最新の ID を狙った攻撃に備える！
アカウントの可視化で実現する
『侵入を前提とした』
最強のランサムウェア対策

シスコシステムズ合同会社　セキュリティ事業部

アカウントエグゼクティブ
有光　祥太郎

ソリューションズエンジニア
西田　光貴

2026/11/18

情報漏洩インシデントの「5大攻撃パターン」

① 境界VPN・露出管理機能の悪用	VPN機器の脆弱性突破に加え、インターネットに露出した社内管理画面やCMSの脆弱性を直接攻撃
② 委託先SaaSの連鎖侵害	自社が堅牢でも、利用中の問い合わせSaaSや保守会社が侵害され、複数顧客のDBが横串で窃取
③ Web API認可不備・A2B攻撃	アプリを解析してバックエンドAPIを特定し、認可制御の不備を突いて大量の会員データを自動スクレイピング
④ 仮想化基盤標的ランサムウェア	個別端末ではなく仮想化基盤（ハイパーバイザー）とオンラインバックアップを同時に暗号化し事業停止
⑤ 人的・運用ミス	サイバー攻撃を伴わない設定ミス（何年間も気づかれず放置）、非表示シート残存、外部生成AIへの誤入力

© 2026 Cisco and/or its affiliates. All rights reserved.

国が求める対策ポイント

内閣官房国家サイバー統括室
不正アクセスによる漏えい等の事案を踏まえた対応について

ウェブシステム等の適切な管理

1. 脆弱性の適切な管理
   インターネットに公開されていない内部のサーバ等も含める
2. アカウント管理・認証
   ・MFAを導入する
   ・アクセス権を必要最小限にする
   ・不要なアカウントを速やかに無効化する
3. レジリエンスの向上
   ・ログを適切に管理・保管する
   ・不正な通信やアクセスを監視する
   ・外部からの異常な認証試行を把握する

サプライチェーンを通じた侵害への対策

1. 委託先企業等のセキュリティ対策状況の把握
2. 委託契約におけるセキュリティ要件の明確化
3. 情報共有範囲の適正化
4. サプライチェーン全体のリスクマネジメント

データの適切な管理

1. 保有する情報資産の適切な管理
2. 保有情報の最小化
3. 適切なアカウント管理・アクセス制御
   ・業務上必要な者のみにアクセスを許可する
   ・閲覧権限と更新権限を適切に分離する
   ・管理者権限の付与を必要最小限とする
   ・定期的にアカウントや権限設定を確認する
4. データ保護の徹底
5. ログ取得・監視・分析の強化

https://www.cyber.go.jp/pdf/press/taiou.pdf

© 2026 Cisco and/or its affiliates. All rights reserved.



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』

© 2026 Cisco and/or its affiliates. All rights reserved.

Duoによる Identity Security

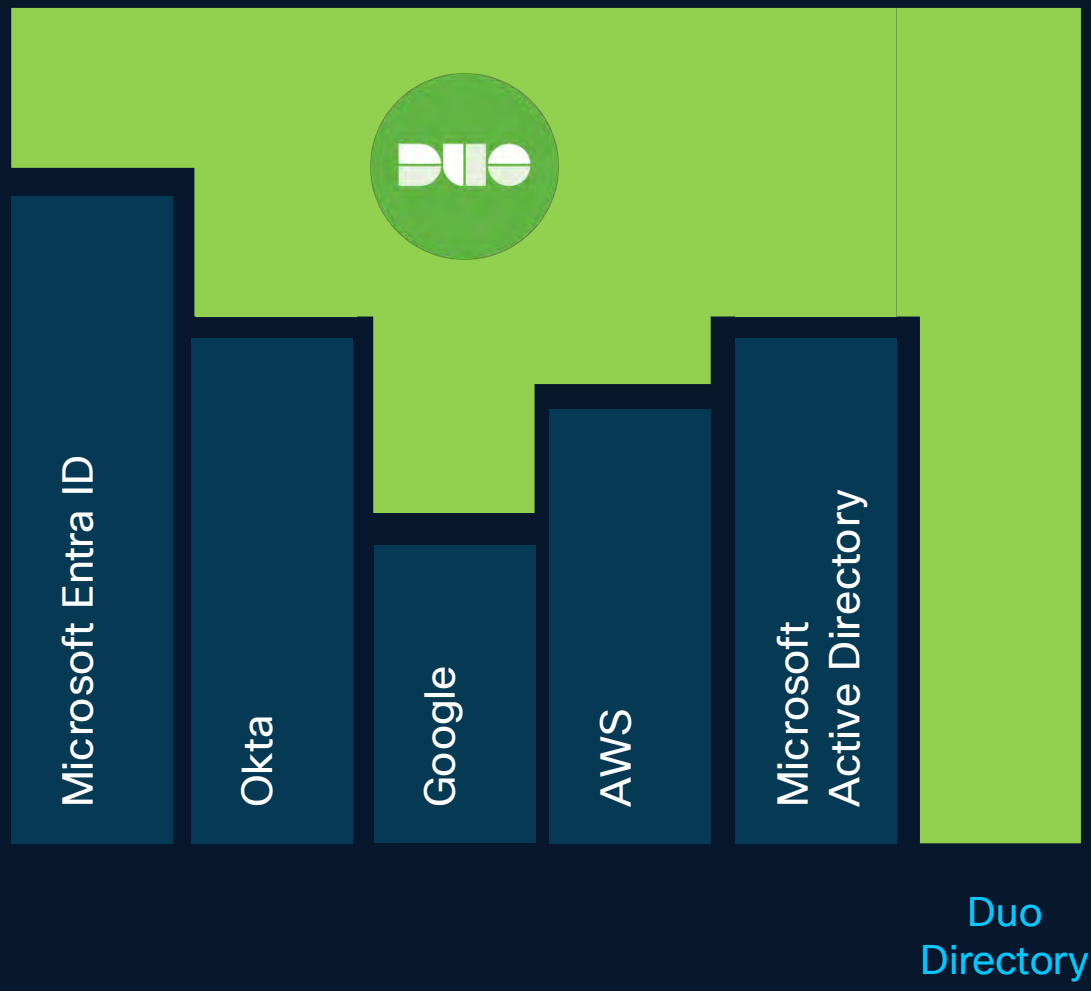
高い安全性

低いコスト

シンプルさ

© 2026 Cisco and/or its affiliates. All rights reserved.

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

© 2026 Cisco and/or its affiliates. All rights reserved.

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

© 2026 Cisco and/or its affiliates. All rights reserved.

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



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



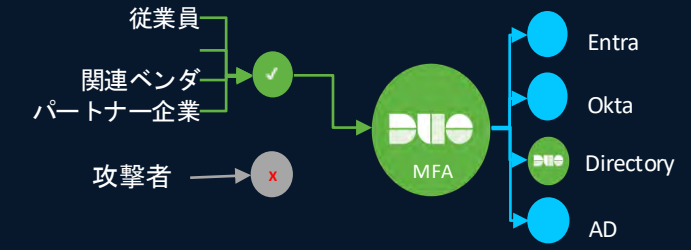
PCの可視化



モバイルの可視化

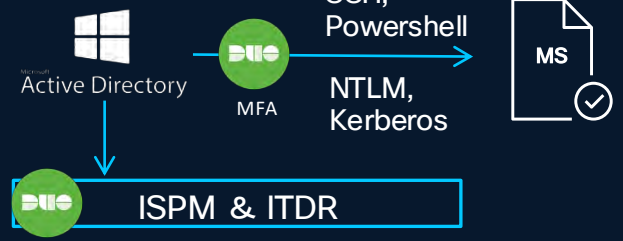
既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤

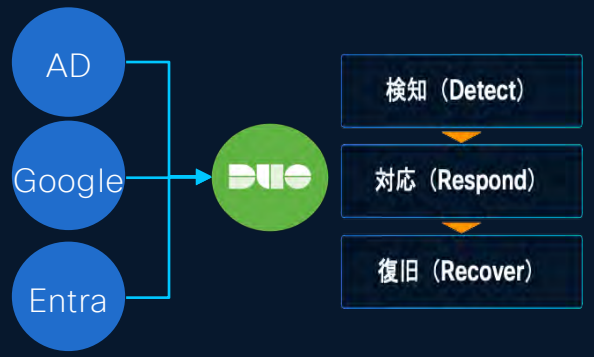


オンプレ環境 Active Directory保護

Active Directoryを標的とした攻撃を阻止



ISPM & ITDR

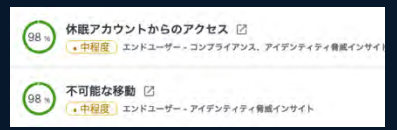


ISPM　アイデンティティの健全性管理



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



怪しい振る舞いのユーザーを即座に特定・隔離

© 2026 Cisco and/or its affiliates. All rights reserved.

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

パスワードレス　近接認証

モバイルApp　Desktop

SMS　電話

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



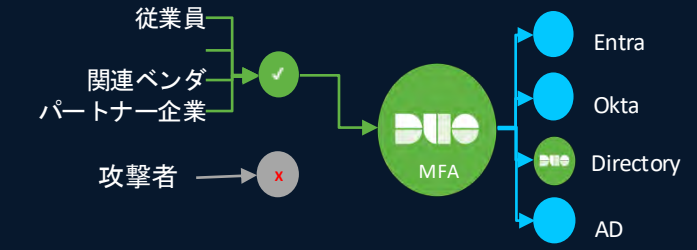
PCの可視化



モバイルの可視化

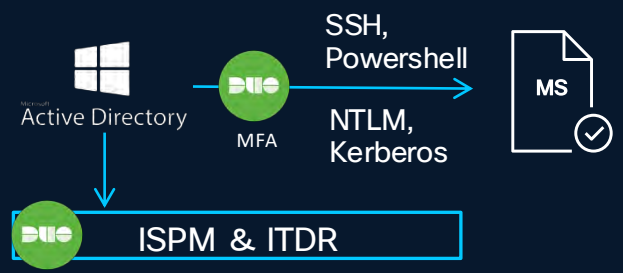
既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤

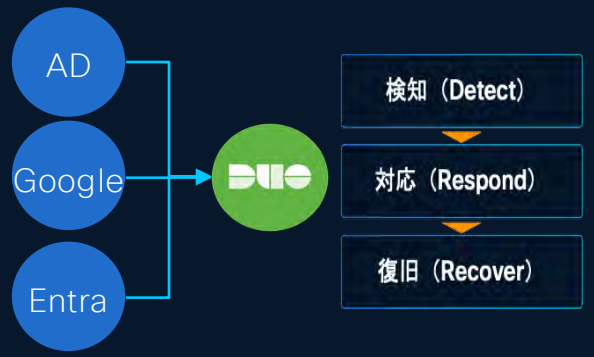


オンプレ環境 Active Directory保護

Active Directoryを標的とした攻撃を阻止



ISPM & ITDR

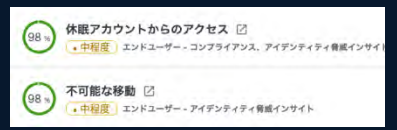


ISPM　アイデンティティの健全性管理



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

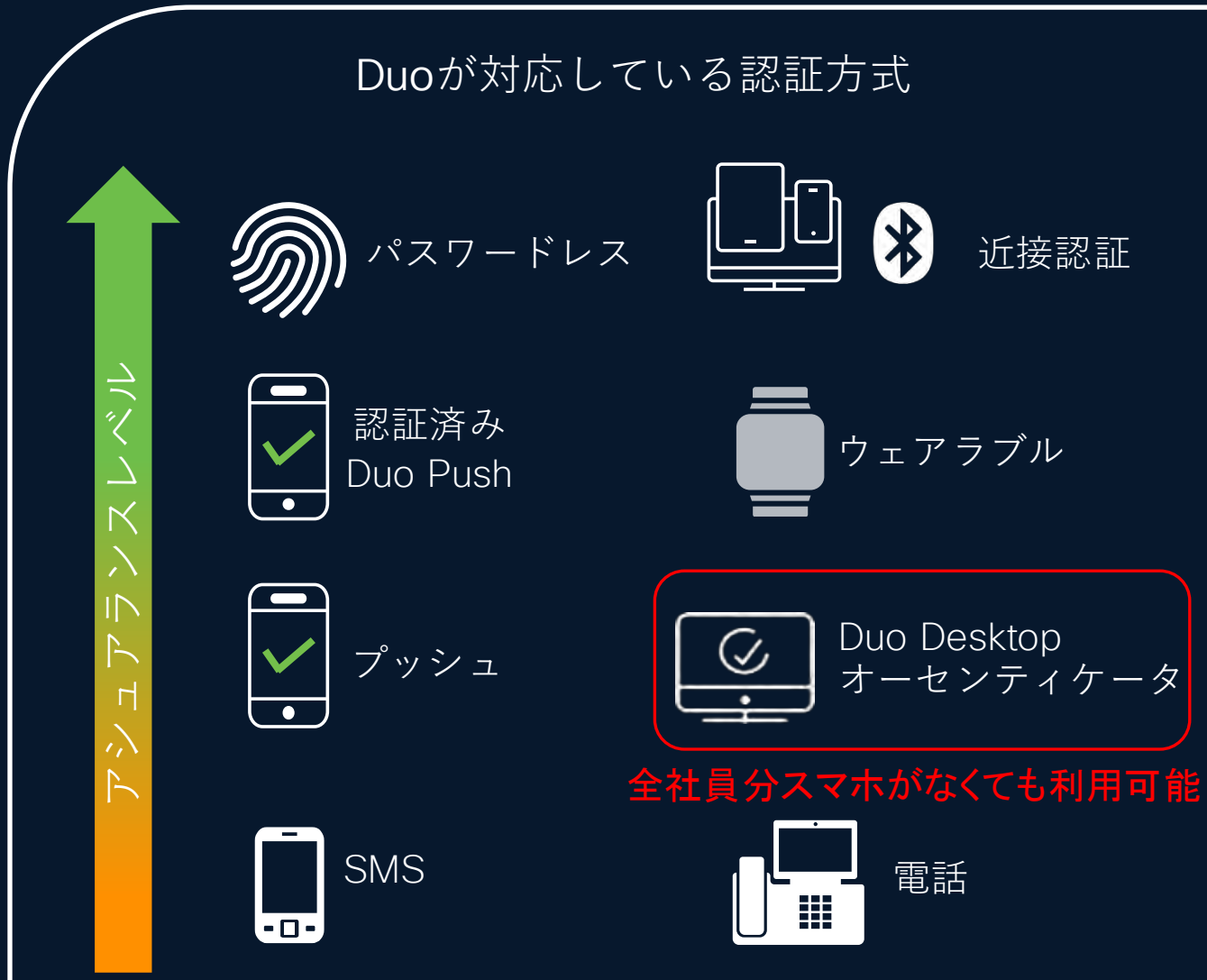


怪しい振る舞いのユーザーを即座に特定・隔離

© 2026 Cisco and/or its affiliates. All rights reserved.

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



© 2026 Cisco and/or its affiliates. All rights reserved.

Duo Push プッシュ通知 - 1タップで認証
セキュアで簡単な多要素認証（暗号化された認証方式）



登録済みMFAオプションの中から選択



プッシュ通知を選択した場合



登録しているスマートフォンにプッシュ通知され、ワンタップで承認

© 2024 Cisco and/or its affiliates. All rights reserved.

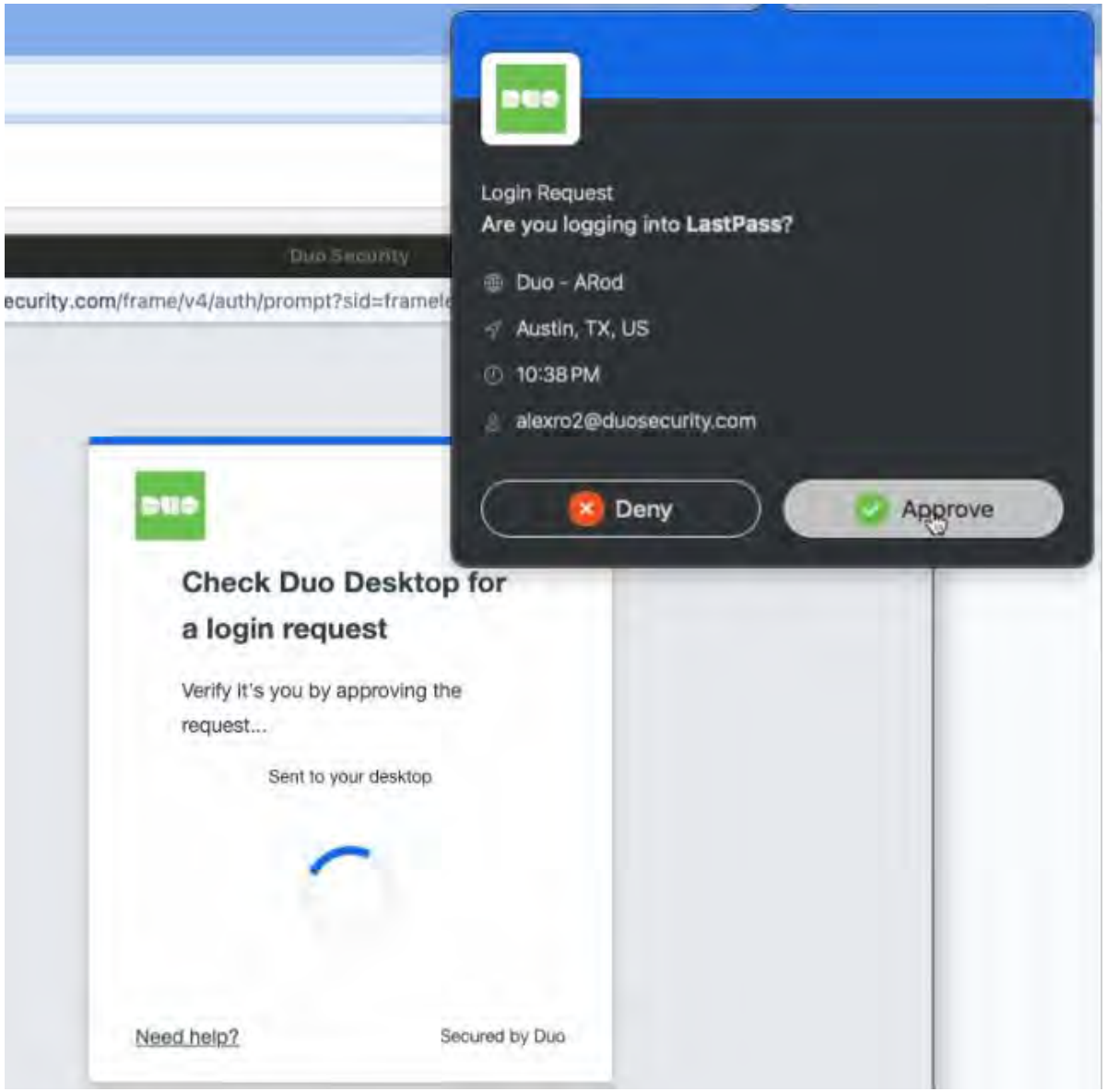
Duo Desktop Authentication

Use Case

- 全社員分スマホが配布できていない
  スマホがない社員がいる
- コールセンタや工場などの従業員に2FA認証デバイスが支給されていない
- クリーンルーム、データセンターなどの制限されたエリアでモバイル（Duo Push）を使えない

Solution

- 単一のデスクトップまたはラップトップ上でDuo DesktopにからDuo Pushを呼び出し、MFA認証を実施
- 上記ユースケースにおいて追加コストなくMFA認証を利用可能



© 2024 Cisco and/or its affiliates. All rights reserved.

リスクベース認証 ：リスクパターン

既知の攻撃パターンが検出されると自動的にステップアップ認証を要求



User Marked Fraud

ユーザーにより認証要求が不正であることを示す



Push Harassment

ユーザーが複数のプッシュを受信し、そのすべてが失敗している



Push Spray

1つのIPアドレスが複数の異なるユーザーにリクエストを送信



Consecutive Failures

1つのIP + IKEY (integration key)に複数の障害が発生



Country Code Mismatch

認証デバイスとアクセスデバイスが別々の国にある場合



Unrealistic Travel

最後に認証に成功した時間/場所から、到達することが不可能な場所から認証されたユーザー

Push通知→番号入力・生体認証にステップアップ
毎回番号入力は面倒…という場合におすすめ

© 2024 Cisco and/or its affiliates. All rights reserved.

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

パスワードレス　近接認証

モバイルApp　Desktop

SMS　電話

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



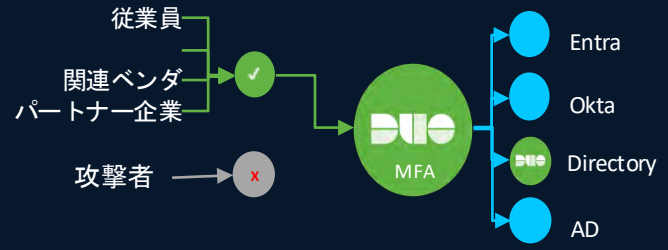
PCの可視化



モバイルの可視化

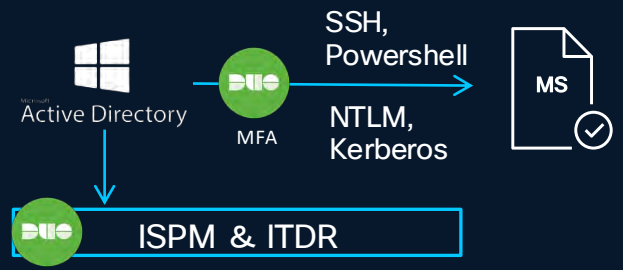
既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤

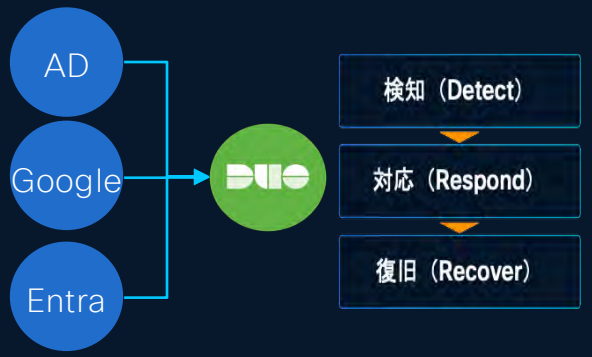


オンプレ環境 Active Directory保護

Active Directoryを標的とした攻撃を阻止



ISPM & ITDR

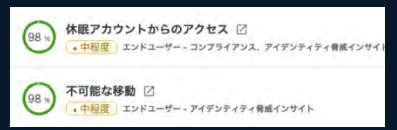


ISPM　アイデンティティの健全性管理



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



怪しい振る舞いのユーザーを即座に特定・隔離

© 2026 Cisco and/or its affiliates. All rights reserved.

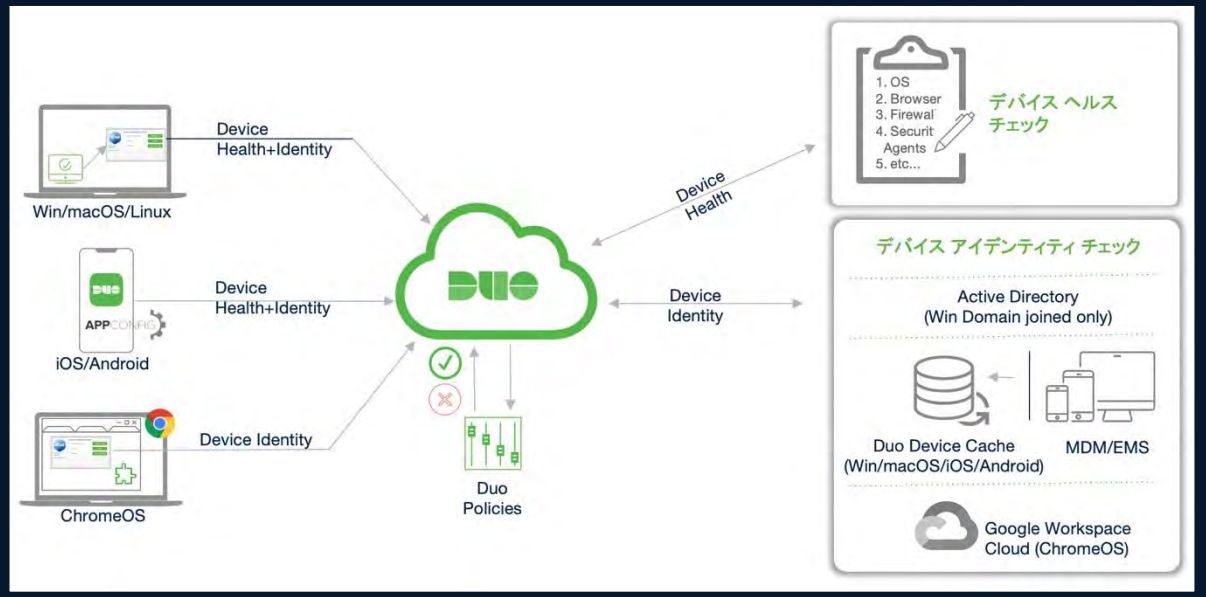
デバイストラスト　証明書に頼らないリアルタイムなデバイス認証

Device Health – デバイスのコンプライアンスチェック

- アクセス時にデバイスのセキュリティ情報を取得し、セキュリティ コンプライアンスチェックと検疫を実施
- OSバージョン（パッチ）、ブラウザバージョン、Firewallの状態、セキュリティエージェントの動作などを検査

Trusted Endpoints – デバイス認証 –

- アクセス時に、MDM/EMSとAPI連携によるデバイス認証や手動登録によるデバイスのユニークなIDを利用したデバイス認証で管理デバイスとして認識
- デバイスの盗難や紛失の際、Block-Listに追加することで、そのデバイスからのアクセスをブロックする



© 2026 Cisco and/or its affiliates. All rights reserved.

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



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



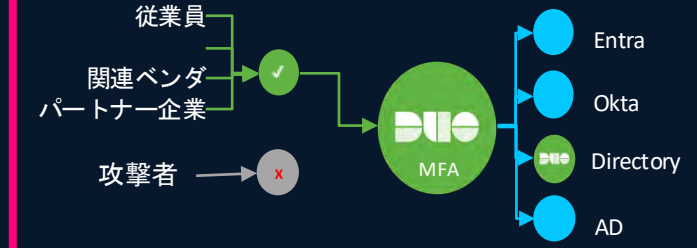
PCの可視化



モバイルの可視化

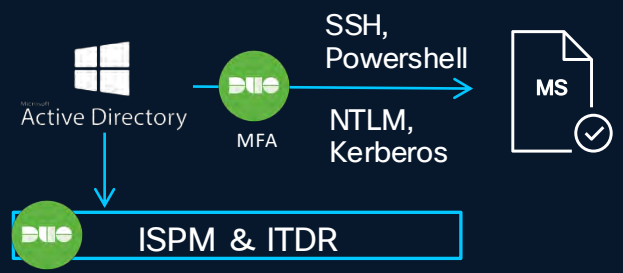
既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤

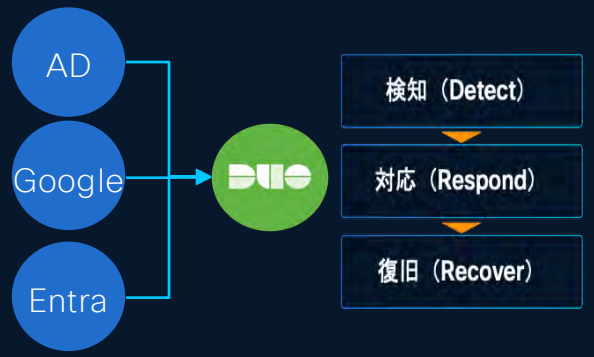


オンプレ環境 Active Directory保護

Active Directoryを標的とした攻撃を阻止



ISPM & ITDR

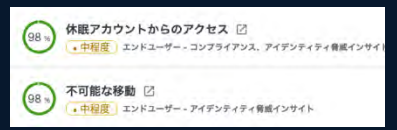


ISPM　アイデンティティの健全性管理



MFA未適用、休眠ID、過剰特権アカウント

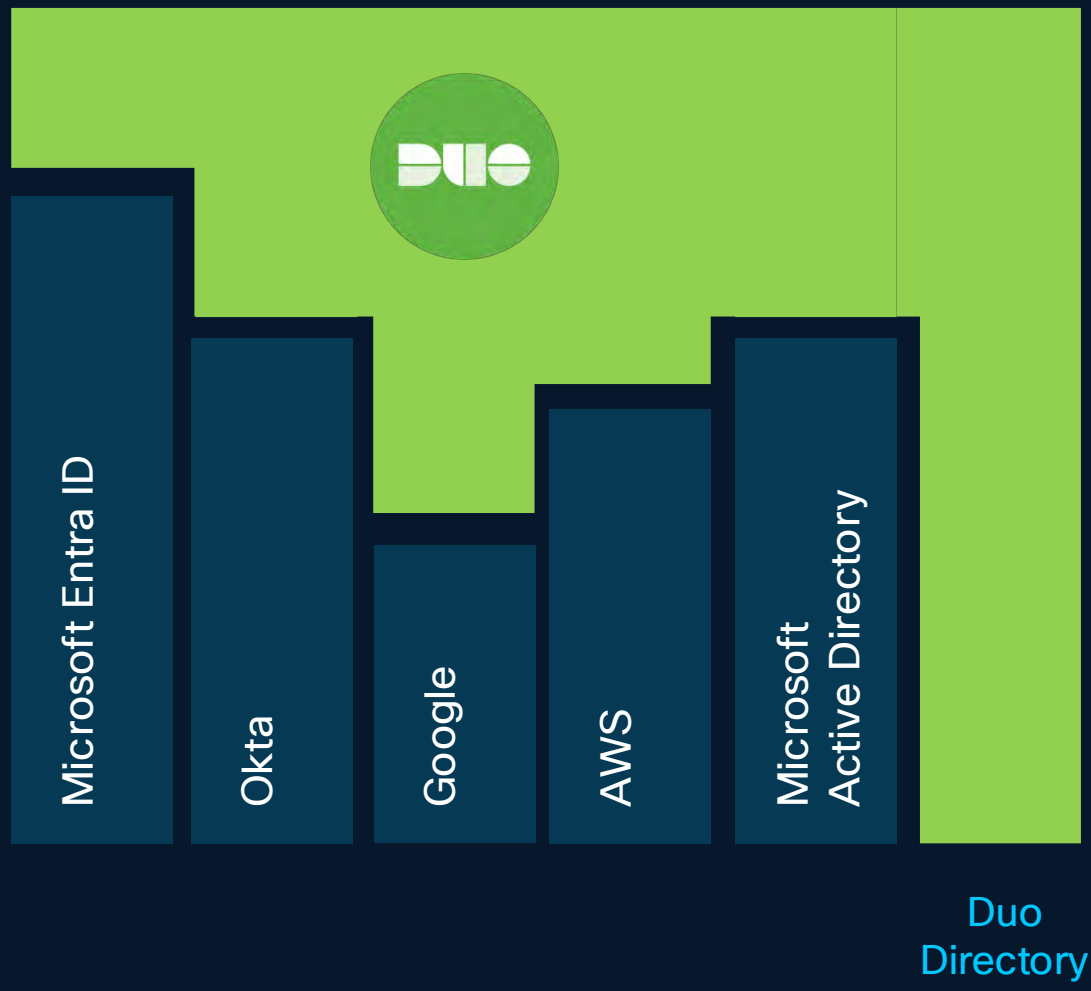
ITDR アイデンティティの振る舞い検知



怪しい振る舞いのユーザーを即座に特定・隔離

© 2026 Cisco and/or its affiliates. All rights reserved.

DuoはIdentityのセキュリティにフォーカス

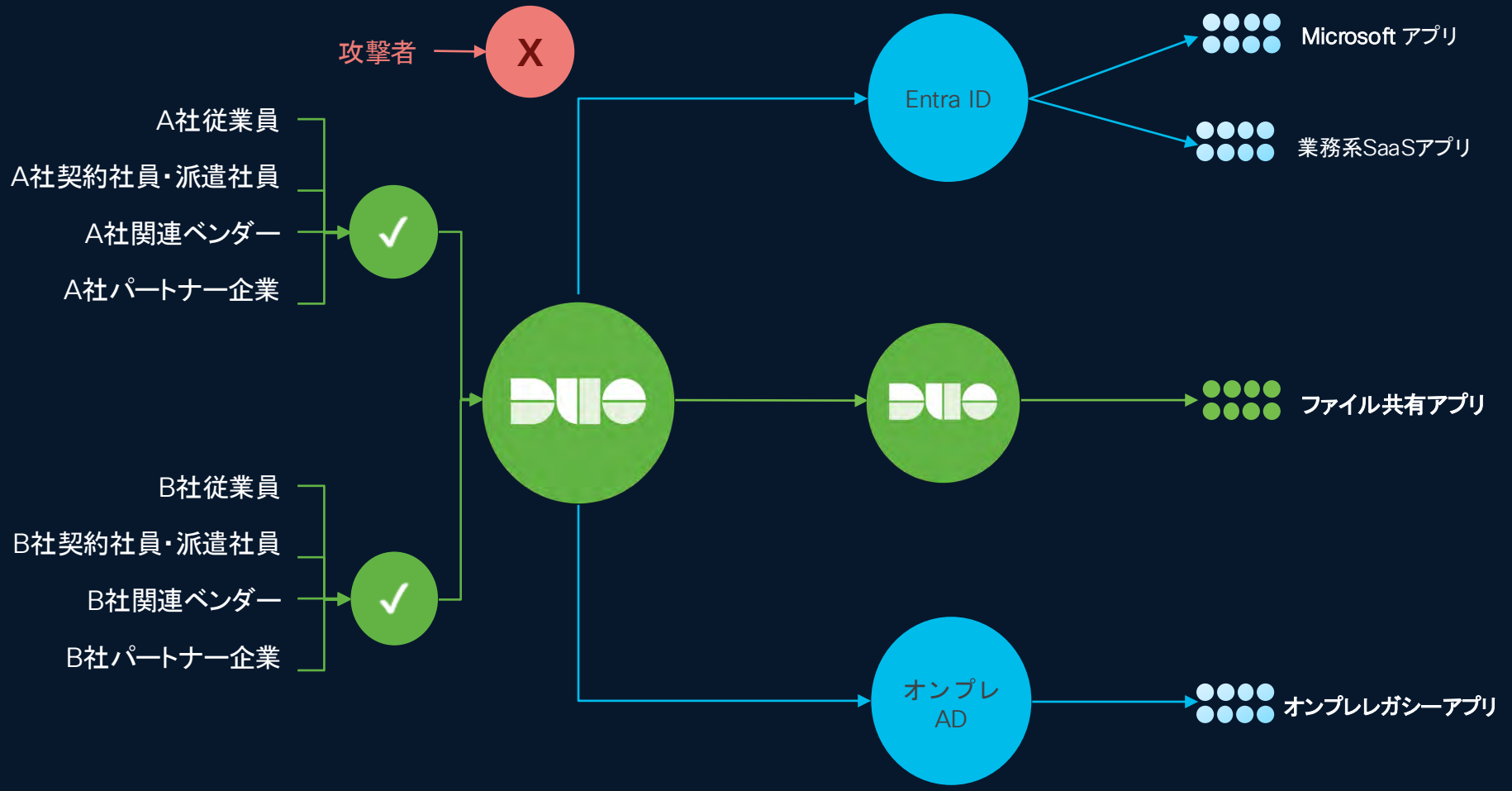


複雑なID環境へ強力なセキュリティを柔軟に安価に提供し、ギャップを埋める

ユーザーの快適性を損なわず、すべてのユーザーを守る

© 2026 Cisco and/or its affiliates. All rights reserved.

グループ企業のID管理の一元化
業務委託先へのIDセキュリティの実装とガバナンス強化



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
- 双方のアプリへアクセスする一時的なアクセス権はDuoでも保持可能。アクセス権の漏れや重複を排除。

© 2025 Cisco and/or its affiliates. All rights reserved.

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



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



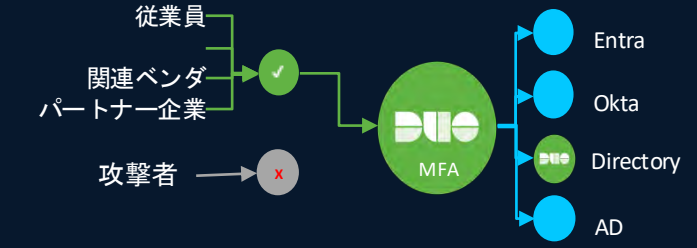
PCの可視化



モバイルの可視化

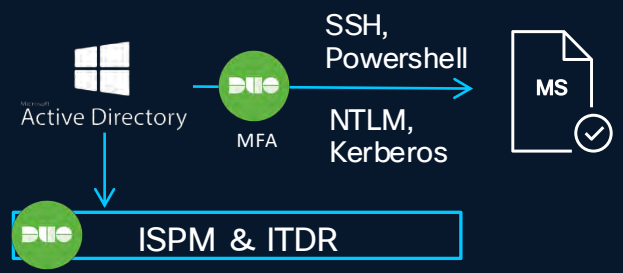
既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤

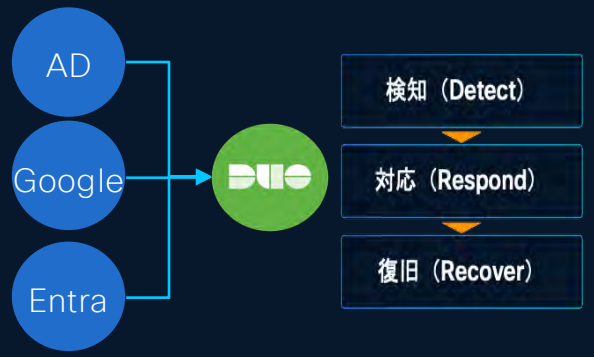


オンプレ環境 Active Directory保護

Active Directoryを標的とした攻撃を阻止



ISPM & ITDR

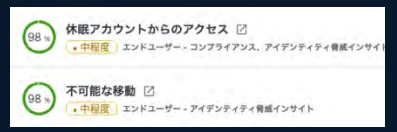


ISPM　アイデンティティの健全性管理



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



怪しい振る舞いのユーザーを即座に特定・隔離

© 2026 Cisco and/or its affiliates. All rights reserved.

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

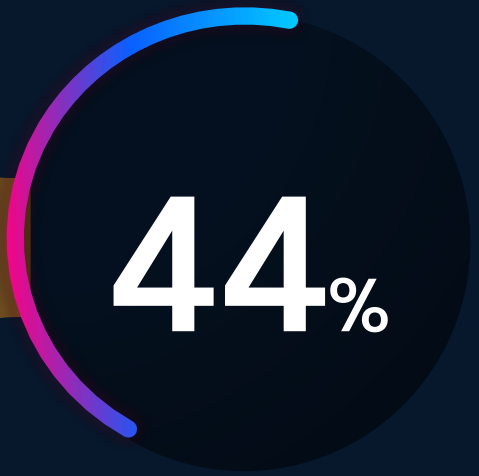


90% of Fortune 1000

© 2026 Cisco and/or its affiliates. All rights reserved.

ADが攻撃者の格好の標的になっている

- Active Directory
  - *カスタムコンフィグレーション*
  - *複数ドメイン*
  - *レガシーシステムとの連携*
  - *管理者アカウント・特権アカウント*
  - *一時ユーザ・サービスアカウント・NHI*

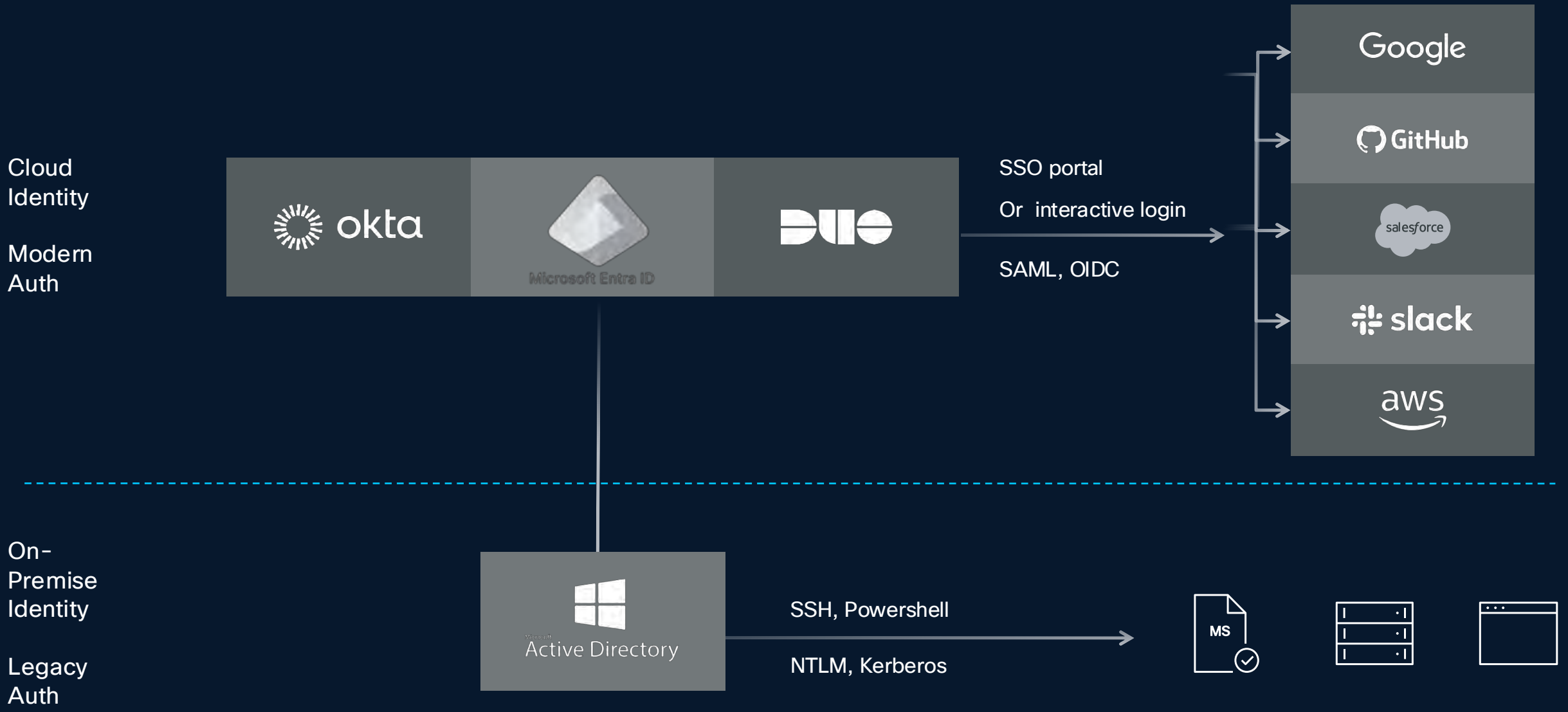


Active Directoryを標的とした
アイデンティティへの攻撃

Cisco Talos Incident Response | Active Directory-based Attacks

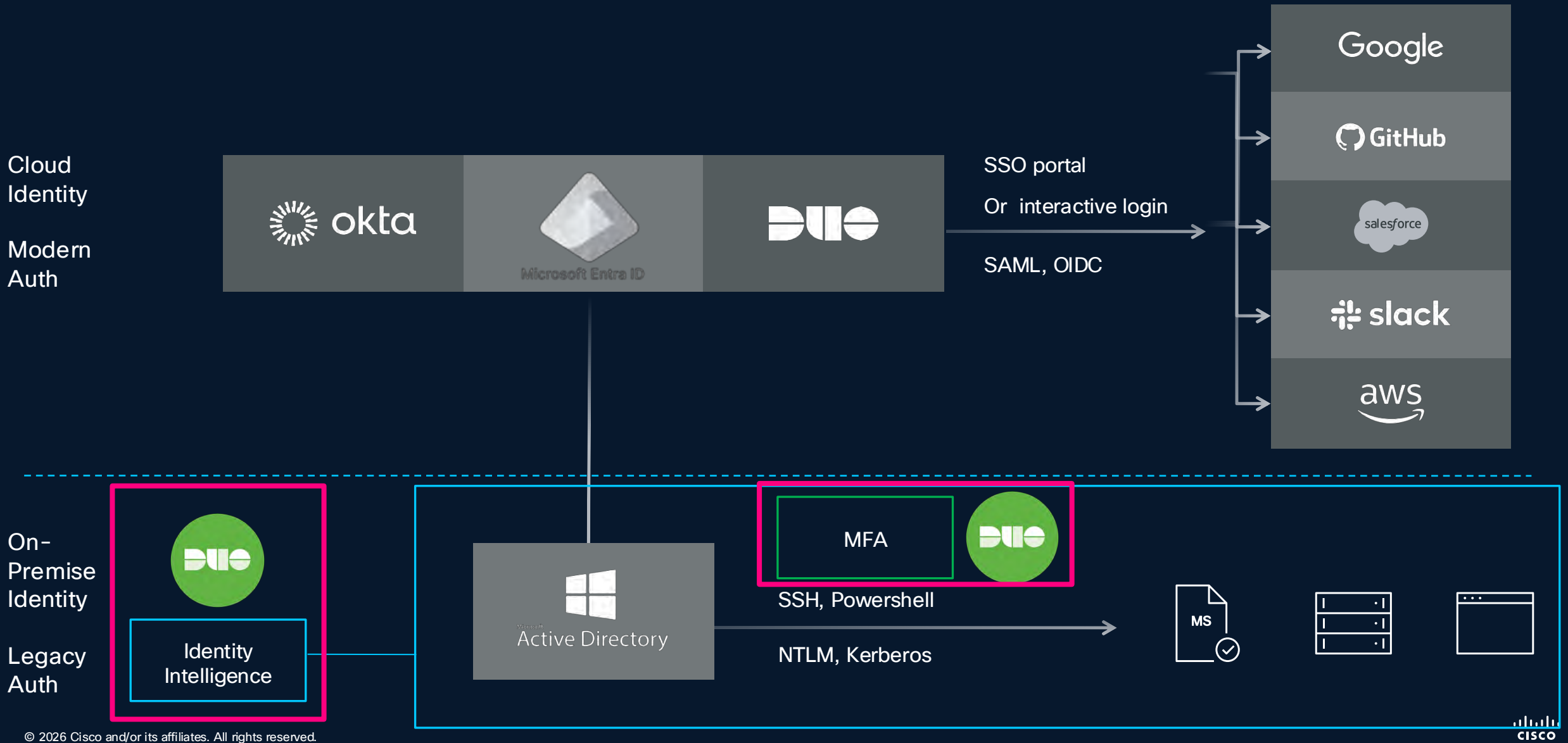
© 2026 Cisco and/or its affiliates. All rights reserved.

クラウドのアイデンティティは既に保護されている



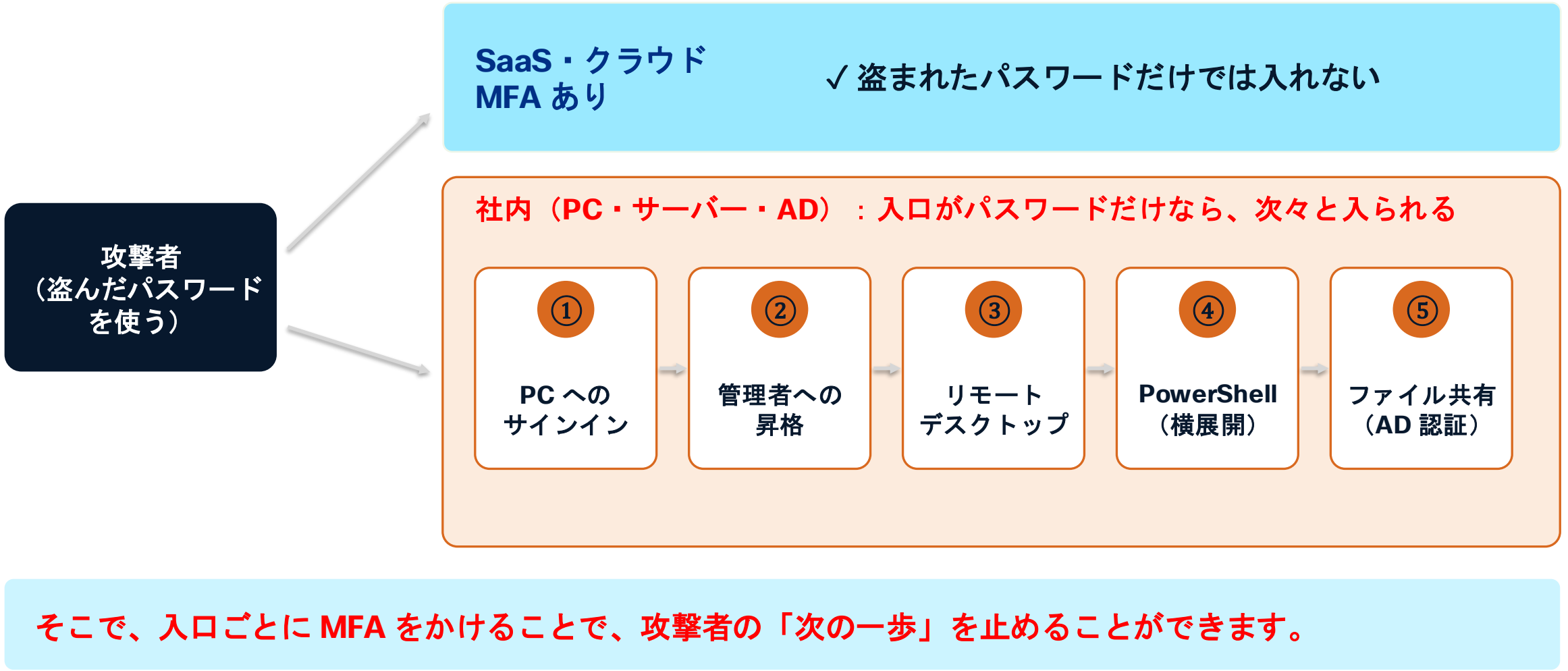
© 2026 Cisco and/or its affiliates. All rights reserved.

Active Directory Defenseはレガシーインフラを保護



© 2026 Cisco and/or its affiliates. All rights reserved.

社内の入口が、パスワードだけになっていないか



そこで、入口ごとに MFA をかけることで、攻撃者の「次の一歩」を止めることができます。

© 2026 Cisco and/or its affiliates. All rights reserved.

Windows と AD のログインを、5つの入口で守る

実演



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

実演



②
管理者への昇格

一般ユーザーから
管理者権限を取る

Duo Authentication for
Windows Logon

全エディション



③
リモート
デスクトップ

別の端末から
サーバーに入る

Duo Authentication for
Windows Logon

全エディション

実演



④
PowerShell
リモート

画面なしで次の
サーバーへ（横展開）

Duo Windows Command
Line Protection

Advantage / Premier



⑤
ファイル共有

AD 認証を使う接続

Duo Legacy AD Protection

Advantage / Premier

①〜③　端末に Duo を入れて守る

④⑤　DC・サーバーで守る

5つの入口を、同じ Duo Mobile の Push で守る（ツールをバラバラにしない）

© 2026 Cisco and/or its affiliates. All rights reserved.

Windows と AD のログインを、5つの入口で守る

実演



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

実演



② **管理者への昇格**

一般ユーザーから管理者権限を取る

Duo Authentication for Windows Logon

全エディション



③ **リモートデスクトップ**

別の端末からサーバーに入る

Duo Authentication for Windows Logon

全エディション

実演



④ **PowerShell リモート**

画面なしで次のサーバーへ（横展開）

Duo Windows Command Line Protection

Advantage / Premier



⑤ **ファイル共有**

AD 認証を使う接続

Duo Legacy AD Protection

Advantage / Premier

①〜③　端末に Duo を入れて守る

④⑤　DC・サーバーで守る

5つの入口を、同じ Duo Mobile の Push で守る（ツールをバラバラにしない）

© 2026 Cisco and/or its affiliates. All rights reserved.



© 2026 Cisco and/or its affiliates. All rights reserved.

Windows と AD のログインを、5つの入口で守る

実演



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

実演



② **管理者への昇格**

一般ユーザーから管理者権限を取る

Duo Authentication for Windows Logon

全エディション



③ **リモートデスクトップ**

別の端末からサーバーに入る

Duo Authentication for Windows Logon

全エディション

実演



④ **PowerShell リモート**

画面なしで次のサーバーへ（横展開）

Duo Windows Command Line Protection

Advantage / Premier



⑤ **ファイル共有**

AD 認証を使う接続

Duo Legacy AD Protection

Advantage / Premier

①〜③　端末に Duo を入れて守る

④⑤　DC・サーバーで守る

5つの入口を、同じ Duo Mobile の Push で守る（ツールをバラバラにしない）

© 2026 Cisco and/or its affiliates. All rights reserved.



デモ動画はウェビナー録画にてご確認ください

© 2026 Cisco and/or its affiliates. All rights reserved.

Windows と AD のログインを、5つの入口で守る

実演



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

実演



② **管理者への昇格**

一般ユーザーから管理者権限を取る

Duo Authentication for Windows Logon

全エディション



③ **リモートデスクトップ**

別の端末からサーバーに入る

Duo Authentication for Windows Logon

全エディション

実演



④ **PowerShell リモート**

画面なしで次のサーバーへ（横展開）

Duo Windows Command Line Protection

Advantage / Premier



⑤ **ファイル共有**

AD 認証を使う接続

Duo Legacy AD Protection

Advantage / Premier

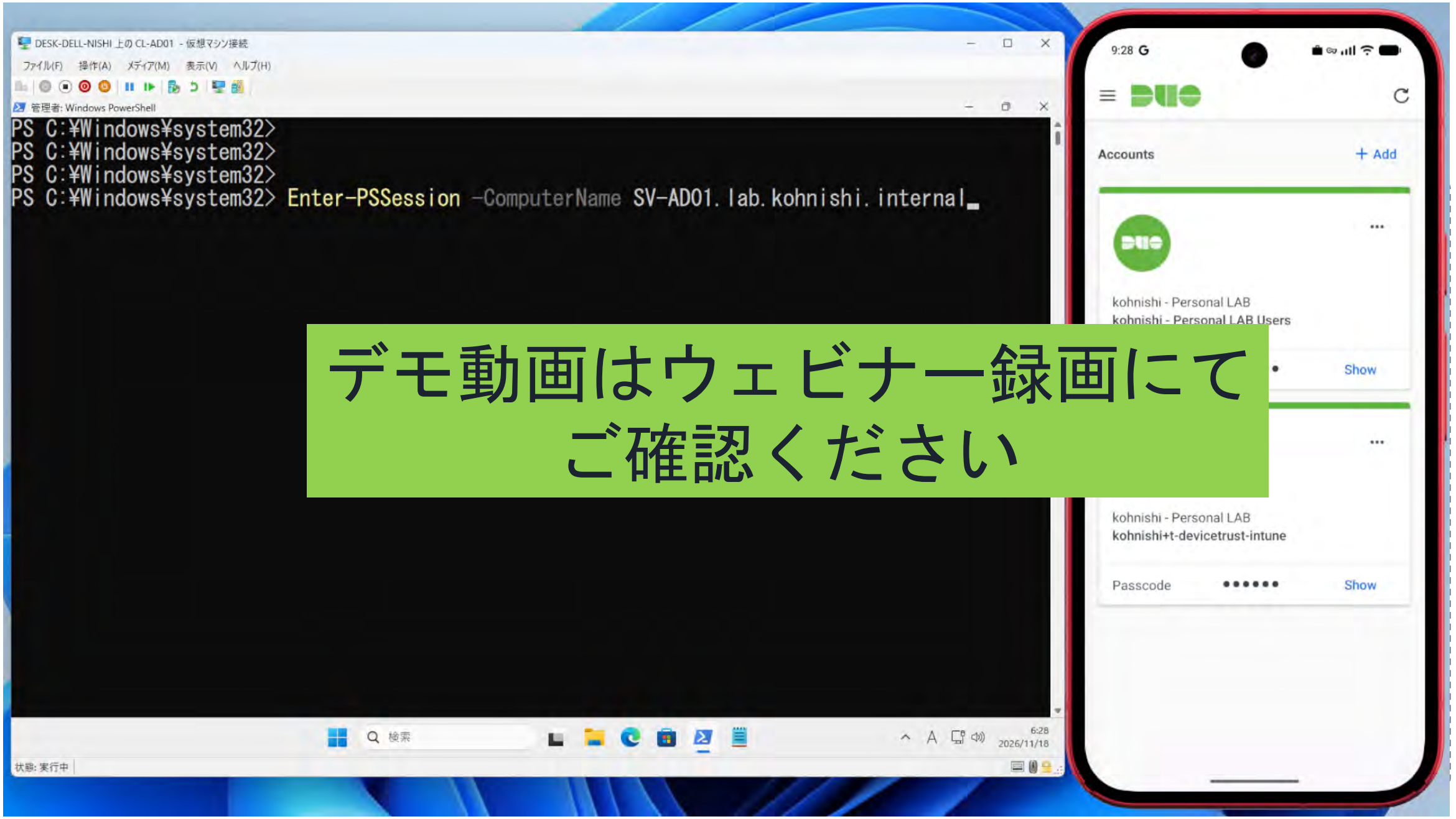
①〜③　端末に Duo を入れて守る

④⑤　DC・サーバーで守る

5つの入口を、同じ Duo Mobile の Push で守る（ツールをバラバラにしない）

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco



デモ動画はウェビナー録画にて
ご確認ください

© 2026 Cisco and/or its affiliates. All rights reserved.

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

パスワードレス　近接認証

モバイルApp　Desktop

SMS　電話

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



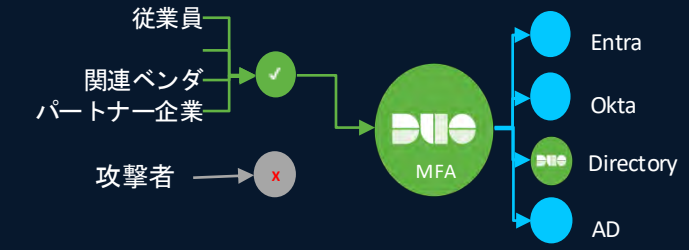
PCの可視化



モバイルの可視化

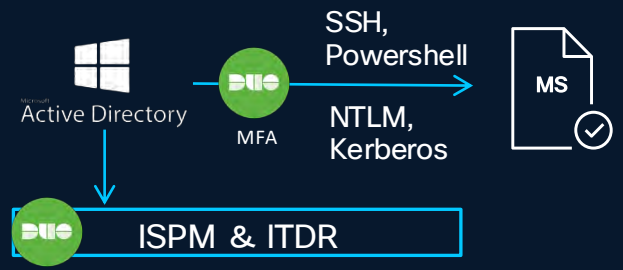
既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤

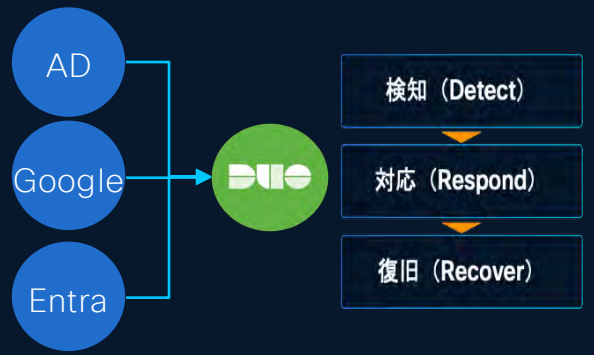


オンプレ環境 Active Directory保護

Active Directoryを標的とした攻撃を阻止



ISPM & ITDR

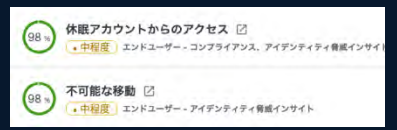


ISPM　アイデンティティの健全性管理



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



怪しい振る舞いのユーザーを即座に特定・隔離

© 2026 Cisco and/or its affiliates. All rights reserved.

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）

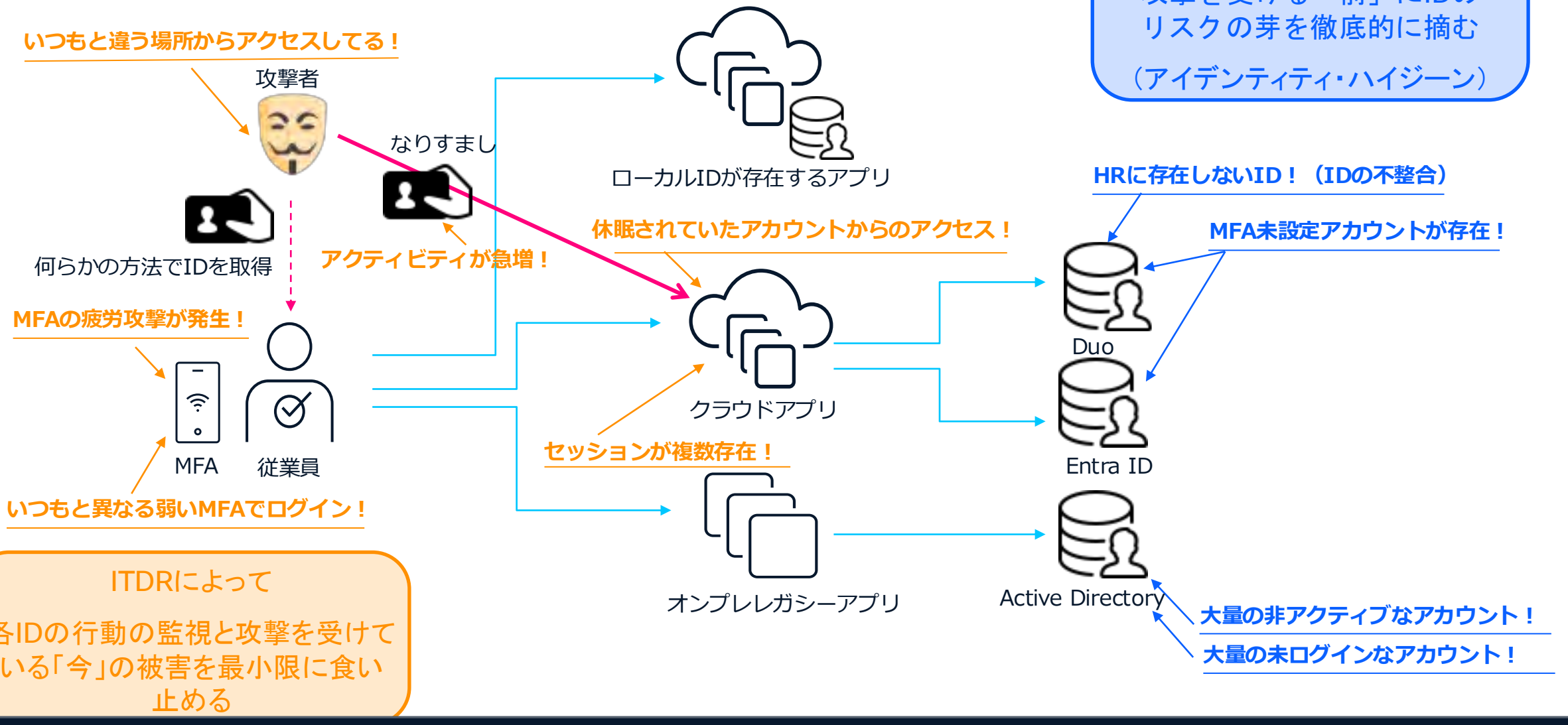
© 2026 Cisco and/or its affiliates. All rights reserved.

Duo(CII)で認証環境を監視する

ISPMによって

攻撃を受ける「前」にIDの
リスクの芽を徹底的に摘む

（アイデンティティ・ハイジーン）



ITDRによって

各IDの行動の監視と攻撃を受けて
いる「今」の被害を最小限に食い
止める

ISPMとITDRを組み合わせた認証環境の監視が重要

© 2026 Cisco and/or its affiliates. All rights reserved.

今回のデモ環境：3つの ID 基盤を CII に接続

設定は「接続」のみ。収集は読み取り中心で、既存環境は変更しません

Microsoft Entra ID
API 連携

Active Directory
定期スクリプト で情報を送信

Duo
認証ログ / MFA

→

Cisco Identity Intelligence

ID 情報を1か所に集約
点数・推奨・検知を算出

→

Dashboard
点数と推奨で全体像

Checks
弱点を一覧で

Users
人物単位で確認

接続状況（実画面）

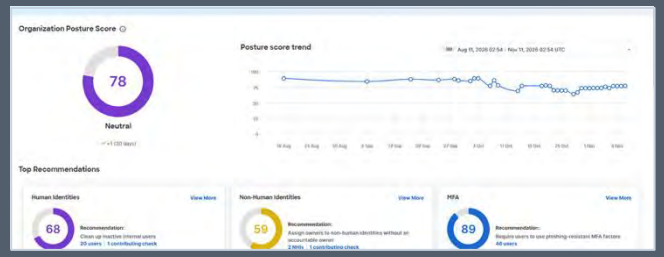


© 2026 Cisco and/or its affiliates. All rights reserved.

連携すると何が分かるか：3つの切り口

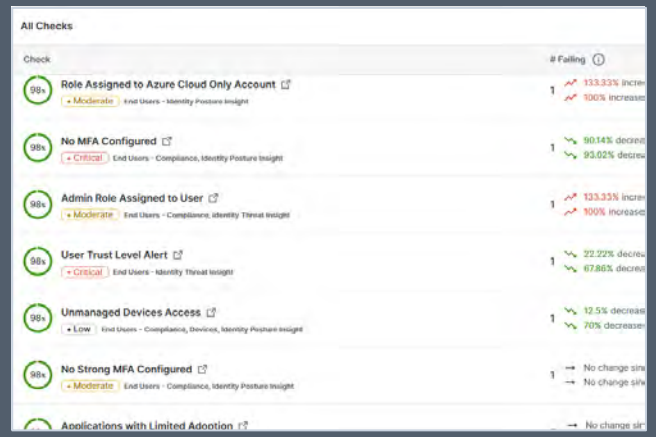
Dashboard で全体 → Checks で弱点 → Users で人物。

1 Dashboard



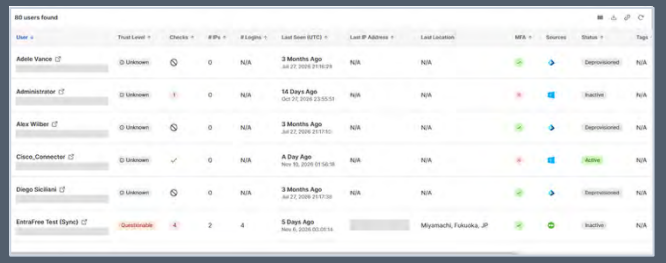
Posture Score と、領域別の推奨。
Human / NHI / MFA の中で、
どこから直すかが分かる

2 Checks



弱点一覧。重大度と該当件数つき

3 Users



人物単位。どの基盤の何の Check に掛かっているか、MFA・信頼度とあわせて確認

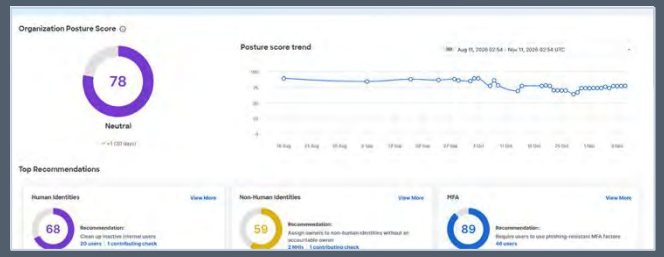
ポイント：検知ルールの設定や集計は不要。接続した時点から、基盤をまたいだ同じ画面で確認できます。

© 2026 Cisco and/or its affiliates. All rights reserved.

連携すると何が分かるか：3つの切り口

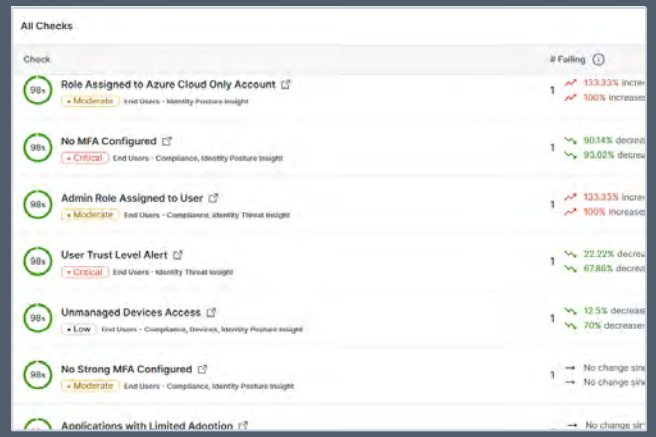
Dashboard で全体 → Checks で弱点 → Users で人物。

1 Dashboard



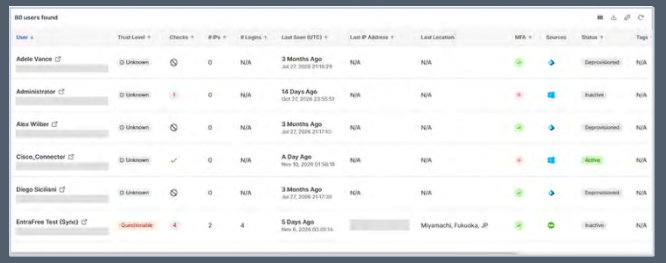
Posture Score と、領域別の推奨。
Human / NHI / MFA の中で、
どこから直すかが分かる

2 Checks



弱点一覧。重大度と該当件数つき

3 Users



人物単位。どの基盤の何の Check に掛かっているか、MFA・信頼度とあわせて確認

ポイント：検知ルールの設定や集計は不要。接続した時点から、基盤をまたいだ同じ画面で確認できます。

© 2026 Cisco and/or its affiliates. All rights reserved.

データをもとにスコアリング

組織の態勢スコア

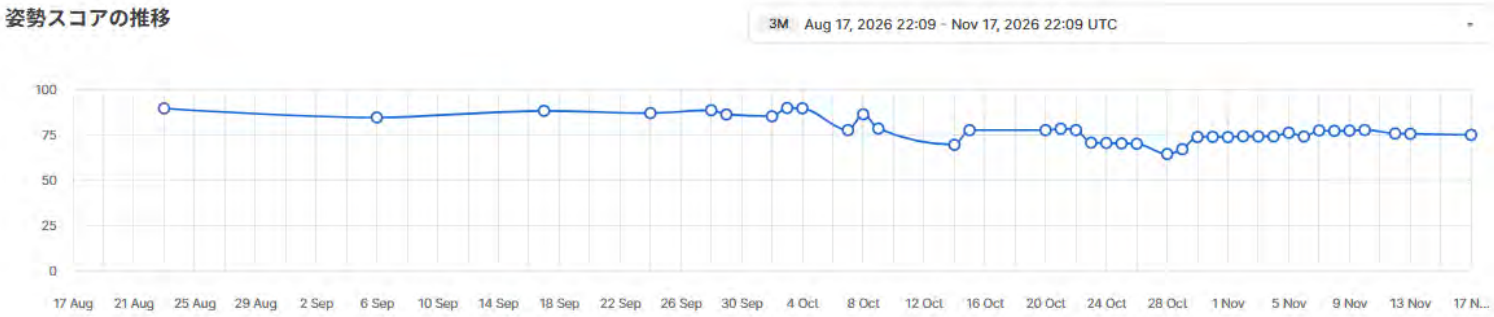


中立

-2 (30日間)

御社の姿勢スコアは、同規模の組織の中で下位20パーセンタイルに該当します。

姿勢スコアの推移



セキュリティを高めるための推奨事項を提示

特におすすめのアイテム

人間のアイデンティティ　もっと見る



中立

推奨事項：
非アクティブな内部ユーザーを削除する
24ユーザー | 1枚の寄付小切手

人間以外のアイデンティティ　もっと見る



弱い

推奨事項：
責任の所在が明確でない非人間的なアイデンティティに所有者を割り当てる
2 NHIs | 1枚の小切手（寄付）

MFA　もっと見る



良い

推奨事項：
ユーザーに対し、フィッシング対策機能を備えた多要素認証（MFA）の認証要素の使用を義務付ける
46人のユーザー

「人間のアイデンティティ」の概要

50 合計	24 非アクティブな内部ユーザー
0 アクセス権を持つ非アクティブな管理者	0 認証ツールを共有する管理者

非人間的アイデンティティの概要

5 合計	2 所有者が割り当てられていないNHI
0 多要素認証（MFA）が設定されていないアカウント	0 管理者権限を持つアカウント

MFAの概要

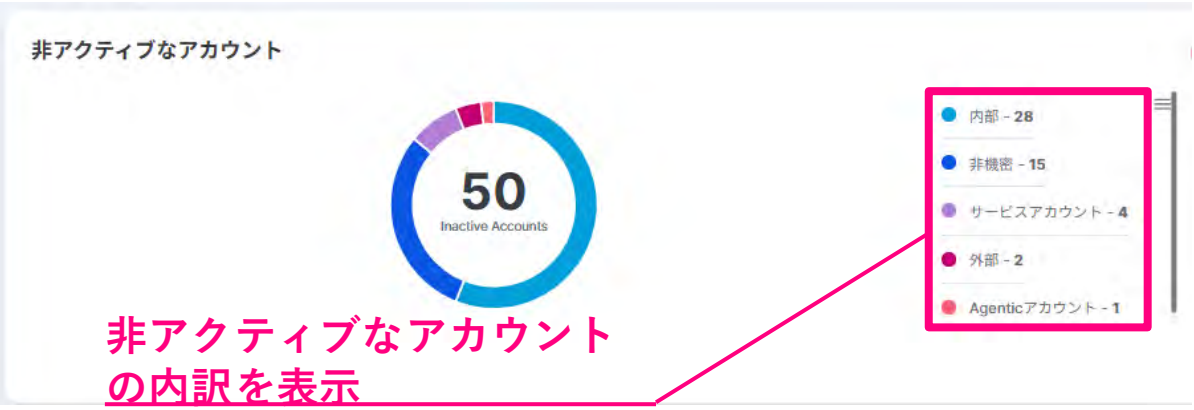
1 多要素認証（MFA）が設定されていないユーザー	0 脆弱なMFAが使用されていた
0 多要素認証（MFA）を設定していない管理者	46 フィッシング対策機能付きMFAを利用していないユーザー

認証強度が低いMFAを用いているユーザー数の表示

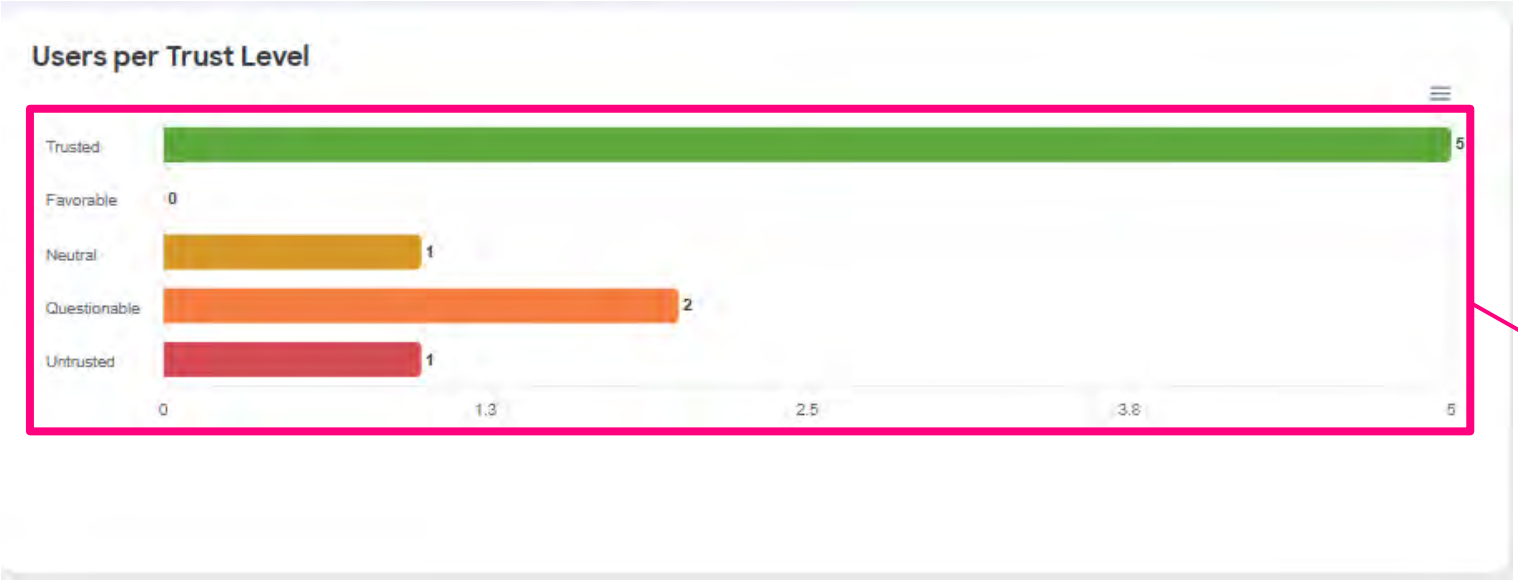
© 2026 Cisco and/or its affiliates. All rights reserved.



アクティブ・非アクティブな
アカウント数を表示



非アクティブなアカウント
の内訳を表示



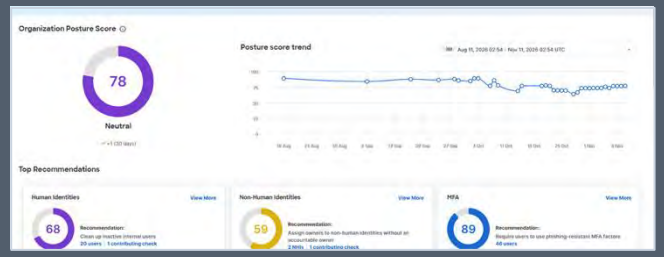
ユーザーの信頼度についても評価

© 2026 Cisco and/or its affiliates. All rights reserved.

連携すると何が分かるか：3つの切り口

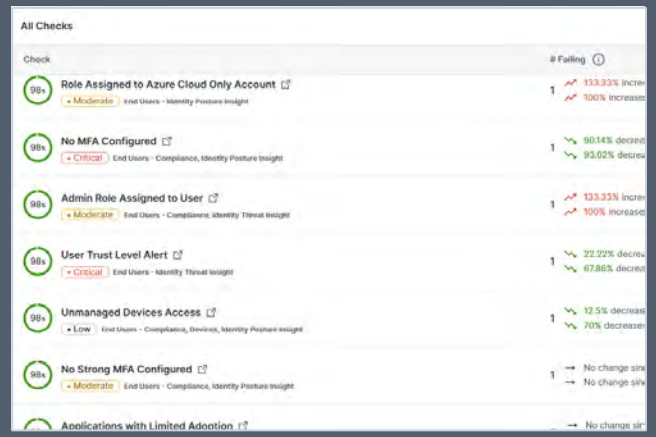
Dashboard で全体 → Checks で弱点 → Users で人物。

1 Dashboard



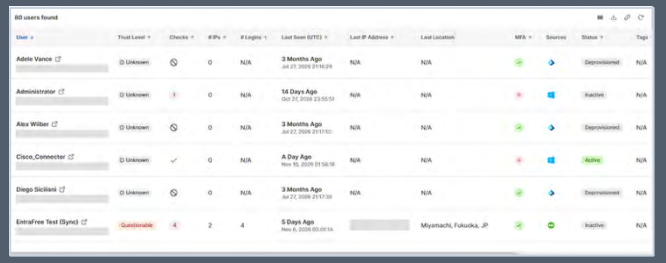
Posture Score と、領域別の推奨。
Human / NHI / MFA の中で、
どこから直すかが分かる

2 Checks



弱点一覧。重大度と該当件数つき

3 Users



人物単位。どの基盤の何の Check に掛かっているか、MFA・信頼度とあわせて確認

ポイント：検知ルールの設定や集計は不要。接続した時点から、基盤をまたいだ同じ画面で確認できます。

© 2026 Cisco and/or its affiliates. All rights reserved.

チェック	# 失敗	# 除外
57% 非アクティブユーザー • 適度 エンドユーザー - コンプライアンス、IDポスチャインス	24 → 先週から変更なし ↘ 15.95% 先月から減少	0
60% 所有者が割り当てられていないNHI • 致命的 非人間的アイデンティティ - アイデンティティ姿勢の洞察、非人間的アイデンティティ、コンプライアンス	2 → 先週から変更なし ↗ 44% 先月からの増加	該当なし
60% 一度もログインしていません • 致命的 エンドユーザー - コンプライアンス、IDポスチャインス	22 ↗ 32.76% 先週から増加 ↗ 111.76% 先月からの増加	0
80% 所有者が削除されたNHI • 致命的 非人間的アイデンティティ - アイデンティティ姿勢の洞察、非人間的アイデンティティ	1 → 先週から変更なし ↗ 63.64% 先月からの増加	該当なし
89% 認証情報を共有するユーザー • 致命的 エンドユーザー - コンプライアンス、IDポスチャインス	6 → 先週から変更なし → 先月から変更なし	0
92% 非人間による認証パスワードの有効期限切れエラー • 適度 エンドユーザー - アイデンティティの姿勢に関する洞察、非人間型アイデンティティ	4 → 先週から変更なし ↗ 63.64% 先月からの増加	0
94% Kerberoastableアカウント • 適度 エンドユーザー - アイデンティティ・ポスチャ・インサイト	3 → 先週から変更なし ↗ 58.82% 先月からの増加	0
94% MFA洪水 • 致命的 エンドユーザー - アイデンティティ脅威インサイト	3 ↘ 8.7% 先週からの減少 ↘ 12.9% 先月から減少	0
94% ユーザー信頼レベルアラート • 致命的 エンドユーザー - アイデンティティ脅威インサイト	3 ↗ 16.67% 先週から増加 ↗ 45.95% 先月からの増加	0

一度もログインしていない
アカウントを検出（ISPM）

MFA洪水攻撃を受けている可能性
のあるアカウントを検知（ITDR）

© 2026 Cisco and/or its affiliates. All rights reserved.

MFAは設定されていません 致命的

推奨される対策を表示

詳細

少なくとも1つの認証ソースで多要素認証（MFA）が有効になっていないユーザーを検出します。

これらのユーザーはデータ漏洩やシステム侵害に対してより脆弱であるため、これらの脆弱性に対処することが極めて重要です。すべてのユーザーはシステムへのアクセスに多要素認証（MFA）を使用する必要があります。

ユーザーが1日間の猶予期間内である場合、またはフェデレーションアカウントを所有している場合は、このチェックに不合格になることはありません。

必要に応じて、カスタム検出設定で新規アカウントの猶予期間を組織の手順に合わせて調整してください。これにより、チェック結果の精度と実用性が向上する可能性があります。

リスクについてさらに詳しく知る



推奨される対策

プライマリIDプロバイダーやMFAプロバイダーではない場合でも、すべてのIDソースでMFAを強制的に有効にしてください。これにより、設定ミスによってユーザーが別のIDソース経由でサインインし、MFAを回避してしまうことを防ぎます。

多要素認証（MFA）の適用除外となる正当な理由があるアカウント、または緩和策が講じられているアカウントを特定します。これらのアカウントは、追跡と検出を容易にするため、外部システムに記録します。

免除対象口座については、一時的な除外措置を適用して不具合を解消し、その後、必要に応じて定期的に口座を見直して状況を評価および更新してください。

最終報告更新
2026年11月17日 18:22:45 UTC

トピック
コンプライアンス、アイデンティティの姿勢に関する洞察

フレームワーク
Miter ATT&CK T1078、Mitre ATT&CK T1110、NIST 800-53 AC-2、NIST 800-63-3、CIS 6.3、CIS 6.4、CIS 6.5、NIST CSF PR.AC-7、ASD Essential 8、CMMC IA.3.083、PCI DSS 8.2、Mitre 緩和策M1032

互換性 最終データ収集
マイクロソフト エントリー ID オクタ デュオ
Google Workspace GitHub

タグ
＋タグを追加

設定を確認する
- カスタム検出設定
- リスト設定
- 通知設定

失敗ユーザー
1
↑ 16.67%（過去7日間）
↓ 87.59%（過去30日間）
ユーザーの1.79%が失敗

統合に失敗したユーザー数
kohnishi-entraid-22c3s5200c - 1
失敗したユーザーの100.00%

タイプ別の失敗ユーザー数
内部 - 1
失敗したユーザーの100.00%

⚠ このチェックに関する自動通知は設定されていません。
このチェックに不合格となったユーザーに関する自動レポートを受け取りたい場合は、通知を設定してください。

1人のユーザーが失敗しました　ユーザーを表示　ダウンロードリスト

ユーザー	優先アカウント	最初に観測された時刻（UTC）	管理者に通知済み	ユーザー/管理者に通知済み
kohnishi-admin@22c3s5200c.onmicrosoft.c...		2026年11月14日 12:58:37	通知なし	1 最新版：2026年11月14日 14:59:02 UTC

除外対象ユーザー
0

保護されていないユーザーが失敗
0

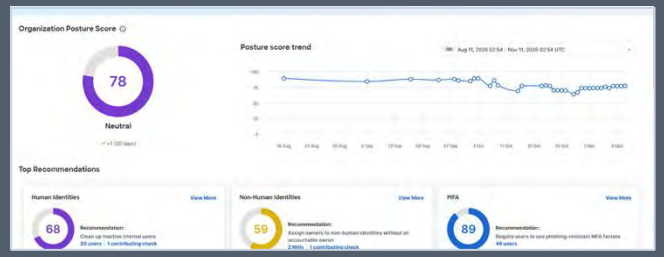
具体的に対象となっている
アカウントを表示

© 2026 Cisco and/or its affiliates. All rights reserved.

連携すると何が分かるか：3つの切り口

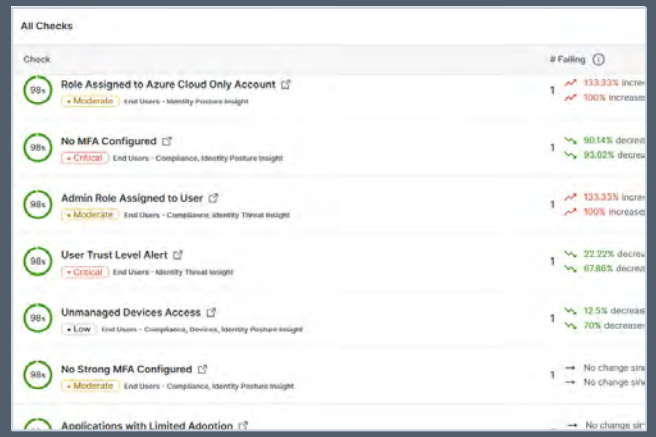
Dashboard で全体 → Checks で弱点 → Users で人物。

1 Dashboard



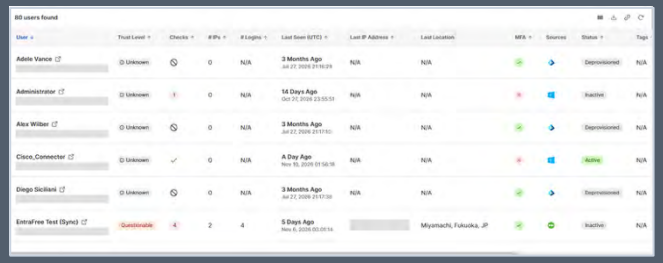
Posture Score と、領域別の推奨。
Human / NHI / MFA の中で、
どこから直すかが分かる

2 Checks



弱点一覧。重大度と該当件数つき

3 Users

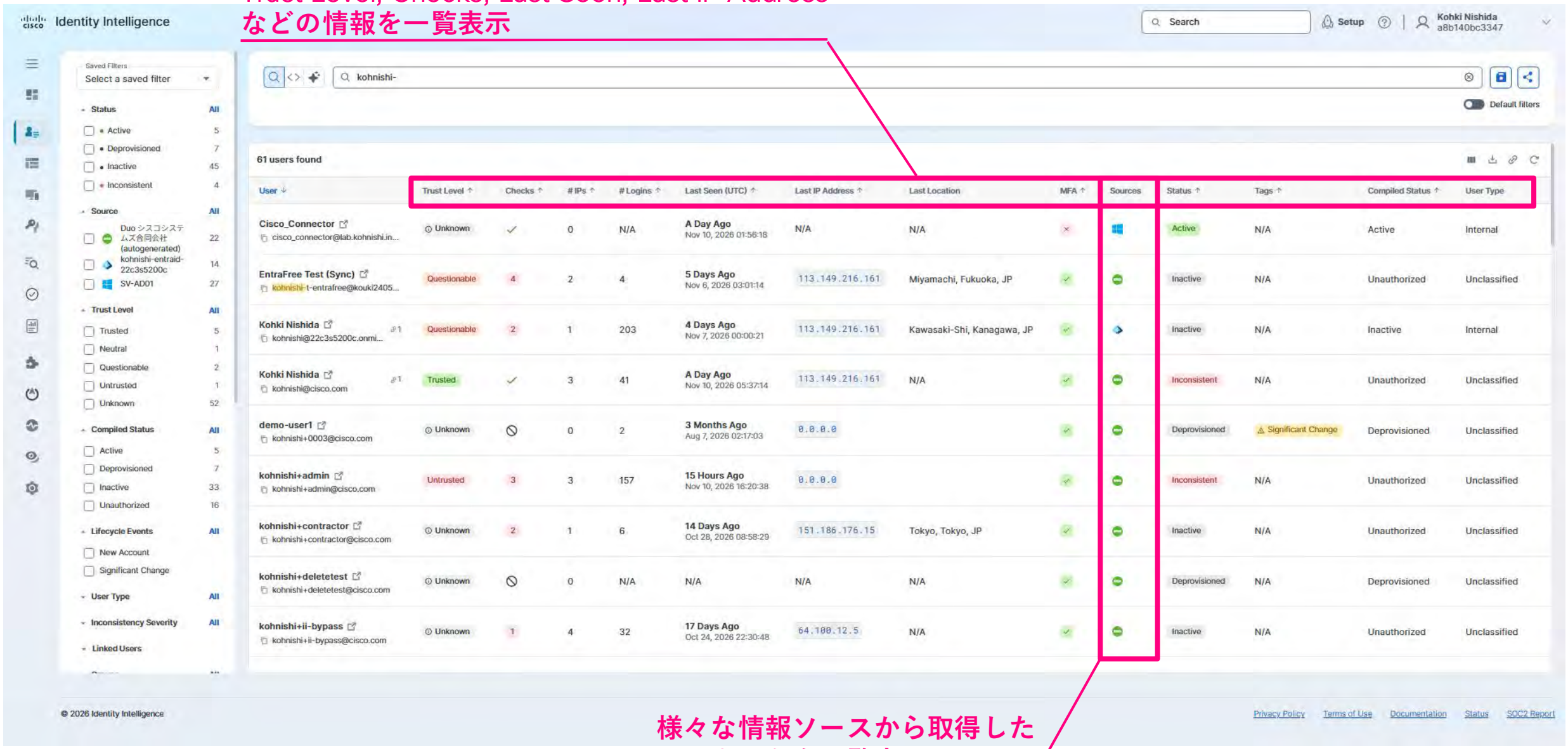


人物単位。どの基盤の何の Check に掛かっているか、MFA・信頼度とあわせて確認

ポイント：検知ルールの設定や集計は不要。接続した時点から、基盤をまたいだ同じ画面で確認できます。

© 2026 Cisco and/or its affiliates. All rights reserved.

Trust Level, Checks, Last Seen, Last IP Address
などの情報を一覧表示



様々な情報ソースから取得した
アカウントを一覧表示

© 2026 Cisco and/or its affiliates. All rights reserved.

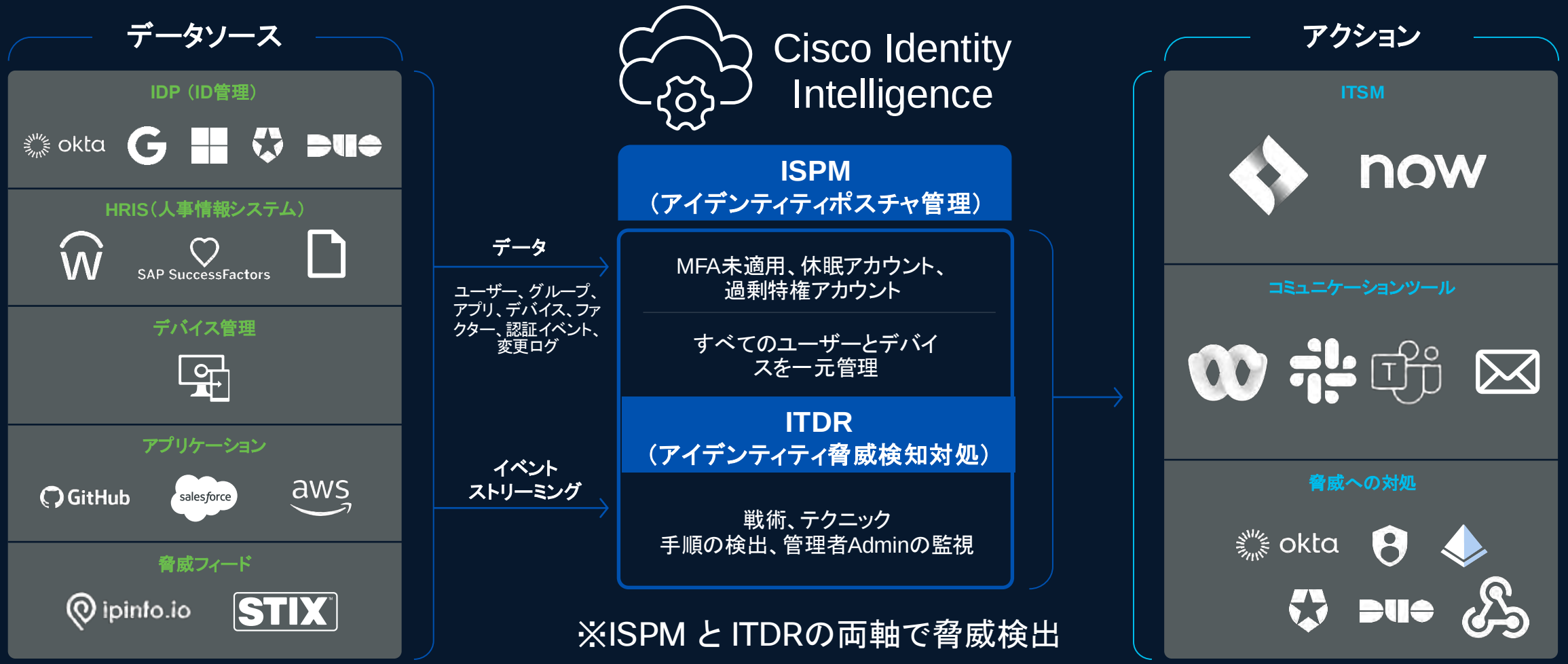
ユーザーの信頼レベルと、その根拠を表示



ログイン履歴、ログイン試行回数を表示

© 2026 Cisco and/or its affiliates. All rights reserved.

既存ID基盤の構成変更なく、Identityのポスチャチェック、脅威検知が可能



© 2026 Cisco and/or its affiliates. All rights reserved.

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



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



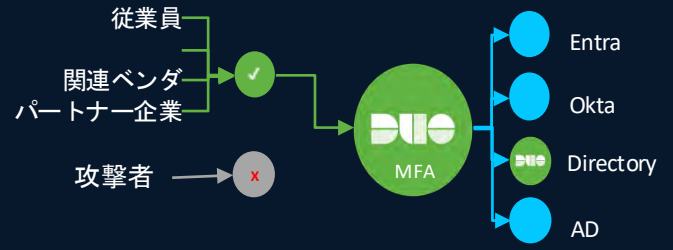
PCの可視化



モバイルの可視化

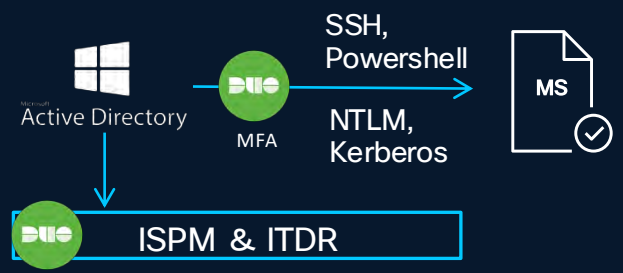
既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤

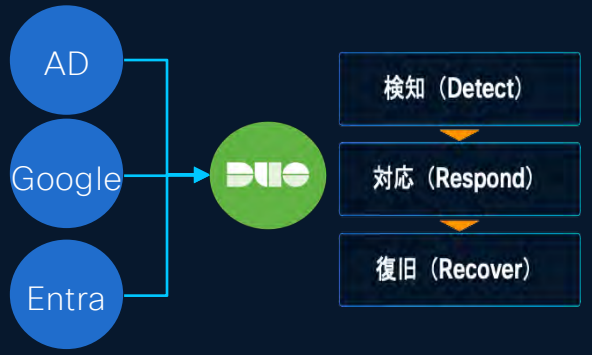


オンプレ環境 Active Directory保護

Active Directoryを標的とした攻撃を阻止



ISPM & ITDR

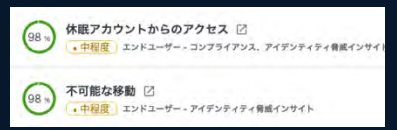


ISPM　アイデンティティの健全性管理



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

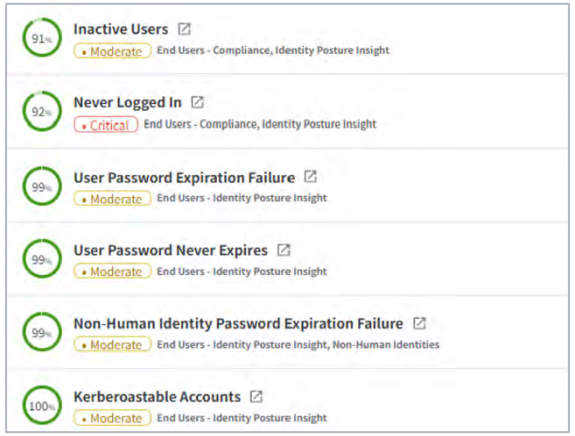


怪しい振る舞いのユーザーを即座に特定・隔離

© 2026 Cisco and/or its affiliates. All rights reserved.

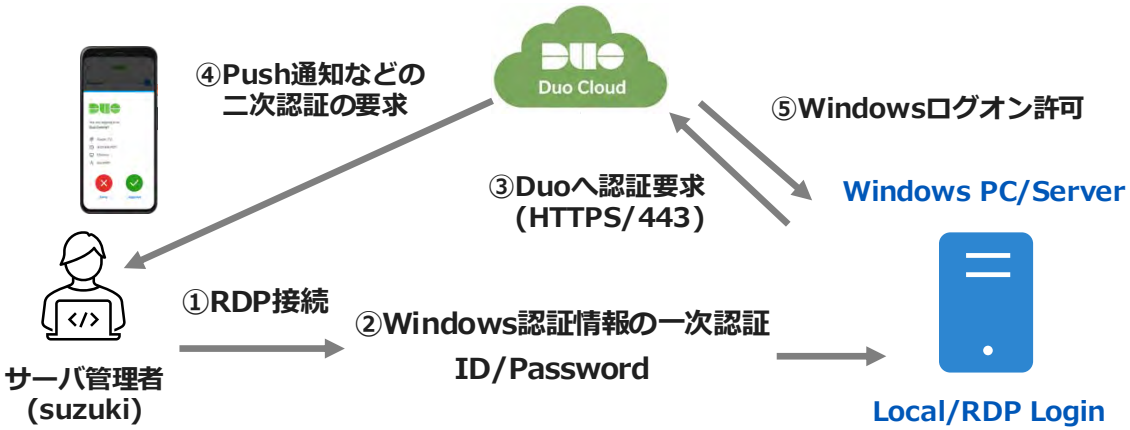
オンプレ環境むけのDuoによるID Security

Active Directoryに存在するIDの可視化とリスク検出

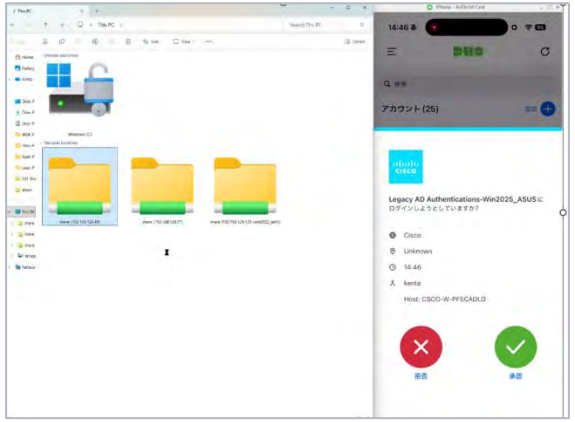


- ✓ Identity Intelligenceと連携して、オンプレミスのActive Directoryの全ユーザー（管理者、ゲスト、サービスアカウントなど）を含むアイデンティティの完全なインベントリを提供
- ✓ 過剰権限や休眠アカウント、Kerberoasting攻撃などのリスクを可視化

Windows Server, Linux向けのRDP時にMFAを実装



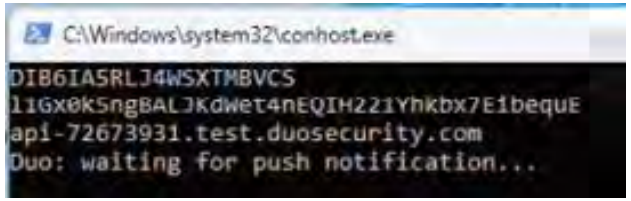
MFAの挿入によるレガシー認証の保護

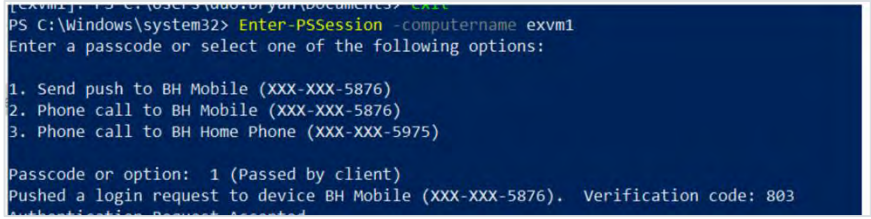


共有フォルダ（NTLM認証）へのアクセス

- ✓ Active Directoryの認証プロトコル（KerberosやNTLM）に対して、MFAをシームレスに挿入し、不正アクセスを防止
- ✓ アプリ側ではなく、ドメインコントローラー（DC）に軽量なフィルターを1つ導入するだけ
- ✓ 特定グループや端末への適用も可能

Windows, Linux Command Line Protection





- ✓ SSHやリモートPowerShellへのログイン時にMFAを適用する機能も提供

© 2025 Cisco and/or its affiliates. All rights reserved.


CISCO