Cisco Security Webinar

Duoによるアイデンティティ・セキュリティの再定義

～ランサムウェアへの対抗からAIエージェントの動的統制～

平岡龍弘

Cisco Security, APJC Duo Sales Lead
2026.3.17

Agenda

15:00-15:25

- 最新の脅威動向とDuoのご紹介　スピーカー: 平岡 龍弘

15:25-15:55

- AI Agentのセキュリティ　スピーカー: 稲澤 敏

15:55-16:00

- QA・クロージング

脅威リサーチ Talos

2025 年上半期における日本でのランサムウェア被害

2025 年上半期の日本でのランサムウェア被害は、前年比140%

主に日本の中小企業を標的とし、最も影響を受けている業種は**製造業**

日本に最も被害を出しているのは「**Qilin**」ランサムウェアグループ

6 月下旬に新しいランサムウェアグループ「**Kawa4096**」が現れ、日本の 2 社が攻撃された可能性

Qilinランサムウェアの侵入アプローチ（Talos Blogからの抜粋）

Latest Qilin TTPs

Initial Access

Talos は、単一の確定した初期侵入経路を明確に特定することはできませんでした。
しかしながら、いくつかの事例においては、攻撃者がダークウェブ上に漏えいした管理者認証情報を悪用して VPN アクセスを取得し、さらにグループポリシー（Active Directory GPO）を変更して、

リモートデスクトッププロトコル（RDP）を有効化し、被害組織のネットワークへ到達した可能性があると、中程度の確信度をもって評価しています。

図 6 に示したインシデントでは、Talos は、認証情報がダークウェブ上に流出していたことを確認しました。
約 2 週間後、漏えいした認証情報を使用した可能性のある多数の NTLM 認証試行が VPN に対して行われ、その結果、侵入が成功しました。
侵害された VPN から、攻撃者はドメインコントローラーおよび最初に侵入されたホストに対して RDP 接続を実行しました。

この活動は、先に確認された認証情報の流出と時間的な関連が見られますが、両者の間に明確な因果関係を立証するための十分な証拠は得られていません。
特筆すべき点として、この事例で問題となった VPN には多要素認証（MFA）が設定されておらず、そのため攻撃者は認証情報を入手することで制限なくアクセスできる状況となっていました。

主なランサムウェアの攻撃フロー

VPN侵害からランサムウェア実行までの全貌

初期侵入
Initial Access

漏洩した認証情報によるVPNアクセス

MFAが弱い、VPNが古い、アカウント漏洩等のリスクを狙う。

偵察
Discovery

“nltest.exe” ,”net.exe”のよる情報収集。

ドメコンの列挙、追加のアカウント情報取得。

認証情報の摂取
Credential Access

AD資格情報のダンプ SharpDecryptPw, Mimikatz による認証情報摂取

WinRARで圧縮、Cyberduckでクラウドへ転送

権限昇格
Privilege Escalation

複数のアカウント (管理者を含む) に対するNTLM認証。

目的はドメイン管理者権限の取得。

水平移動
Lateral Movement

接続されたネットワーク共有フォルダに移動し、価値あるホストへアクセス拡大

防御回避
Defense Evasion

難読化PowerShellによるAMSI無効化。EDR・セキュリティツールの削除。

ログや監視を無効化し発見されにくくする。

影響
Impact

データ流出 (Exfiltration)、Qilin ランサムウェアの展開、ADの完全な侵害によるドメイン再構築の必要性。

復旧妨害
Inhibit Recovery

Windows イベントログおよびVSS スナップショットの削除。

最終段階として復旧不能に近い状態に追い込む。

アイデンティティが重要な要素として利用された侵害の割合

Cisco Talos インシデント対応チーム | 2024 年版『一年の総括』

従来の IAM では安全性を確保できていない

低い安全性

高いコスト

複雑さ

Duoによる Identity Security

高い安全性

低いコスト

シンプルさ

Cisco Duo

Cisco Duoが提供する卓越したIdentity Security

IAM

セキュリティFirstの
ID管理基盤

MFA・SSO

フィッシングの可能性を
完全に排除

Identity Intelligence

AIで継続的に信頼性を検証
ITDR・ISPM

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提供

アイデンティティの攻撃対象

攻撃者が新入社員にブルートフォース攻撃やパスワードスプレー攻撃を仕掛ける

登録

攻撃者が
MFA バイパスを試行

OS ログイン

攻撃者がデバイスに物理的にアクセス

アプリケーションへのログイン

攻撃者が安全性の低い MFA 方式にフォールバック

攻撃者がセッション Cookie の窃取を試行

セッション中

ヘルプデスク

攻撃者がヘルプデスクでディープフェイクのソーシャルエンジニアリングを試行

Duoはセキュリティのための認証基盤

登録

信頼できる登録ソース

OS ログイン

フィッシングに強い MFA

アプリケーションへのログイン

フィッシングに強い MFA

セッション中

セッションの乗っ取り防止

ヘルプデスク

深い信頼の再確立

シームレスで安全な信頼の引き継ぎ

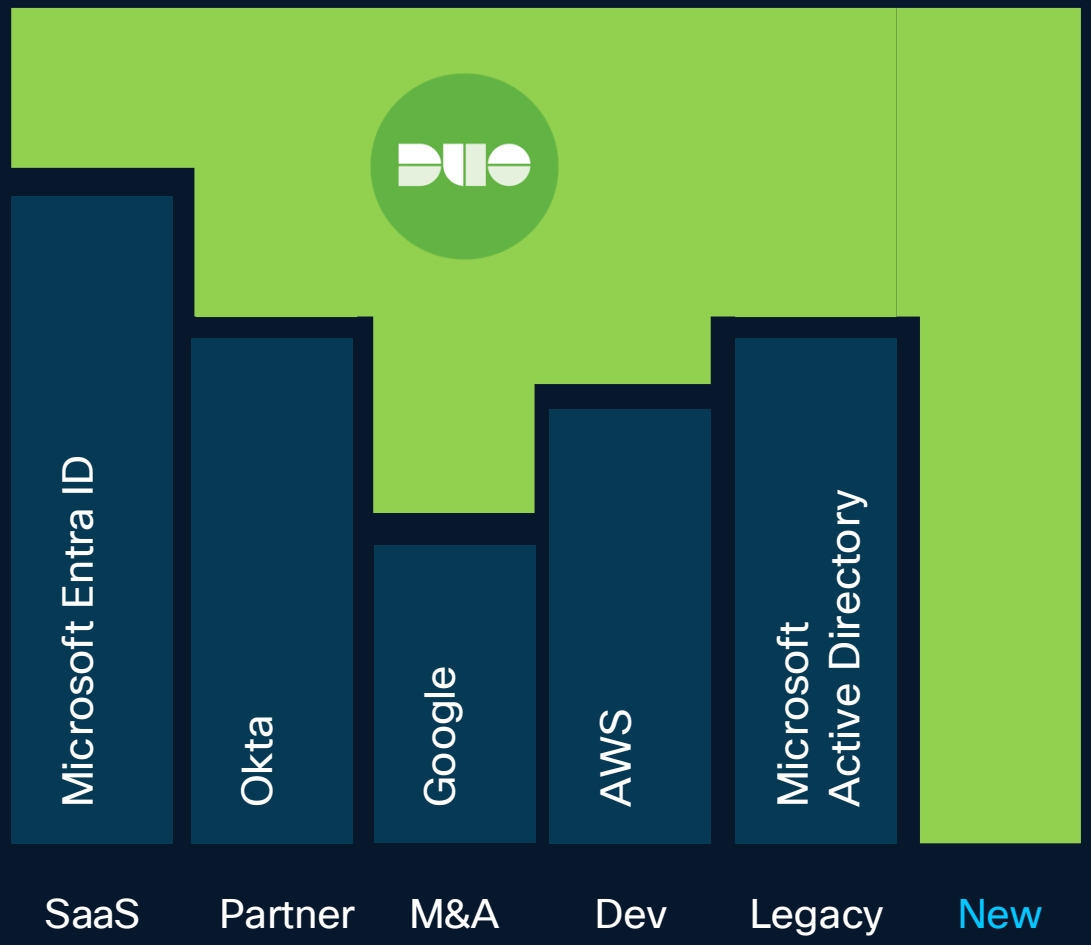
Identity Intelligence

Gartnerのレポート

Gartner® Peer Insights™ 2026 Voice of the Customerのユーザー認証部門で「Customers Choice」に選出

Voice of the Customer for User Authentication

DuoはIdentityのセキュリティにフォーカス



複雑なID環境へ強力なセキュリティを柔軟に安価に提供し、ギャップを埋める

ユーザーの快適性を損なわず、すべてのユーザーを守る

MFA・SSO

フィッシングの可能性を完全に排除

Cisco Duoが提供する卓越したIdentity Security

IAM

セキュリティFirstの
ID管理基盤

MFA・SSO

フィッシングの可能性を
完全に排除

Identity Intelligence

AIで継続的に信頼性を検証

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提供

新しいアイデンティティの攻撃対象領域

攻撃者は進化している。その一歩先を行くことが必要。

登録

信頼できる登録ソース

OS ログイン

フィッシングに強い MFA

アプリケーションへのログイン

フィッシングに強い MFA

セッション中

セッションの乗っ取り防止

ヘルプデスク

深い信頼の再確立

シームレスで安全な信頼の引き継ぎ

Identity Intelligence

MFA強度の階層

フィッシング耐性や攻撃の難易度に基づくセキュリティレベルの分類

MFAなし

攻撃者の理想的なターゲット
極めて危険

侵入のリスク大

電話・SMS

SIMスワップや通信傍受に極めて弱い。自動音声の脆弱性。

傍受のリスク大

メール・OTP

メール乗っ取りや、偽サイトへの入力ミスを防げない。

通知(承認のみ)

内容を見ずに承認する「MFA疲労攻撃」に脆弱

疲労攻撃のリスク

通知(マッチング)

PC画面の数字をスマホで入力。
Duo推奨設定。

「うっかり承認」を物理的に防ぎ、ヒューマンエラーを大幅に低減

近接認証

物理的な距離制限により遠隔攻撃を遮断。

パスワードレス

公開鍵暗号を使用。偽サイトでは認証不可。

フィッシング耐性MFA

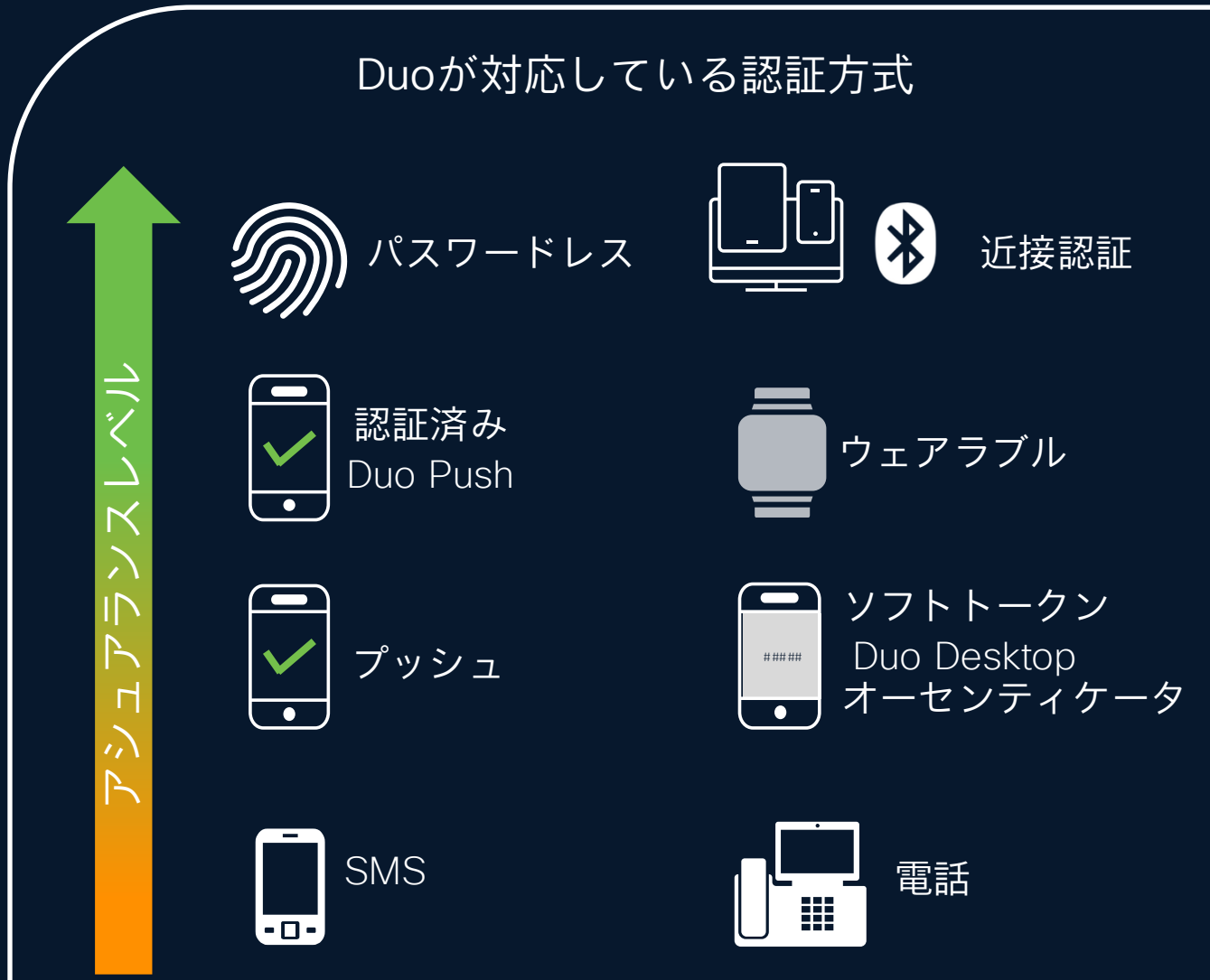
AiTMのリスク

規制当局によるフィッシング対策の推奨

NIST AAL 1 | NIST AAL 2 | NIST AAL 3

環境に合わせた多様なMFA

- 業界をリードする多様な認証手段
- ユーザーまたはアプリケーショングループごとに柔軟な認証ポリシーが設定可能
- フィッシングに強いMFA とパスワードレスを簡単に導入
- ニーズに応じて、複数の要素やオフラインの認証手段を展開



Cisco Duoが提供する卓越したIdentity Security

IAM

セキュリティFirstの
ID管理基盤

MFA・SSO

フィッシングの可能性を
完全に排除

Identity Intelligence

AIで継続的に信頼性を検証

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提供

新しいアイデンティティの攻撃対象領域

攻撃者は進化している。その一歩先を行くことが必要。

登録

信頼できる登録ソース

OS ログイン

フィッシングに強い MFA

アプリケーションへのログイン

フィッシングに強い MFA

セッション中

セッションの乗っ取り防止

ヘルプデスク

深い信頼の再確立

シームレスで安全な信頼の引き継ぎ

Identity Intelligence


一度だけ認証
Workday


Web サイトへのアクセス
アプリケーションの利用
VPN へのアクセス
別の Web サイトへのアクセス

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

IAM

セキュリティFirstのID管理基盤

Cisco Duoが提供する卓越したIdentity Security

IAM

セキュリティFirstの
ID管理基盤

MFA・SSO

フィッシングの可能性を
完全に排除

Identity Intelligence

AIで継続的に信頼性を検証

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提供

新しいアイデンティティの攻撃対象領域

攻撃者は進化している。その一歩先を行くことが必要。

登録

信頼できる登録ソース

OS ログイン

フィッシングに強い MFA

アプリケーションへのログイン

フィッシングに強い MFA

セッション中

セッションの乗っ取り防止

ヘルプデスク

深い信頼の再確立

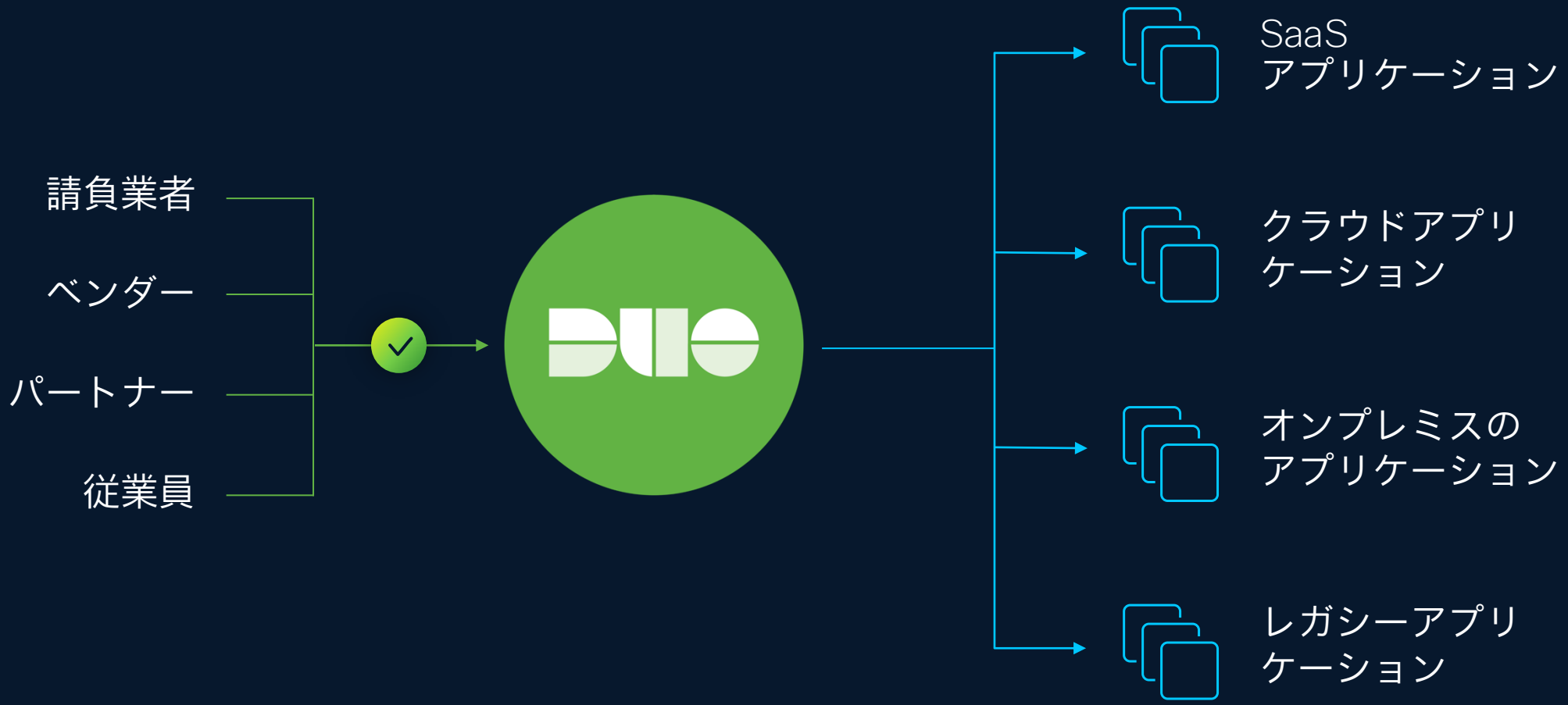
シームレスで安全な信頼の引き継ぎ

Identity Intelligence

スタンドアロンの
IAM が必要

既存 IAM のアイデンティティブローカー

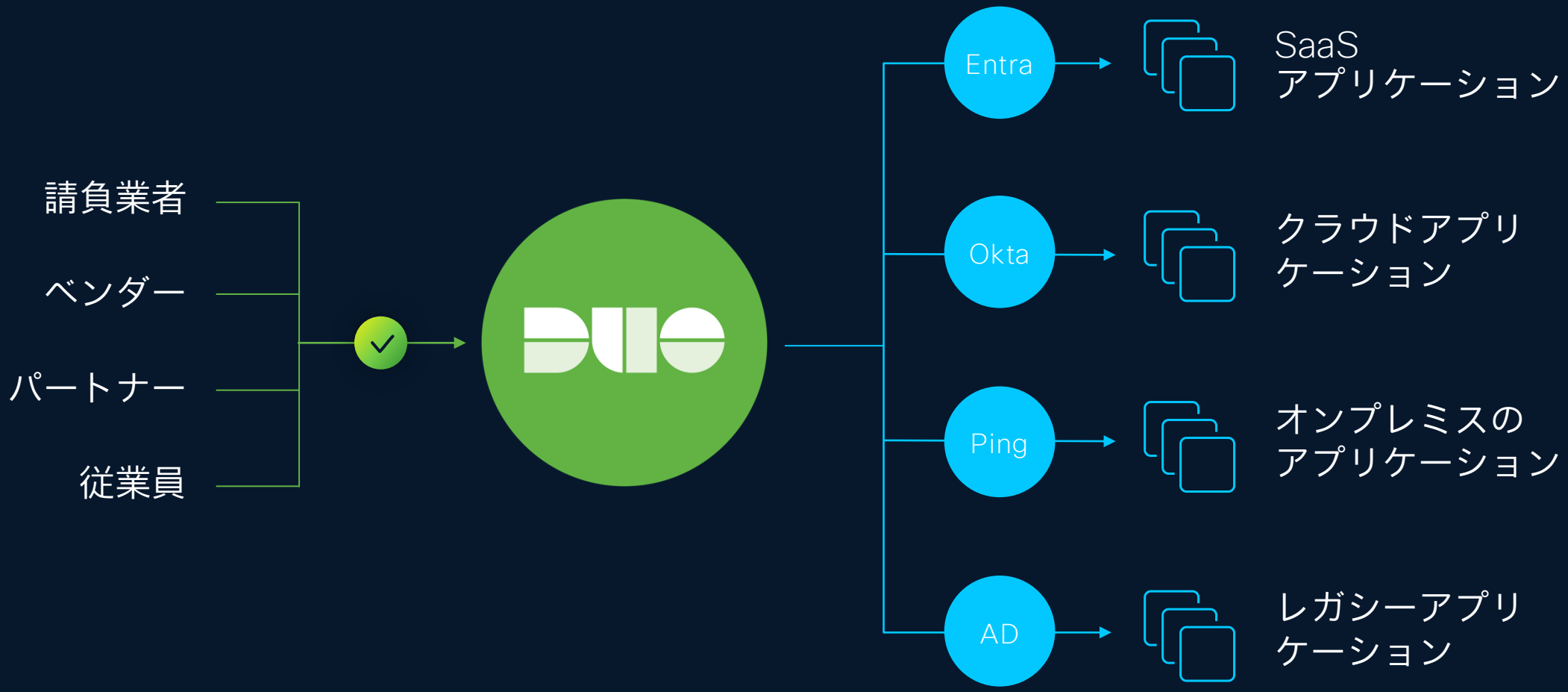
サードパーティユーザー用の
代替ディレクトリ



スタンドアロンの
IAM が必要

既存 IAM のブローカー

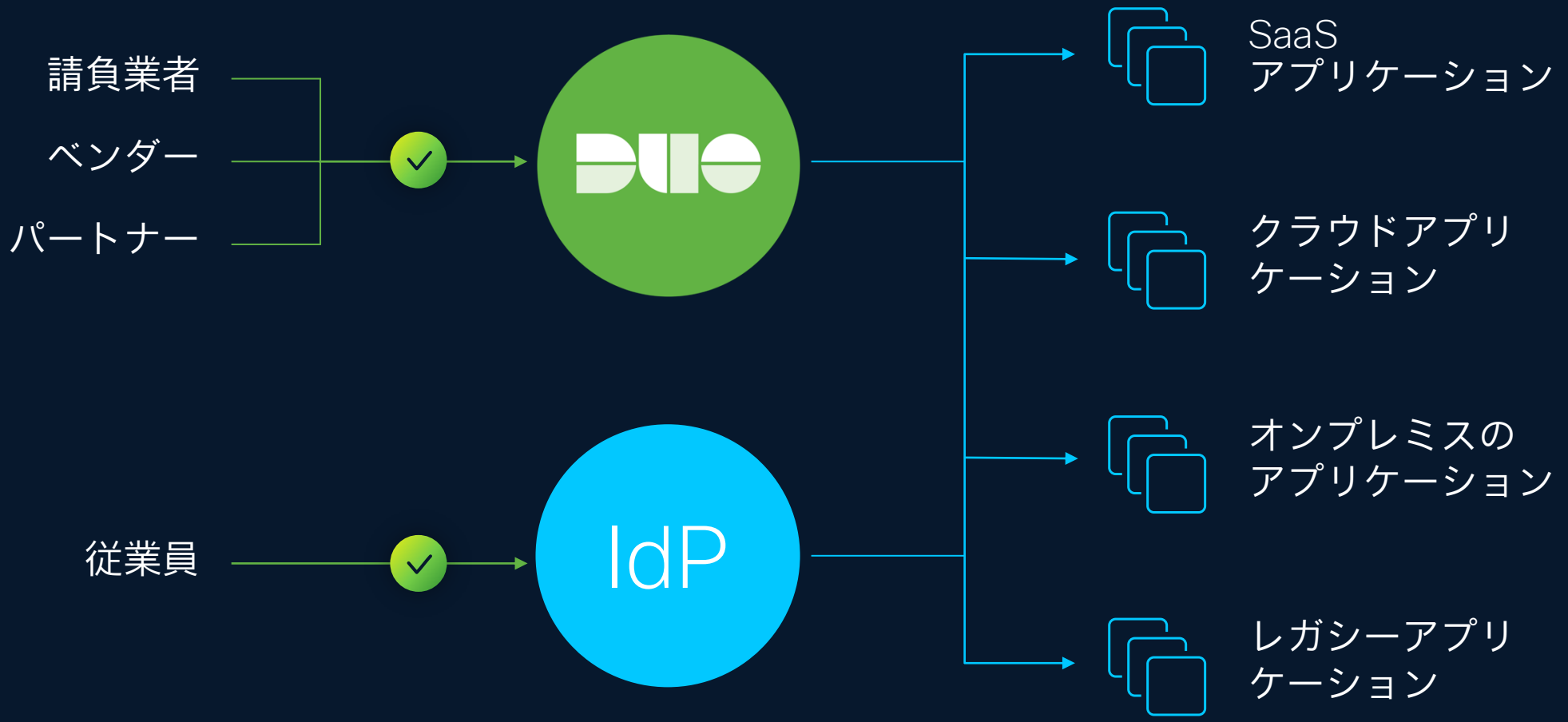
サードパーティユーザー用の
代替ディレクトリ



スタンドアロンの
IAM が必要

既存 IAM のアイデンティ
ティブローカー

サードパーティユーザー用の
代替ディレクトリ



- 本人の信頼性を確実に確認

Duo Identity Verification Integration

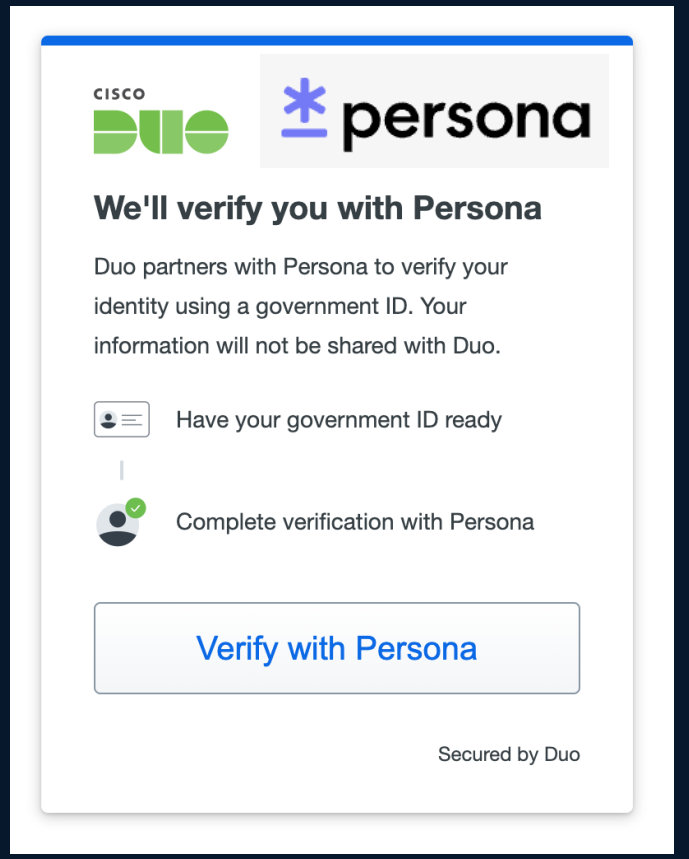
ユースケース

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。

Identity Intelligence

AIで継続的に信頼性を検証

Cisco Duoが提供する卓越したIdentity Security

IAM

セキュリティFirstの
ID管理基盤

MFA・SSO

フィッシングの可能性を
完全に排除

Identity Intelligence

AIで継続的に信頼性を検証

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提供

新しいアイデンティティの攻撃対象領域

攻撃者は進化している。その一歩先を行くことが必要。

登録

信頼できる登録ソース

OS ログイン

フィッシングに強い MFA

アプリケーションへのログイン

フィッシングに強い MFA

セッション中

セッションの乗っ取り防止

ヘルプデスク

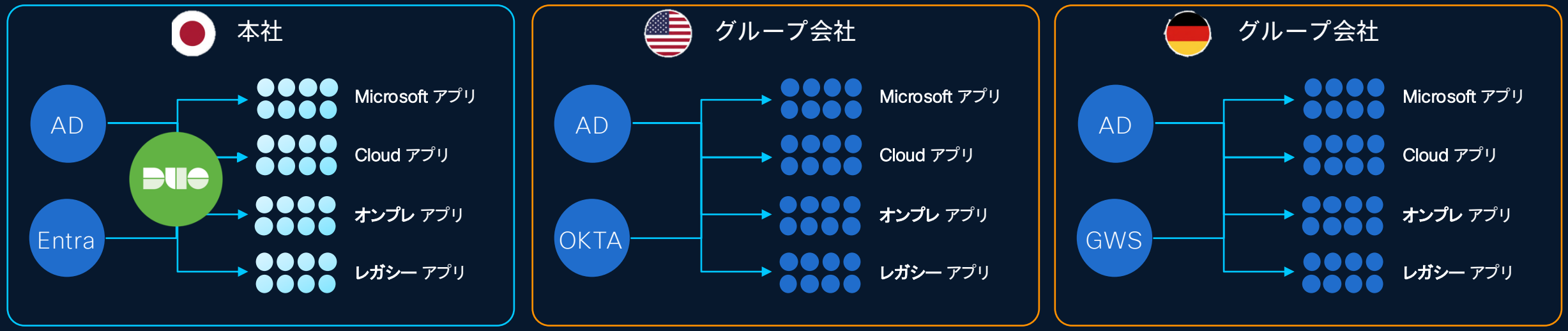
深い信頼の再確立

シームレスで安全な信頼の引き継ぎ

Identity Intelligence

Use Case：複数環境のID振る舞い分析

課題：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



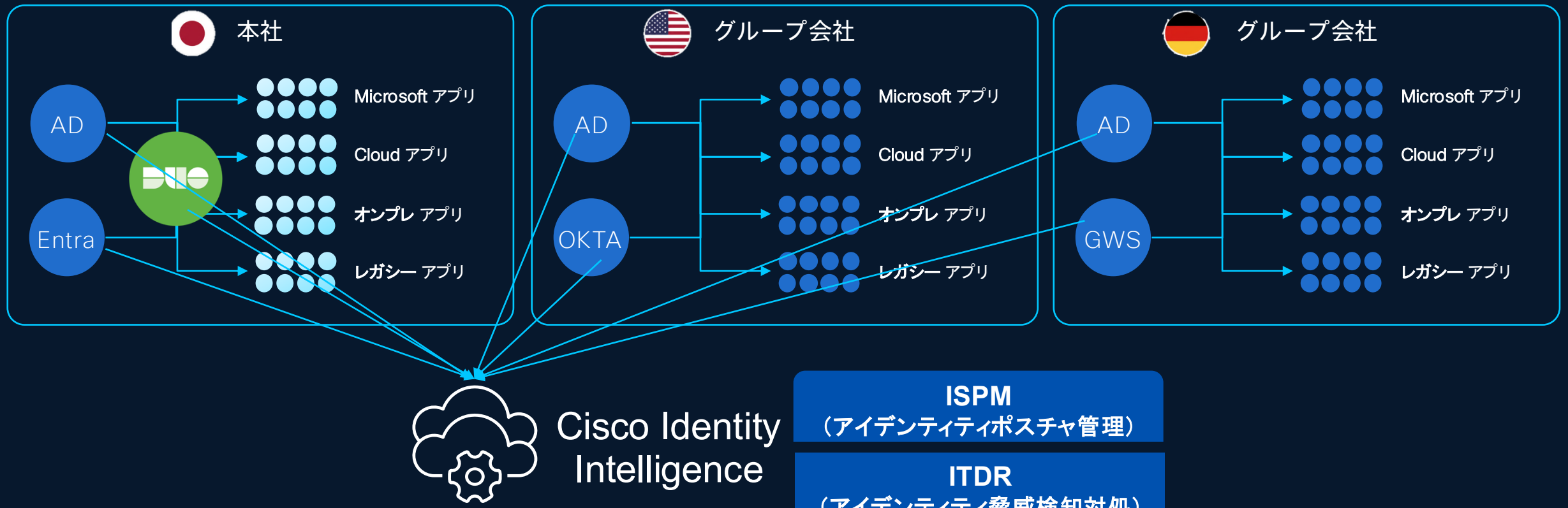
全て可視化可能

一部日本のユーザも登録されるも可視化不可

一部日本のユーザも登録されるも可視化不可

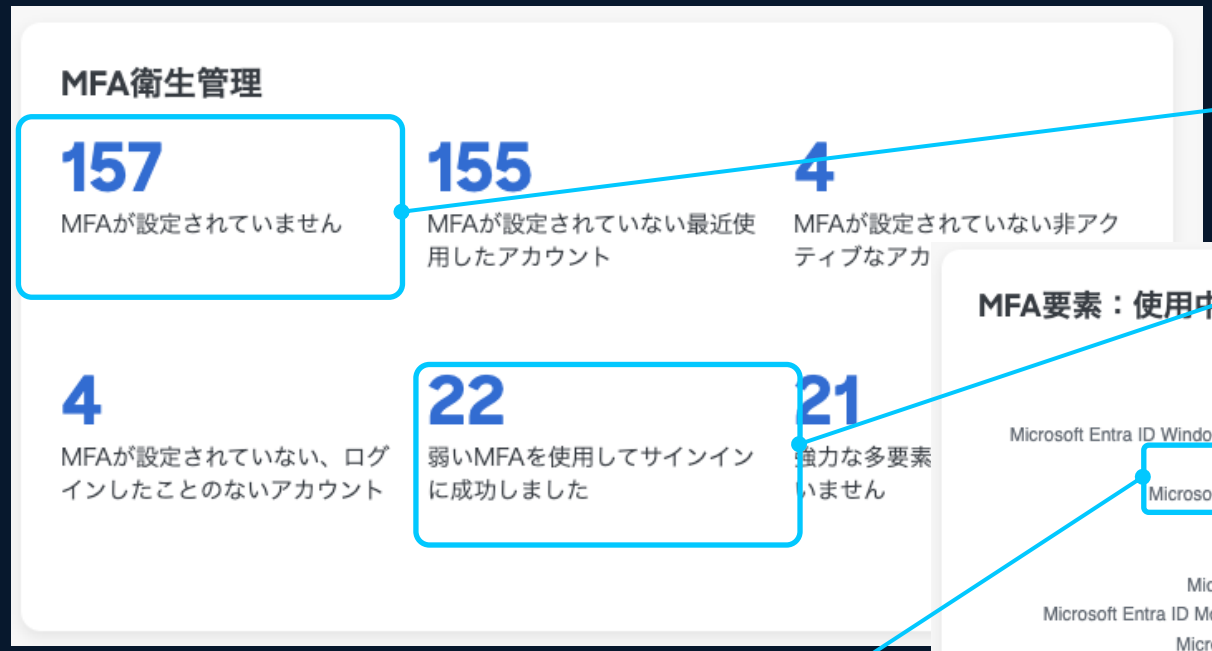
Use Case：複数環境のID振る舞い分析

解決：全てのIdPを連携させてNHIも含めたID環境を可視化可能



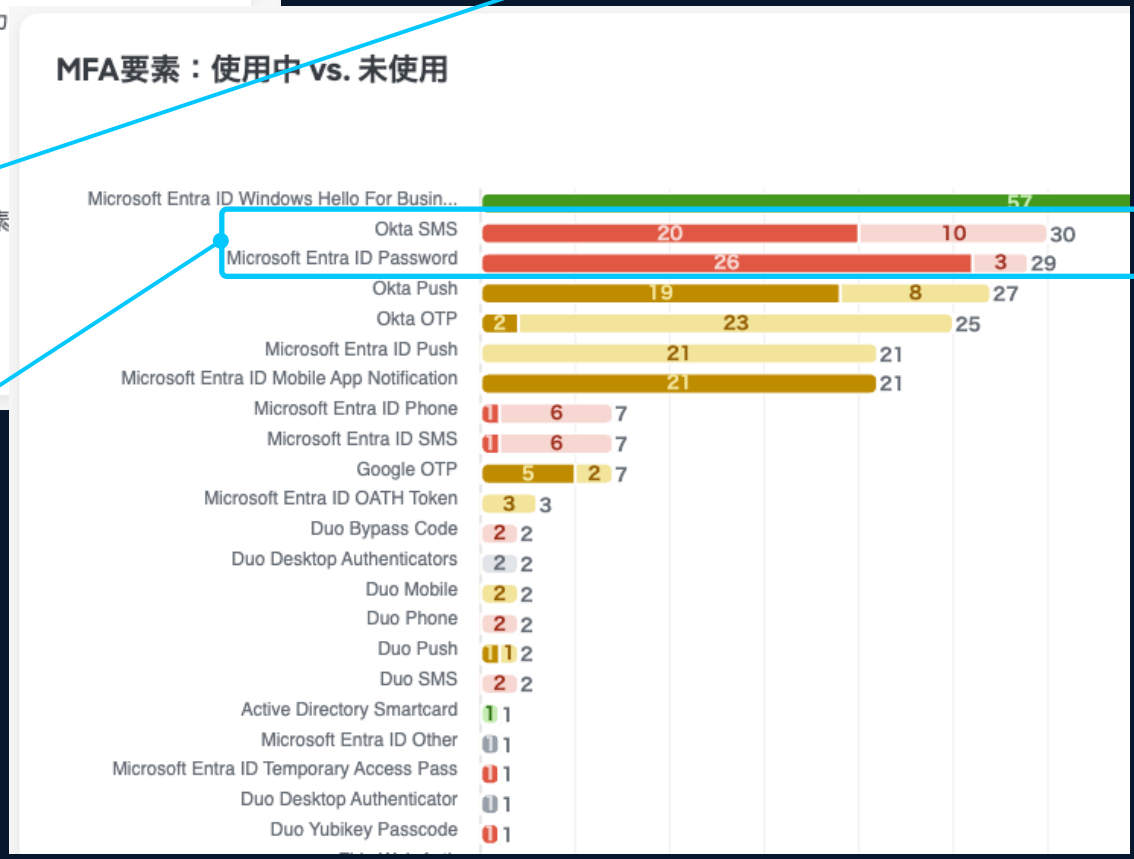
ISPM

MFA の適用範囲



MFA未設定のアカウントを洗い出し

弱いMFAアカウントの洗い出し



IdP毎のMFA利用状況を可視化

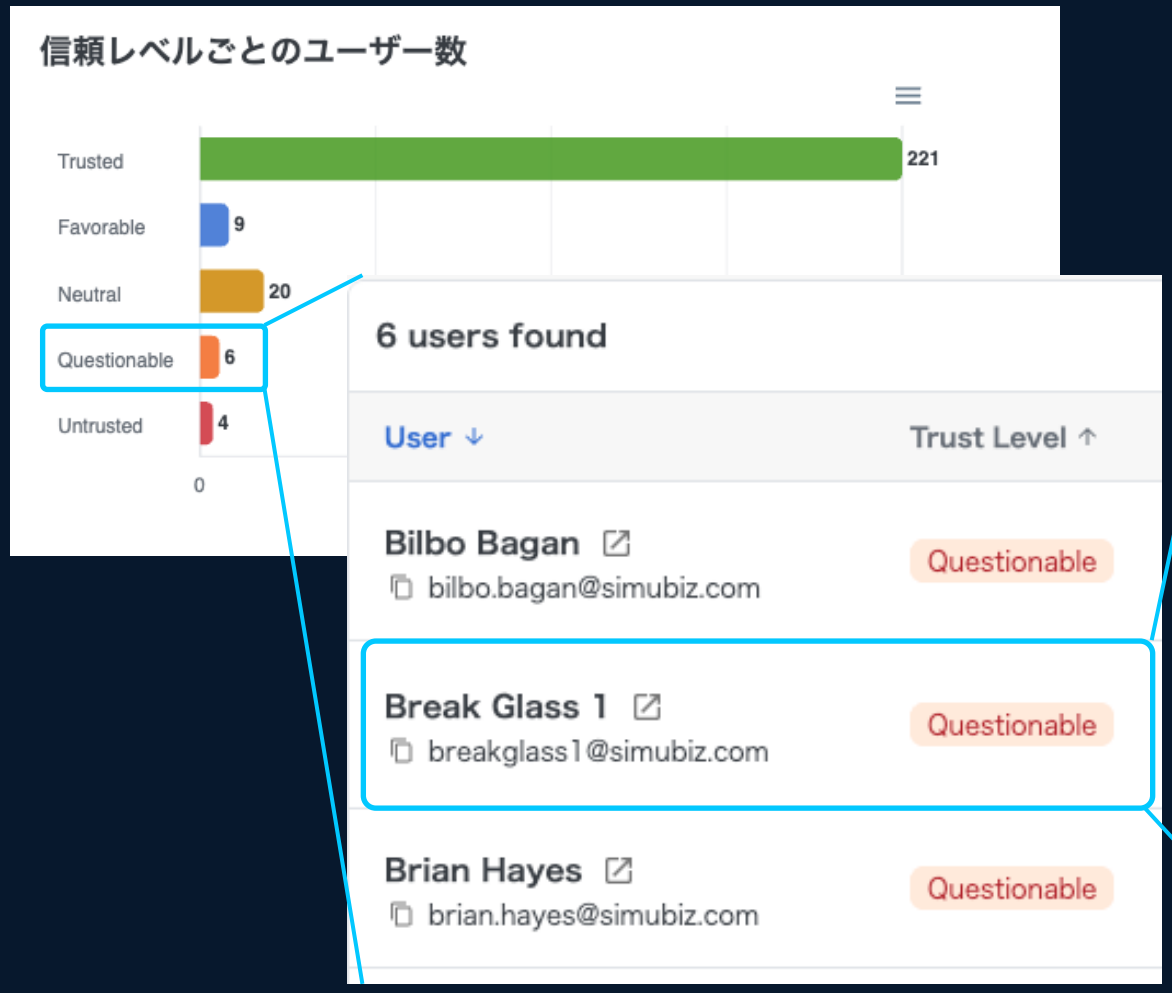
ITDR

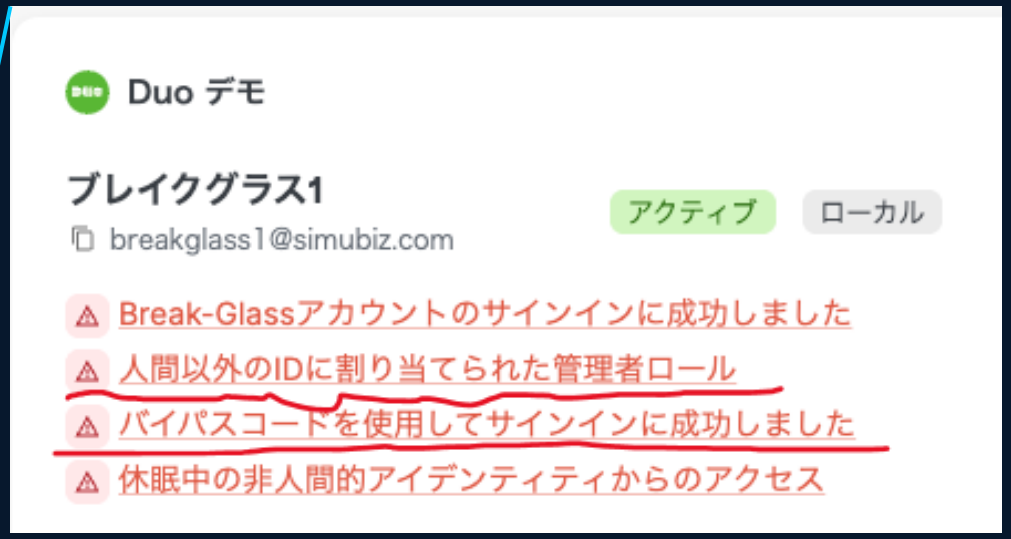
Identityの振る舞い検知

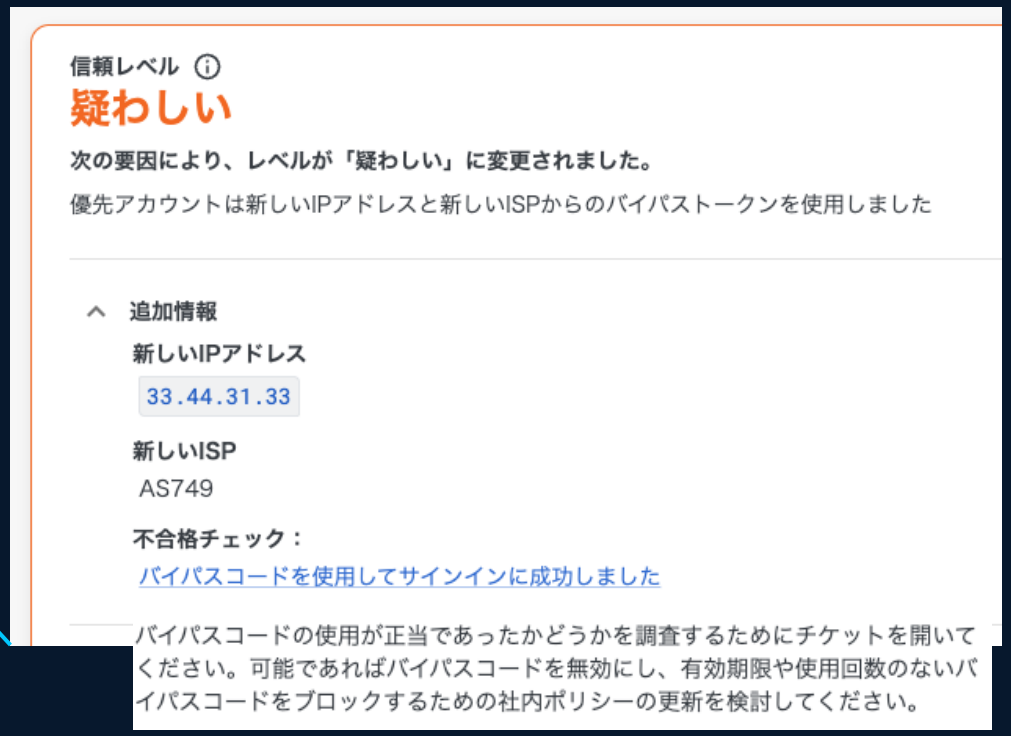
- 複数のIdPを跨いで、怪しい振る舞いをしているユーザーを即座に特定
- AIとMLを活用して、アイデンティティの異常や不審なふるまいを検知
- Mitre ATT&CK や CIS などのセキュリティフレームワークに脅威を簡単にマッピング

ITDR

ユーザー単位で信用レベルを特定

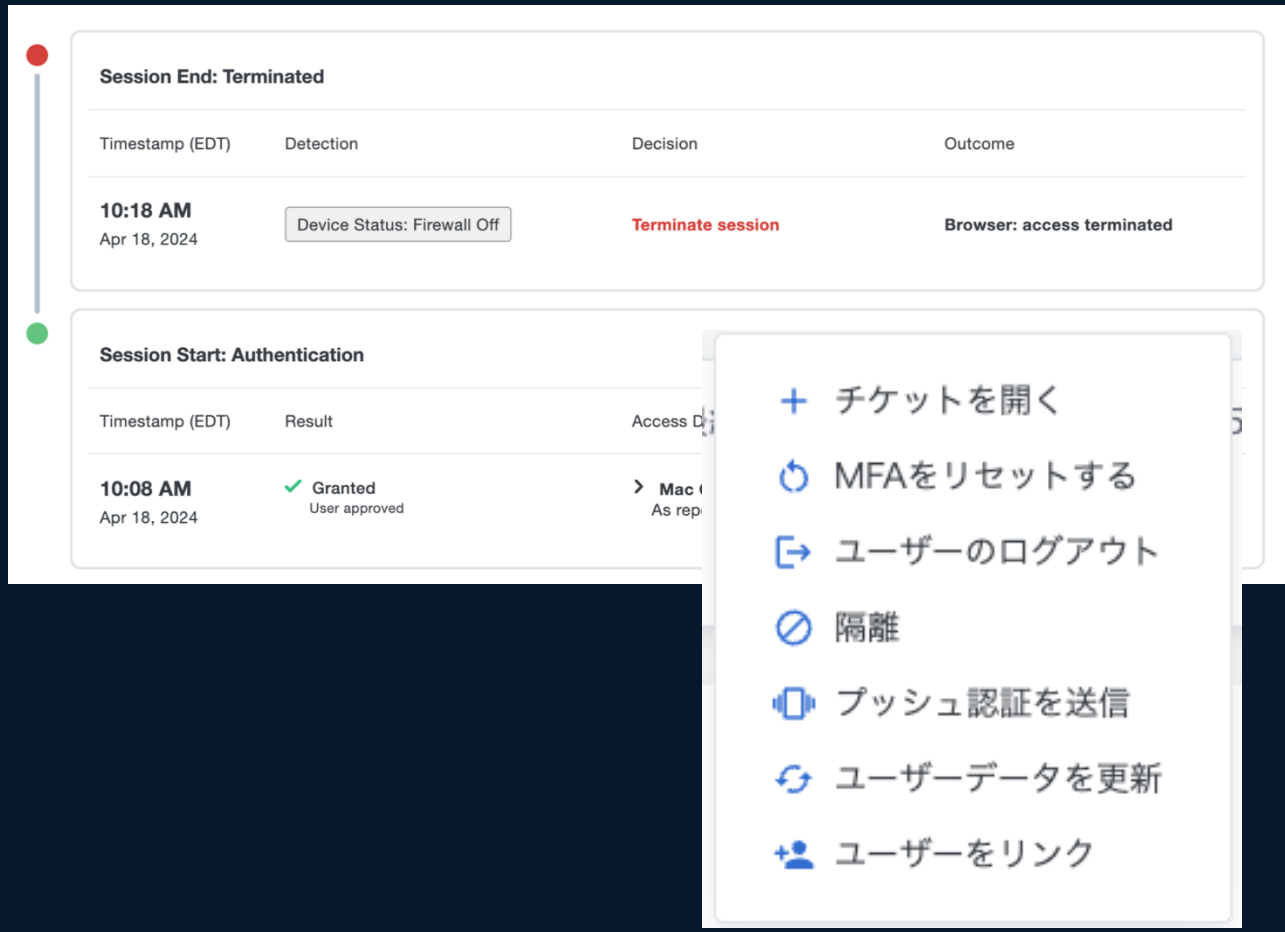






アイデンティティに関するアクションを自動化

- 信用レベルに基づき、隔離やログアウトを実施
- ITSM およびメッセージングツールとの連携により、修復ワークフローを自動化
- アイデンティティのリスクデータをSplunk/XDRに取り込み、包括的なDetection Responseを実現
- Secure Accessと連携することで、Trust Levelのコンテクストを利用可能　- Private Preview -



Cisco Identity Intelligenceの製品連携

DuoIAM

Duo MFA

Cisco Identity Intelligence

特定（Identify）

防御（Protect）

検知（Detect）

対応（Respond）

復旧（Recover）

Secure Access

ZTNA | SWG | DLP | FWaaS | CASB | Browserl solation

Cisco XDR

EDR
NDR
ITDR

Detection
(相関分析・優先付け)

Response
(隔離/通知・自動化)

Splunk Enterprise Security™

SEIM
ログ集約・相関分析
根本原因分析

SOAR
プレイブック・
対応自動化

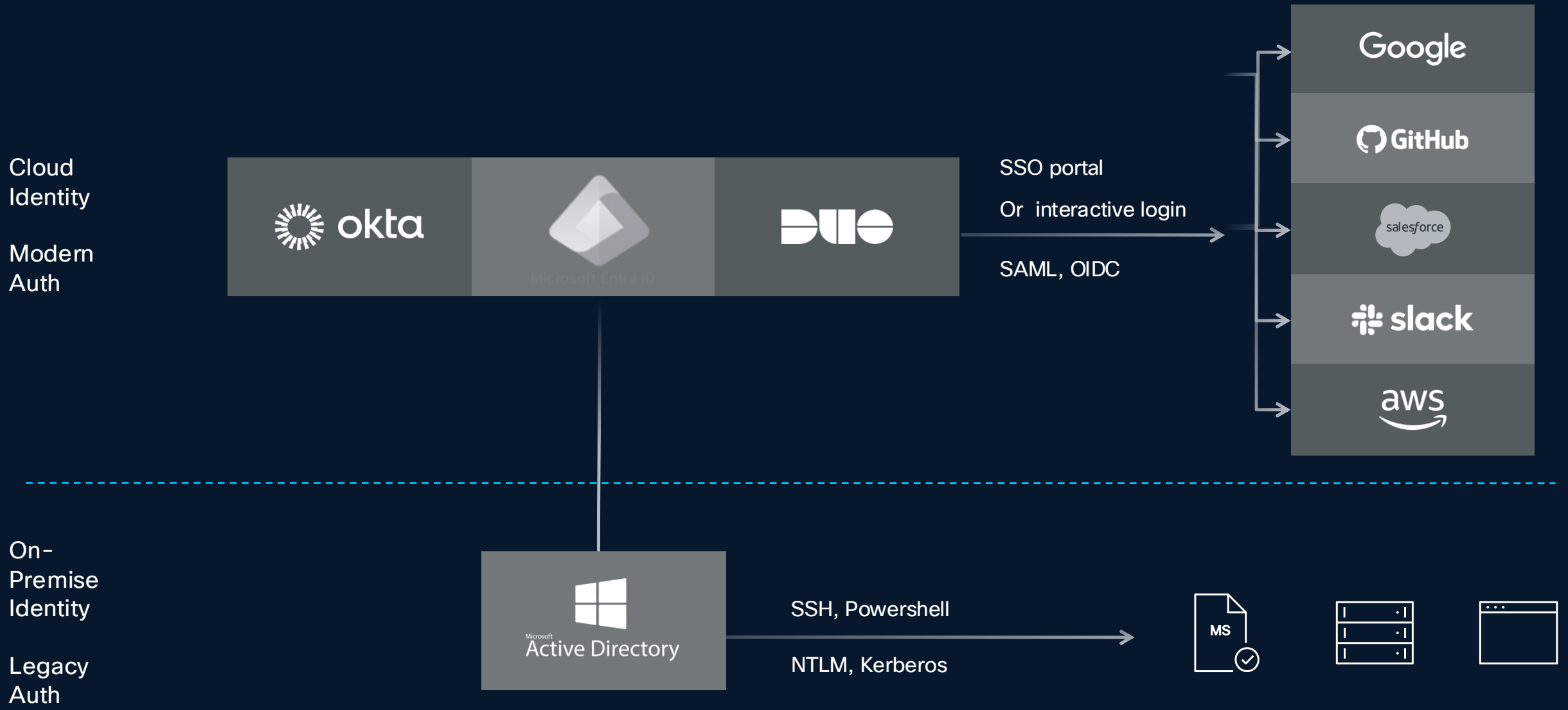
AD Defence

Active Directoryは未だに大多数の企業で使われている

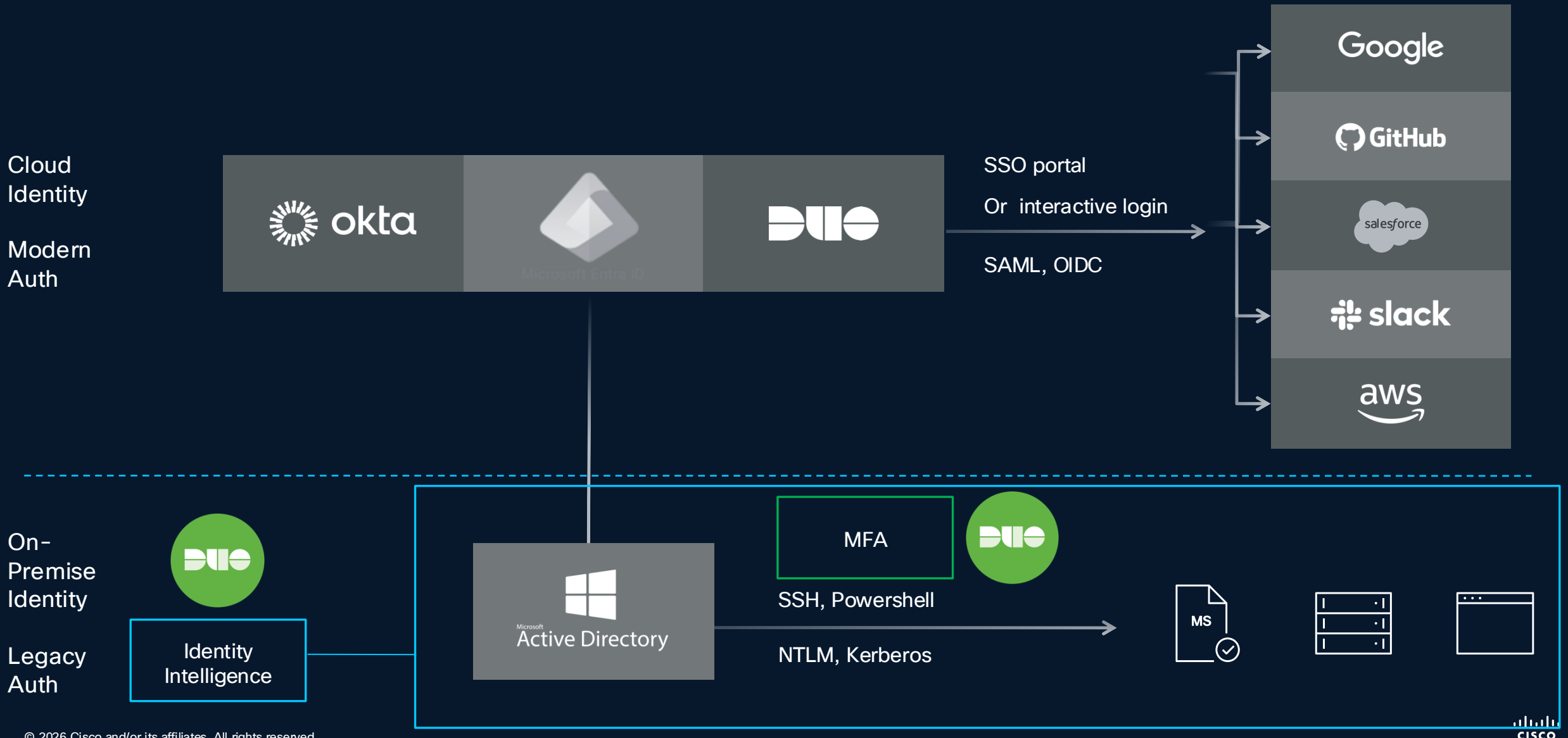
Active Directoryを使用してユーザーや資産を管理している企業

90% of Fortune 1000

クラウドのアイデンティティは既に保護されている



Active Directory Defenseはレガシーインフラを保護



ライセンス

料金とパッケージ

Duo Essentials

シンプルで効果的なツールを導入してワークフォースのアイデンティティ境界を保護します。

3 ドル | ユーザー | 月

- Duo Directory
- 完全なパスワードレス
- 近接認証
- AI Assistant
- 多要素認証
- シングルサインオン（SSO）
- Trusted Endpoints
- アプリケーション数の制限なし

Duo Advantage

ログイン前、ログイン時、ログイン後に機能する継続的なアイデンティティ セキュリティにアップグレードします。

6 ドル | ユーザー | 月

- Duo Passport
  - セッション保護
- Cisco Identity Intelligence
- 適応型認証
- リスクベースの認証

Duo Premier

保護を拡張し、クラウド、オンプレミス、プライベート アプリケーションやプライベートリソースに簡単にアクセスできます。

9 ドル | ユーザー | 月

- VPN を使用しない安全なリモートアクセス
- サードパーティ EDR エージェントチェック

シームレスな本人確認：**Persona** とのパートナーシップ


CISCO