

Security Summit Tokyo 2025

AI時代に必須の セキュリティファーストの新IAMソリューション

Hiroki Hata, Satoshi Inazawa

2025年8月

アメリカ時間の2025年5月28日に発表



= MFA ?

“

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を守れてきたのでしょうか？

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

Duo は信頼できるIdentity管理としてIAMを再定義します

セキュリティ意識の増加
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
セキュリティ対策に
複雑なホスチャ機能
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

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
(ITDR)

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

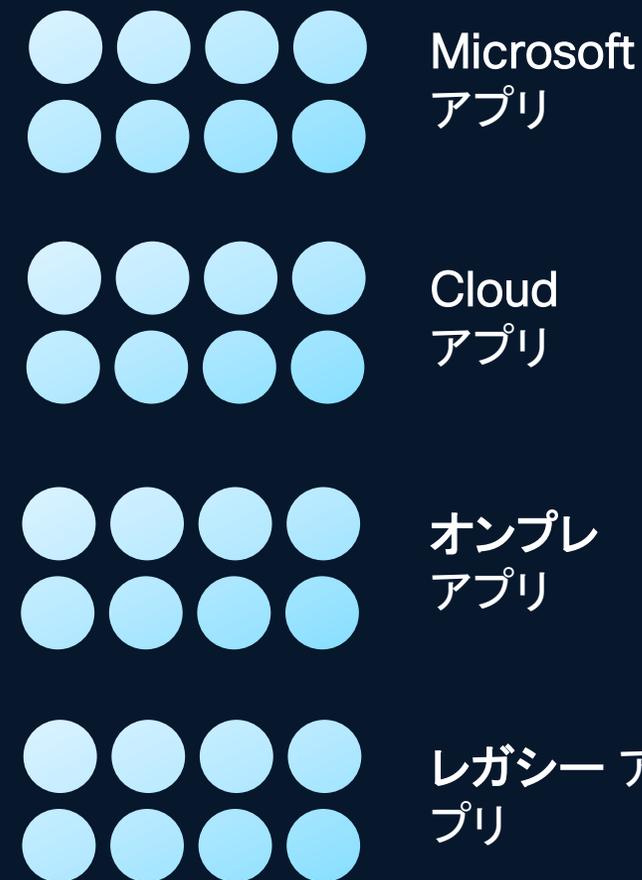
-  柔軟なDirectory管理
-  完全パスワードレス
 - 強固なMFAがデフォルト
 - アクセスデバイスの信頼性を確保
-  柔軟で簡単な設計・設定

Duo Directory 単体で利用可能 (パスワードも保持)

従業員
契約社員・派遣社員
関連ベンダー
パートナー企業

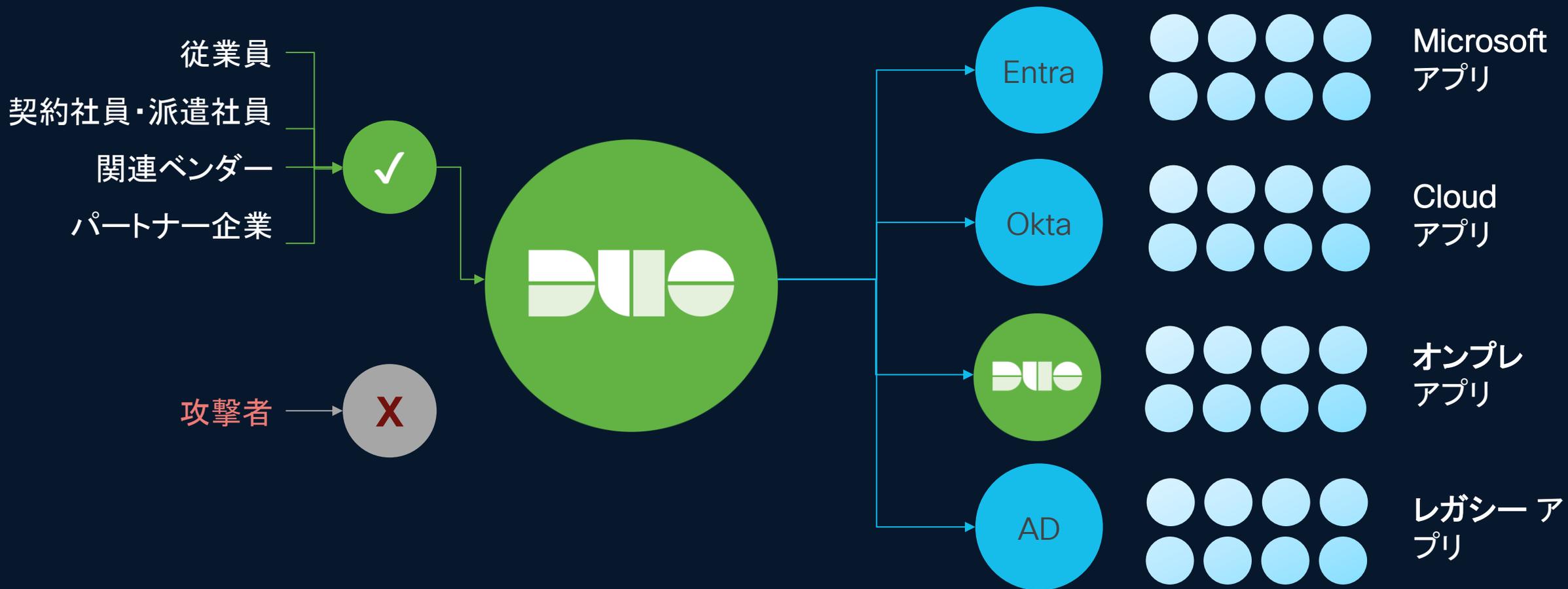


攻撃者



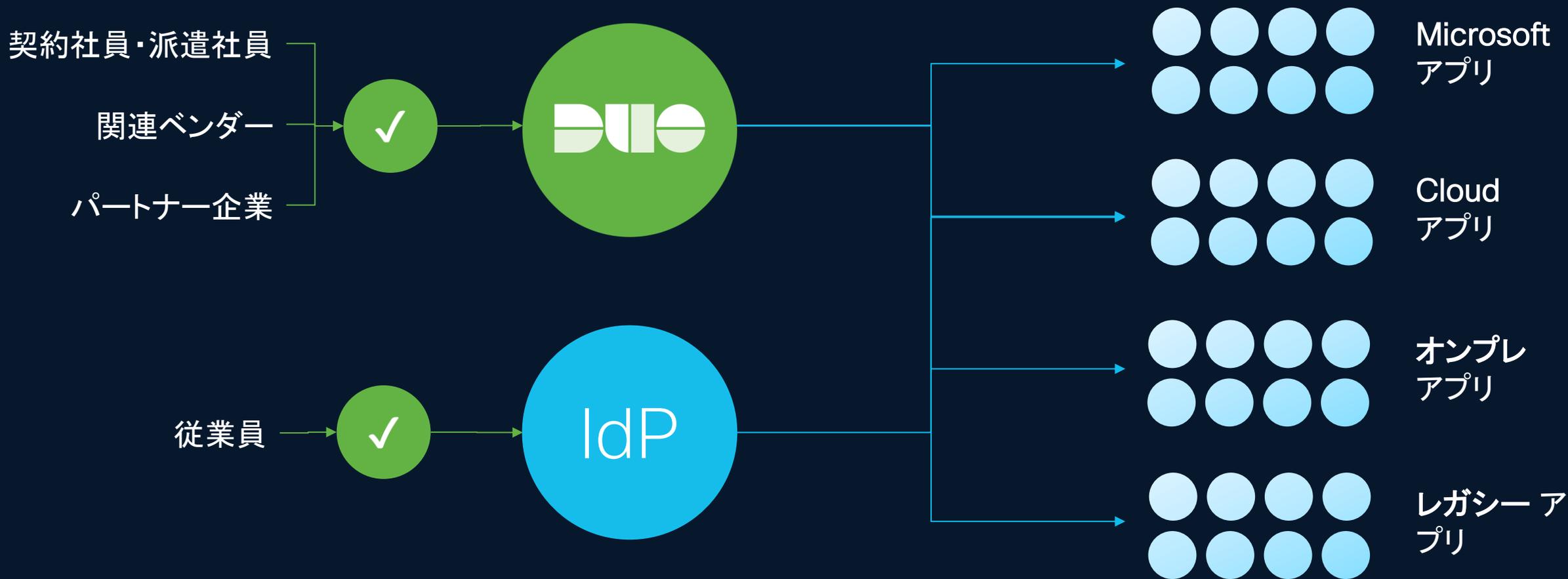
他のIDPの前面にDuoを置き、Duo Directoryを並行稼働

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はセキュリティを維持しながら従業員以外のIdentityへのアクセス制御を提供します

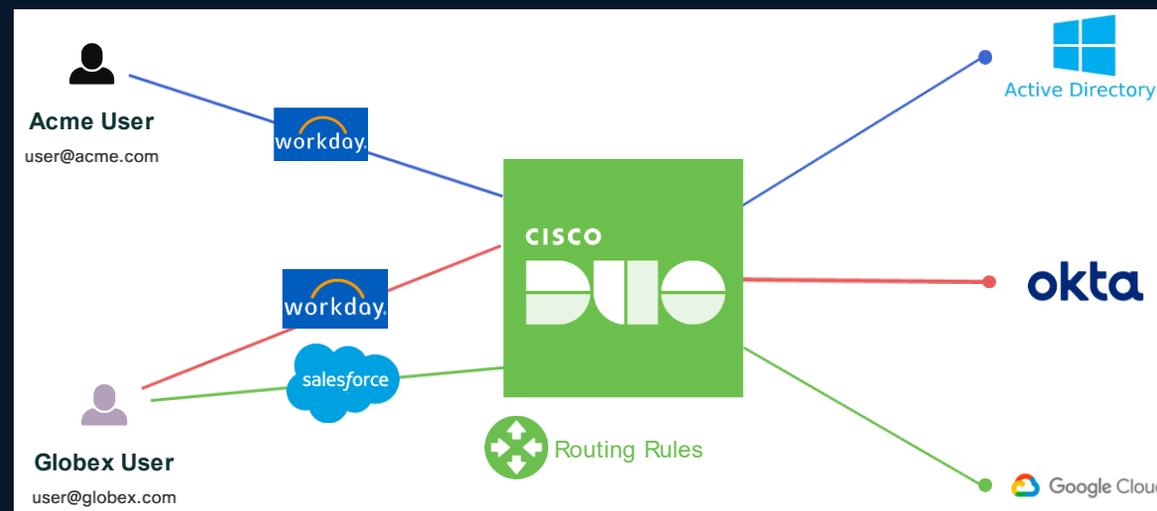


Duo SSO Routing Rules

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UIもシンプルに。



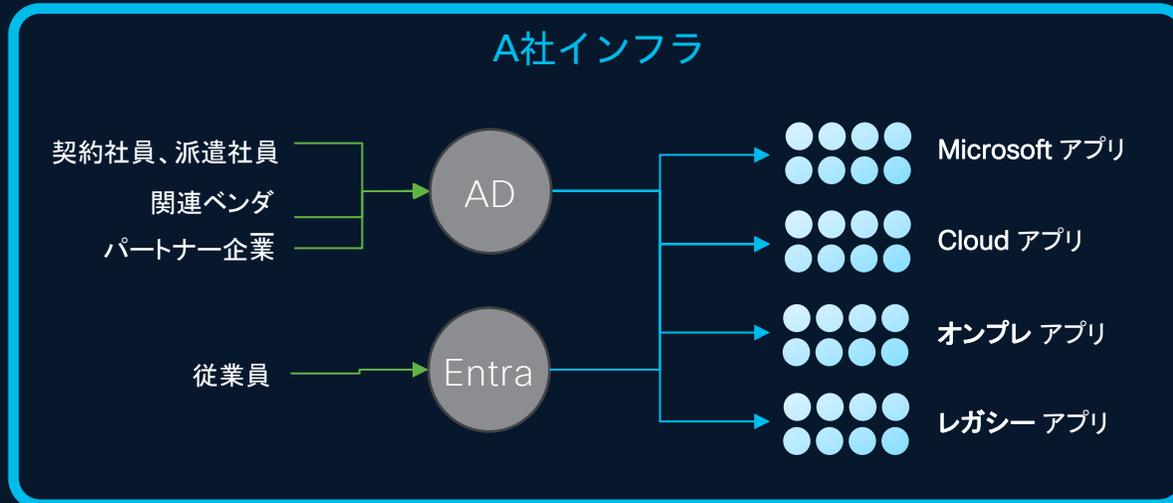
SSO Routing Rules 動作概要



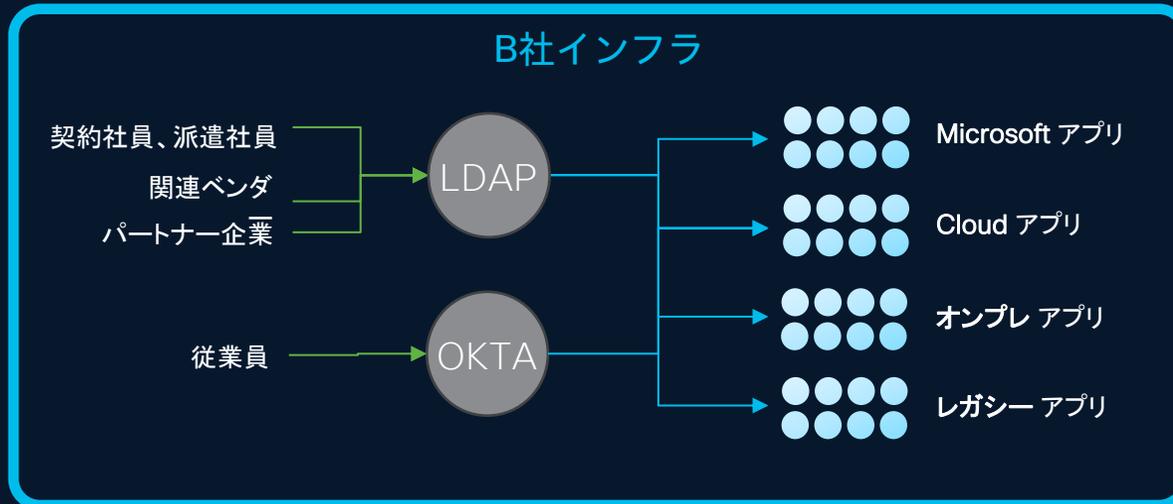
Duo IAM検討事例

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

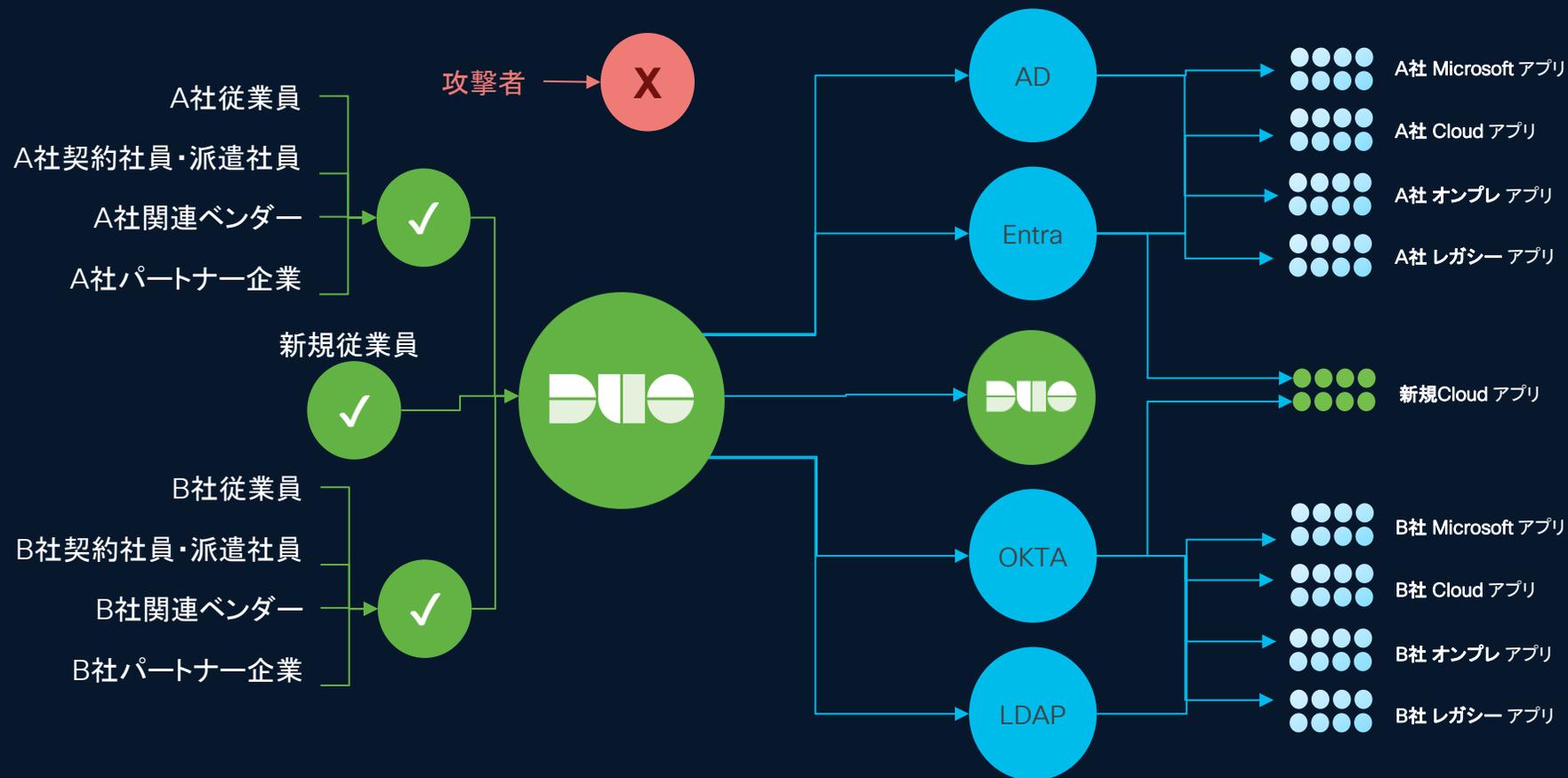


- 主要課題②**
セキュリティとコンプライアンスの複雑性
- 統合期間中のセキュリティリスク増加 (30%高い侵害率)
 - 各社の権限管理ルール of 統合困難
 - コンプライアンス要件の不一致
 - 一時的なアクセス権の重複や漏れ
 - 監査ログの統合と整合性確保

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

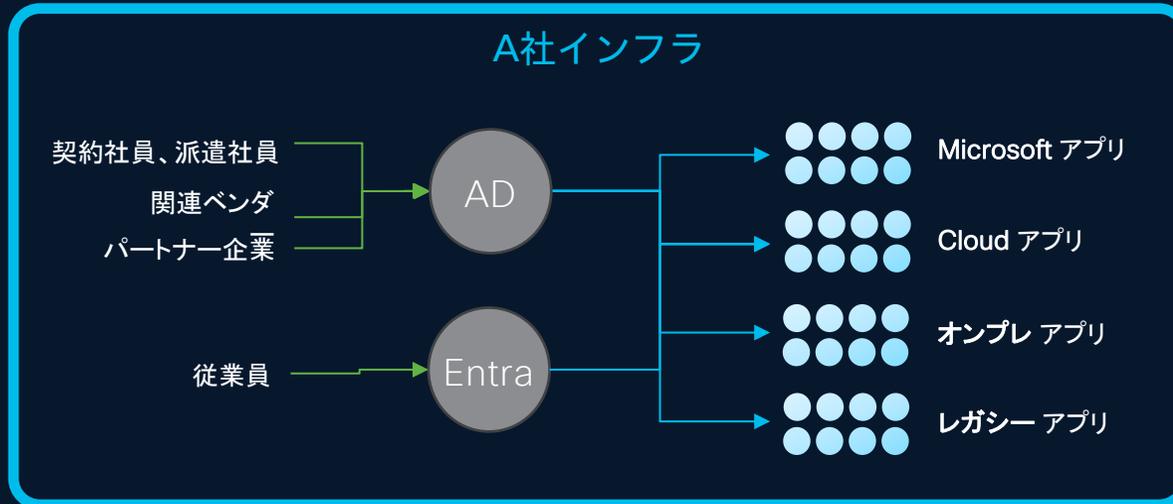
- 複雑な既存システムの困難な統合を実施する必要なし
- ユーザ属性やフォーマットはそのままDuoにてアクセスポリシーを設定可能

コンプライアンスを統合

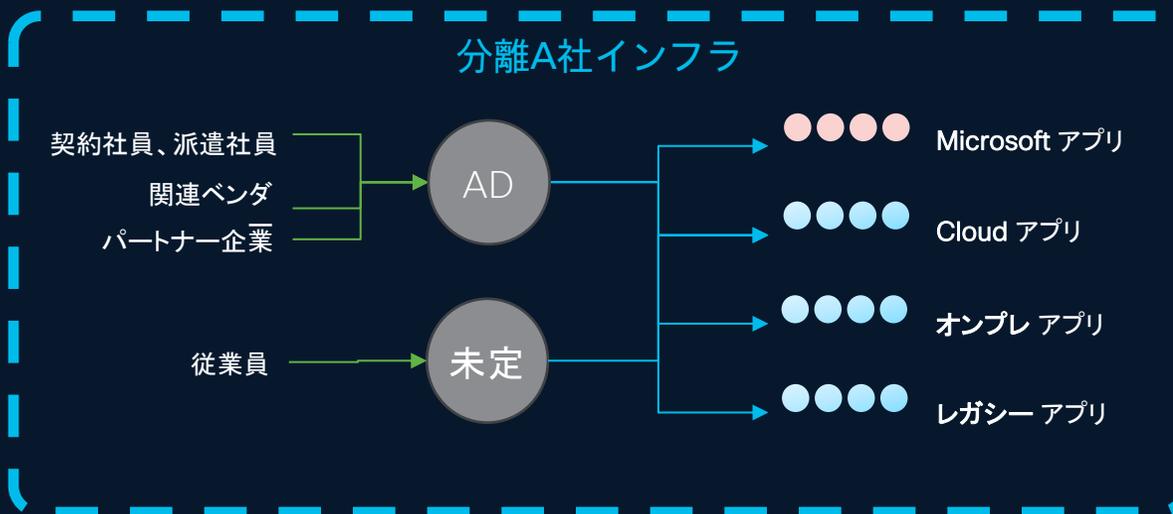
- 統一ポリシーをDuoのみで設定すれば、そのまま適用可能
- 監査ログも同時に統一
- 一時的なアクセス権はDuoにて保持可能

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

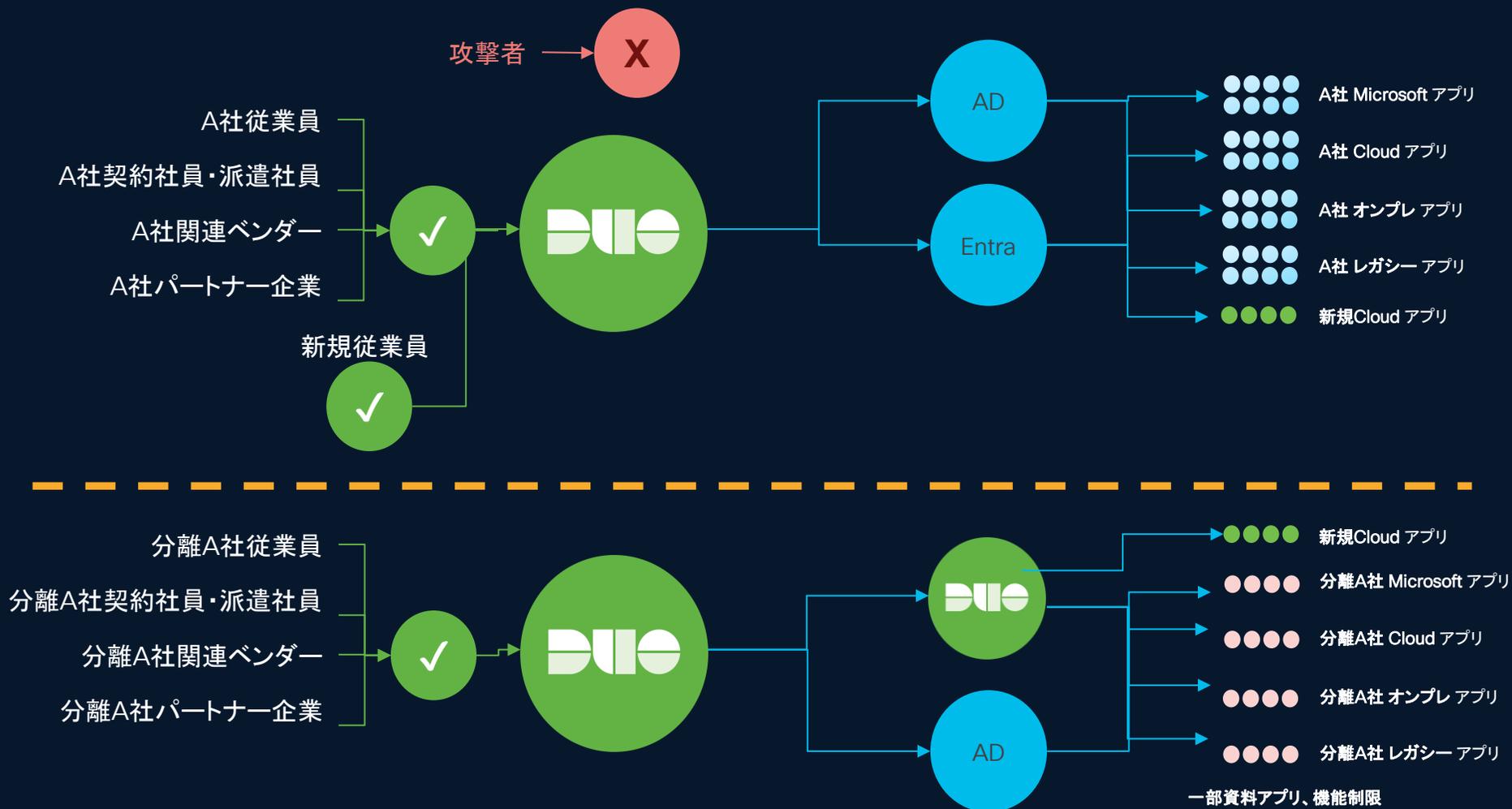


- 主要課題②**
分離リスク
- 分離期間中の業務遅延・停止リスク
 - 複雑なアクセス制限と問い合わせ対策
 - 監査ログの分離と整合性確保

ユースケース② 企業分離 → システム離脱

効果

→ 強固なセキュリティに守られた柔軟な企業分離を実現



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

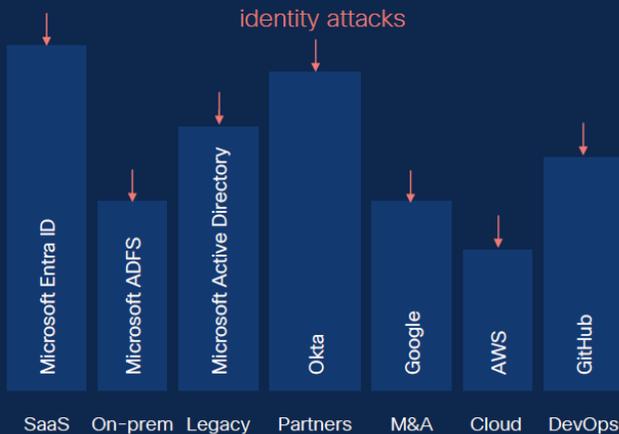
- 新規IDPに依存することなく、DuoのIDPで分離を実現可能
- 簡単な設計でポリシーの分離が実現可能。

BCP対策にも利用可能

Cisco: 複雑なアイデンティティの課題をDuoで解消

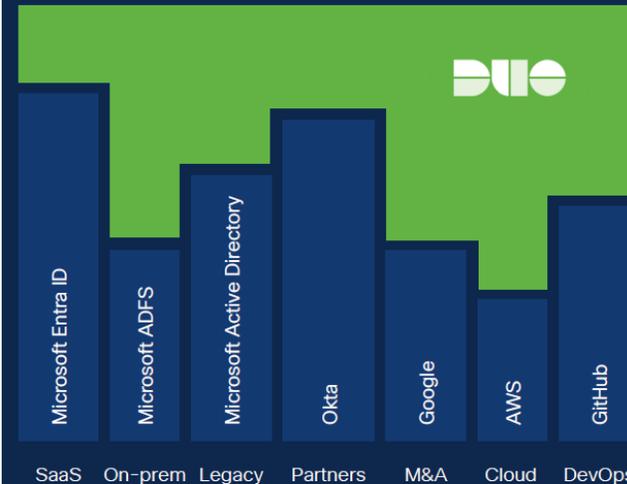
シスコ社内のIdP環境の実例

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

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



Passwordless authentication methods

Users will only be allowed to authenticate without a password when using the checked methods. Passwordless authentication is only available to SSO applications.

- Platform authenticators**
Built-in authenticators that require a biometric, PIN, or passcode (e.g., Face ID, Touch ID, Windows Hello, or Android fingerprint and face recognition)
- Roaming authenticators (e.g., security keys)**
USB, Bluetooth, or NFC security keys that require user verification via biometric or PIN
- Duo Push**
After a successful two-factor authentication, a "known-device" cookie is placed in the browser, allowing use of Duo Push without a password. When approving the Duo Push, Duo Mobile will require a biometric, PIN, or passcode. [Learn more about passwordless Duo Push.](#)
- Bypass code**

Insights

Authentications using more secure methods
Such as platform authenticators, roaming authenticators, or Duo Push

Monthly active passwordless users
Out of 650 total users in your organization

Category	Count	Percentage
Used passwordless at least once	634	95%
Did not use passwordless	16	5%

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)

end-to-end で狙われるIdentity

攻撃対象は拡大しており、脅威は急速に拡大している⇒MFA だけではもはや不十分

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

Application ログイン

中間セッション

ヘルプデスク

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

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

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



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

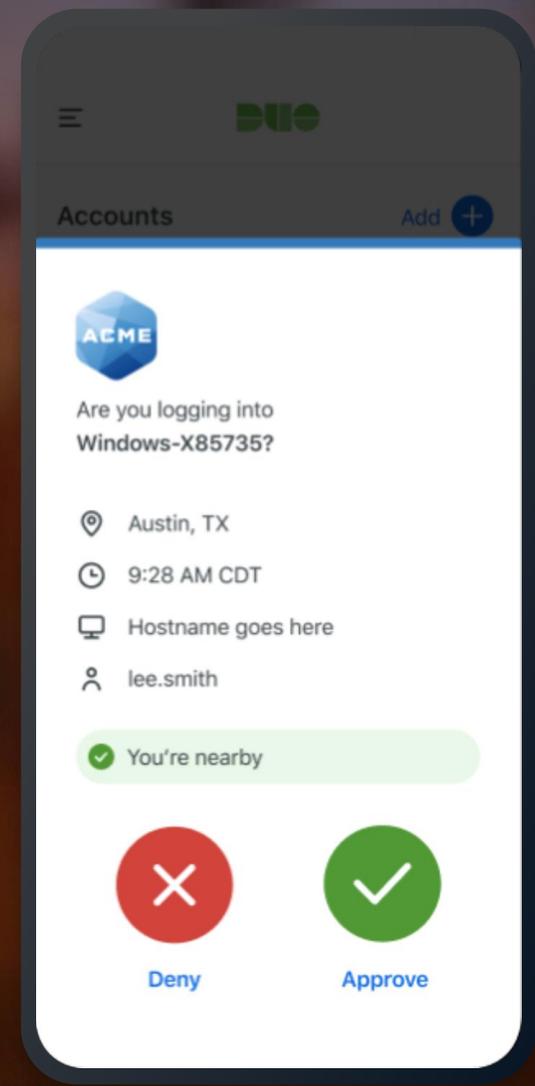
シームレスにセキュリティを確実に保護

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



近接認証 Proximity Verification

Bluetooth Low Energy (BLE)



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



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

本人の信頼性を確実に確認

Duo Identity Verification Integration

ユースケース



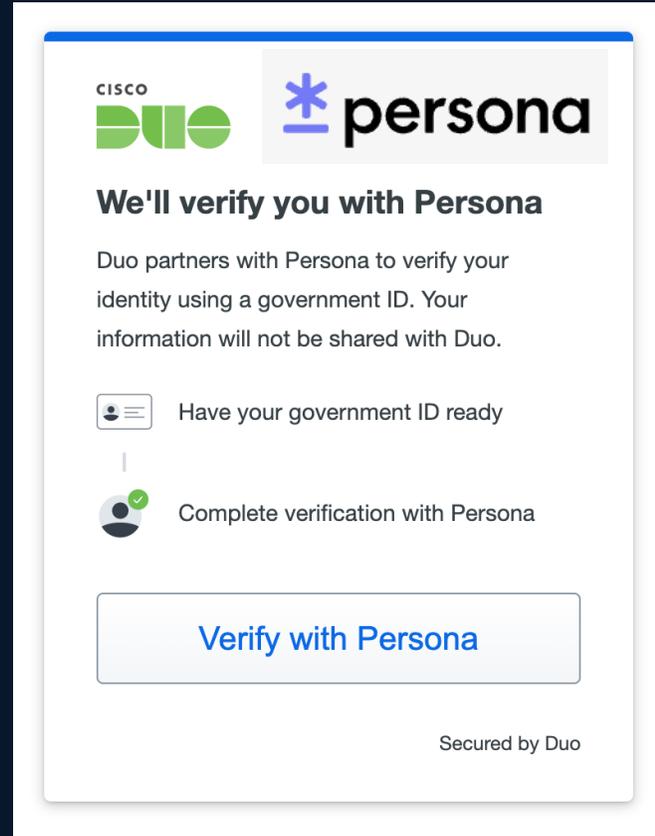
ID新規登録

- 新入社員のID新規登録時の本人確認
- パートナーID新規登録時の本人確認



ヘルプデスク

- 問い合わせ時の本人確認
- 脅威検出時の本人確認

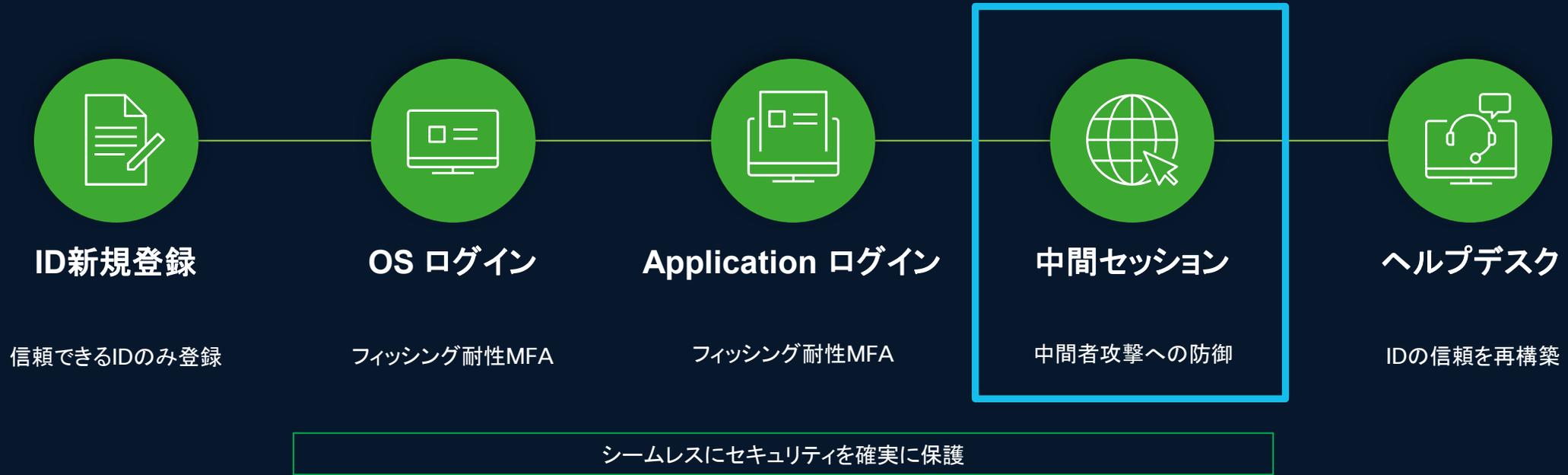


信頼を確立するために、ユーザーはDuoに保存されている情報を照合し、政府発行のIDと自撮り写真を提出しなければならない。



Helpdesk Identity Verification

Duoは end-to-end のフィッシング耐性プロセスを提供



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

セッション盗難防止 (Session Theft Protection)



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。

Duo がセッション・クッキーを排除 - 特許出願中の独自技術

Identityの信頼を再定義

統合Identity Intelligence

継続的に信頼を検証する

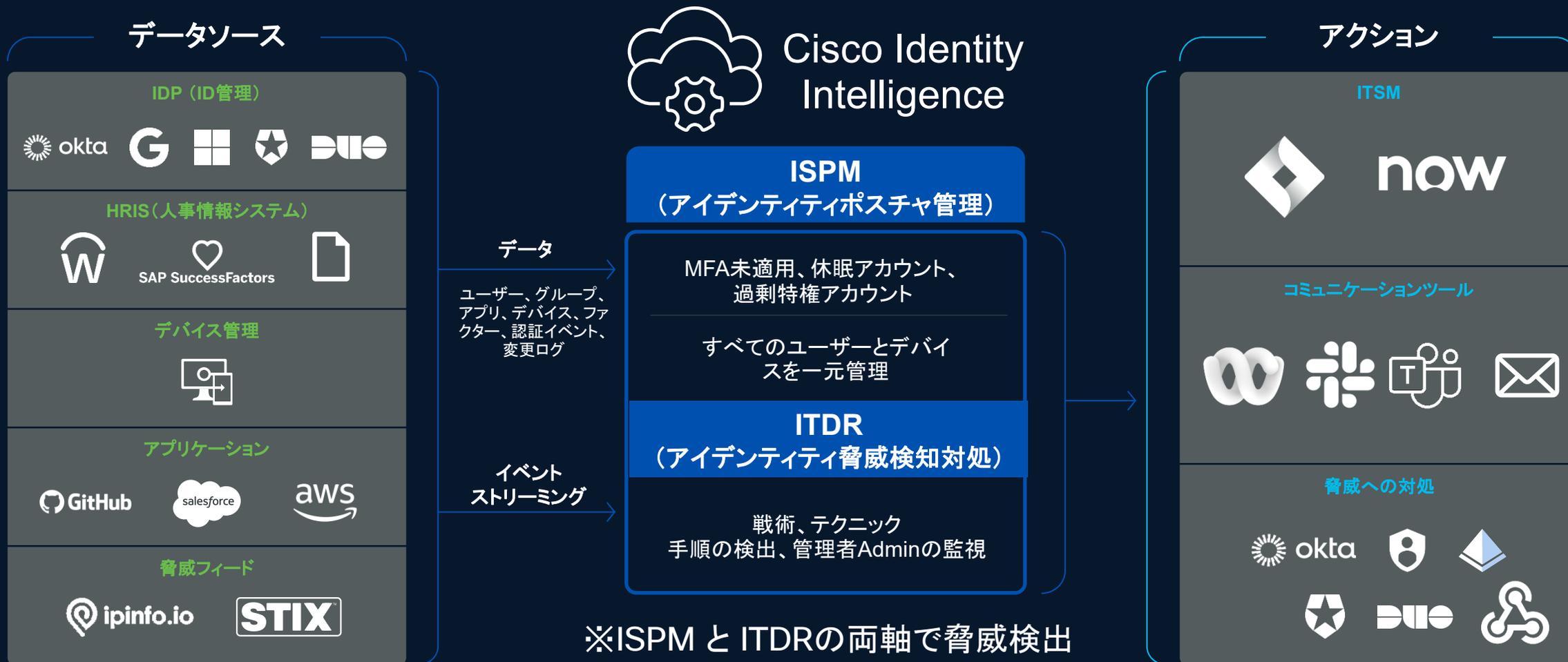
複数のIDPにまたがり広範囲でIDを可視化することにより、Identity脅威の検出と対応を強化。セキュリティを大幅に向上させることが可能。

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
- ユーザー一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

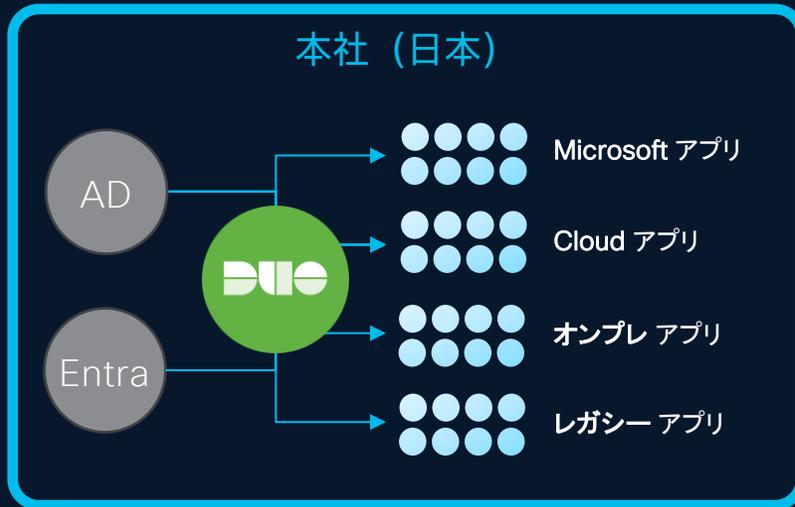
ID環境に対する可視化→ポスチャ→脅威検出→対応を強力に実現



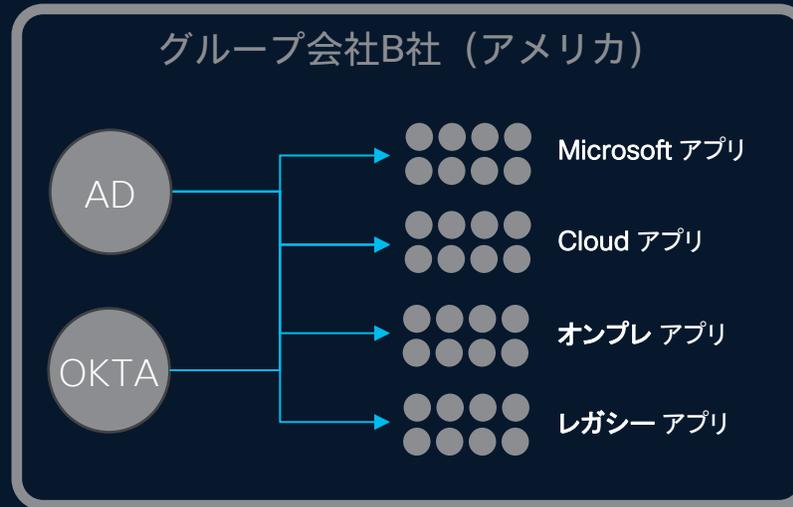
Cisco Duo (多要素認証・デバイス認証) Advantageに搭載

ユースケース④ 海外環境のIDP可視化

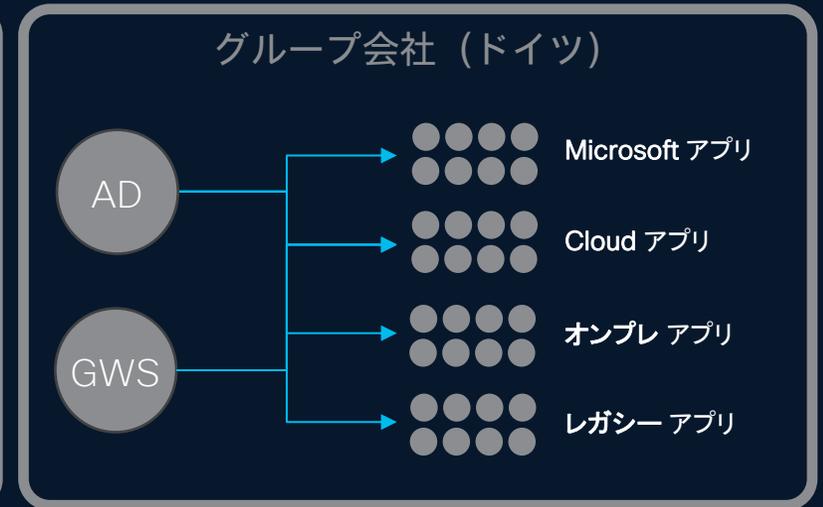
課題



日本の管理下のため、
全て可視化可能



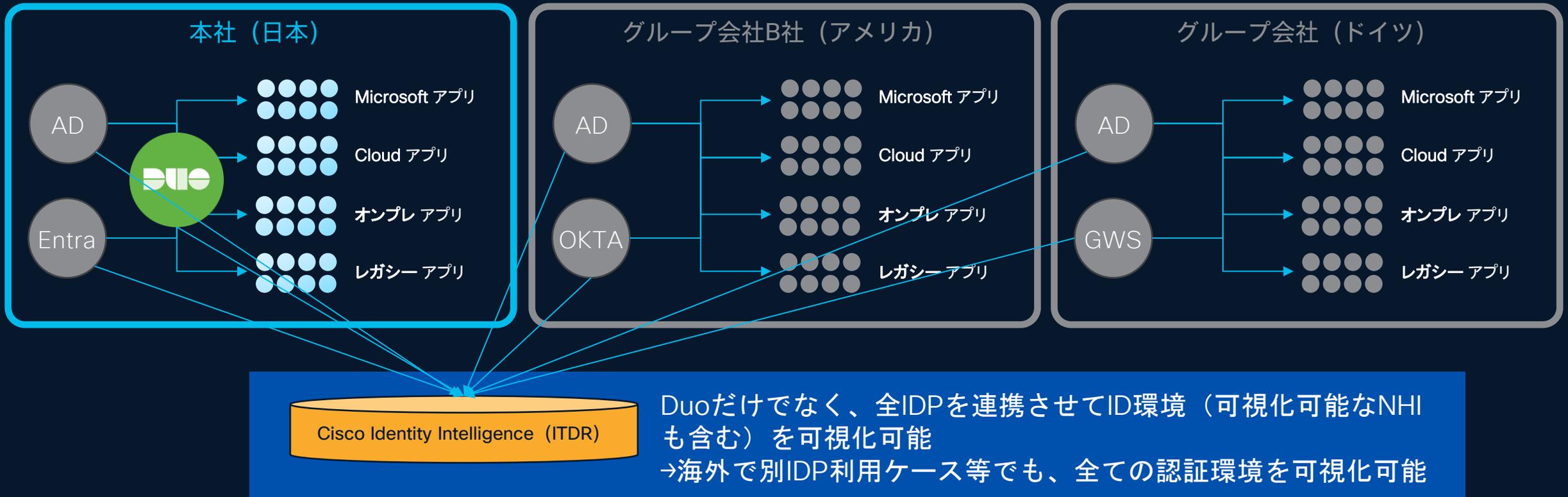
アメリカ管理下、
一部日本のユーザも登録さ
れるも可視化不可



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

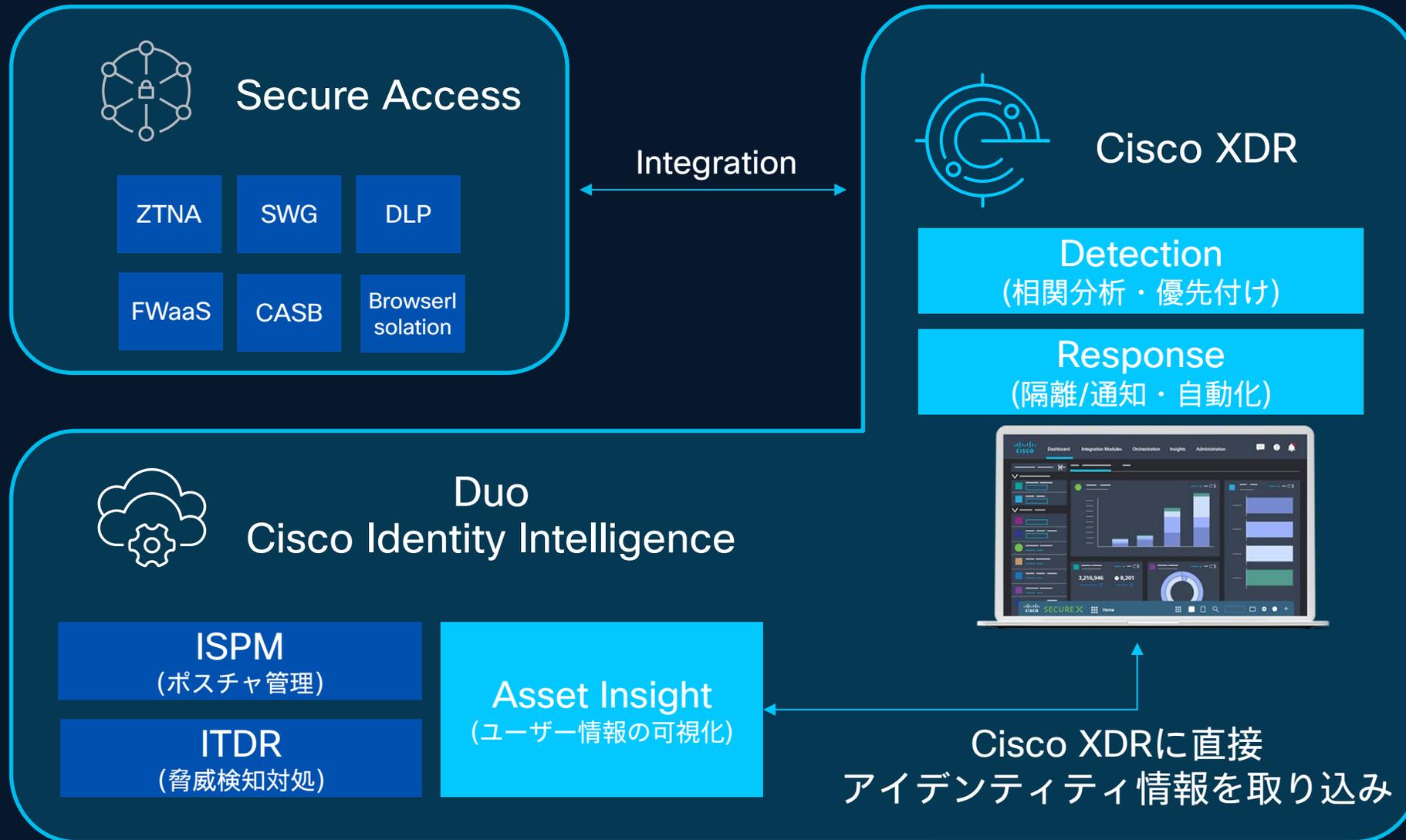
ユースケース④ 海外環境の可視化利用



Duo IAMの柔軟性とCIIの拡張性がポイント

Cisco Identity Intelligence Demo

The slide features a dark blue background with a gradient that transitions to a lighter blue on the right side. A pattern of small, semi-transparent blue dots is scattered across the lower half of the slide, creating a digital or network-like aesthetic. The title text is centered in the upper half of the slide.



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

The screenshot displays the 'Users and User Groups' management interface. A table lists users, with 'Josh Green' highlighted. The 'Trust Level' column shows 'Neutral'. A callout box provides details on the trust level:

- Trust Level:** Neutral
- Last updated:** Feb 04 2025 5:11:49 PM UTC
- Reasons for Neutral status:**
 - SpecialAccount
 - ResurrectedAccount
 - 1. access-from-dormant-account

Cisco Identity IntelligenceのTrust Levelが
Secure Accessで将来的に利用可能に

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

The screenshot displays the 'User Trust Profiles' configuration page in the Cisco Secure Access interface. The page is titled 'User Trust Profiles' and includes a sub-header: 'User trust profiles adaptively modify authentication and security based on trust levels—untrusted, neutral, trusted—incorporated into access rules, powered by Cisco Identity Intelligence. Help'. Below this, there is a search bar and a table of profiles. The table has columns for 'Profile name', 'Assigned to', and 'Used in'. One profile is listed: 'System-provided' (Default for private access policy rules), assigned to 'All private resources', and used in '0 rules'. Below the table, there is a detailed view of the 'Trusted' trust level, showing its 'Authentication controls' (Single Sign On) and 'Security Controls' (IPS: Connectivity Over Security, IPS: Security Over Connectivity, Geolocation: US only). A blue callout box with white text is overlaid on the bottom right of the screenshot, stating: 'Cisco Identity IntelligenceのTrust Levelが Secure Accessで将来的に利用可能に'. The interface also shows a sidebar with navigation options like Home, Connect, Resources, Secure, Experience Insights, Monitor, Admin, and Workflows. On the right side, there are panels for 'Trusted' settings, 'Authentication controls', 'Authentication Options' (with Single Sign On selected), 'IPS Profile' (Enabled), and 'Geolocation' (Enabled).

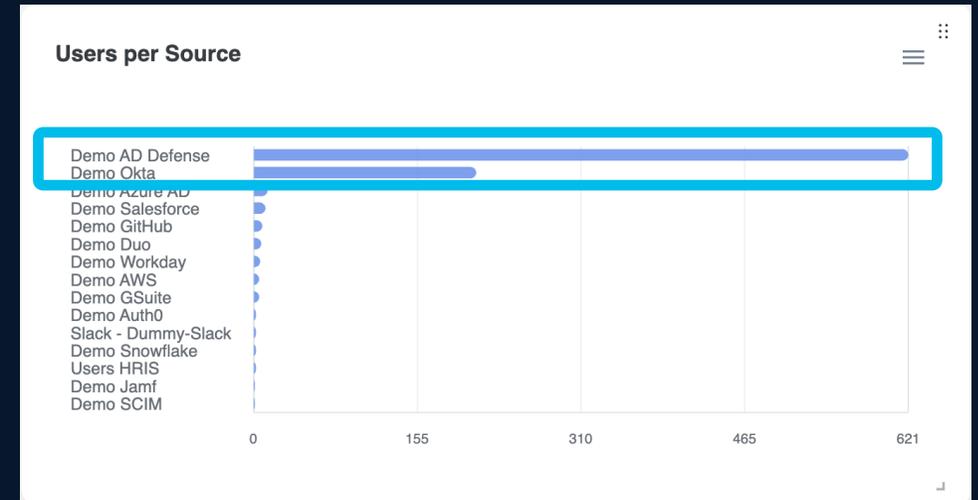
Cisco Identity IntelligenceのTrust Levelが
Secure Accessで将来的に利用可能に

Active Directory Defense (Private Preview前)

Integration Status
No Providers Synced
14 waiting for collection
[Last data collection](#)

Providers

- SCIM Demo AD Defense**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo Azure AD**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo GitHub**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- SCIM Demo SCIM**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo Workday**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- aws Demo AWS**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo Duo**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo Jamf**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo Salesforce**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Slack - dummy-slack**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo Auth0**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo GSuite**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo Okta**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records
- Demo Snowflake**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 0 records



**Cisco Identity Intelligence
オンプレADサポートがPrivate Previewに**

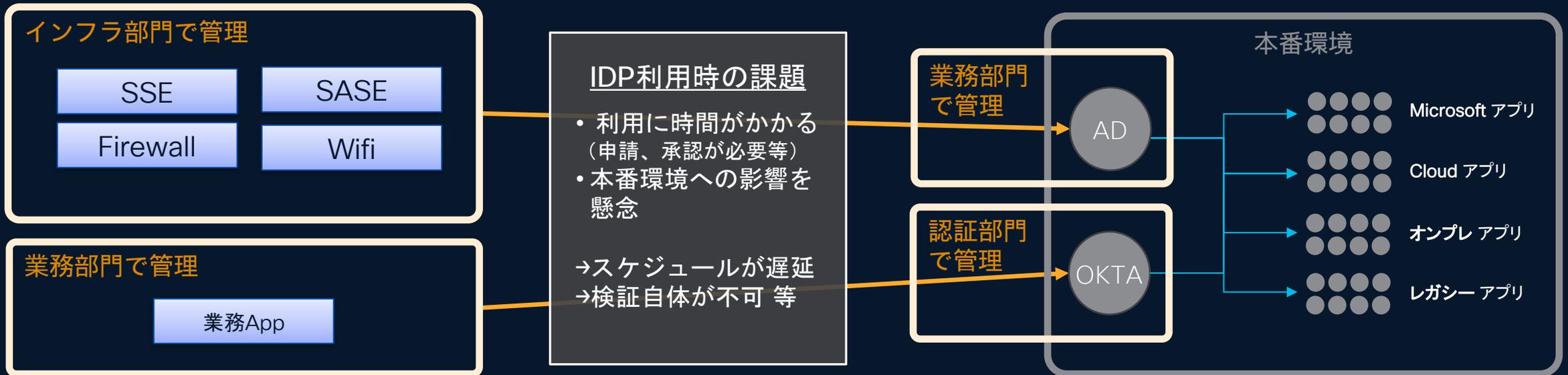
621 users found

# IPs	# Logins	Last Seen (UTC)	Last IP Address	Last Location	MFA	Providers	Status
(Admin) Adelle Francesco	1	3, 2025 11:01:11	N/A	N/A	×	SCIM	Active
(Admin) Balan Malachi	1		N/A	N/A	×	SCIM	Inactive
(Admin) Burdette Dan	4	4, 2025 13:48:31	N/A	N/A	×	SCIM	Inactive
(Admin) Burdette Izabella	8	8, 2025 10:33:05	N/A	N/A	×	SCIM	Inactive
(Admin) Dessie Judge	1	1, 2025 12:27:34	N/A	N/A	×	SCIM	Active
(Admin) Echo Mauricio	1	1, 2025 00:13:43	N/A	N/A	×	SCIM	Active

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

- 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



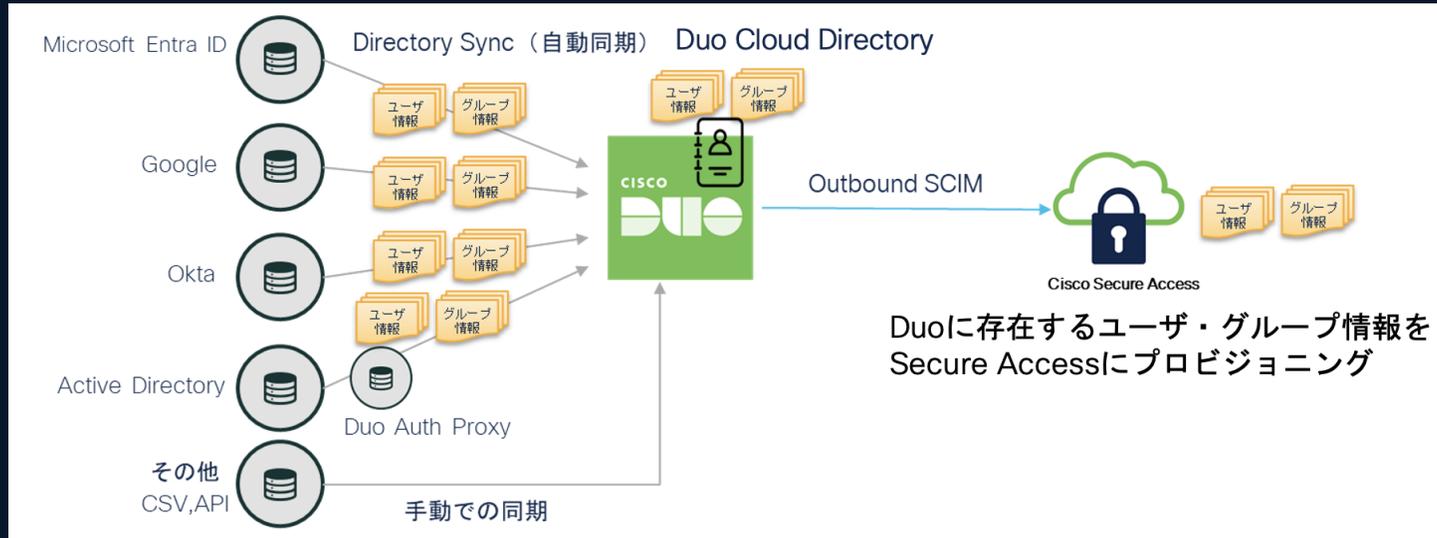
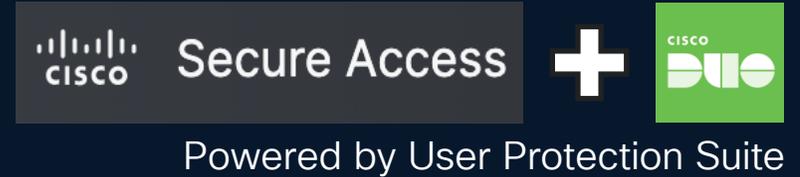
IDP連携が必要だが簡単に利用できず、検討・スケジュールが遅延

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

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



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

その他Duoの価値

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せん。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時間で導入
- 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）

エンドユーザー一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

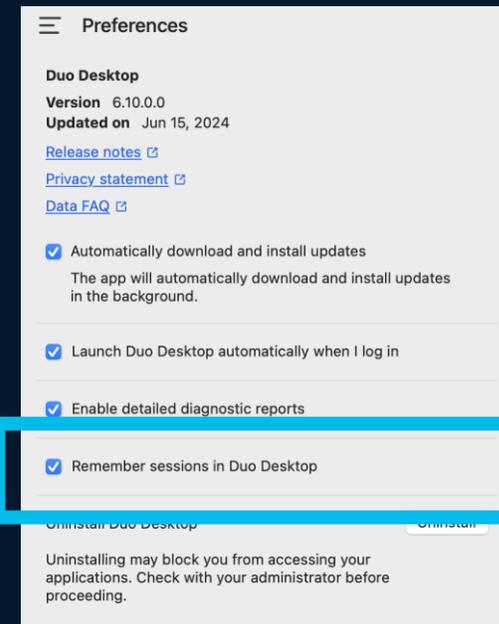
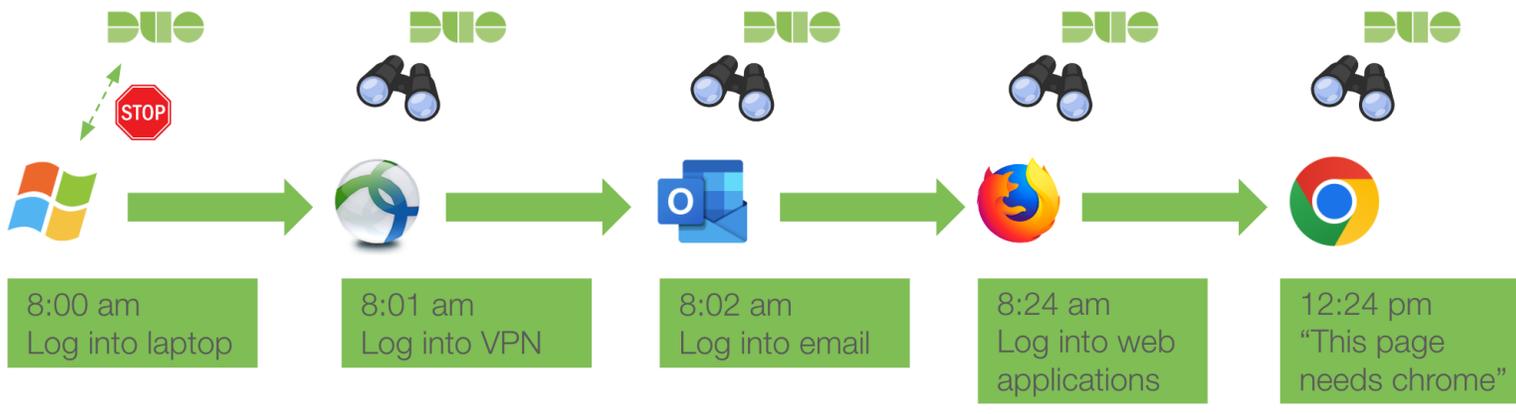
PC ログオン

VPN接続

メール参照

Webアプリ1

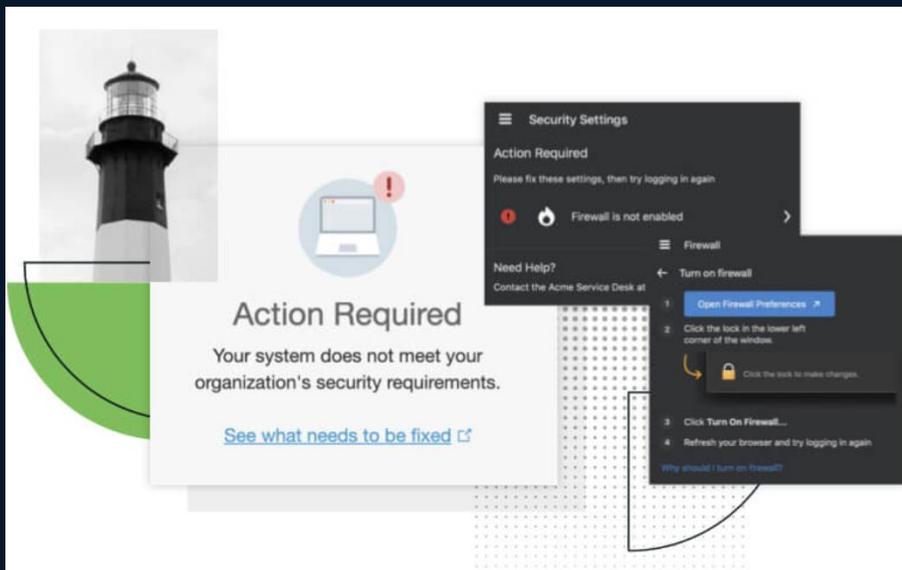
Webアプリ2



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



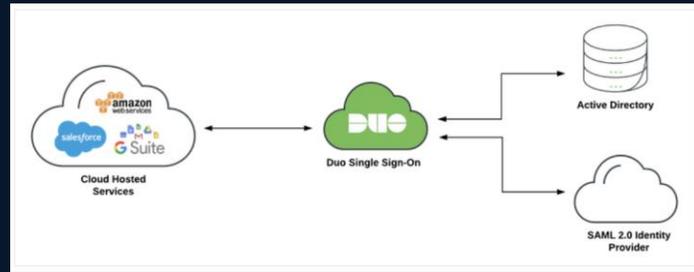
ユーザーによる簡単デバイス管理



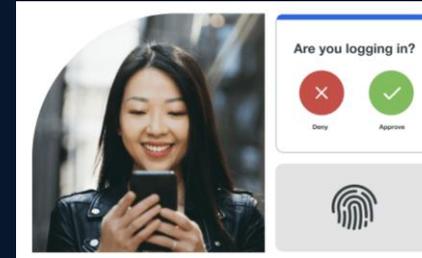
デバイス環境変更時に、エンドユーザーと管理者業務を大幅に削減可能

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



創業当時から追求するユーザーエクスペリエンス



ビデオの概要

Duo シングル サインオンを構成する

必要な役割: オーナー

1 Duo 管理パネルにログインし、「アプリ」

2 「認証ソースの追加」ページで、認証ソースを使用するオプションの下部にあるボタンを

認証ソースを設定する

必要な役割: 所有者、管理者、またはアプリケーション マネージャー

Duo シングル サインオンを使用すると、Active Directory (AD) ドメインとフォレスト、または SAML ID プロバイダーを単一の認証ソースとして使用できます。

環境内で複数の AD および SAML 認証ソースを使用している場合は、ルーティングルールを使用して、ユーザーをアプリケーション アクセスの適切な認証ソースに誘導できます。

アクティブディレクトリ

以下の手順に従って、オンプレミスの認証プロキシをまず Duo シングルサインオンに接続できるように設定してください。次に、認証プロキシを介して Active Directory ドメインコントローラーと通信するように Duo シングルサインオンを設定してください。

AD 認証の計画

初めて Active Directory を設定する場合、「」して同意するよう求められます。追加の AI 再度表示されません。

<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ド
ダンスや動画で解説。機能開発と同時にガイドダンスも更新。
→常に最新の環境とともに最新のドキュメントを提供

Device Health

Security Settings

Action Required

Please fix these settings, then try logging in again

- Firewall is not enabled

ユーザ画面

ファイアウォールがオフになっています

管理者は簡単に問題点を把握できる

ユーザが何が問題なのか把握できる

1つのエントリーでアクセスデバイスの状態(バージョン、ビルド番号、セキュリティチェック、ロケーション)を確認することができます。

認証ログ画面

イベント発生時、即時ログに反映される!

Duo Admin Panel

Timestamp (JST)	Result	User	Application	Access Device	Authentication Method
04:32:27 2022年2月24日	Denied	duodemo	Duo Central	Windows 10, version 21H1 (19043.1466) As reported by Device Health	Unknown
Device Health Application Instance: Chrome 97.0.4692.99 Firewall: Not installed Flash: Not installed Java: Not installed Device Health Application: X Off Firewall: On Encryption: Set Password: Set Security Agents: Running: Windows Defender Location: Minatomirai, 14, Japan IP: 218.221.174.253 Trusted Endpoint: determined by Device Health					

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

どのような環境でも最小の工数で設定可能

ベースが認証Deny→許可設定のみ

Group policies
O365 Edit | Replace | Unassign

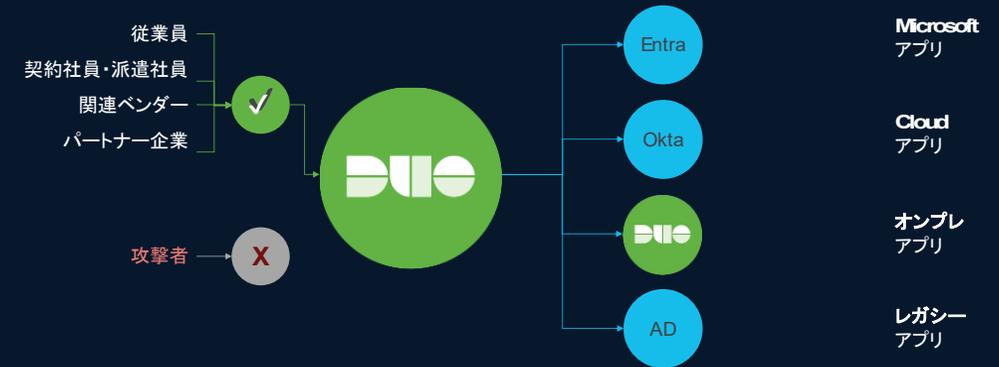
This policy applies to 1 group: **Staff**

- 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



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

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

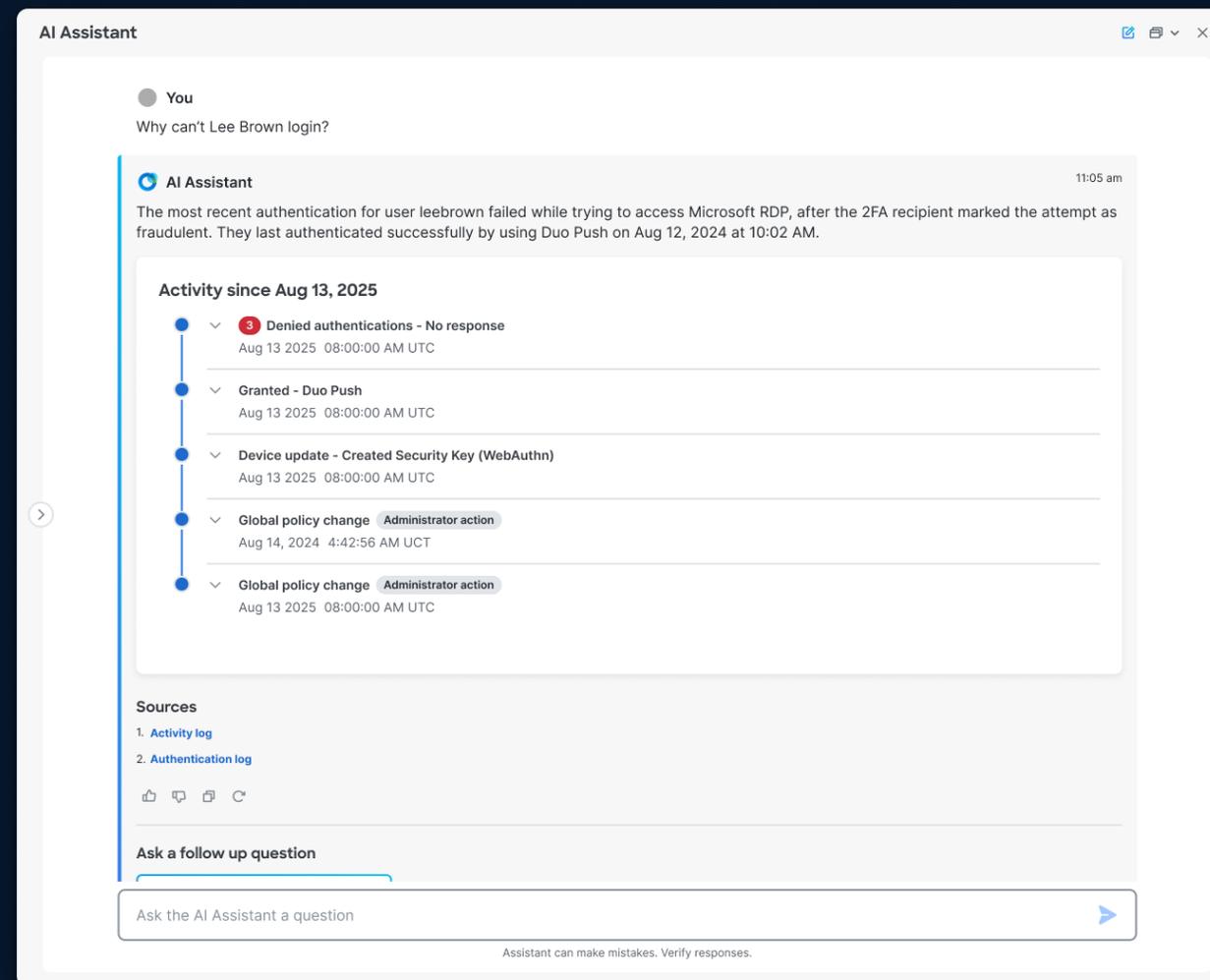
“How do I set group policy?”

→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。

Pricing & Packaging

Duo Essentials

シンプルで効果的なツールを導入し、従業員のアイデンティティ境界を保護

\$3 | User | Month

- Duo Directory
- Complete Passwordless
- Proximity Verification
- AI Assistant
- Multi-Factor authentication
- Single Sign-On
- Trusted Endpoints
- Unlimited applications

Duo Advantage

ログイン前、ログイン中、ログイン後に機能する継続的なアイデンティティ・セキュリティへのアップグレード

\$6 | User | Month

- Duo Passport
 - Session Protection
- Cisco Identity Intelligence
- Adaptive authentication
- Risk-based authentication

Duo Premier

クラウド、オンプレミス、プライベートのアプリケーションやリソースへの保護と容易なアクセスを拡大

\$9 | User | Month

- Secure VPN-less remote access
- 3rd party EDR agent check

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

