

いますぐにできる Identity Security Duo Update /Duo Roadmap



平岡 龍弘
Identity Security担当 営業

坂川 健太
Identity Security担当 SE

免責事項

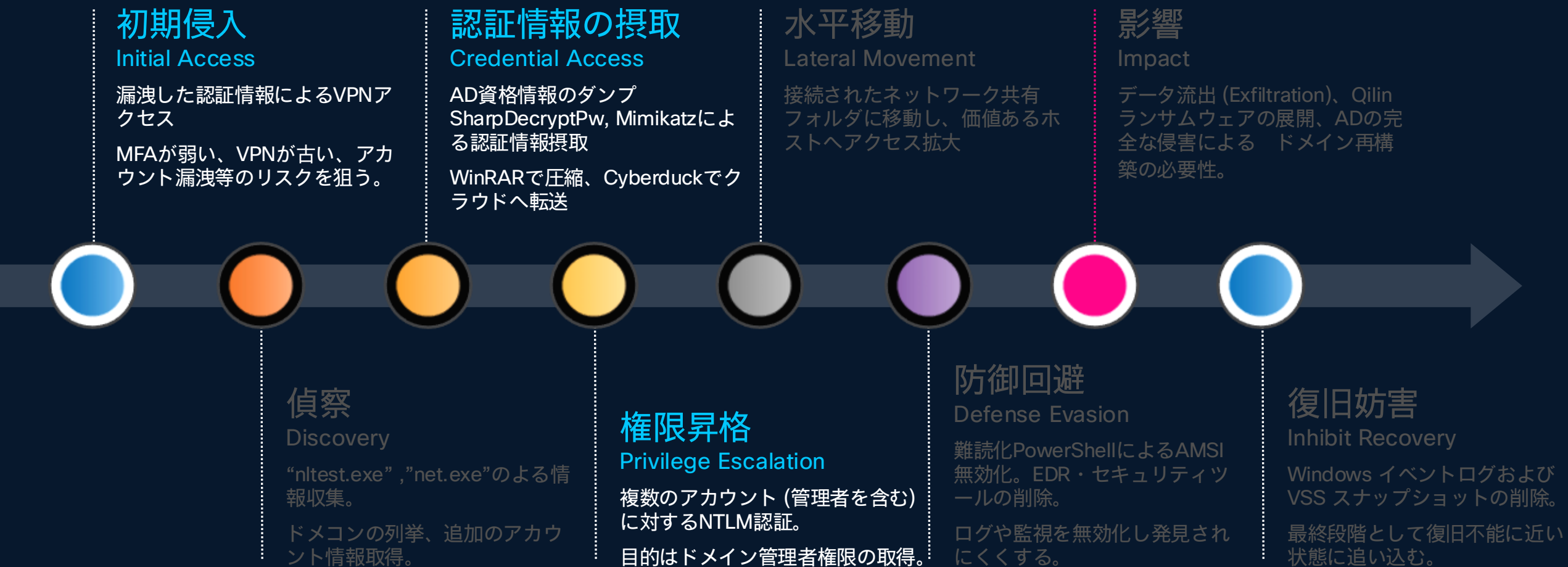
本日記載の内容はロードマップや開発段階のものが多く含まれます。

ロードマップはシスコの独断で変更されることがあり、シスコは本文書に記載された製品または機能の提供の遅延または提供の不履行について一切責任を負いません。

Cisco Duo

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



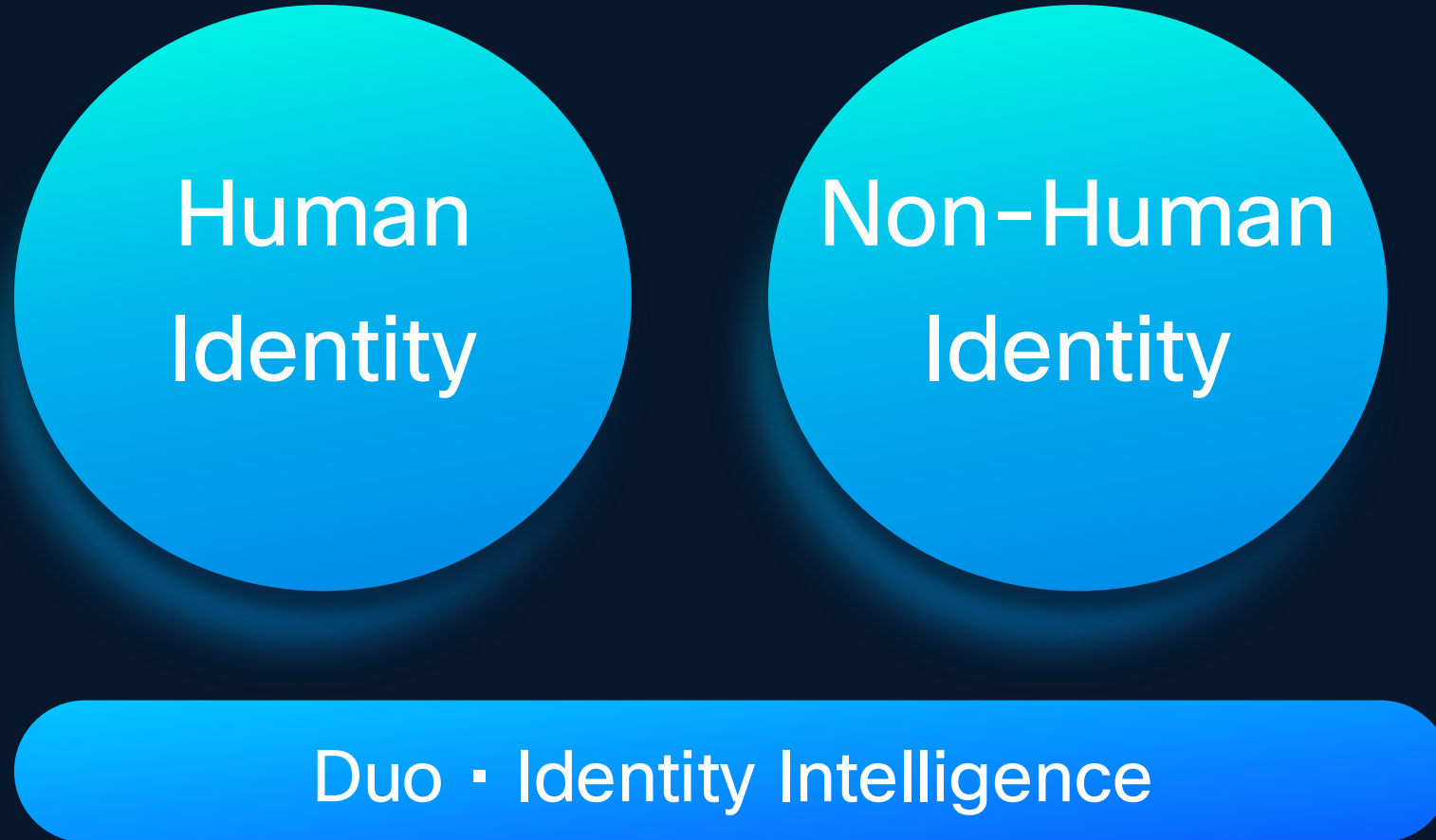


60
パーセント

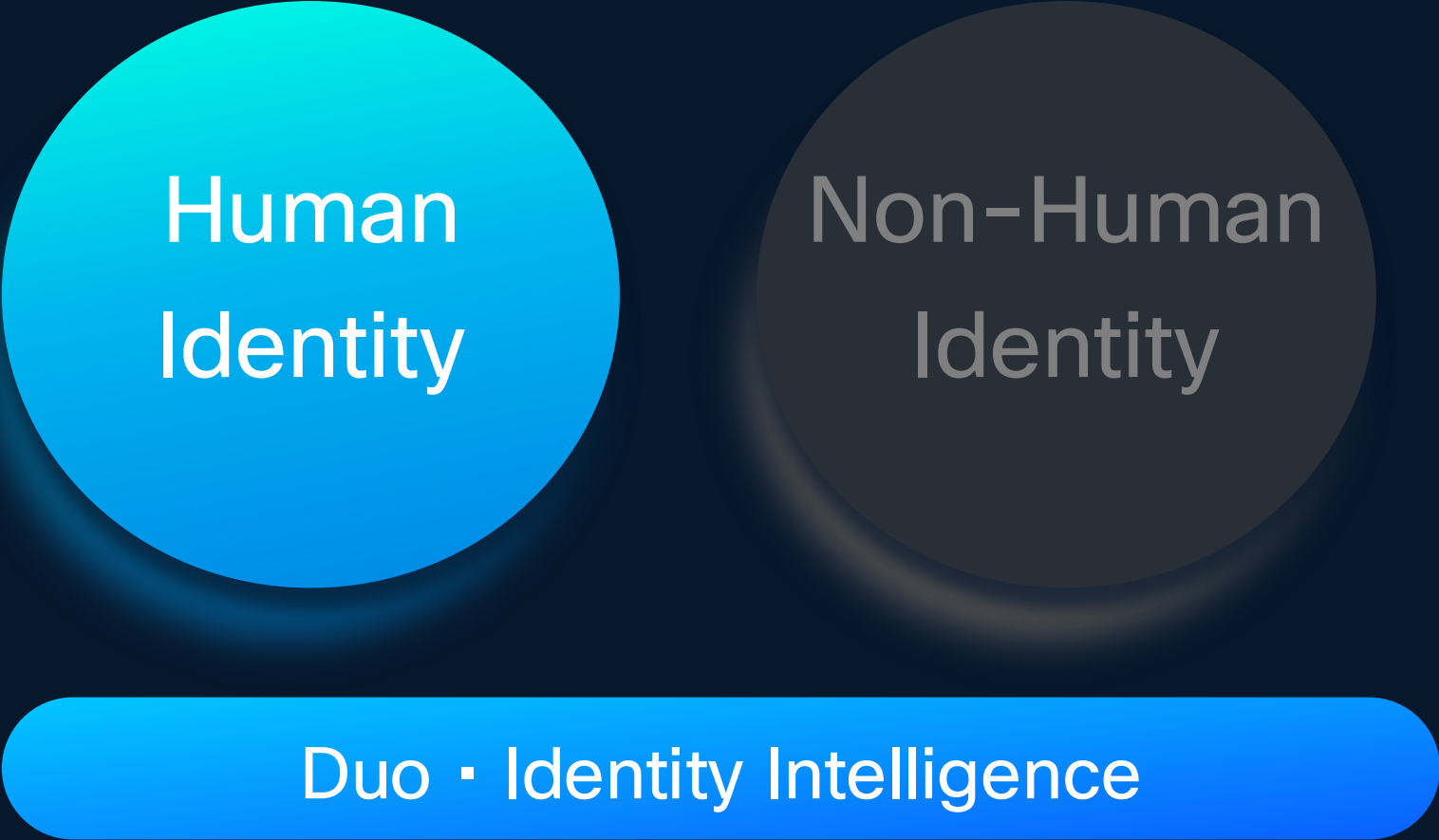
アイデンティティが重要な要素として利用された侵害の割合

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

Duoによる保護範囲



Duoによる保護範囲



Human
Identity

Non-Human
Identity

Duo - Identity Intelligence

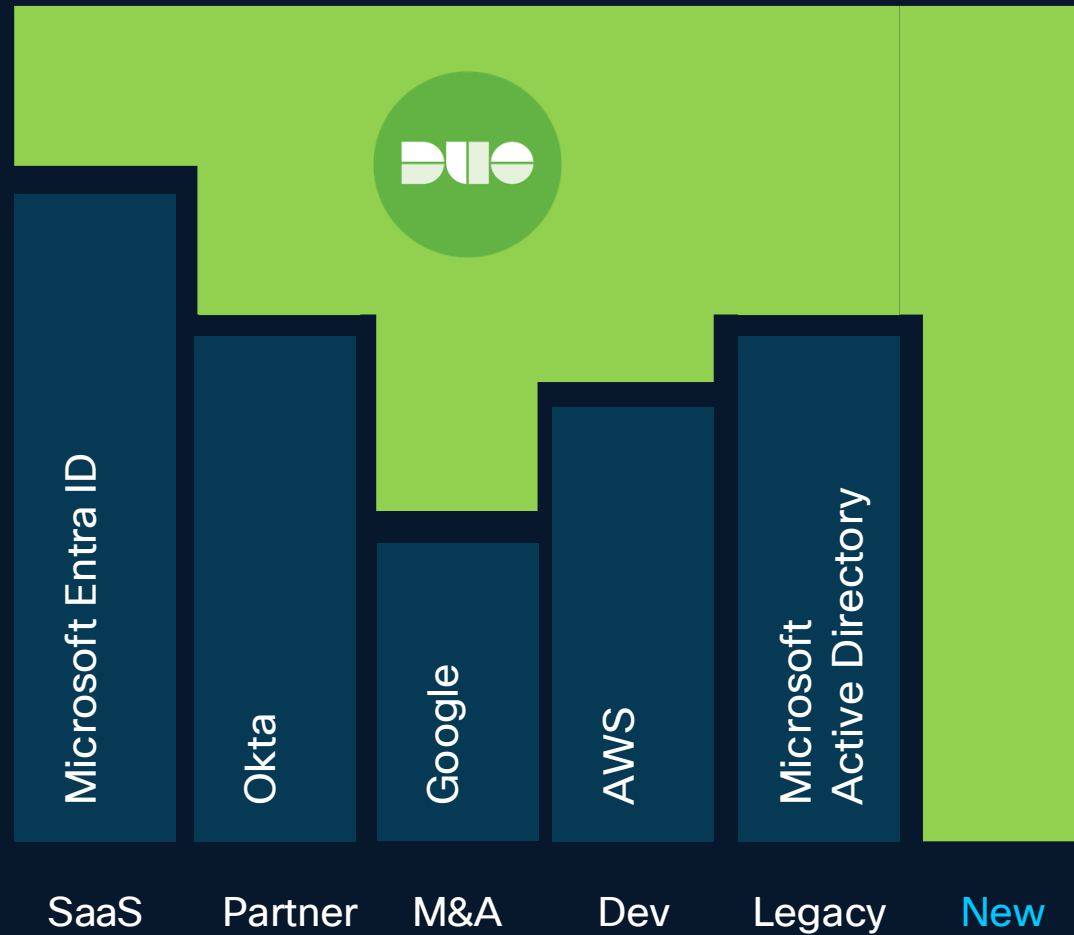
Duoによる Identity Security

高い安全性

低いコスト

シンプルさ

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

Gartnerのレポート



Gartner® Peer Insights™ 2026 Voice of the Customerのアクセスマネジメント領域で

Customers Choice に選出

<https://www.gartner.com/doc/reprints?id=1-2NADO242&ct=260501&st=sb>

Cisco Duoが選ばれる理由

アイデンティティへの攻撃を阻止するセキュリティファーストIAM

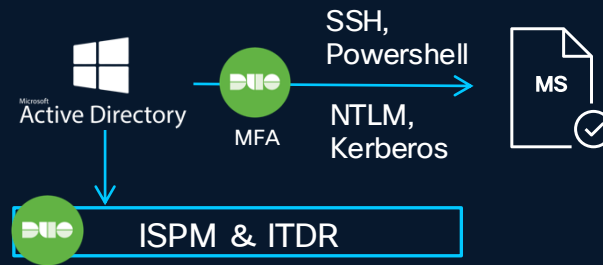
フィッシング対策MFA

組織に合わせた柔軟なMFA



Active Directory保護

Active Directoryを標的とした攻撃を阻止



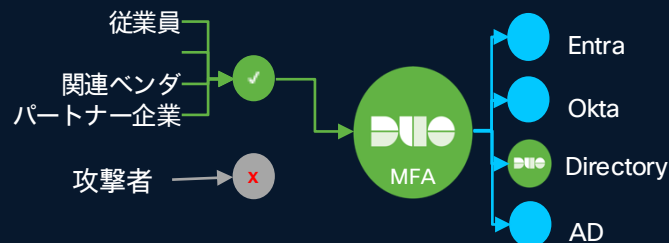
デバイスポスチャー

証明書に頼らない
安全なデバイスだけ認証を許可

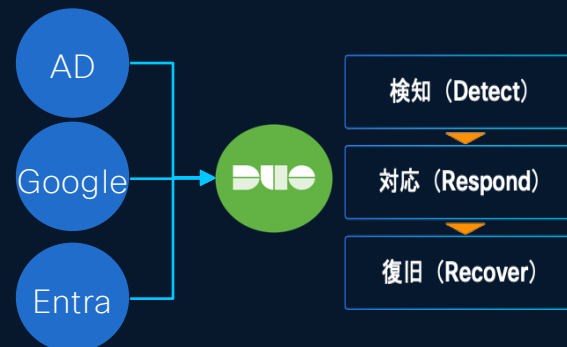


既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤



ISPM & ITDR



ISPM アイデンティティの健全性管理

MFA衛生管理
157
MFAが設定されていません

4
MFAが設定されていない、ログインしたことがないアカウント

MFA未適用、休眠ID、過剰特権アカウント

ITDR アイデンティティの振る舞い検知

98% 休眠アカウントからのアクセス
98% 不可能な移動

怪しい振る舞いのユーザーを即座に特定・隔離

Cisco Duoが選ばれる理由

アイデンティティへの攻撃を阻止するセキュリティファーストIAM

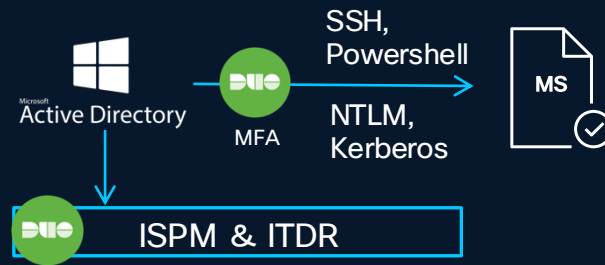
フィッシング対策MFA

組織に合わせた柔軟なMFA



Active Directory保護

Active Directoryを標的とした攻撃を阻止



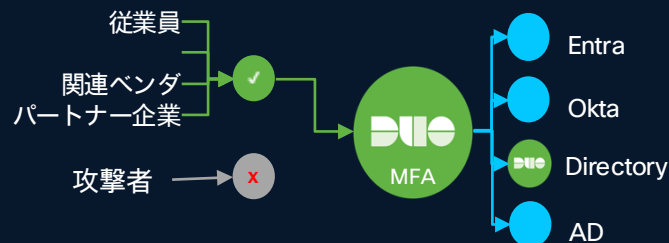
デバイスポスチャー

証明書に頼らない
安全なデバイスだけ認証を許可

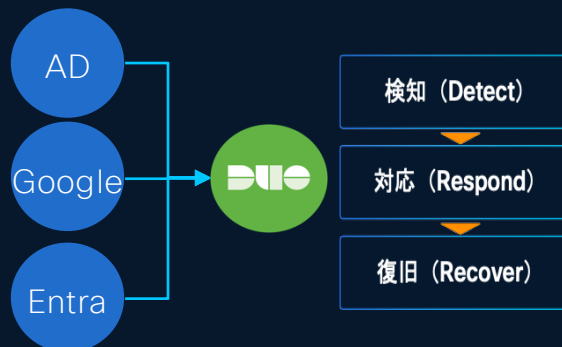


既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤



ISPM & ITDR



ISPM アイデンティティの健全性管理

MFA衛生管理

157

MFAが設定されていません

4

MFAが設定されていない、ログインしたことのないアカウント

MFA未適用、休眠ID、過剰特権アカウント

ITDR アイデンティティの振る舞い検知

98% 休眠アカウントからのアクセス 中程度

98% 不可能な移動 中程度

怪しい振る舞いのユーザーを即座に特定・隔離

AD Defense

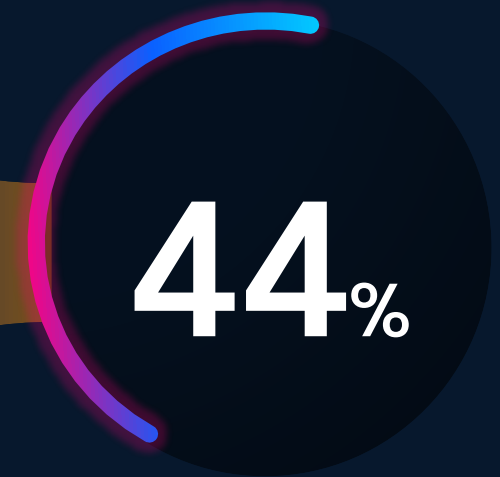
Active Directoryは 未だに大多数の企業で 使われている

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

ADが攻撃者の格好の標的になっている



Active Directoryを標的とした
アイデンティティへの攻撃

Cisco Talos Incident Response | Active Directory-based Attacks

事例：某大学のランサムウェア攻撃



約19万人

の個人情報が外部へ流出

実際に起きたこと

4月：フィッシングなど何らかの手段で、関係者のアカウント情報が窃取

IDを起点に学園内に侵入し、ランサムウェアで全6キャンパスに障害

認証情報 最大43,451件が暗号化、ポータル・公式サイト停止

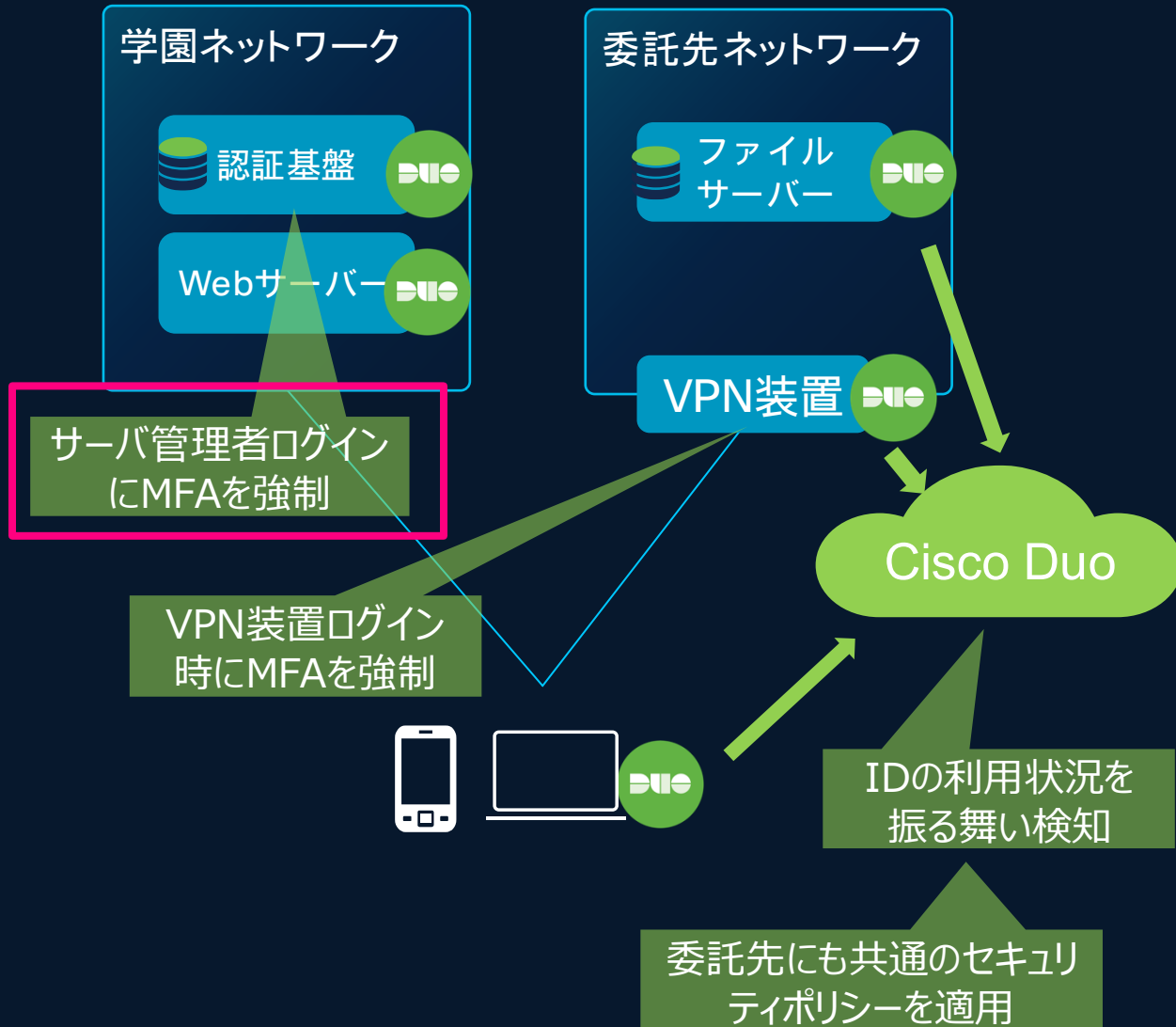
11月：今度は委託先サーバーが被害

リモート保守の入口から、窃取した管理者アカウントで侵入

教職員・学生・保護者のID/パスワード漏洩の恐れ

MFA未実装サービスを緊急停止、全員パスワード一括リセット

事例：某大学のランサムウェア攻撃

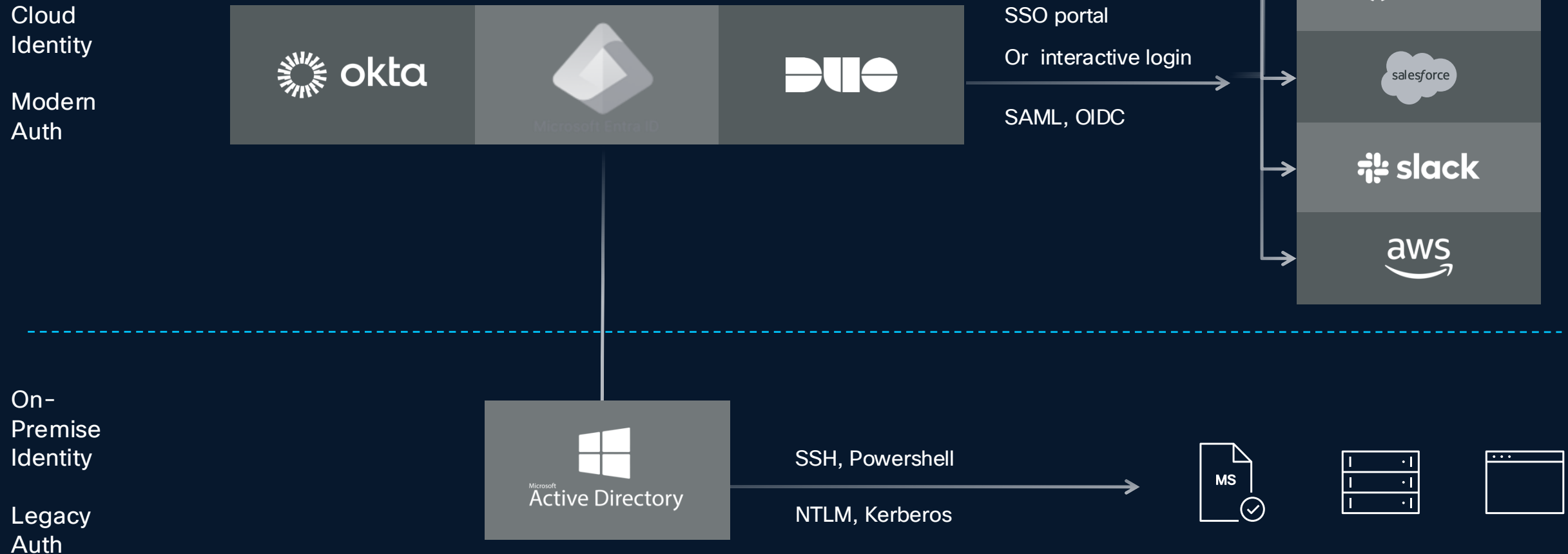


Duo導入の効果

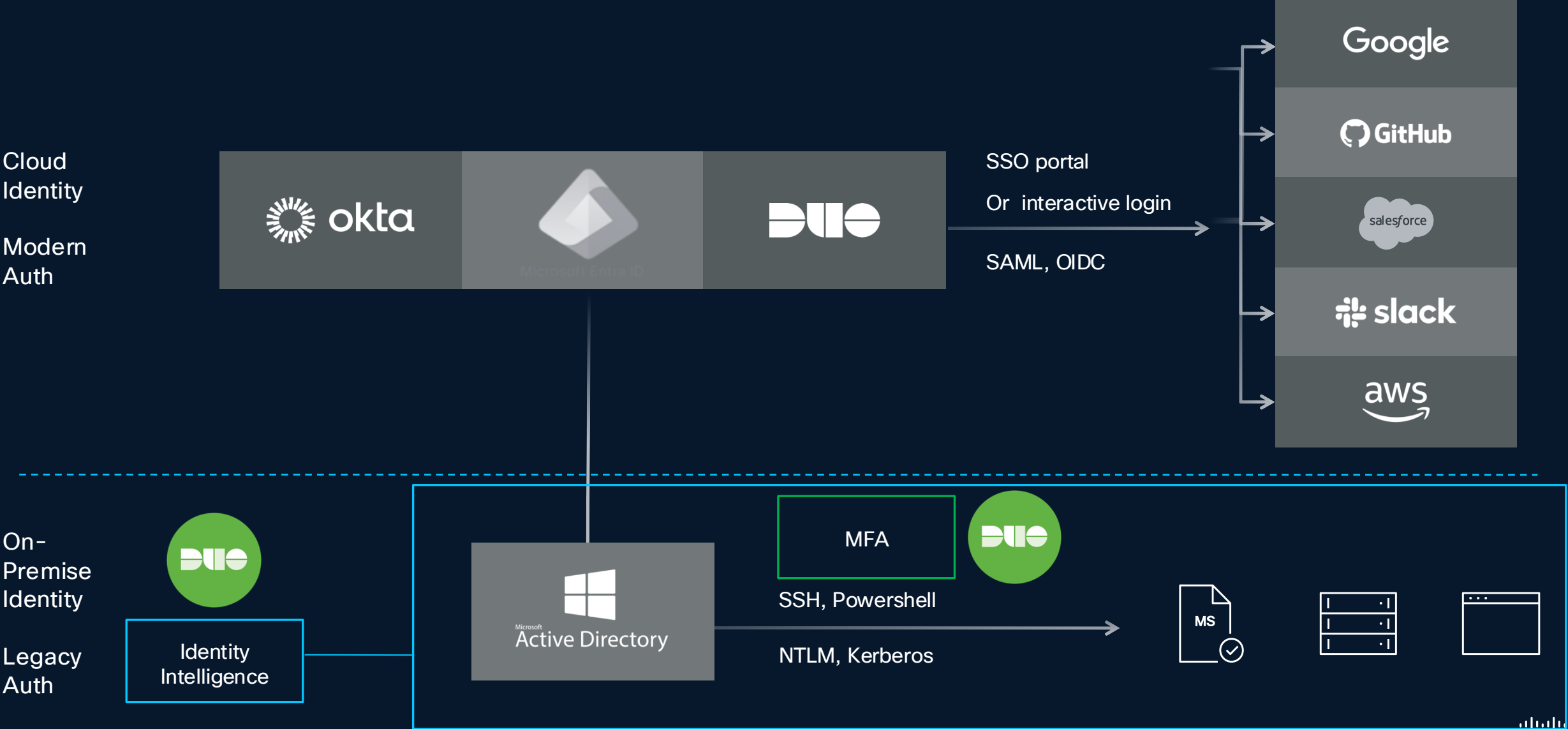
-  **全サービスにMFAを強制**
盗まれた認証情報だけでは侵入できない
-  **Trusted Endpointsで端末を検証**
未管理・不審な端末からの接続をブロック
-  **ISPM / ITDRで常時監視**
休眠アカウントや異常ログインを継続検知
-  **委託先も含めた共通のセキュリティポリシーを適用**
必要なアプリだけに最小権限でアクセス

共通のセキュリティポリシーでアイデンティティを保護

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



Demo

- AD Defense

Duo は、Windows と Active Directory のログインも守る

サインイン・権限昇格・リモート デスクトップ・ PowerShell・ ファイル共有の5場面

	守る入口	攻撃者が狙う場面	機能の名称	対応エディション
デモ 1	PC へのサインイン	盗んだパスワードで PC に入る	Duo Authentication for Windows Logon	全エディション
デモ 2	管理者権限への昇格	一般ユーザーから管理者権限を取る		
デモ 3	リモート デスクトップ	別の端末からサーバーに入る		
デモ 4	PowerShell リモート接続	画面なしで次のサーバーへ（横展開）	Duo Windows Command Line Protection	Advantage / Premier
デモ 5	ファイル共有	AD 認証を使う接続全般	Duo Legacy AD Protection	Advantage / Premier

手元・昇格・リモート・コマンド・AD を、同じ Duo Mobile の Push で守る

動画は、左が PC の画面、右がスマートフォン（Duo Mobile）の画面です

デモ 1 | PC へのサインインに MFA

見せること

Windows のサインイン画面でパスワードを入力すると、Duo の認証が始まります。

流れ

- 1 ユーザー名とパスワードでサインイン
 - 2 Duo の認証画面が表示される
 - 3 スマートフォンの Duo Mobile に届いた通知（Push）を承認
 - 4 デスクトップが開く
-

ポイント

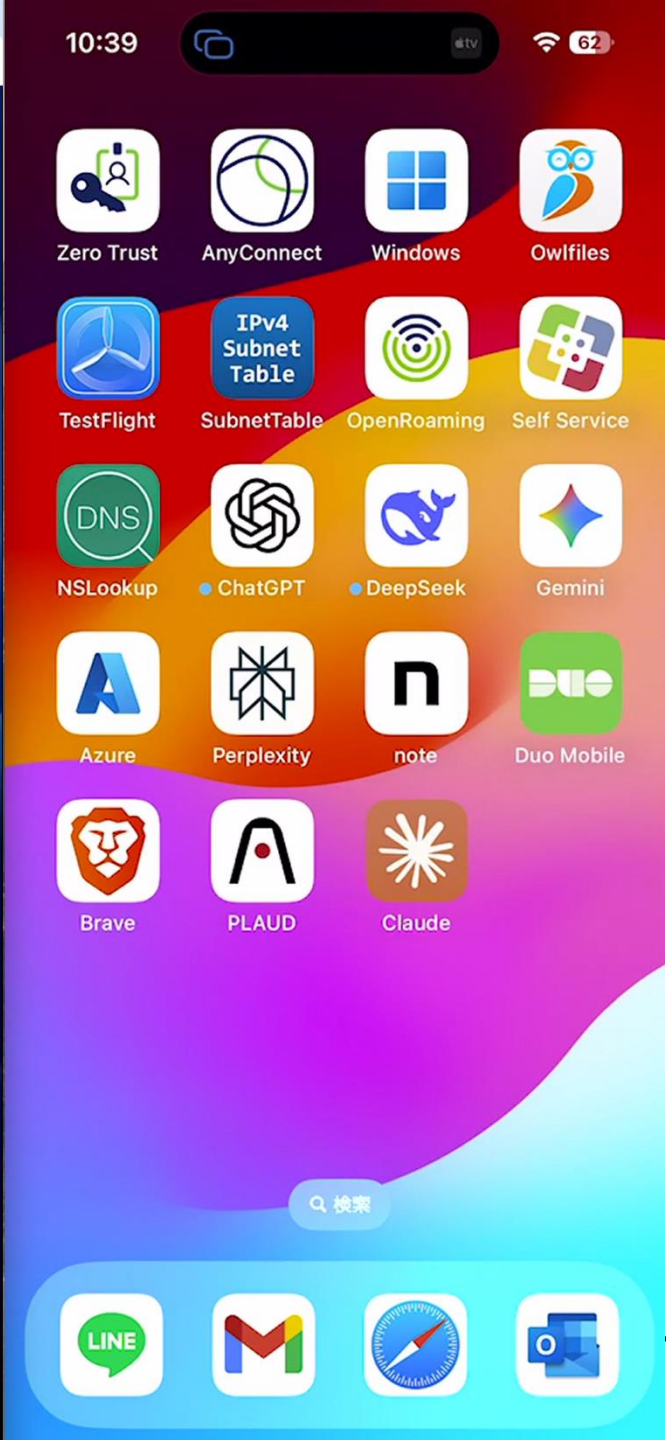
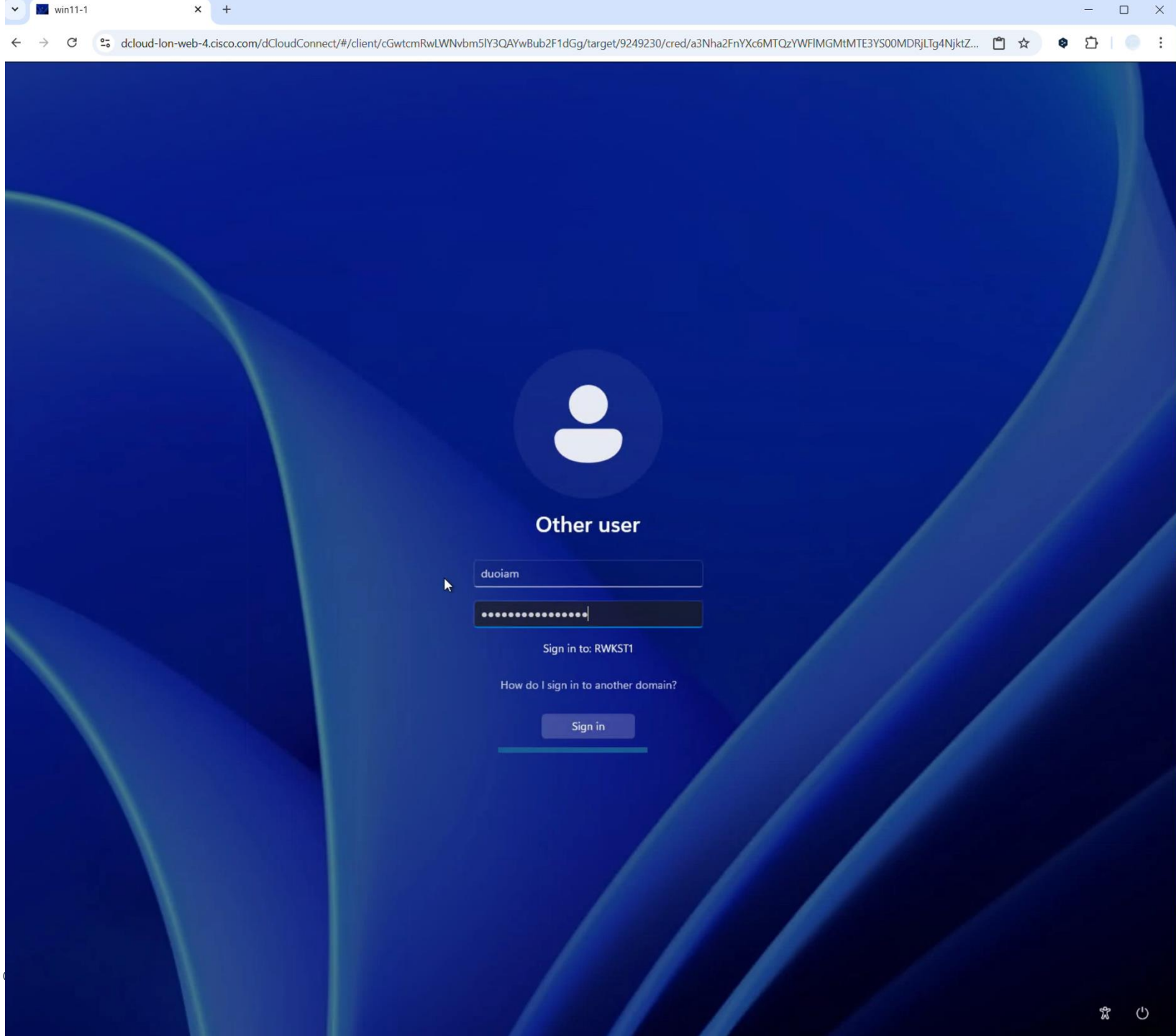
パスワードが漏れても、Push を承認しない限り PC は使えません。

デモする機能

Duo Authentication for Windows Logon

※ Push の画面には「RDP: Microsoft RDP」と表示されます。デモ 1～3 は同じアプリケーションのため、同じ名前になります。

※ 動画の左が PC、右がスマートフォン（Duo Mobile）の画面です。



デモ 2 | 管理者権限への昇格に MFA

見せること

サインイン済みの PC でも、UAC 昇格のときに Duo の認証がかかります。

流れ

- 1 コマンド プロンプトを「管理者として実行」
 - 2 UAC の画面で資格情報を入力
 - 3 Push を承認
 - 4 管理者としてコマンド プロンプトが起動
-

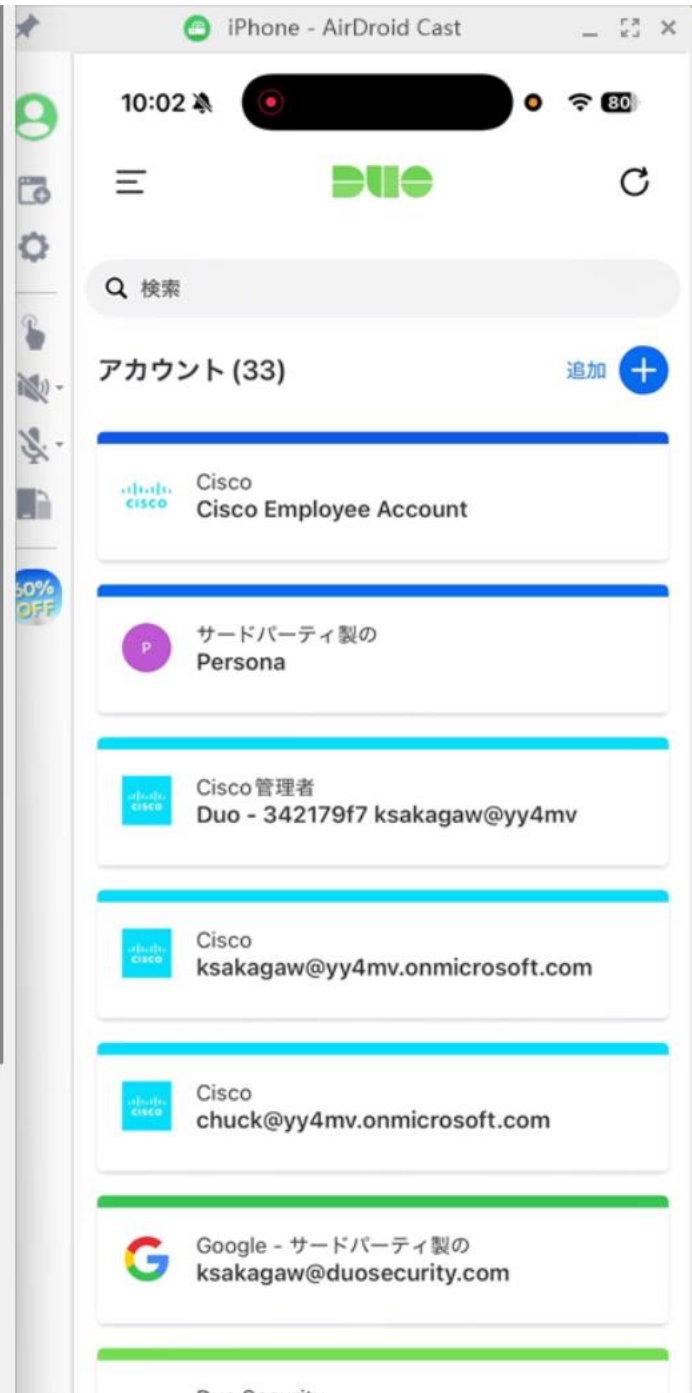
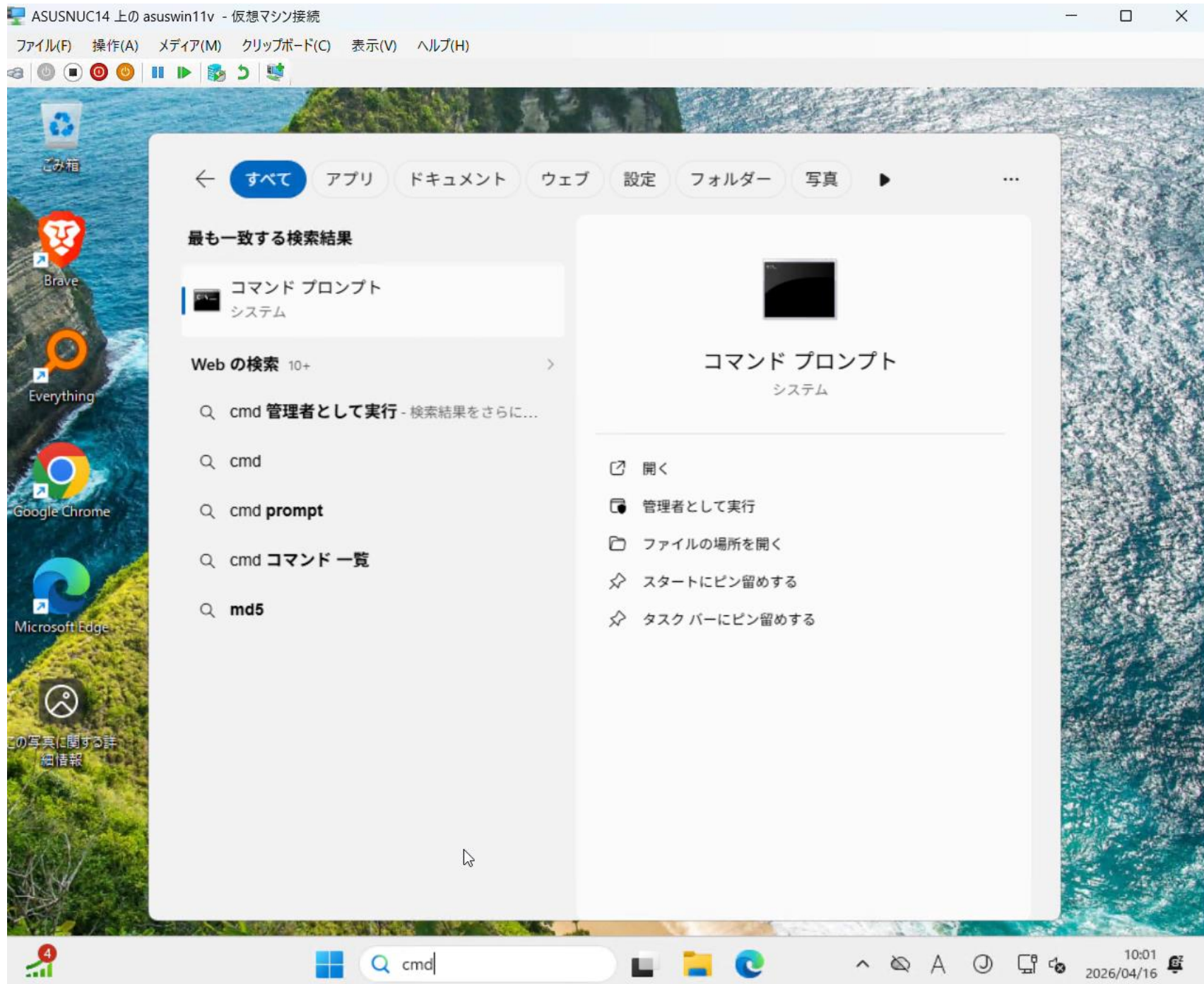
ポイント

サインイン済みでも、管理者権限を使う瞬間にもう一度本人確認します。

デモする機能

Duo Authentication for Windows Logon

※ Push の画面には「Elevation: Microsoft RDP」と表示されます（末尾の名称は伏せています）。デモ 1・3 と同じアプリケーションです。



デモ 3 | リモート デスクトップ接続に MFA

見せること

リモート デスクトップで接続すると、接続先で Duo の認証がかかります。

流れ

- 1 踏み台からリモート デスクトップで接続
 - 2 接続先に切り替わり、Duo の認証画面が表示される
 - 3 Push を承認
 - 4 接続先で `whoami`・`ipconfig`・`hostname` の結果を確認
-

ポイント

リモートからの入口も、手元の PC と同じ仕組みで守れます。

デモする機能

Duo Authentication for Windows Logon

※ Push の画面には「RDP: Microsoft RDP」と表示されます（デモ 1 と同じアプリケーション）。

Browser tabs: dCloud Session View, jumper

Address bar: dcloud-rtp-web-4.cisco.com/dCloudConnect/#/client/cGwtcmRwLWNvbm5lY3QAYwBub2F1dGg/target/16076499/cred/a3Nha2FnYXc6NWVkm...

Desktop background: Windows 10 blue wallpaper

Desktop icons:

- This PC
- Network
- DbVisualizer 23.2.3
- Google Chrome
- Demo Ready
- Putty
- Tftpd64

Remote Desktop Connection dialog box:

Computer: 198.18.133.11

User name: duoiam

You will be asked for credentials when you connect.

Buttons: Show Options, Connect, Help

Taskbar:

Type here to search

System tray: 4:59 PM, 8/15/2025

Mobile home screen with app icons:

- Zero Trust
- AnyConnect
- Windows
- Owlfiles
- TestFlight
- SubnetTable
- OpenRoaming
- Self Service
- DNS
- NSLookup
- ChatGPT
- DeepSeek
- Gemini
- Azure
- Perplexity
- note
- Brave
- PLAUD
- Claude
- Duo Mobile

Bottom dock:

- LINE
- Gmail
- Compass
- Teams

Top status bar: 0:59, signal strength, 35% battery

デモ 4 | コマンドラインのリモート接続に MFA

見せること

Enter-PSSession によるリモート接続は、攻撃者が横展開に使う経路です。ここでも Push の承認が必要です。

流れ

- 1 Enter-PSSession でリモート接続
 - 2 資格情報を入力
 - 3 「Pushed a login request」と表示され、Push を承認
 - 4 認証成功の表示の後、whoami / hostname で接続先を確認
-

ポイント

Windows Logon では守れない「画面のない接続」を、この製品で守ります。

デモする機能

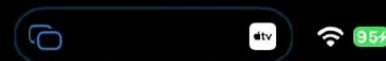
Duo Windows Command Line Protection Advantage / Premier

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

```
PS C:\WINDOWS\system32> whoami  
cisco\ksakagaw  
PS C:\WINDOWS\system32>  
PS C:\WINDOWS\system32> hostname
```

```
PS C:\WINDOWS\system32>  
PS C:\WINDOWS\system32>
```

20:43



検索

アカウント (40)

追加



Cisco
Cisco Employee Account



サードパーティ製の
Persona



Cisco 管理者
Duo - 342179f7 ksakagaw@yy4mv



Cisco
ksakagaw@yy4mv.onmicrosoft.com



Cisco
chuck@yy4mv.onmicrosoft.com



Amazon Web Services - サードパーティ製の
AWS_Authapp@730406060103



Google - サードパーティ製の

デモ 5 | Active Directory の認証に MFA

見せること

共有フォルダーを開くときの Active Directory 認証で、Duo の Push が届きます。

流れ

- 1 共有フォルダーを開く
 - 2 資格情報を入力（Windows セキュリティの画面）
 - 3 Push（Legacy AD Authentications）を承認
 - 4 フォルダーが開く
-

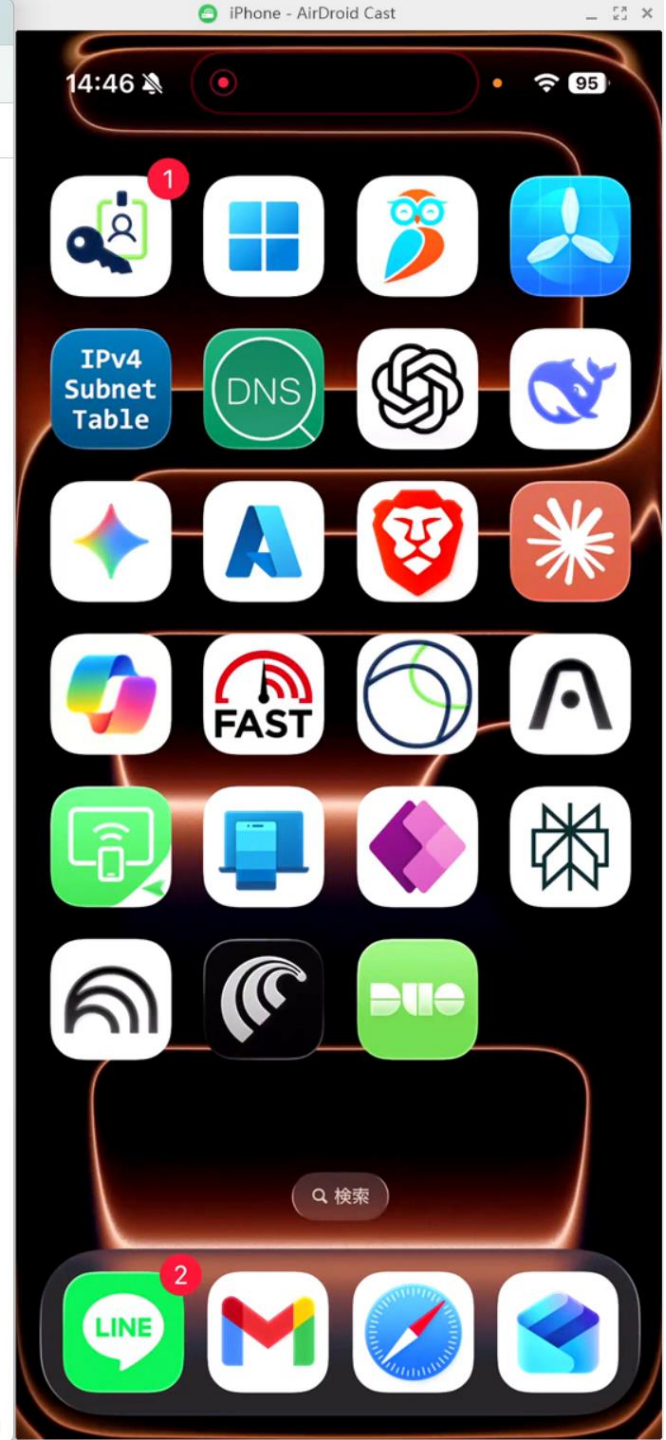
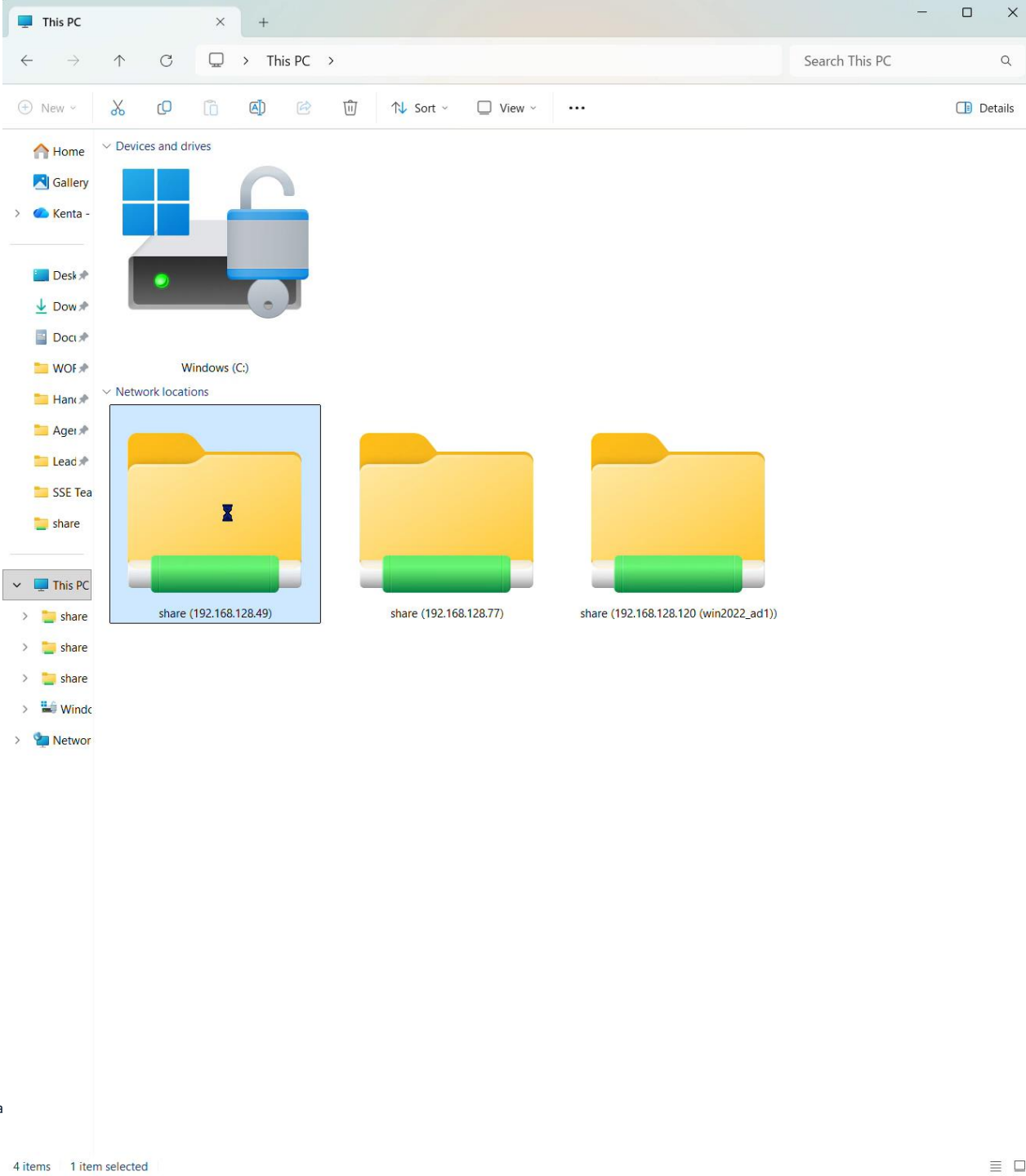
ポイント

Active Directory の認証（Kerberos / NTLM）そのものに MFA をかけます。

デモする機能

Duo Legacy AD Protection Advantage / Premier

※ Push に表示される接続元の端末名は伏せています。



Identity Intelligence

Cisco Duoが選ばれる理由

アイデンティティへの攻撃を阻止するセキュリティファーストIAM

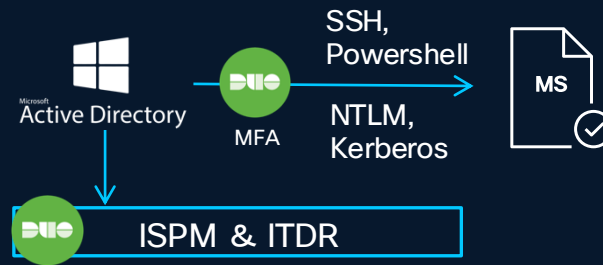
フィッシング対策MFA

組織に合わせた柔軟なMFA



Active Directory保護

Active Directoryを標的とした攻撃を阻止



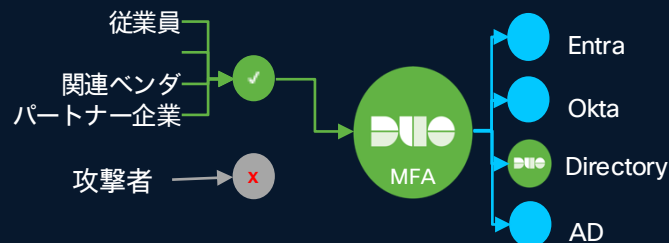
デバイスポスチャー

証明書に頼らない
安全なデバイスだけ認証を許可

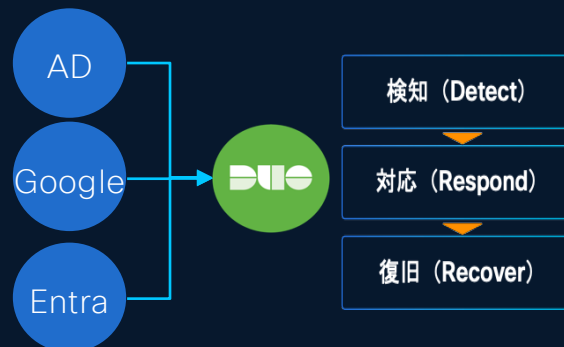


既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤



ISPM & ITDR



ISPM アイデンティティの健全性管理

MFA衛生管理
157
MFAが設定されていません

4
MFAが設定されていない、ログインしたことのないアカウント

MFA未適用、休眠ID、過剰特権アカウント

ITDR アイデンティティの振る舞い検知

98% 休眠アカウントからのアクセス
98% 不可能な移動

怪しい振る舞いのユーザーを即座に特定・隔離

そもそも何か？

- **ISPM (Identity Security Posture Management)**
 - ✓ 組織全体のアイデンティティに関するセキュリティ上の弱点を継続的に評価・改善するアプローチ
- **ITDR (Identity Threat Detection and Response)**
 - ✓ 認証情報の窃取、権限昇格、横移動など、アイデンティティを標的にした脅威を検出・対応するフレームワーク

観点	ISPM（予防）	ITDR（検知・対応）
目的	弱点の事前発見・修正	リアルタイム脅威の検知とアクション
アプローチ	継続的なポスチャ評価	行動分析・異常検知
例	MFA設定不備、休眠アカウント、等	MFA洪水攻撃、セッションハイジャック、等
タイミング	攻撃前（プロアクティブ）	攻撃中・後（リアクティブ）

IDが見えないことによるリスク

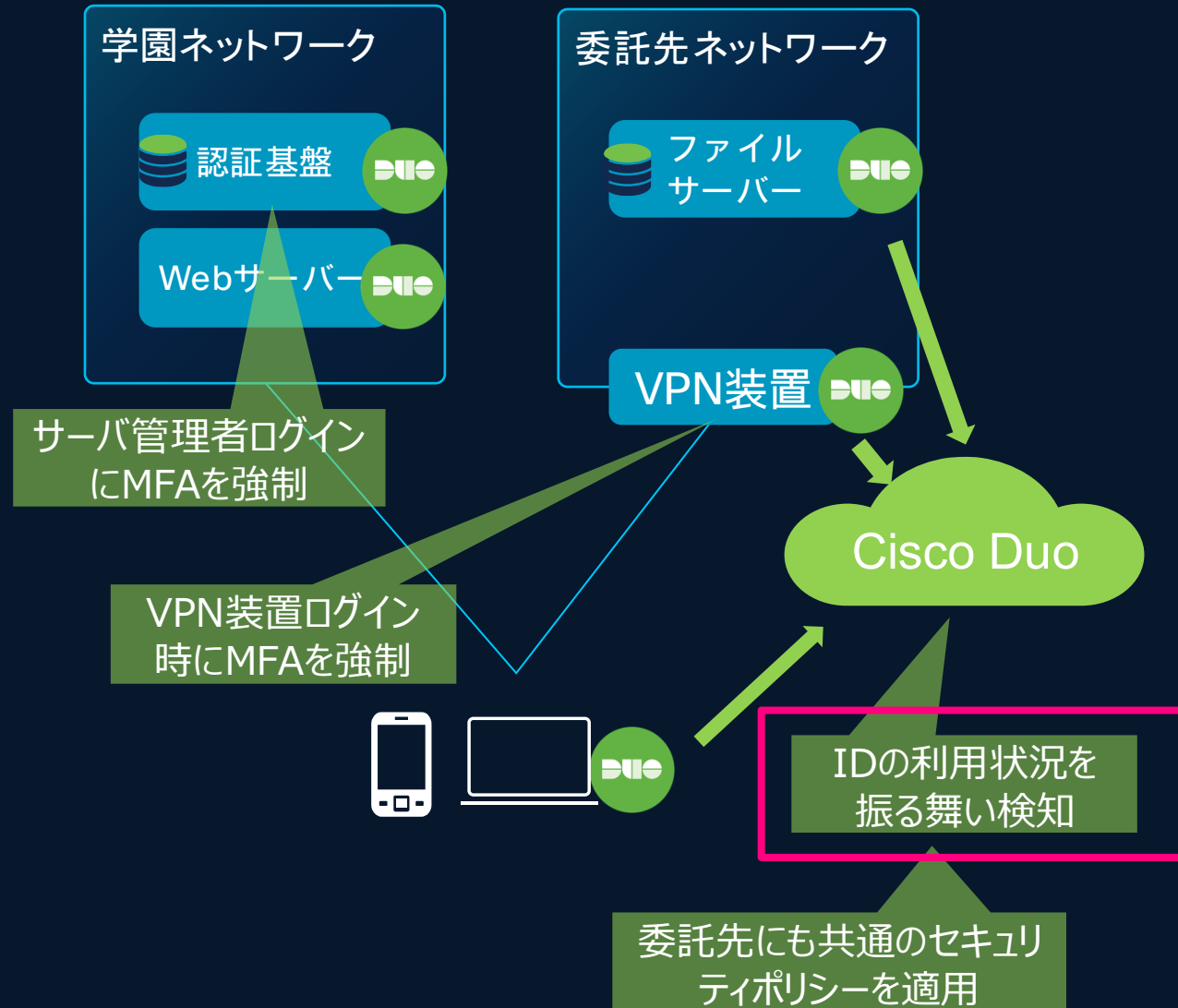
休眠アカウントによる
不正アクセス

コンプライアンスと
監査対応

AIによる
Non Human Identityの追跡

MFAのポリシー外設定

事例：某大学のランサムウェア攻撃

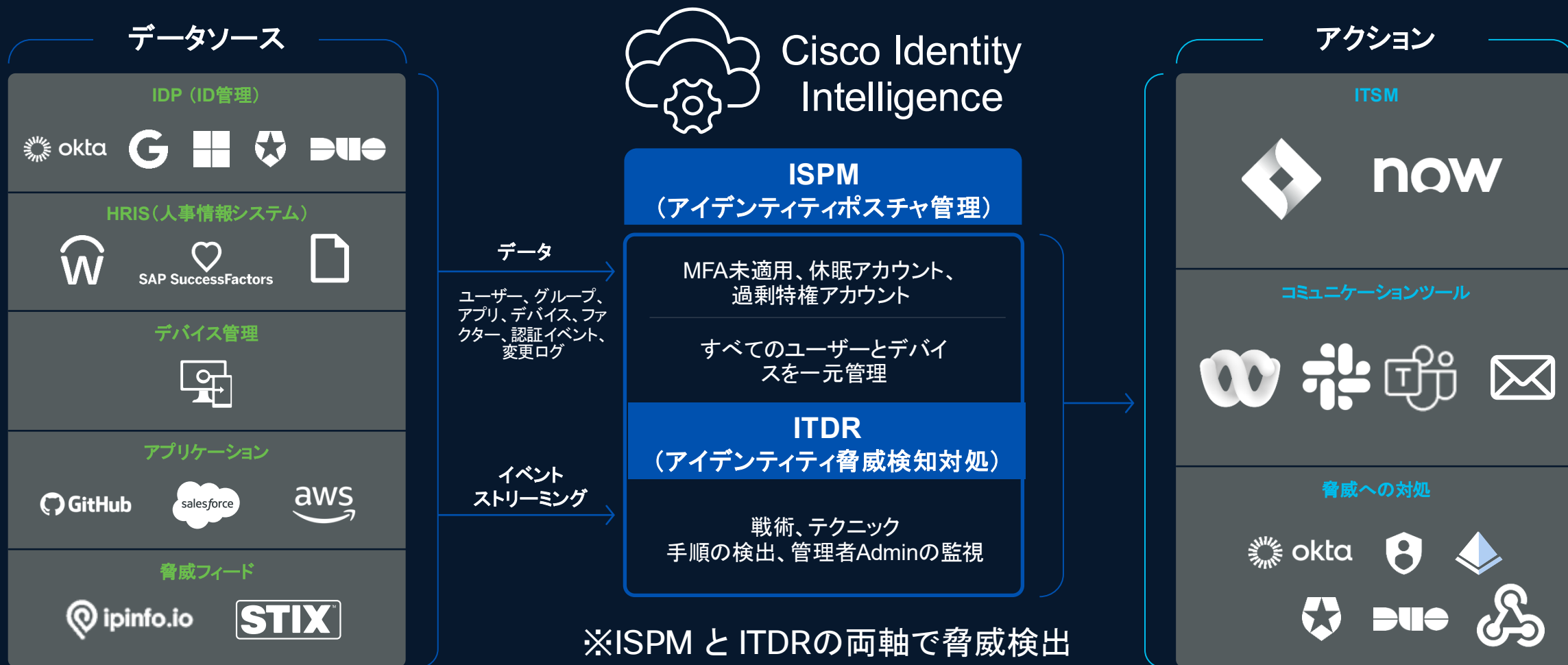


Duo導入の効果

-  **全サービスにMFAを強制**
盗まれた認証情報だけでは侵入できない
-  **Trusted Endpointsで端末を検証**
未管理・不審な端末からの接続をブロック
-  **ISPM / ITDRで常時監視**
休眠アカウントや異常ログインを継続検知
-  **委託先も含めた共通のセキュリティポリシーを適用**
必要なアプリだけに最小権限でアクセス

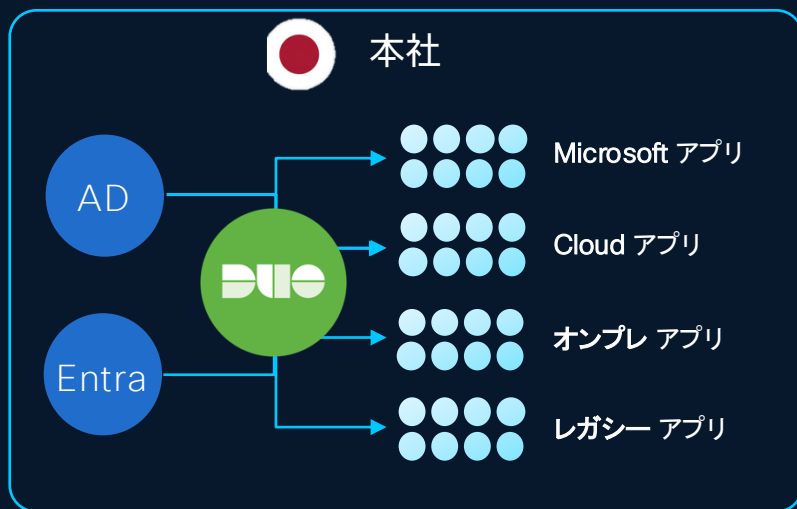
共通のセキュリティポリシーでアイデンティティを保護

IDの 可視化→ポスチャ→脅威検出→対応を - One Platform - で実現

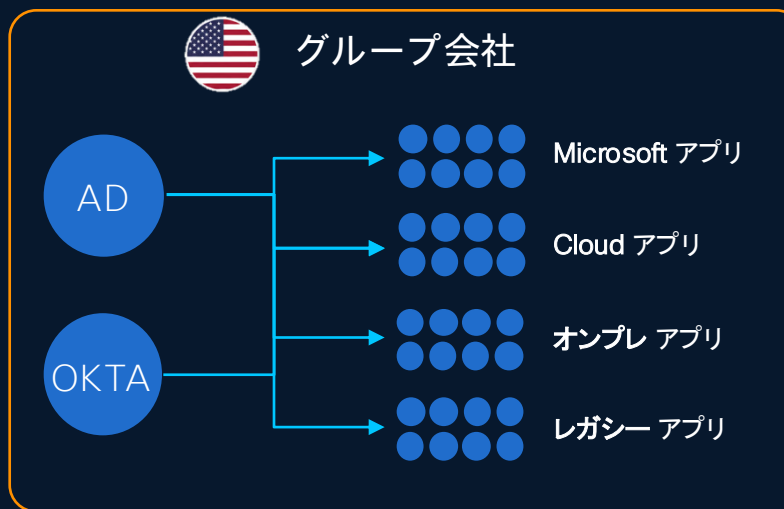


Use Case: 複数環境のID振る舞い分析

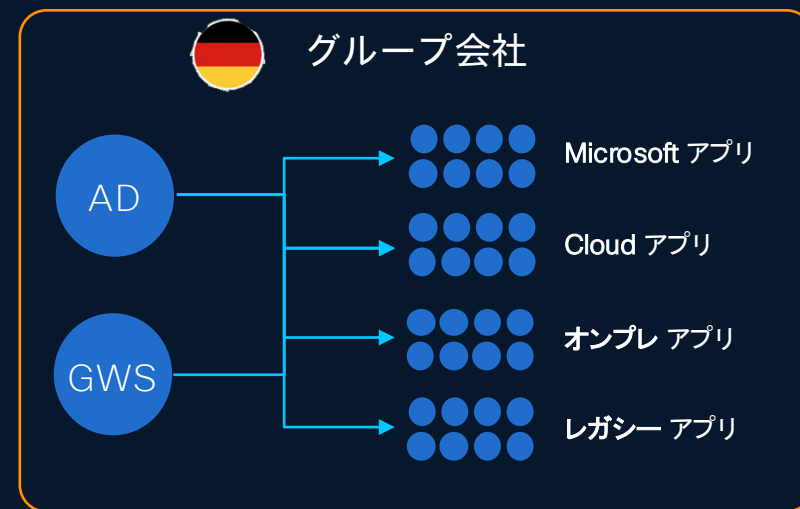
課題: 海外拠点を含めた**ID環境の可視化が困難**で統合管理ができない



全て可視化可能



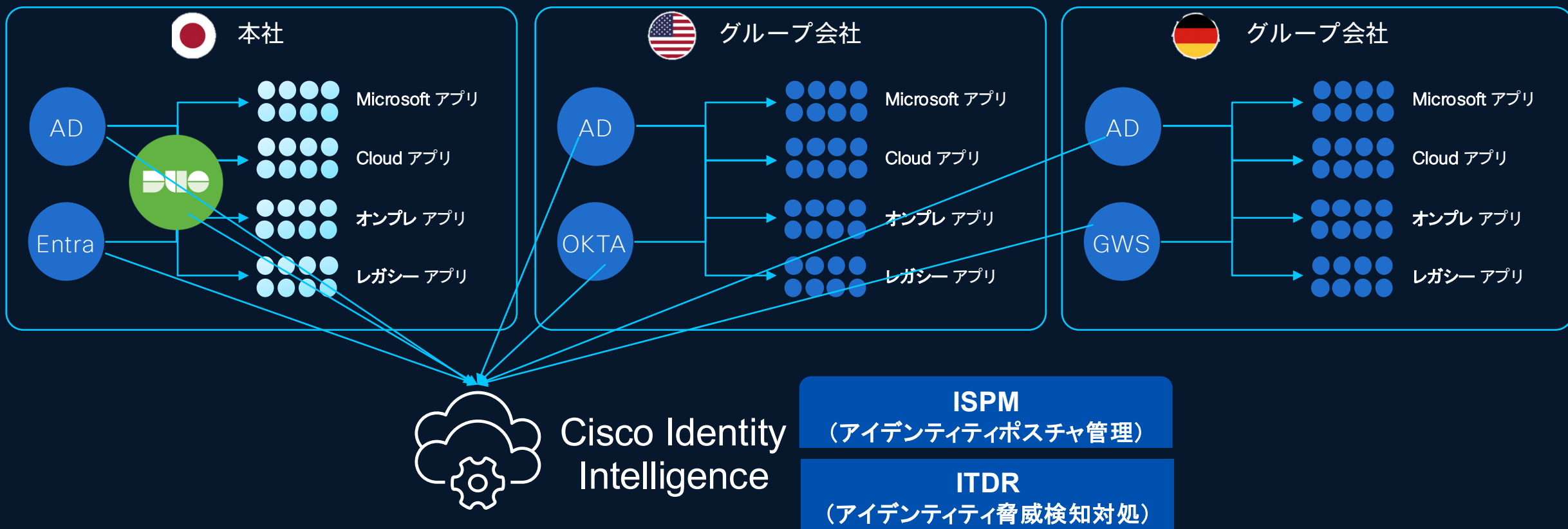
一部日本のユーザも登録される
も**可視化不可**



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



Duoによる保護範囲

Human
Identity

Non-Human
Identity

Duo - Identity Intelligence

Demo

- Cisco Identity Intelligence (CII)

CII は、ID のリスクを 3 つの観点で確認できる

Entra ID ・ Okta ・ Duo などに分散した ID 情報を、API 連携で横断して可視化

見えること		使う画面
観点 1	危険なユーザーの特定 Trust Level の低いユーザーと、その理由	Threats → User 360
観点 2	管理者のログイン状況 管理者の数と、直近のログイン元・場所	Identities / Threats
観点 3	組織の弱点と改善の優先順位 組織のスコア、優先して直す項目、MFA の利用状況	Overview / MFA

危険なユーザー ・ 管理者 ・ 組織の弱点を、同じ Cisco Identity Intelligence で確認する

サービスアカウントや AI エージェントなど、人以外のアイデンティティは、後続の Astrix セッションで扱います



Overview ▾

Configure



Download PDF Report

Dashboard

Users

Applications

Devices

Non-Human Identities

Campaigns

Checks

Reports

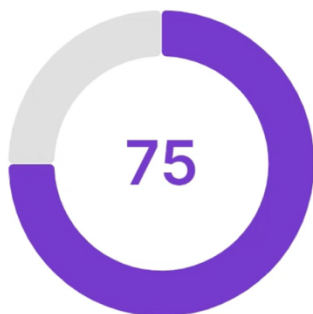
Integrations

ISE Monitoring

System Logs

Tenant Settings >

Organization Posture Score ⓘ



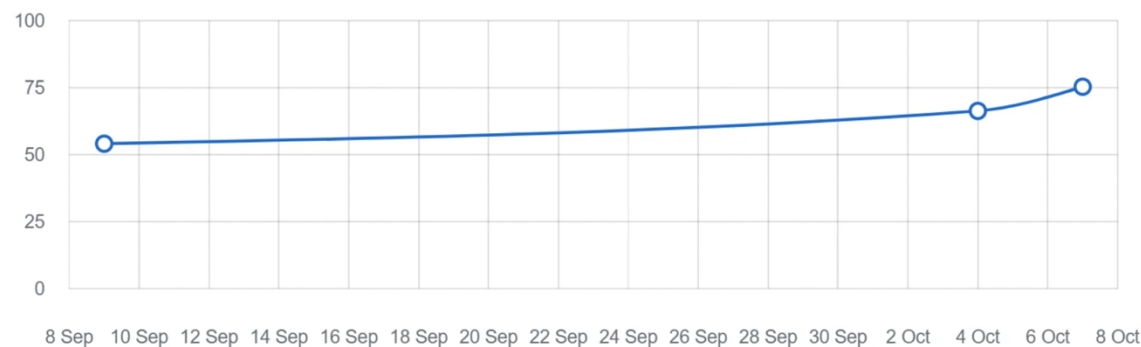
Neutral

↗ +21 (29 days)

⚠ Your posture score falls within the lowest 20th percentile for similarly sized organizations.

Posture score trend

30d Sep 08, 2026 12:59 - Oct 08, 2026 12:59 UTC ▾



Top Recommendations

Human Identities



Recommendation:
Review AD accounts with password or account issues and

Non-Human Identities



Recommendation:
Assign owners to non-human identities without an

CII は、ID のリスクを 3 つの観点で確認できる

Entra ID ・ Okta ・ Duo などに分散した ID 情報を、API 連携で横断して可視化

見えること		使う画面	
観点 1	危険なユーザーの特定	Trust Level の低いユーザーと、その理由	Threats → User 360
観点 2	管理者のログイン状況	管理者の数と、直近のログイン元・場所	Identities / Threats
観点 3	組織の弱点と改善の優先順位	組織のスコア、優先して直す項目、MFA の利用状況	Overview / MFA

危険なユーザー ・ 管理者 ・ 組織の弱点を、同じ Cisco Identity Intelligence で確認する

サービスアカウントや AI エージェントなど、人以外のアイデンティティは、後続の Astrix セッションで扱います



Overview ▼

[Configure](#)[Download PDF Report](#)

Dashboard



Users



Applications



Devices



Non-Human Identities



Campaigns



Checks



Reports



Integrations



ISE Monitoring

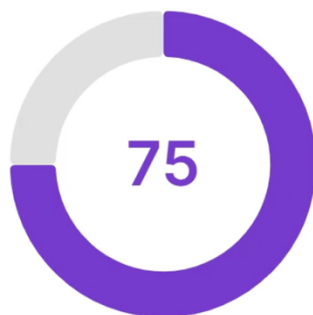


System Logs



Tenant Settings >

Organization Posture Score ⓘ



Neutral

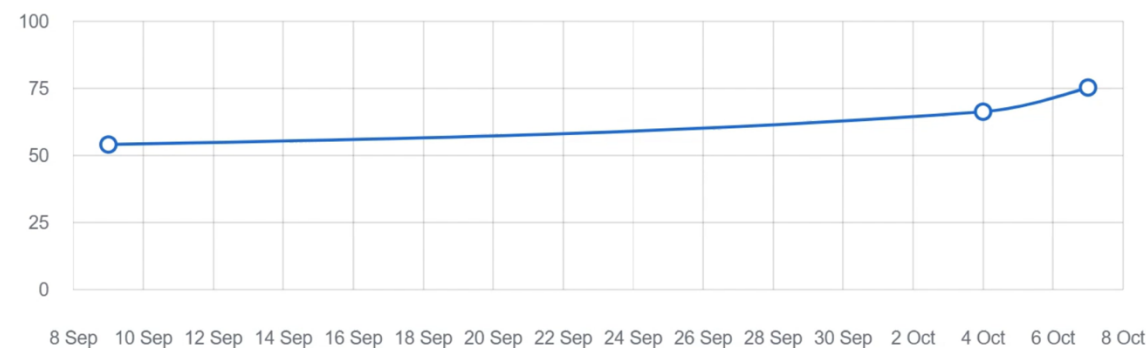
~ +21 (29 days)



Your posture score falls within the lowest 20th percentile for similarly sized organizations.

Posture score trend

30d Sep 08, 2026 13:08 - Oct 08, 2026 13:08 UTC ▼



Top Recommendations

Human Identities



Recommendation:
Review AD accounts with password or account issues and

Non-Human Identities



Recommendation:
Assign owners to non-human identities without an

CII は、ID のリスクを 3 つの観点で確認できる

Entra ID ・ Okta ・ Duo などに分散した ID 情報を、API 連携で横断して可視化

見えること		使う画面	
観点 1	危険なユーザーの特定	Trust Level の低いユーザーと、その理由	Threats → User 360
観点 2	管理者のログイン状況	管理者の数と、直近のログイン元・場所	Identities / Threats
観点 3	組織の弱点と改善の優先順位	組織のスコア、優先して直す項目、MFA の利用状況	Overview / MFA

危険なユーザー ・ 管理者 ・ 組織の弱点を、同じ Cisco Identity Intelligence で確認する

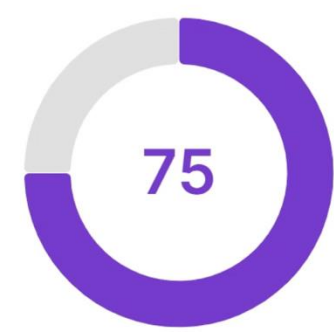
サービスアカウントや AI エージェントなど、人以外のアイデンティティは、後続の Astrix セッションで扱います

 Overview ▾

 Configure   Download PDF Report

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

Organization Posture Score



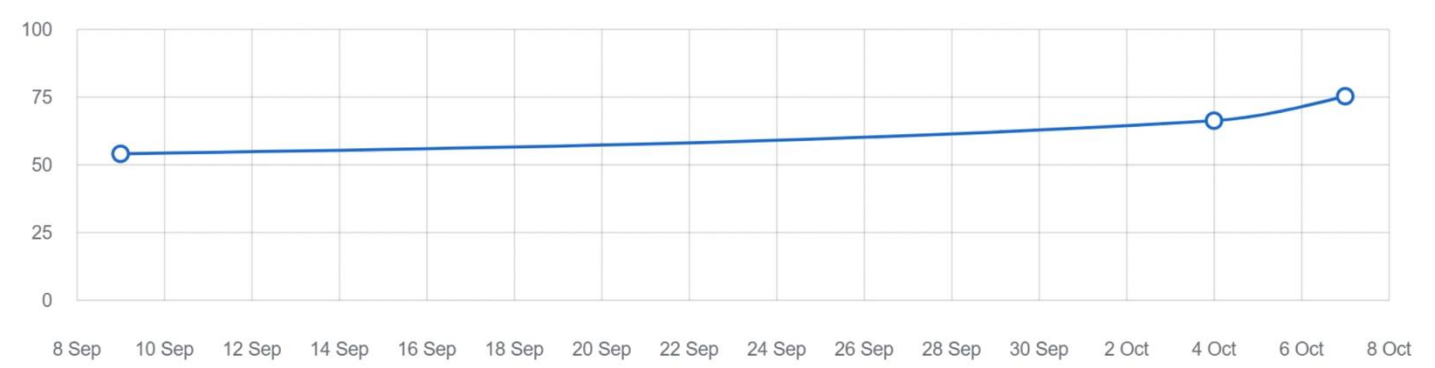
Neutral

↗ +21 (29 days)

 Your posture score falls within the lowest 20th percentile for similarly sized organizations.

Posture score trend

30d Sep 08, 2026 14:40 - Oct 08, 2026 14:40 UTC ▾



Top Recommendations

Human Identities



Recommendation:
Review AD accounts with password or account issues and remediate as needed

Non-Human Identities



Recommendation:
Assign owners to non-human identities without an accountable owner

CII は、ID のリスクを 3 つの観点で確認できる

Entra ID ・ Okta ・ Duo などに分散した ID 情報を、API 連携で横断して可視化

	見えること	使う画面
観点 1 危険なユーザーの特定	Trust Level の低いユーザーと、その理由	Threats → User 360
観点 2 管理者のログイン状況	管理者の数と、直近のログイン元・場所	Identities / Threats
観点 3 組織の弱点と改善の優先順位	組織のスコア、優先して直す項目、MFA の利用状況	Overview / MFA

危険なユーザー ・ 管理者 ・ 組織の弱点を、同じ Cisco Identity Intelligence で確認する

サービスアカウントや AI エージェントなど、人以外のアイデンティティは、後続の Astrix セッションで扱います

Identityの設定チェック

- Identityの設定状況がスコアに反映
- 推奨される対応を実行して徐々にスコアを向上
- 主要なインサイト：
 - MFA の適用範囲、弱いMFAの使用有無
 - 禁止している地域からのアクセス
 - 非アクティブユーザー
- 主なメリット：
 - 休眠アカウントを排除
 - MFA のギャップを強調
 - 過剰な管理者権限を削減



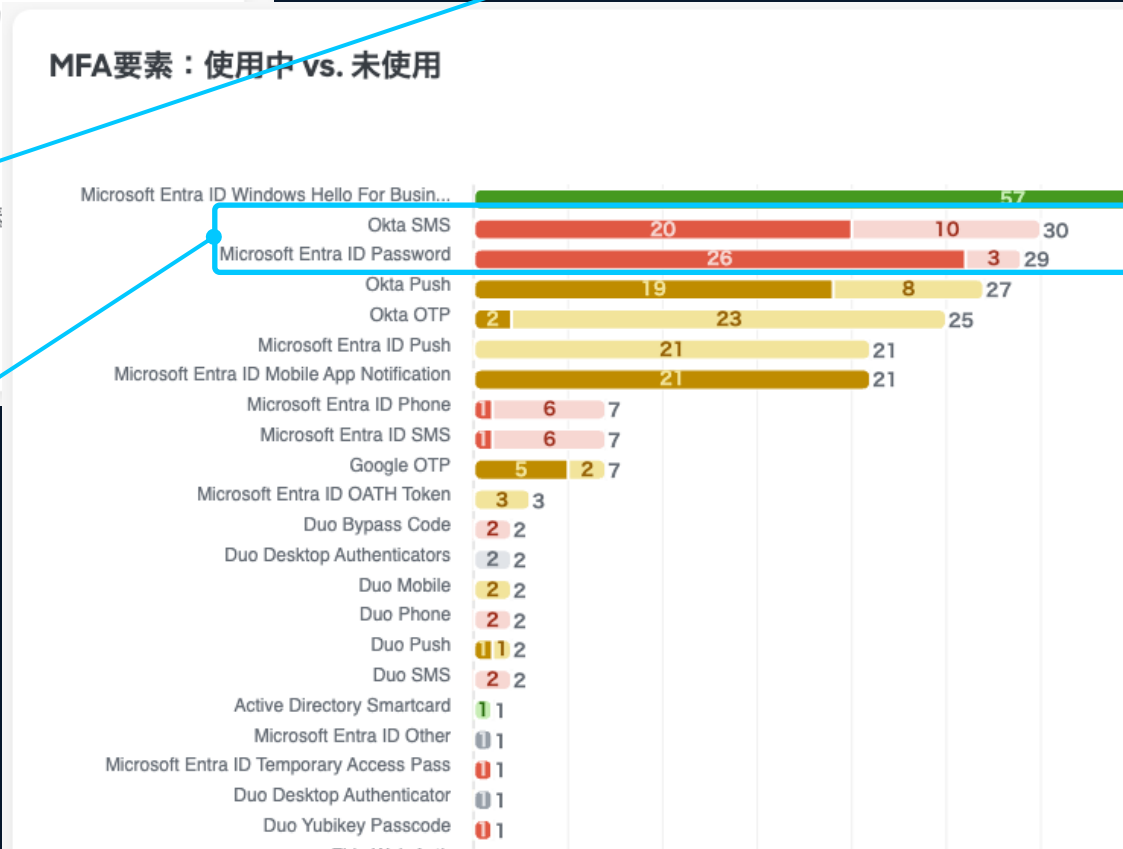
MFA の適用範囲



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

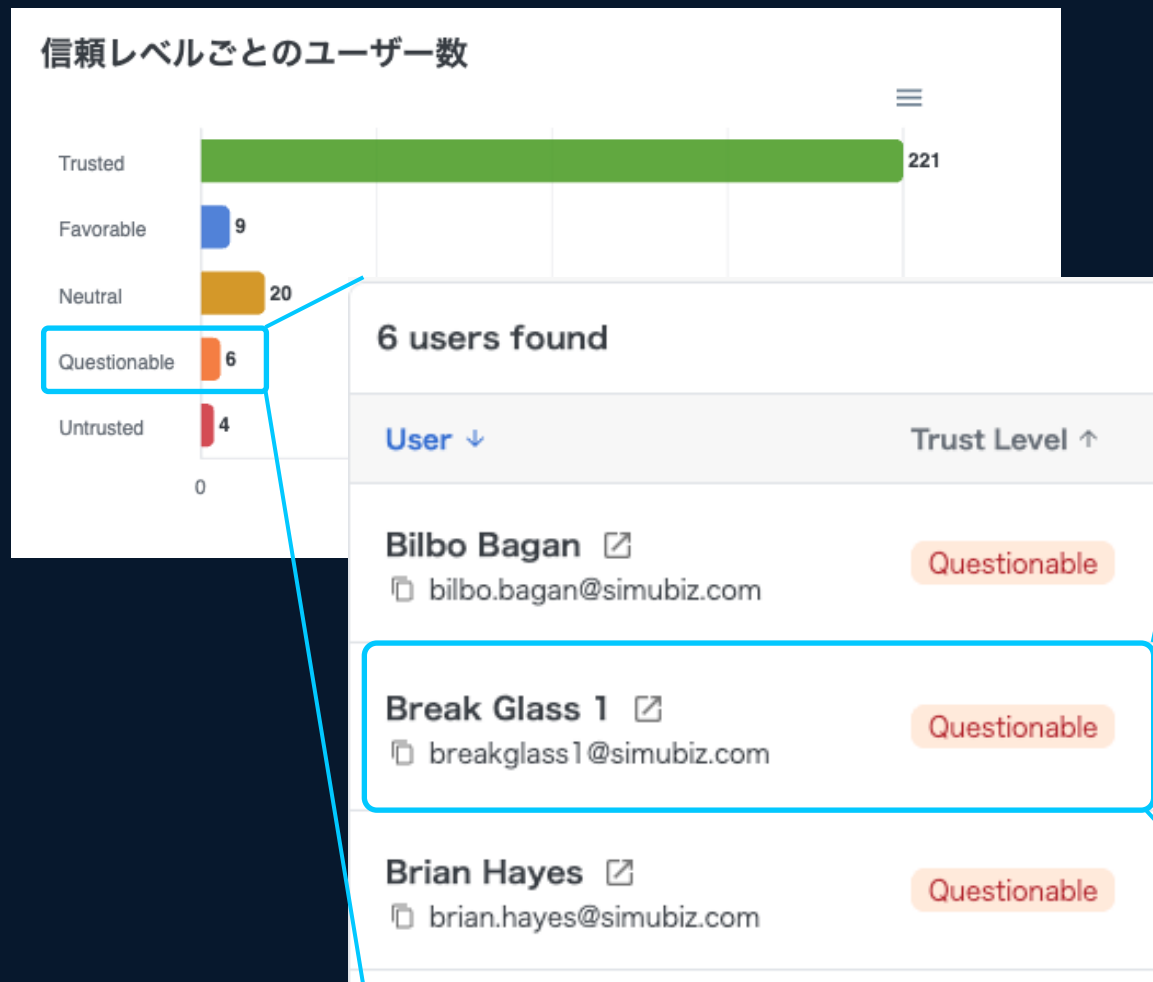


Identityの振る舞い検知

- 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

すべてのチェック			
チェック		不合格	📄
86 % 登録場所の不一致 ☒ • 低 エンドユーザー - アイデンティティ脅威インサイト	44	→ 先週 → 先月	
92 % テナントのための新しい国 ☒ • 中程度 エンドユーザー - アイデンティティ脅威インサイト	25	→ 先週 → 先月	
97 % IP脅威が検出されました ☒ • 重大 エンドユーザー - アイデンティティ脅威インサイト	8	→ 先週 → 先月	
97 % メール転送ルールが定義されているユーザー ☒ • 中程度 エンドユーザー - コンプライアンス、アイデンティティ脅威インサイト	7	→ 先週 → 先月	
98 % 休眠中の非人間的アイデンティティからのアクセス ☒ • 中程度 エンドユーザー - コンプライアンス、アイデンティティ脅威インサイト、非人間アイデンティティ	6	→ 先週 → 先月	
98 % 休眠アカウントからのアクセス ☒ • 中程度 エンドユーザー - コンプライアンス、アイデンティティ脅威インサイト	5	→ 先週 → 先月	
98 % 不可能な移動 ☒ • 中程度 エンドユーザー - アイデンティティ脅威インサイト	5	→ 先週 → 先月	
98 % バイパスコードを使用してサインインに成功しました ☒ • 重大 エンドユーザー - アイデンティティ脅威インサイト	5	→ 先週 → 先月	

ユーザー単位で信用レベルを特定



Duo デモ

ブレイクグラス1

アクティブ

ローカル

breakglass1@simubiz.com

- △ Break-Glassアカウントのサインインに成功しました
- △ 人間以外のIDに割り当てられた管理者ロール
- △ バイパスコードを使用してサインインに成功しました
- △ 休眠中の非人間的アイデンティティからのアクセス

信頼レベル ⓘ

疑わしい

次の要因により、レベルが「疑わしい」に変更されました。

優先アカウントは新しいIPアドレスと新しいISPからのバイパストークンを使用しました

追加情報

新しいIPアドレス

33.44.31.33

新しいISP

AS749

不合格チェック：

[バイパスコードを使用してサインインに成功しました](#)

バイパスコードの使用が正当であったかどうかを調査するためにチケットを開いてください。可能であればバイパスコードを無効にし、有効期限や使用回数のないバイパスコードをブロックするための社内ポリシーの更新を検討してください。

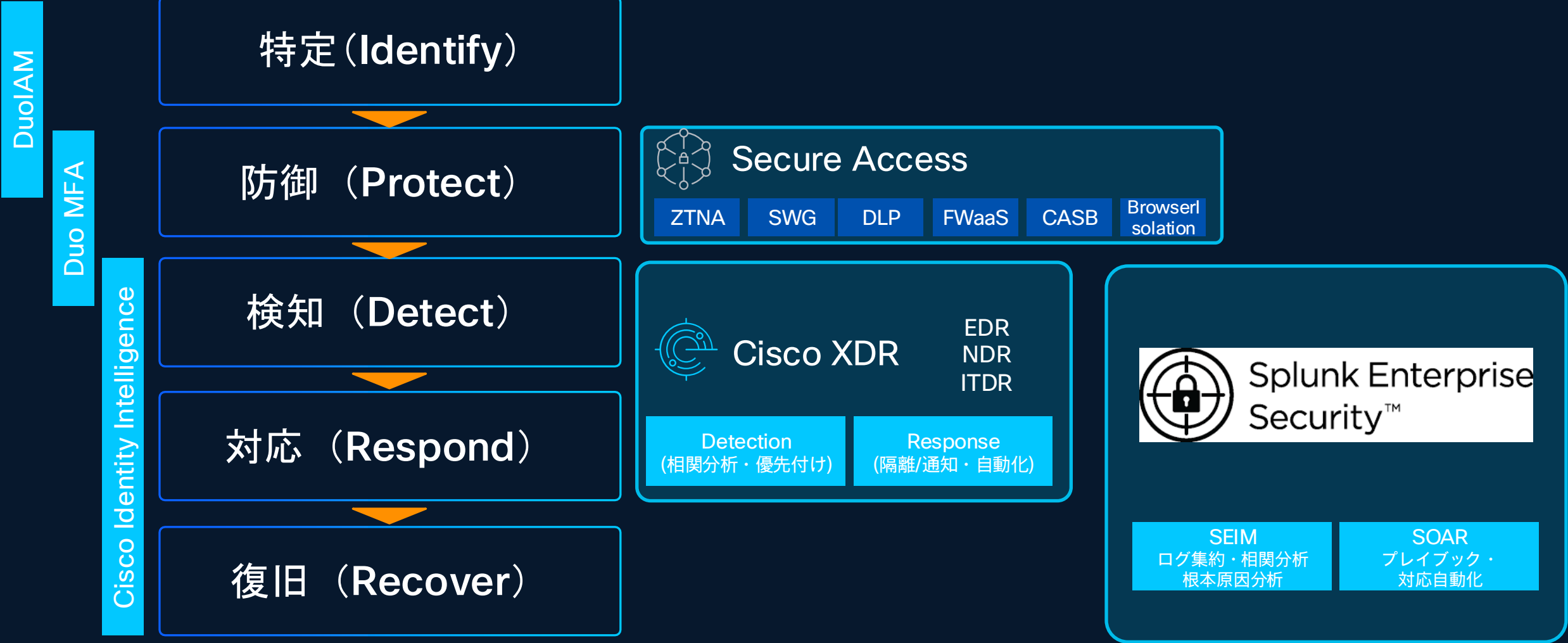
アイデンティティに関するアクションを自動化

- 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のコンテキストを利用可能 - [Private Preview](#) -

The screenshot displays two event logs from the Cisco Secure Access interface. The top log, titled 'Session End: Terminated', shows a session ending at 10:18 AM on April 18, 2024, with the detection 'Device Status: Firewall Off', the decision 'Terminate session', and the outcome 'Browser: access terminated'. The bottom log, titled 'Session Start: Authentication', shows a session starting at 10:08 AM on April 18, 2024, with the result 'Granted' (User approved) and the access device 'Mac'. A dropdown menu is open, listing several automated actions:

- + チケットを開く
- 🔄 MFAをリセットする
- 🔗 ユーザーのログアウト
- 🚫 隔離
- 📱 プッシュ認証を送信
- 🔄 ユーザーデータを更新
- +👤 ユーザーをリンク

Cisco Identity Intelligenceの製品連携



Secure Access – Cisco Identity Intelligence 連携

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 Cisco Secure Access management interface. The main section, 'Users and User Groups', shows a table of users. The user 'Josh Green' is highlighted, and his 'Trust Level' is 'Neutral'. An orange box highlights the 'Trust Level' column header and the 'Neutral' status for Josh Green. To the right, a 'User Details' sidebar is open, showing 'General' information (Name: Josh Green, Email: jgreen@securitydemo.net, Identity Provider: /azure-ad/scimv2) and a 'Trust Level' section. The 'Trust Level' section shows it was last updated on Feb 04 2025 5:11:49 PM UTC and lists factors: SpecialAccount, ResurrectedAccount, and access-from-dormant-account. The 'Groups' section shows 'Cisco-Global-Admins', 'LabUsers', and 'oort_admins'. The 'Events' and 'Associated Rules' sections show 0 items each.

Name	Email	Source	Directory	Trust Level ⓘ	Connected(VPN) ⓘ
Josh Green	jgreen@securitydemo.net	azure	Azure	Neutral	0

User Details

General

Name: Josh Green
Email: jgreen@securitydemo.net
Identity Provider: /azure-ad/scimv2

Trust Level Neutral ⓘ

Last updated: Feb 04 2025 5:11:49 PM UTC

The level changed to **Neutral** because of the following factors:

- SpecialAccount
- ResurrectedAccount
 - 1. access-from-dormant-account

Groups 3 ⓘ

Cisco-Global-Admins LabUsers oort_admins

Events 0 ⓘ

Associated Rules 0 ⓘ

Timing: In Private Preview now

Secure Access – Cisco Identity Intelligence

リスクがあるユーザーアクセスを動的に制御

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 dashboard. The page title is 'User Trust Profiles' with a subtitle explaining that these profiles adaptively modify authentication and security based on trust levels (untrusted, neutral, trusted) incorporated into access rules, powered by Cisco Identity Intelligence. A search bar shows '1 profile'.

Profile name	Assigned to	Used in
System-provided Default for private access policy rules ⓘ	All private resources	0 rules

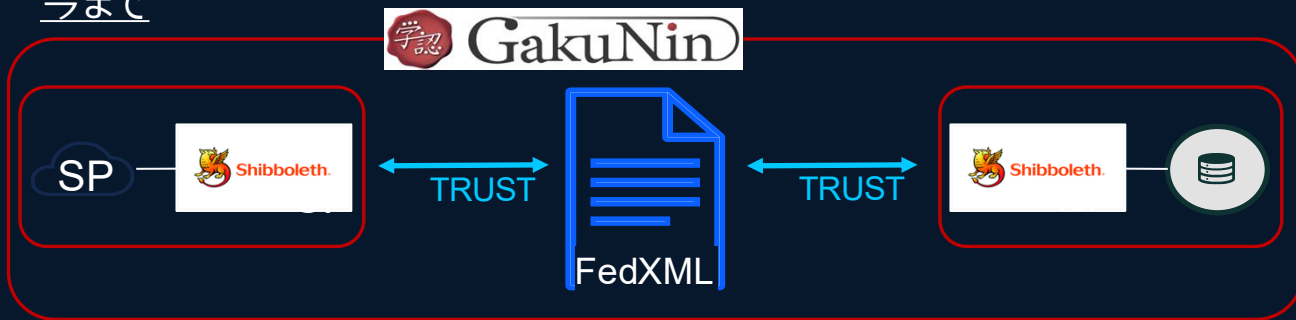
Trust level	Authentication controls	Security Controls
Trusted	Single Sign On	IPS: Connectivity Over Security
Neutral	Reauthenticate Every 24hrs	IPS: Security Over Connectivity Geolocation: US only
Untrusted	Block	-

The right sidebar contains additional settings for the 'Trusted' user trust level, including 'Authentication controls' (Single Sign On, Step up authentication, Duo Push, Block), 'Authentication Options' (Single Sign On selected), 'IPS Profile' (Enabled, IPS Profile enabled based on User Trust Level), 'IPS Profiles' (Connectivity Over Security selected), and 'Geolocation' (Enabled, Access will be allowed depending on Geolocation).

Cirrus Bridge連携

Cirrus Bridge + Duoの効果

今まで



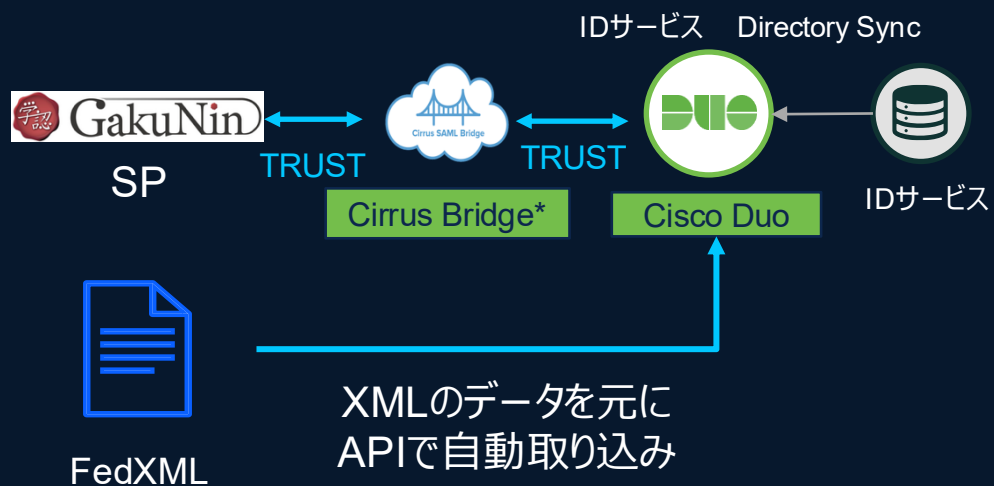
もしくは



SPに必要なデータを手入力

- 設定はCLIのみ
- 運用の負荷、構築、VerUp等

Cisco Duoだと？

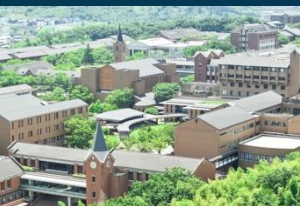


設定はGUI

バージョンアップ不要

選択式でSP追加

IdP運用/移行も簡単



「使いたい」にすぐ応え、研究と学びを止めない Cisco Duoで「学認」対応をクラウド化。工数削減と利便性向上を実現

同志社女子大学は、学術認証フェデレーション「学認」に対応する認証基盤を、オンプレミス機器からCisco DuoとCirrus SAML Bridgeの組み合わせに刷新しました。クラウドに移行することで運用負荷を大幅に軽減。また設定作業が容易になったことで、外注していた作業を内製化でき、新しい学認SPを使いたいという現場の要望に迅速に応えられるようになりました。

課題

- 学認に対応するIdPをオンプレミス機器で運用しており、バージョンアップや脆弱性対応、SSL証明書の更新などが定期的発生
- 新学認SPを追加する設定作業が複雑で外部委託に頼らざるを得ず、コストと時間がかかっていた
- Cisco Duoで多要素認証とシングルサインオンを実現していたが、学認SPは統合できていなかった

ソリューション

- Cisco Duoの既存機能に学術系フェデレーション対応を専門とするCirrus Identity社の「Cirrus SAML Bridge」を組み合わせた解決策をシスコが提案
- 日本のニーズを米国本社にエスカレーションし、Cirrus Identityとの協業体制を構築

結果～今後

- 学認SPの追加作業を内製化し、数カ月から数時間に短縮
- 新しい学認SPを使いたいという要望に、認証面では予算やリードタイムを気にせず対応できる
- Duo Centralのポータルに学認SPも統合
- eduGAINを通じ、海外のフェデレーションの利用も視野に

Why
Cisco?

「学認対応のIdPをCisco Duoで構築。現場のニーズにすぐ応えられます」

同志社女子大学経理部 ネットワークインフラ課課長
長南 敏彦 氏

学校法人同志社 同志社女子大学

所在地

京田辺キャンパス 京都府京田辺市興戸
今出川キャンパス 京都市上京区今出川通寺町西入

URL <https://www.dwc.doshisha.ac.jp/>

製品 & サービス

- Cisco Duo
- Cisco SolutionsPlus (Cirrus SAML Bridge)

