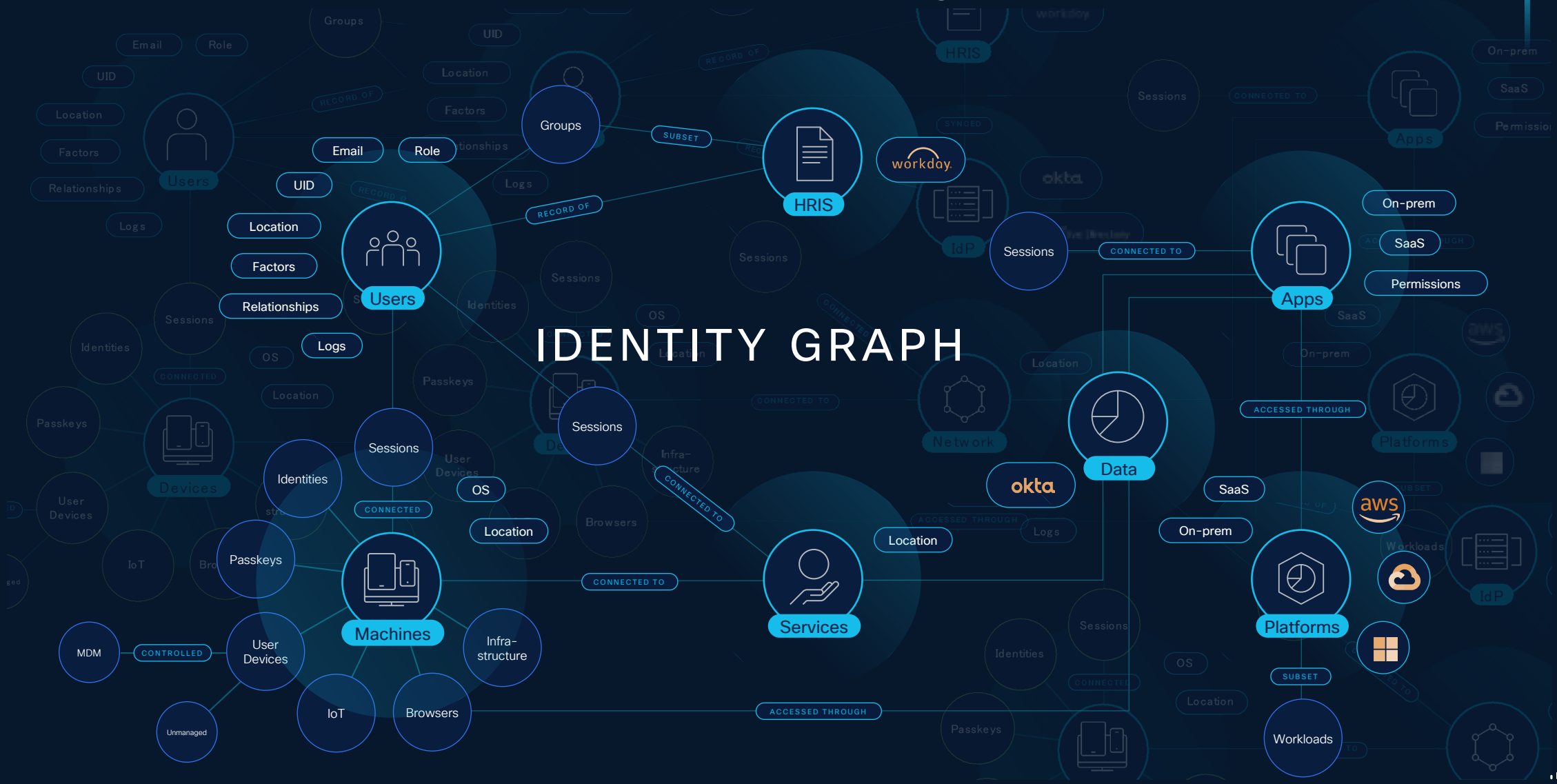
導入当初から AI Assistant利用可能

自動化されたプロビジョニング

他のIDPから簡単にSync可能

Duo IAM検討事例・Demo

Cross-Platform Insights



Identity Intelligence

AWS

Microsoft

GitHub

Salesforce

Cisco ISE

Okta

Auth0

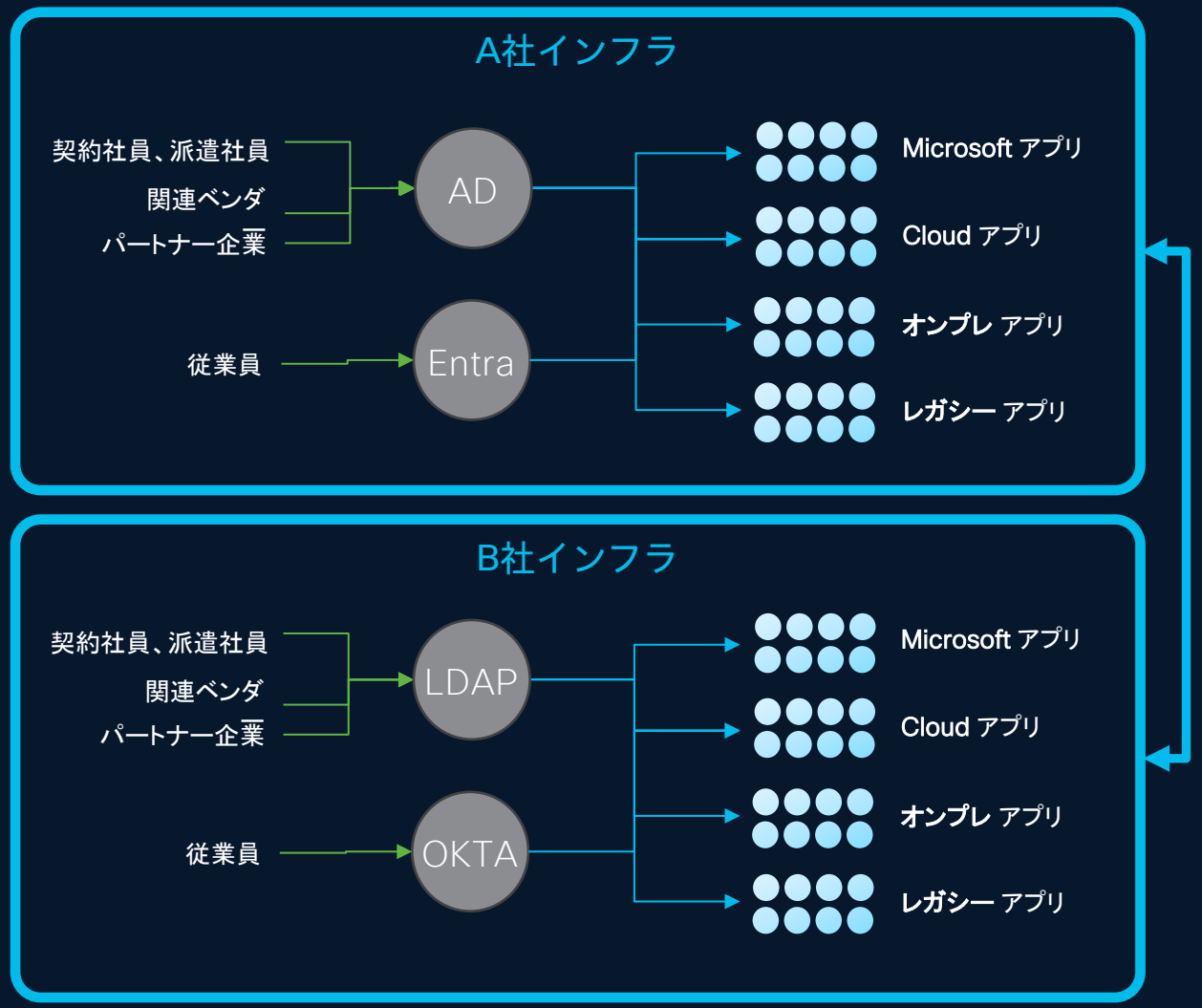
Workday

Google

Duo

ユースケース① 企業合併 → システム統合

課題



主要課題①
IDソースとシステムの乱立

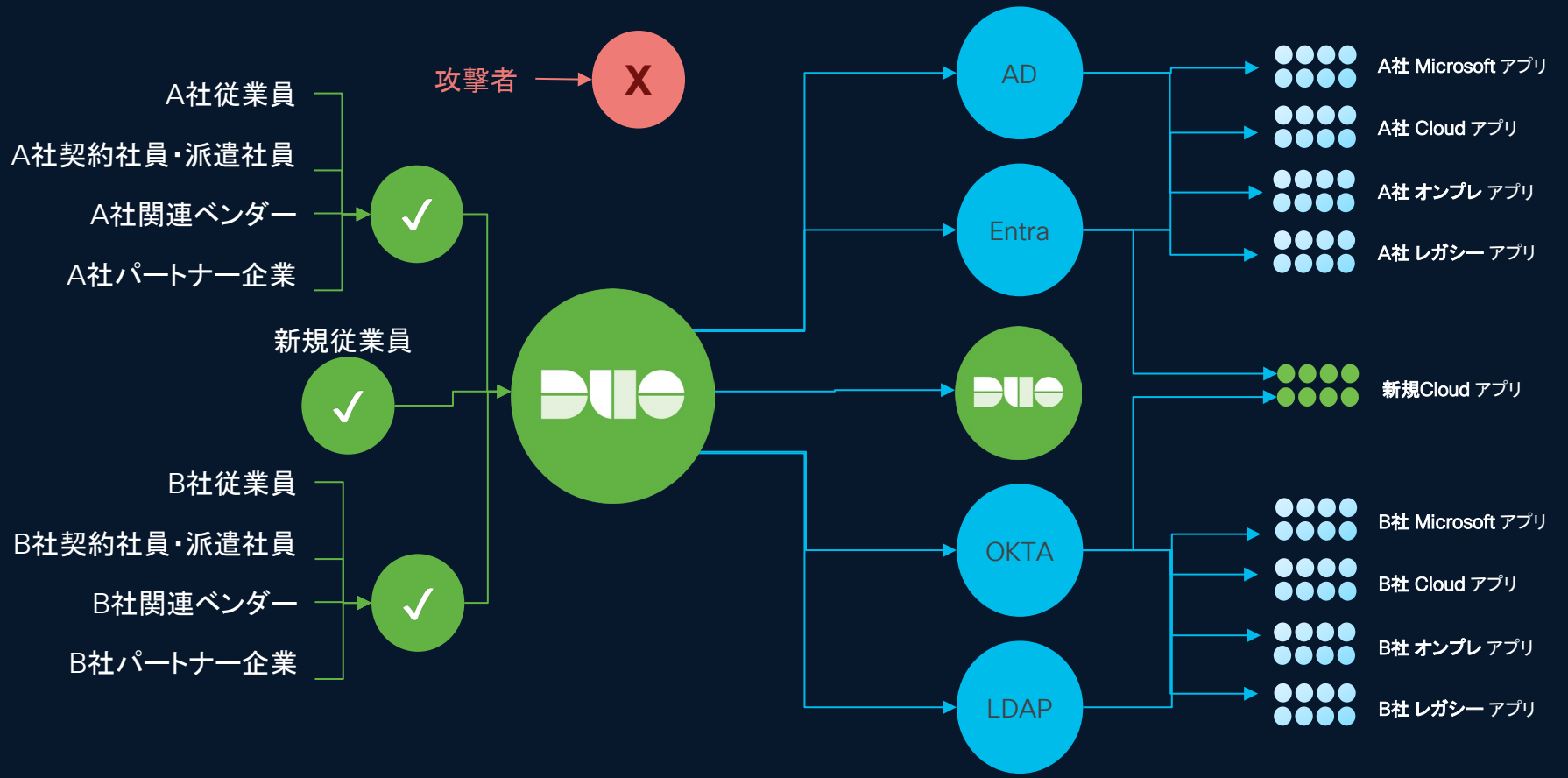
- 各社が独自のActive Directory、LDAP環境を保有
- 異なるIdP（OKTA、EntraID、GWS等）の混在
- ユーザ情報の属性やフォーマットの不整合
- 認証ポリシーとセキュリティ基準の相違
- 既存システムとの依存関係の複雑性

主要課題②
セキュリティとコンプライアンスの複雑性

- 統合期間中のセキュリティリスク増加（30%高い侵害率）
- 各社の権限管理ルールの統合困難
- コンプライアンス要件の不一致
- 一時的なアクセス権の重複や漏れ
- 監査ログの統合と整合性確保

ユースケース① 企業合併 → システム統合　効果

→強固なセキュリティに守られた影響最小限の統合アクセス環境を実現



既存環境への影響最小限

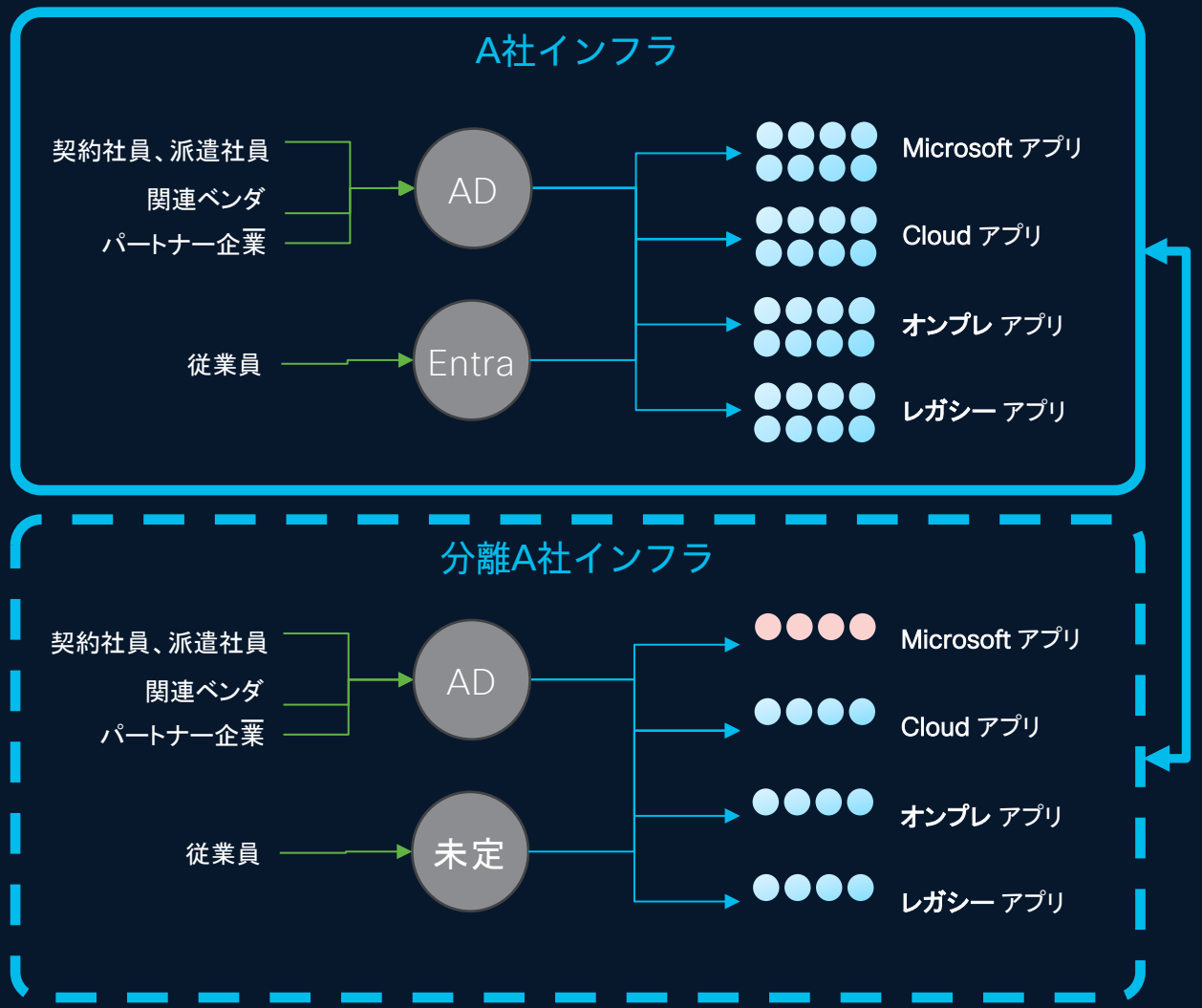
- 複雑な既存システムの困難な統合を実施する必要なし
- ユーザ属性やフォーマットはそのままでDuoにてアクセスポリシーを設定可能

コンプライアンスを統合

- 統一ポリシーをDuoのみで設定すれば、そのまま適用可能
- 監査ログも同時に統一
- 一時的なアクセス権はDuoにて保持可能

ユースケース② 企業分離 → システム離脱

課題

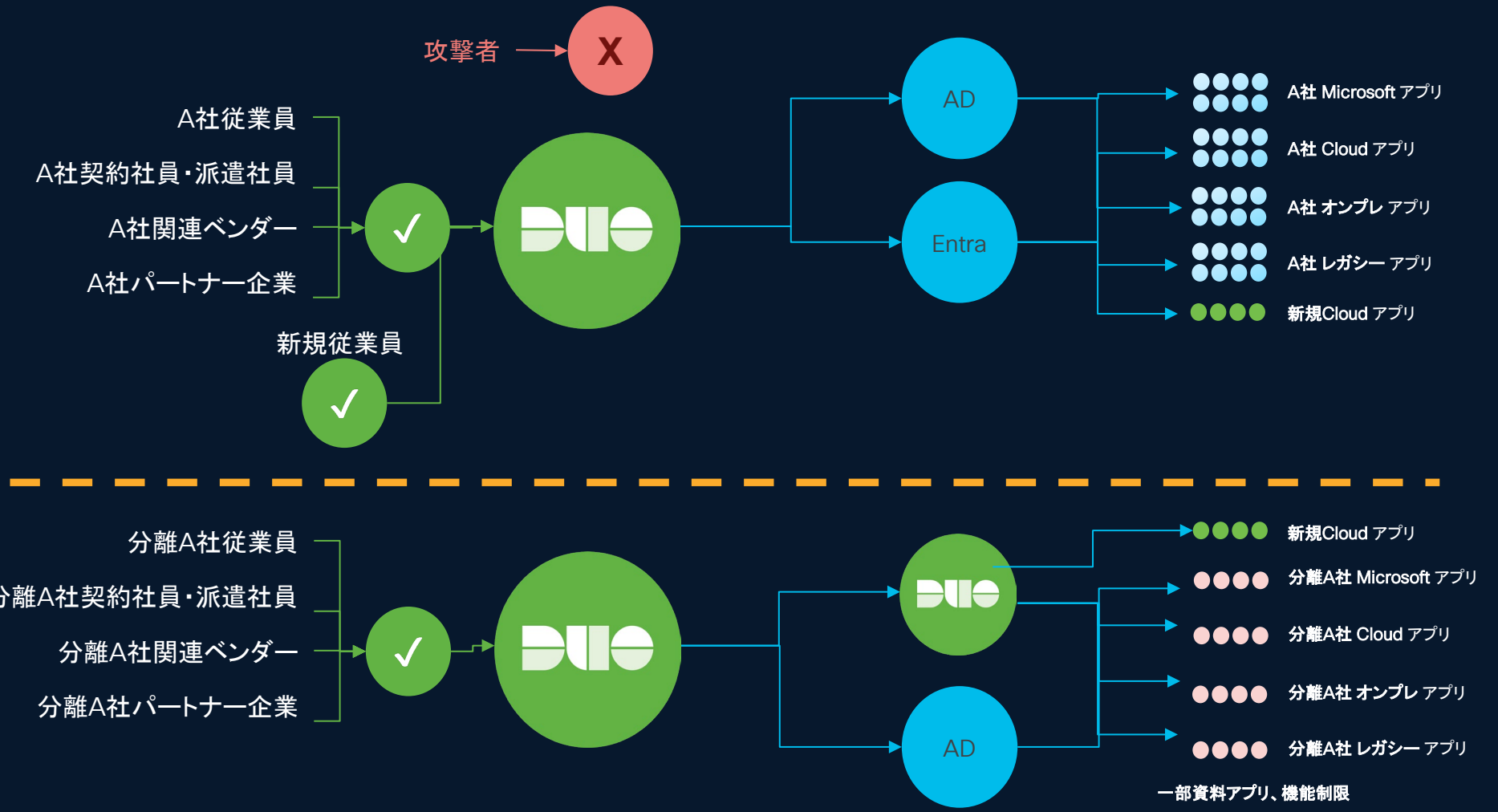


主要課題①
セキュリティリスク
- 情報流出
- 一時的なアクセス権の重複や漏れ

主要課題②
分離リスク
- 分離期間中の業務遅延・停止リスク
- 複雑なアクセス制限と問い合わせ対策
- 監査ログの分離と整合性確保

ユースケース② 企業分離 → システム離脱

→強固なセキュリティに守られた柔軟な企業分離を実現



効果

セキュリティを確保

- アクセス制御のみをDuoが担うことでセキュリティを確保して容易に分離可能

IDPの一時利用

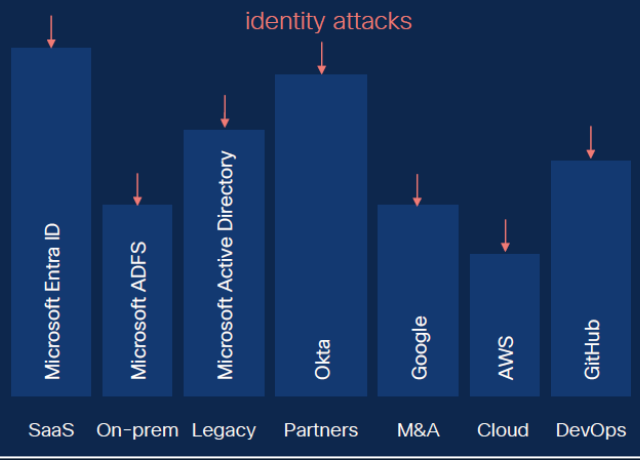
- 新規IDPに依存することなく、DuoのIDPで分離を実現可能
- 簡単な設計でポリシーの分離が実現可能。

BCP対策にも利用可能

複雑なアイデンティティの課題をDuoで解消

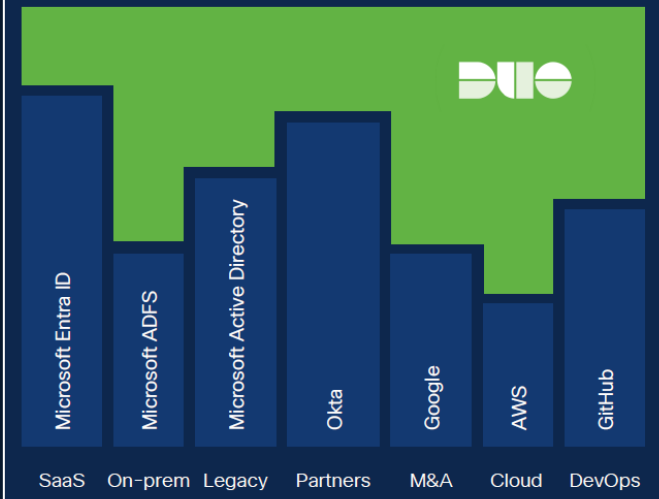
シスコ社内のIdP環境の実例

Identity is the new perimeter



- Identity-based attacks are on the rise (80%+ of cyberattacks involve identity)
- Enterprise customers have 3+ identity providers. Cisco itself has 7 IdPs!
- Complex environments leave customers vulnerable to identity-based attacks

Cisco Duo: a new approach to identity security



Duo provides a layer in front to stop identity-based attacks

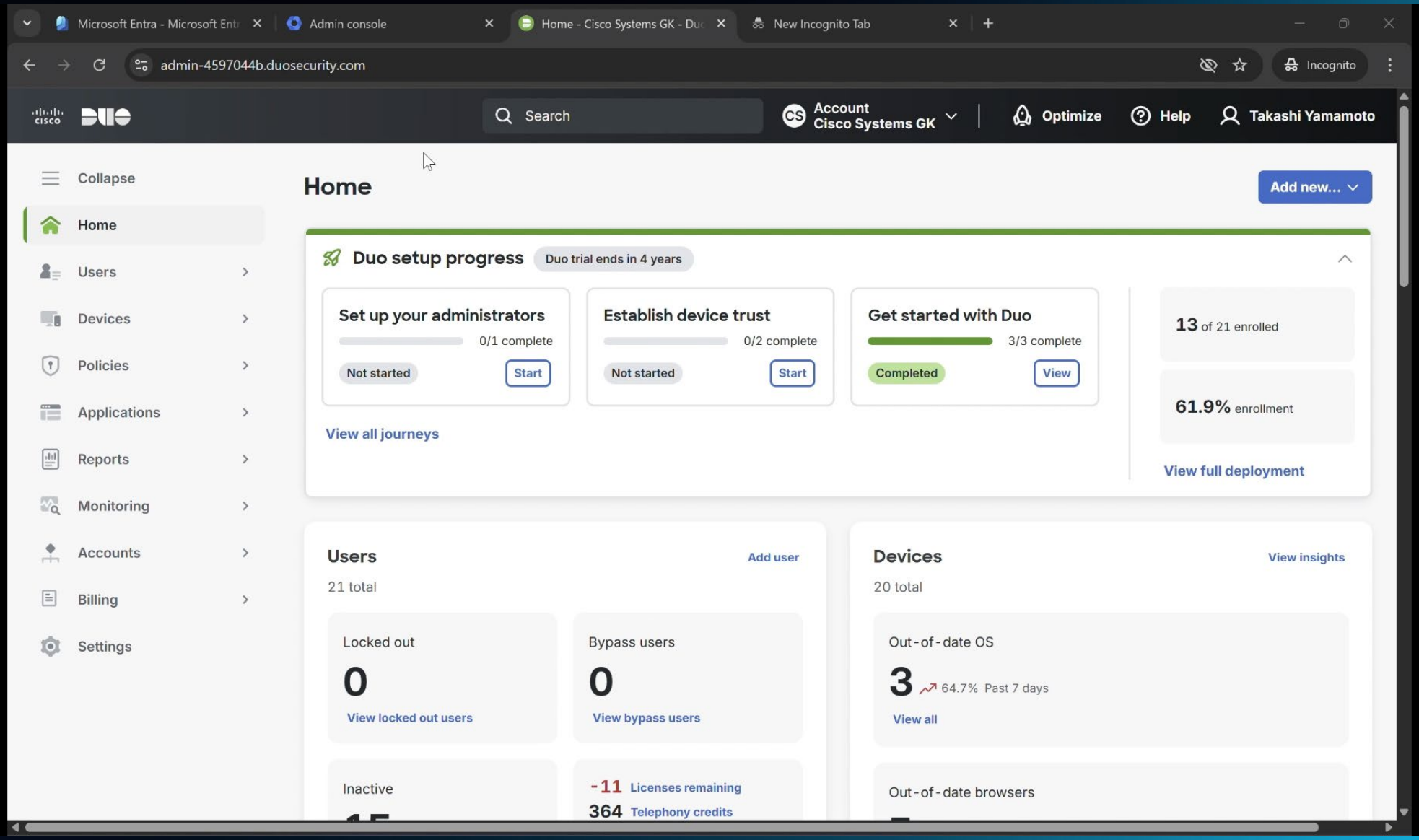
Smoother experience for all types of users

- Self-service workflows
- Fewer help desk tickets
- Minimize productivity interruptions

Stronger security for complex use cases, closing the gap

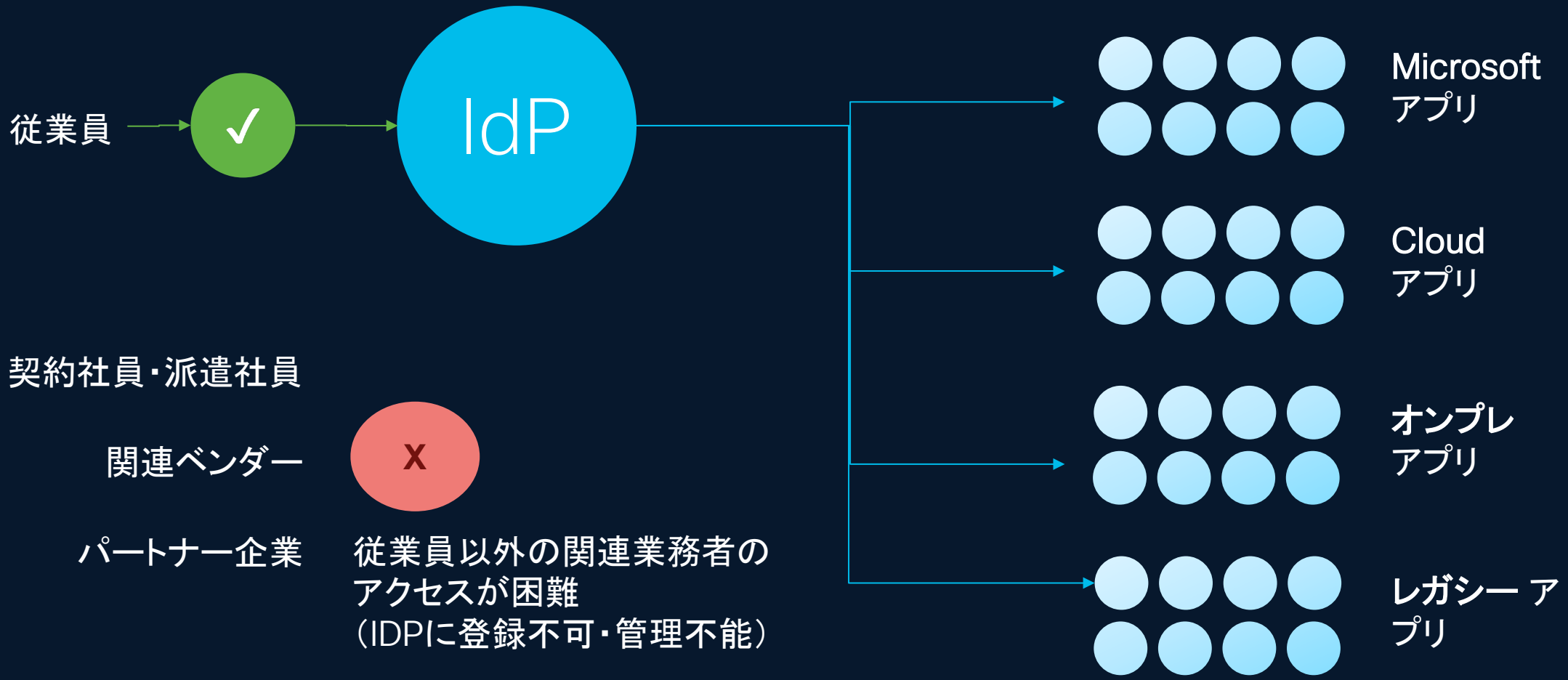
- Phishing-resistant passwordless MFA
- Unmanaged devices and BYOD
- Identity threat detection & response

複数IDPによる認証のDemo
SSO Routing Demo


Microsoft Entra - Microsoft Ent
Admin console
Home - Cisco Systems GK - Du
New Incognito Tab
admin-4597044b.duosecurity.com
Incognito
Search
Account
Cisco Systems GK
Optimize
Help
Takashi Yamamoto
Collapse
Home
Users
Devices
Policies
Applications
Reports
Monitoring
Accounts
Billing
Settings
Home
Add new...
Duo setup progress
Duo trial ends in 4 years
Set up your administrators
0/1 complete
Not started
Start
Establish device trust
0/2 complete
Not started
Start
Get started with Duo
3/3 complete
Completed
View
View all journeys
13 of 21 enrolled
61.9% enrollment
View full deployment
Users
Add user
21 total
Locked out
0
View locked out users
Bypass users
0
View bypass users
Inactive
-11 Licenses remaining
364 Telephony credits
Devices
View insights
20 total
Out-of-date OS
3
64.7% Past 7 days
View all
Out-of-date browsers

ユースケース③ 従業員以外のIDP利用

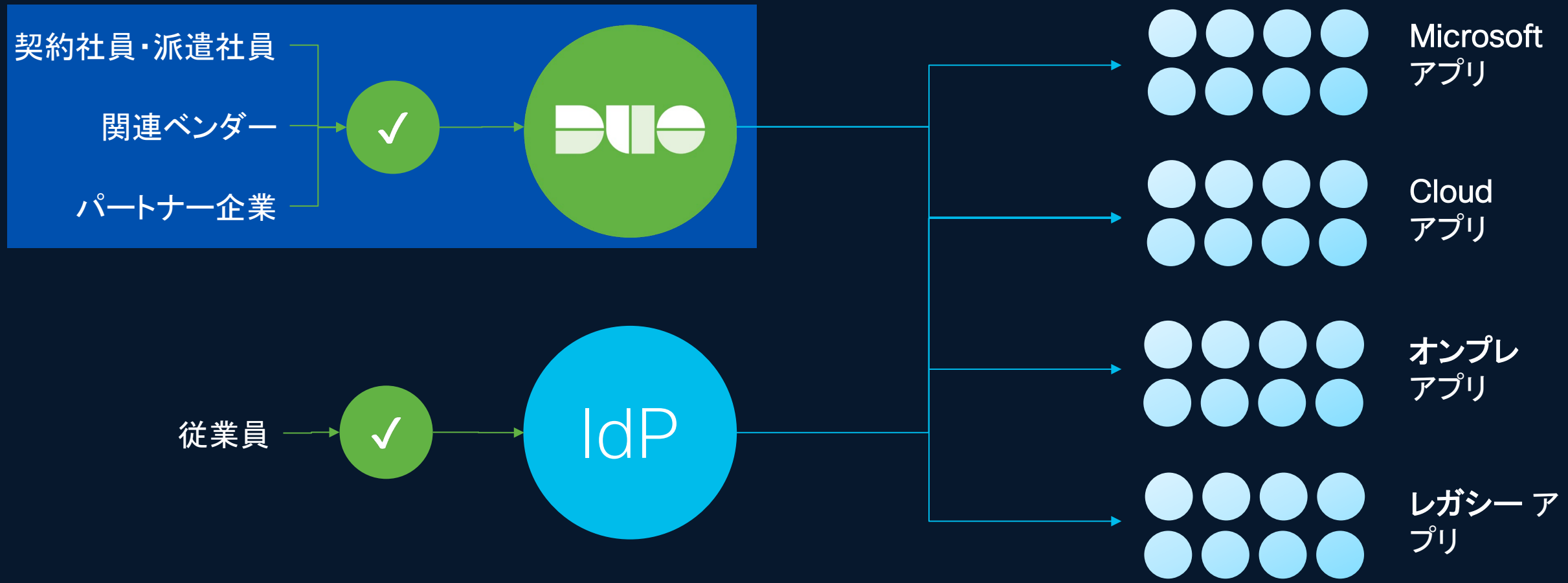
課題



他社との協業できないことがプロジェクトの推進に弊害となっている

ユースケース③ 従業員以外のIDP利用

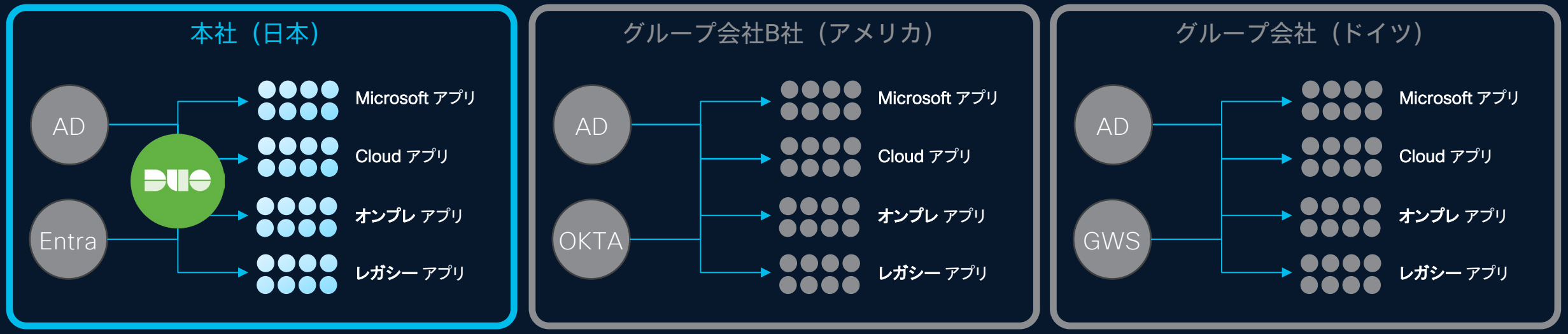
効果



Duo IAMにて関連業務者を管理して、セキュリティを確保

ユースケース④ 海外環境のIDP可視化

課題



日本の管理下のため、
全て可視化可能

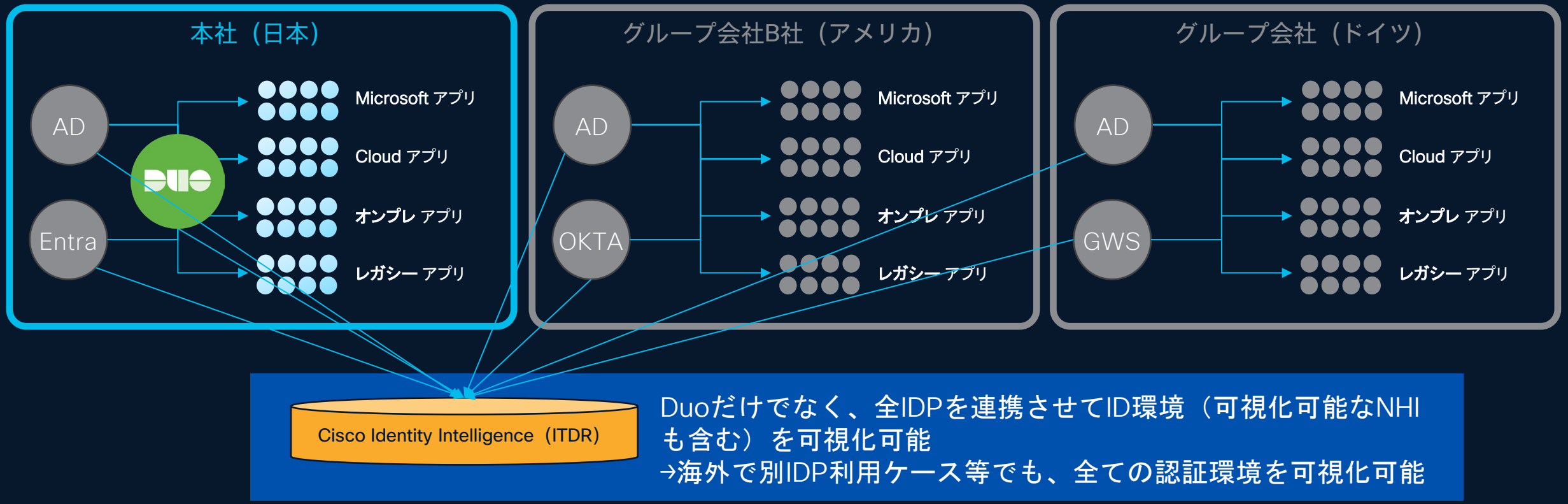
アメリカ管理下、
一部日本のユーザも登録されるも可視化不可

EU（GDPR）管理下、
一部日本のユーザも登録されるも可視化不可

海外拠点を含めたID環境の可視化が困難で統合管理ができない

ユースケース④ 海外環境の可視化利用

効果



Duoだけでなく、全IDPを連携させてID環境（可視化可能なNHIも含む）を可視化可能
→海外で別IDP利用ケース等でも、全ての認証環境を可視化可能

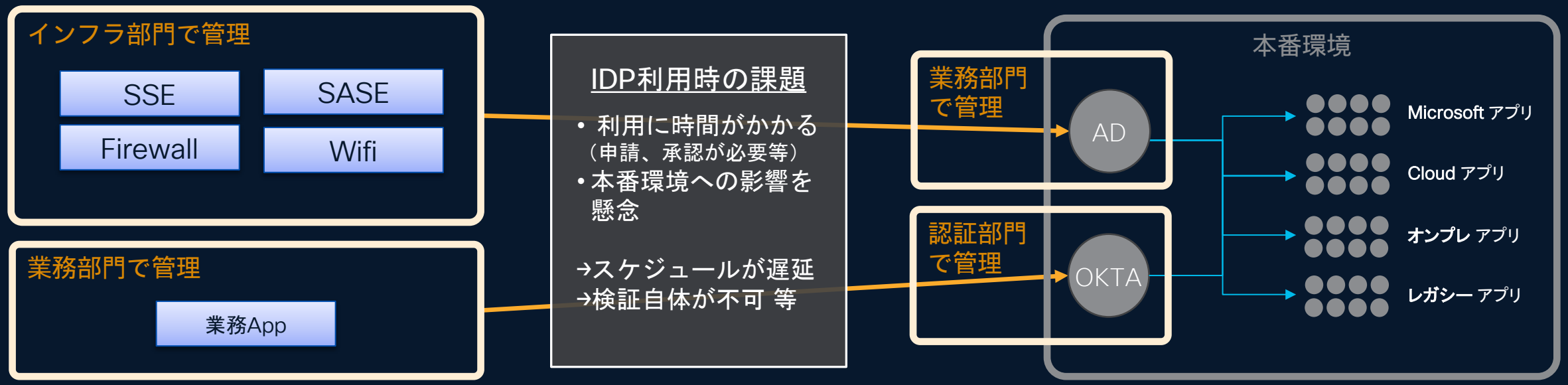
Duo IAMの柔軟性とCIIの拡張性がポイント

海外認証の可視化 Demo
Cisco Identity Intelligence Demo

ユースケース⑤
新規製品本番移行・検証時のIDのテンポラリ利用

課題

- 想定されるユースケース
  - IdPを（自社・自部門）で所有していない
  - IdPの技術的な制限、時間的制限により連携が困難
  - 複数のディレクトリ、IdPが存在し、検証環境を作ることが困難



IDP連携が必要だが簡単に利用できず、検討・スケジュールが遅延

ユースケース⑤
新規製品本番移行・検証時のIDのテンポラリ利用

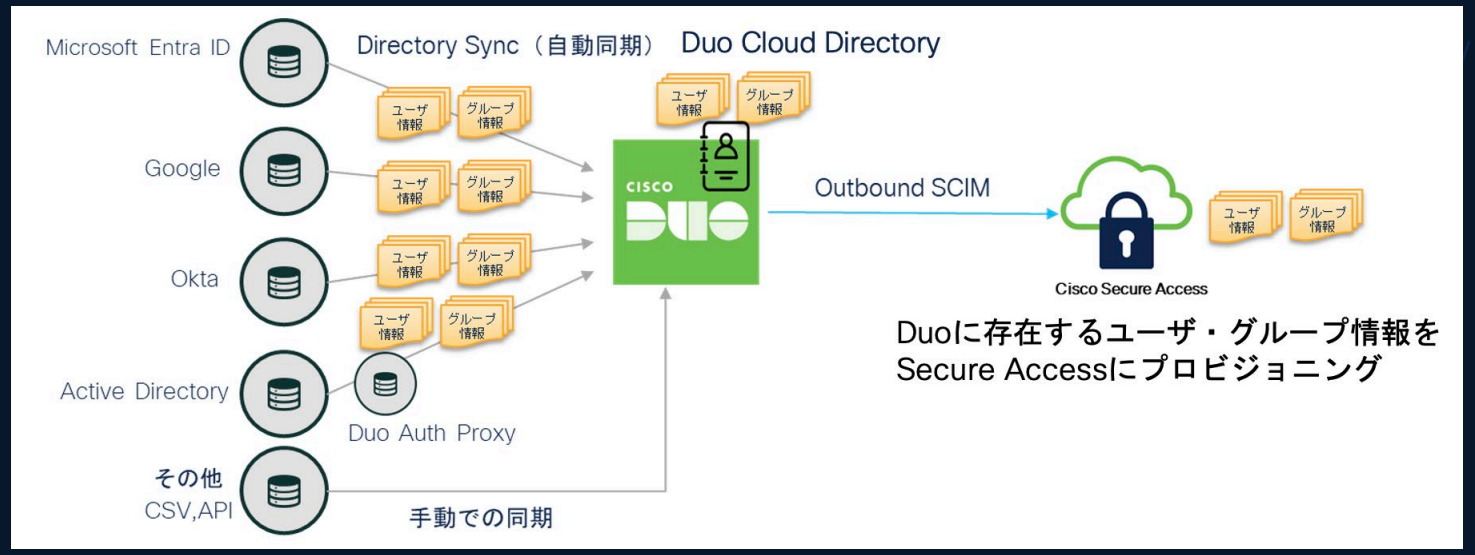
効果

例：Cisco Secure Access検討時のDuo IAMのテンポラリ利用

- IdPをテンポラリとしても本番環境としても利用可能
- 技術的な制限、時間的制限が少ない簡単設計
- 複数のディレクトリ、IdPが存在しても容易に連携可能

Secure Access + Duo

Powered by User Protection Suite



新規製品検討が加速

テストまでの期間短縮
デフォルトセキュリティで安全な検証
本番環境稼働までの一時的な本番利用（VPN等）

Duo IAMの早期稼働とセキュリティがポイント

Secure Access 連携 Demo
Outband SCIM Demo

Cisco Security Summit 2025 Tokyo イベントご案内

2025年8月5日（火） 10:00 – 18:00

ウェスティンホテル東京＠恵比寿（200名規模）

午前中 基調講演

- ✓ NEC Corporate Executive CISO 淵上様
- ✓ Cisco Systems EVP, Operations Thimaya Subaiya
- ✓ Cisco Systems SVP, セキュリティ開発部門 CPO Raj Chopra

午後 テクニカルセッション

- ✓ AIセキュリティ, SASE最前線, Identity Security（ITDR）
- ✓ XDRによるSOC次世代化, 分散ファイアーウォールの考え方
- ✓ Cisco Talosによる日本を取り巻く脅威最前線

登録サイト：https://www.cisco.com/jp/go/securitysummit

日本電気株式会社

Corporate Executive CISO

兼 NEC セキュリティ株式会社 取締役

淵上 真一 氏

NEC様基調講演内容：

「その AI、本当に思い通りに動いてますか？」

NEC様の事業におけるAI活用の現在地や、CISOとしてNECのAIをどのように捉えて、どのように守るべきなのか？

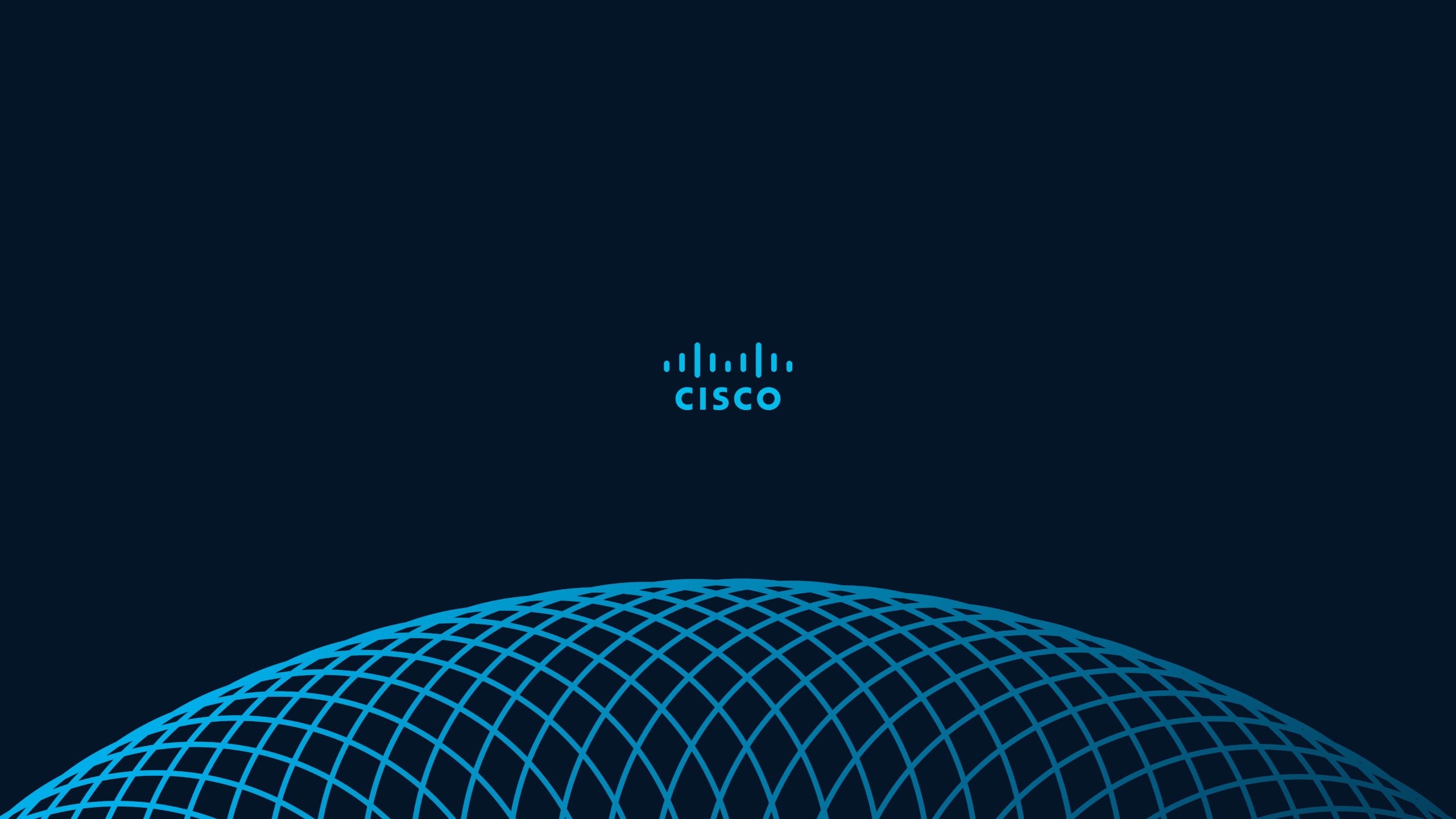
またそれを支える人材育成はどうあるべきなのか？

NEC様における現在地をお話いただきます

Duo IAMのユースケース

① 企業合併 → システム統合
② 企業分離 → システム離脱
③ 従業員以外のIDP利用
④ 海外環境の可視化利用
⑤ 新規製品本番移行・検証時のIDのテンポラリ利用

上記のユースケースがございましたら、
Cisco担当営業までご相談ください。


CISCO