cisco Secure

Duo Day
信用するかしないか、それが重要です！

～Duo で実現するZTNA(Zero Trust Network Access)とは～

Cisco Systems G.K.
Hiroki Hata
Duo Sales Specialist
August.6, 2020

cisco Secure

全米中心に20,000社以上のユーザー Duo Security の価値はどこに？

機能概要とお客様事例のご紹介

Cisco Systems G.K.
Hiroki Hata
Duo Sales Specialist
August.6, 2020

Agenda

- Zero Trust におけるDuoセキュリティの位置付け
- Duoセキュリティ 機能概要
- お客様はなぜDuoを採用するのか?
- まとめ

Zero Trust におけるDuoの位置付け

最新の脅威

今日の進化するアイデンティティ、アプリ、ネットワークへの脅威にリアルタイムで対抗していくため、セキュリティへの新たなアプローチ – Zero Trust - が必要です。

狙われるID/Password

81%の漏洩は搾取されたID /パスワードなどのクレデンシャルによる

狙われるApps

54%ののWebアプリ脆弱性はExploitが公開されている**

狙われる Devices

92% の外部ペネトレーションテストが境界侵入に成功する***

*Verizon Data Breach Investigations Report, 2017
**Imperva, *"The State of Web Application Vulnerabilities in 2018"*, Jan. 9, 2019
***Positive Technologies, *"Penetration testing of corporate information systems: statistics and findings, 2019"* Feb. 6, 2019

シスコゼロトラストアーキテクチャ

シンプル化への道のり:3つの重要な領域におけるシスコゼロトラストアーキテクチャ

ワークフォース

ユーザーとデバイスの信頼を確立して、
アプリケーションへのアクセス権限を決定

ワークプレイス

制御するネットワーク上で、ユーザ/デバイス
およびIoTを含む信頼ベースのアクセス制御
を確立

ワークロード

ワークロードへの権限アクセスを最小限に
抑えながら、攻撃を受ける可能性を最小限
に抑える


ようこそゼロトラストの世界へ

ゼロトラスト
ワークフォース

- 多要素認証 - ユーザの信頼
- デバイス評価 - デバイスの信頼

Duo Security 機能説明

Duo Security が提供する機能

多要素認証によるユーザーの信頼

多要素認証

- 知識要素
- 所有要素
- 生体要素

- ✓ ユーザの認証は瞬時に – ワンタップで承認
- ✓ パスワードに依存しないセキュアなアクセス
- ✓ パスワード漏洩による不正アクセスを防御

端末の信頼性評価

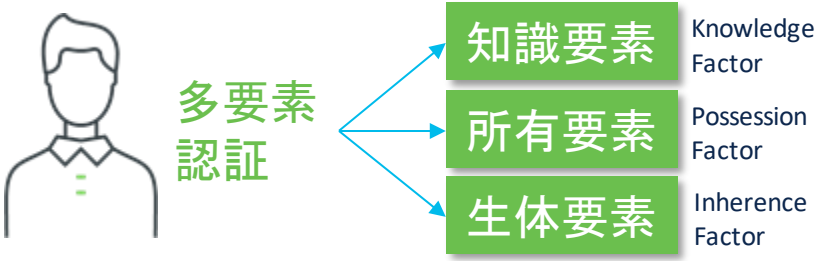
- ✓ 管理デバイスかどうかを検査
- ✓ 危険なデバイスを監視
- ✓ 古いバージョンのOSやブラウザの通知
- ✓ Anti-Virus/Anti-Malwareの検査

多要素認証（MFA）

Duo MFAの認証

ユーザは、既存のプライマリ認証を利用しログイン
(*ユーザが知っているもの*= username + password)

Duo は、ユーザにセカンダリ認証を求める (*ユーザが所有しているもの* = ユーザのスマートフォンのDuo Mobile AppにPush 通知を送信)



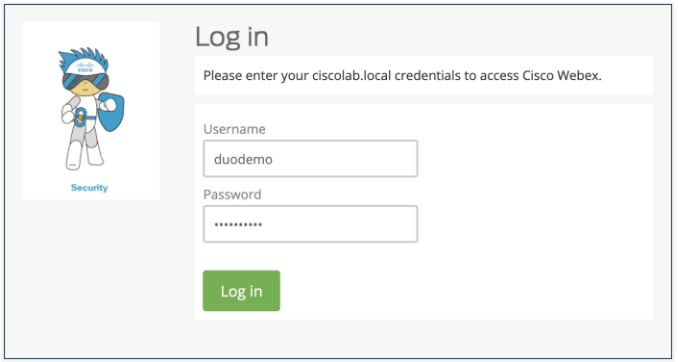
Duo MFAによって

- ✓ アイデンティティベースの攻撃を防ぐ
- ✓ 攻撃者による盗まれたパスワードや侵害されたパスワードの利用を阻止する
- ✓ アプリケーションにゼロトラスト アクセスを提供
- ✓ パスワードのみへの依存度を下げる

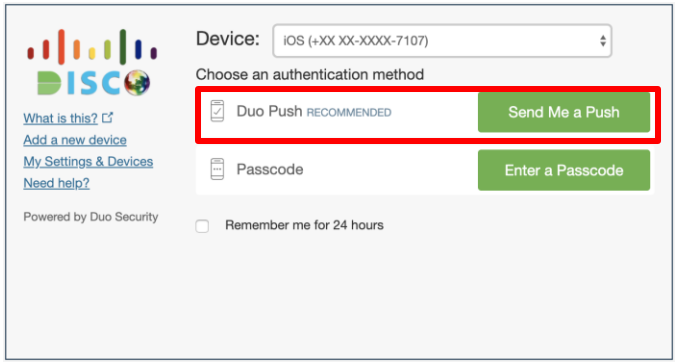
多要素認証の例 - Webexログイン時のSAML認証

1 Webexログイン – メールアドレス入力

2 Duo DAG (SAML IdP) へリダイレクトし、プライマリ認証



3 多要素認証方法選択(Duo Push)



4 Duo Pushで認証

5 Webexログイン成功

あらゆる用途に対応するMFAオプション

認証(MFA)設定
- ユーザグループやアプリケーションごとに　多様なMFAオプションを設定できる
- 容易にユーザ自身でMFAデバイスの追加や削除が可能
  複数MFAデバイス登録可能（認証時に選択可能）

ユーザの使い易さと柔軟性のために複数のオプション（MFAデバイス）を利用可能
- Duo Push 通知
- モバイルパスコード
- 電話へのコール
- SMS
- HOTP トークン
- U2F/WebAuthn（生態認証）
- 緊急時のバイパスコード発行

Duo Mobile

Soft Token

SMS

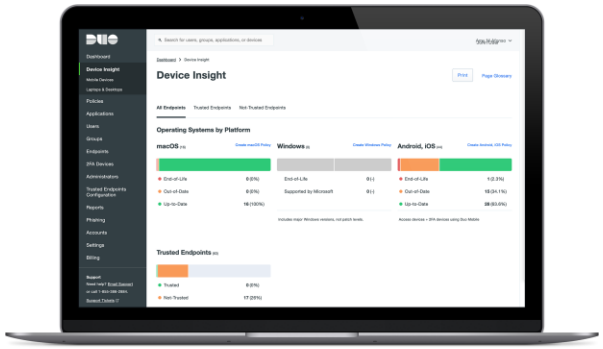

Biometrics


Phone Callback

Hardware Token


U2F Token

デバイスのトラストと可視化



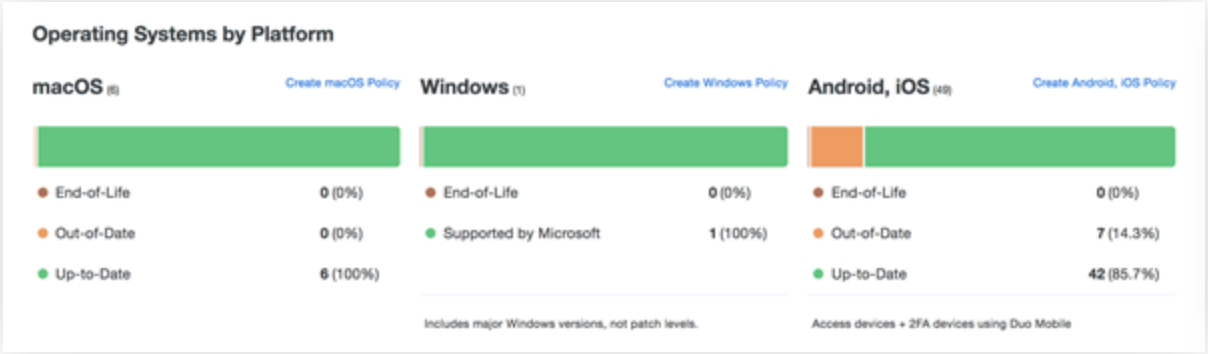
デバイスインサイト（Device insights）

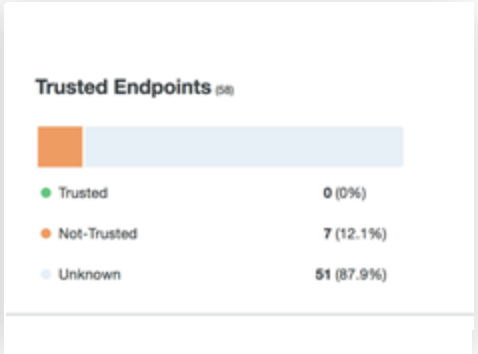
Duo の Unified Endpoint Visibility は、ログイン時にユーザのデバイスを検査（エンドポイントのエージェントインストールは不要）

マネージドあるいはBYOD

Duo の Trusted Endpoints は、デバイスがITによって管理されている場合、エンドポイントマネージメントシステム（Intune, Jamf, AirWatch, Meraki SMなど)と連携して検査

デバイス可視化





モバイルデバイスの可視化

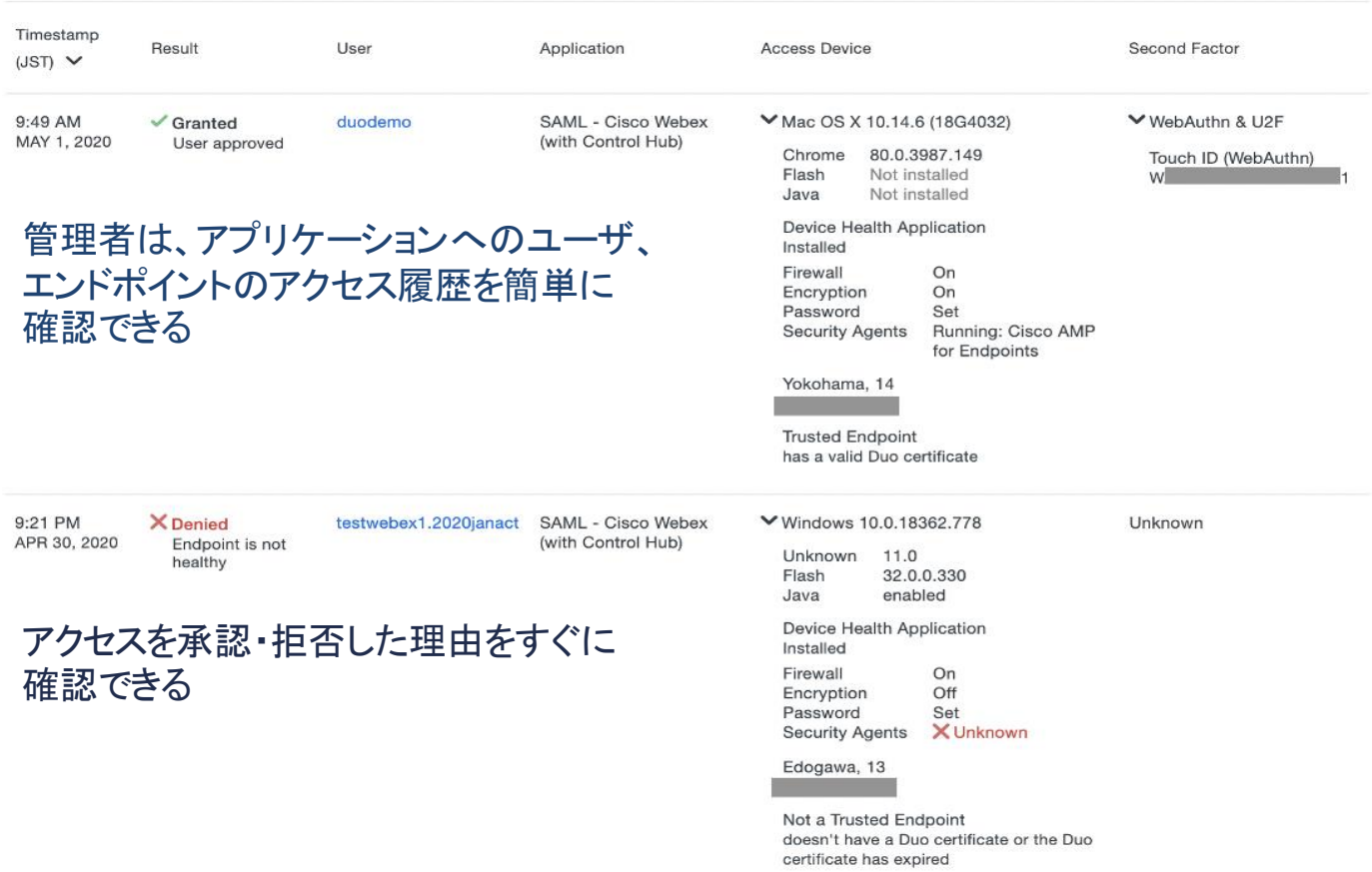
- ✓ コーポレートマネージド 状態
- ✓ バイオメトリックス (指紋/顔認証) 状態
- ✓ スクリーンロック 状態
- ✓ OS コンディション (Tampered) 状態
- ✓ 暗号化 状態
- ✓ プラットフォーム タイプ
- ✓ デバイス OS タイプ & バージョン
- ✓ デバイス オーナー
- ✓ Duo Mobile バージョン

ラップトップ/デスクトップの可視化

- ✓ コーポレートマネージド 状態
- ✓ デバイス オーナー
- ✓ OS タイプ & バージョン
- ✓ ブラウザ タイプ & バージョン
- ✓ Flash & Java プラグイン バージョン
- ✓ OS, ブラウザ, プラグイン 状態
- ✓ ディスク 暗号化
- ✓ Firewall
- ✓ Anti-virus/Anti-malware

cisco Secure

デバイス可視化 – アクセス履歴の確認



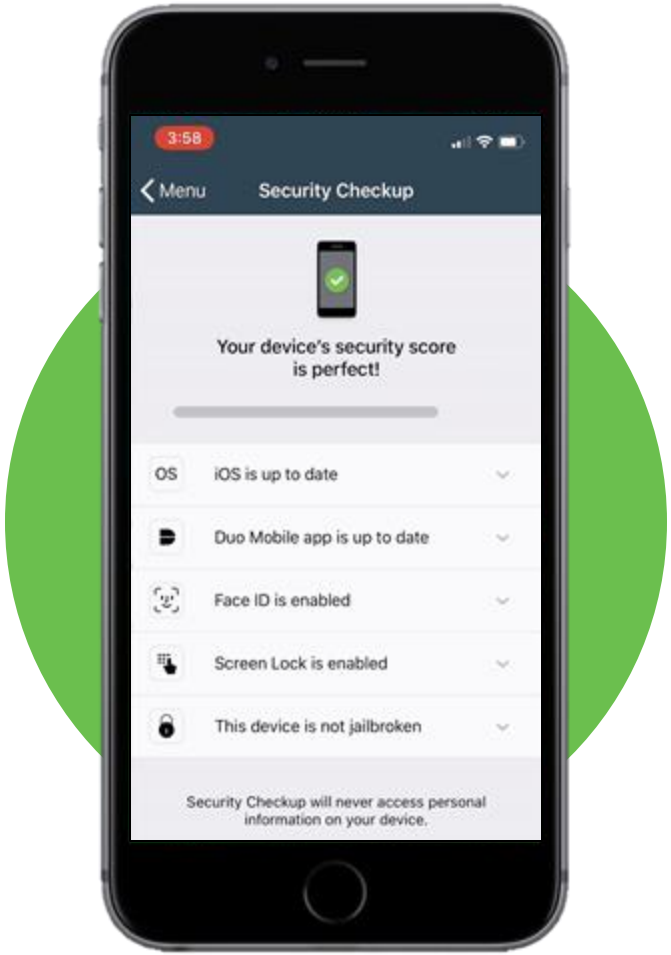
管理者は、アプリケーションへのユーザ、エンドポイントのアクセス履歴を簡単に確認できる

アクセスを承認・拒否した理由をすぐに確認できる

Mobile Device Posture
Duo Mobile アプリケーション

iOS, Android デバイスに対応

- モバイルデバイスのOSが最新かどうかをチェック
- 暗号化されているか、パスコードロック設定されているか確認
- デバイスがJailbreakやRoot化（改ざんされたデバイスか）をチェック
- Managed, Unmanaged のモバイルデバイスに対応



ラップトップ、デスクトップのディープインサイト

Duo Device Health Application:

- Laptop / desktop のセキュリティ健全性確認
- ログイン前にデバイスをチェック
- コーポレート管理、BYODに対応
- Webベースアプリケーションをサポート
- Windows 10 および MacOS
- On-Demandで起動
- AMP for Endpointを含むサードパーティ Anti-Virus/Malwareの検査

適応型ポリシー

カスタマイズ可能なアクセスポリシー（Access Policies）設定により、セキュリティリスクを削減

Role-Based Policy

個々のユーザやグループに基づき、誰がアプリケーションにアクセスできるかを決定するためのポリシーを実行

Device-Based Policy

セキュアで保護されたデバイスあるいはマネージドデバイスのアクセスを許可し、危険なデバイスによるアクセスを防止

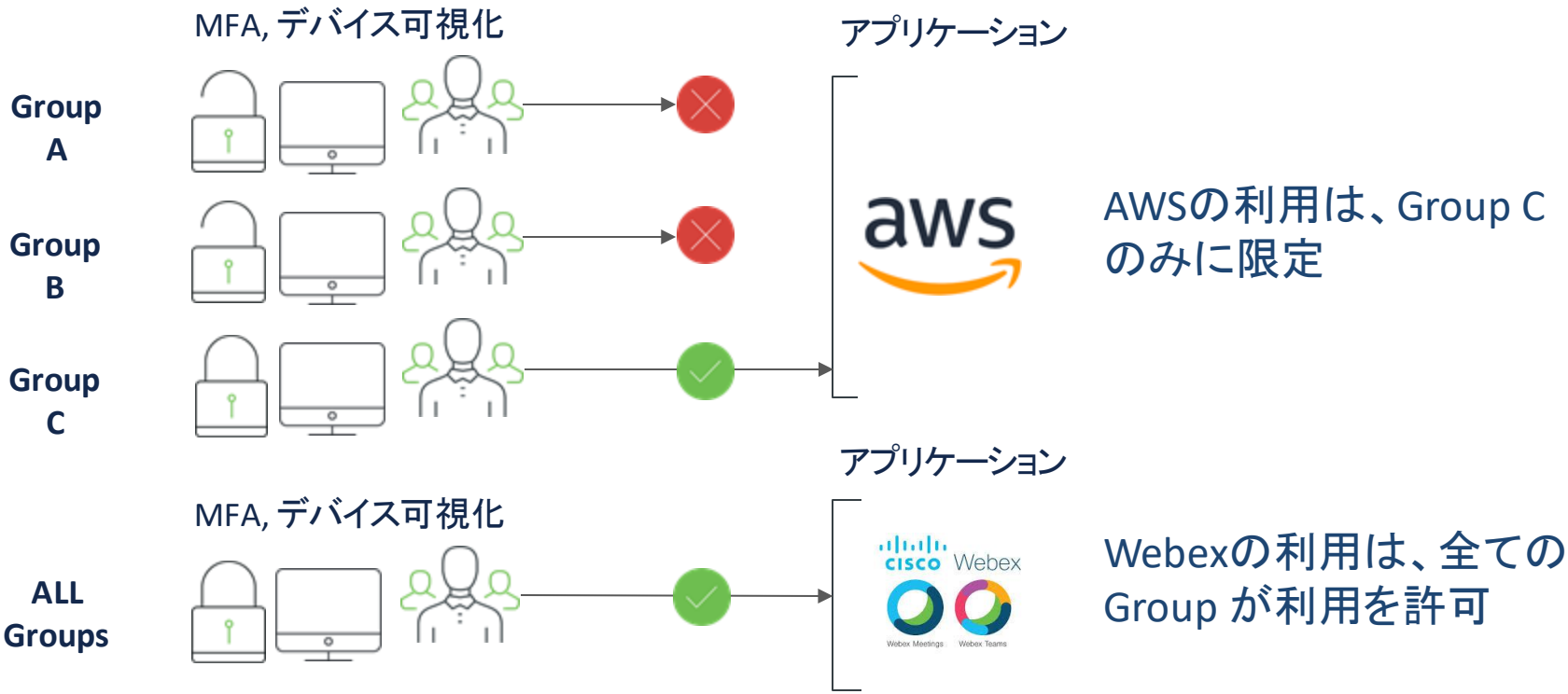
Location-Based Policy

特定のジオロケーションからのアプリケーションへのアクセスを認可あるいは不認可

Network-Based Policy

IPアドレス、サブネットやレンジに基づくアクセスの許可、あるいはTorのような匿名ネットワークからのアクセスを拒否

ポリシー適用例



シンプルなセキュアSSO

ユーザとデバイスの信頼による Duoのシングルサインオン

- 1つのダッシュボードから全ての アプリケーションへ簡単にアクセス
- クラウドアプリケーションを通して 一貫したセキュリティ制御
- 全てのクラウドアプリケーションが セキュアに

連携するアプリケーション（一部）

Microsoft	VPNs	Cloud Apps	On-Premises	SSO	Custom
Office 365	cisco	salesforce	Epic	Microsoft Azure	REST APIS
Outlook	f5	Google Apps	ORACLE PEOPLESOFT	Active Directory Federation Services	WEB SDK
Remote Desktop Services	CITRIX	amazon web services	vmware Horizon View	okta	RADIUS
Windows Server	paloalto NETWORKS	box	>_SSH unix	PingIdentity	SAML
RRAS	Pulse Secure	slack	Shibboleth	onelogin	OIDC

詳細情報: https://duo.com/docs

Duo Securityライセンス

Duo MFA

- 多要素認証
- シングルサインオン（SSO）
- 全てのアプリケーションを保護
- SAML2.0 フェデーレーションクラウドアプリを保護

Duo Access

Duo MFA機能を含む

- 適応型グループベースポリシー制御
- デバイスの可視化
- ユーザベースポリシー
- デバイスベースポリシー

Duo Beyond

Duo Access機能を含む

- 信頼されるエンドポイントの検出
- Duo Network Gateway（リバースプロキシ）
- Anti-Virus/Anti-Malwareの検知

詳細情報: https://www.cisco.com/c/dam/global/ja_jp/products/catalog/pdf/cisco-duo-security-brochure.pdf

機能		Duo MFA	Duo Access	Duo Beyond
ユーザトラスト（多要素認証；MFA）	iOSおよびAndroid向けモバイルアプリ「DuoMobile」のプッシュ通知による認証	●	●	●
	アプリ、SMS、電話着信、ハードウェアトークンによるパスコード認証、生体認証(U2FとWebAuthn)	●	●	●
	電話着信認証およびSMS認証クレジット	●	●	●
	ユーザによる自己登録と自己管理	●	●	●
デバイストラスト（デバイスの可視化）	アプリケーションにアクセスするすべてのデバイスを把握できるダッシュボード	●	●	●
	危険なデバイスを監視および識別		●	●
	ノートPC・デスクトップPCのセキュリティ健全性を可視化（Duoデバイスヘルスアプリケーション）		●	●
	モバイルデバイスのセキュリティ健全性を可視化		●	●
	ノートPCおよびデスクトップPCが企業所有か個人所有か識別			●
	モバイルデバイスが企業所有か個人所有か識別			●
	アンチウイルスやアンチマルウェアなどサードパーティ製エージェントが有効かどうか識別			●
適応型認証/ポリシー	セキュリティポリシーをアプリケーション全体または個別に割り当て	●	●	●
	ネットワークが承認済みかどうかに基づいたポリシー適用	●	●	●
	ユーザの場所に基づいたポリシーを適用		●	●
	ユーザグループ別にセキュリティポリシーを割り当ておよび適用		●	●
	匿名ネットワークをブロック		●	●
	ソフトウェアのサポート期限、暗号化やファイアウォールの有無など、セキュリティ健全性に基づいたノートPCおよびデスクトップPCでのポリシー適用		●	●
	暗号化や改ざん、画面ロック、生体認証の有無など、セキュリティ健全性に基づいたモバイルデバイスでのポリシー適用		●	●
	セキュリティ健全性が低い場合にデバイスを修正するようにユーザに通知		●	●
	エンドポイント管理システムでの登録状況に基づいたデバイスのアプリケーションアクセス制限			●
	MDM登録状況に基づいたモバイルデバイスのアプリケーションアクセス制限			●
シングルサインオン（SSO）とリモートアクセス	無制限でのアプリケーション統合	●	●	●
	すべてのクラウドアプリケーションに対してSSOを提供	●	●	●
	社内Webアプリケーションへ安全にアクセス			●
	SSH経由で特定の社内サーバへ安全にアクセス			●
	AWS、Azure、GCPでホストされているアプリケーションへ安全にアクセス			●

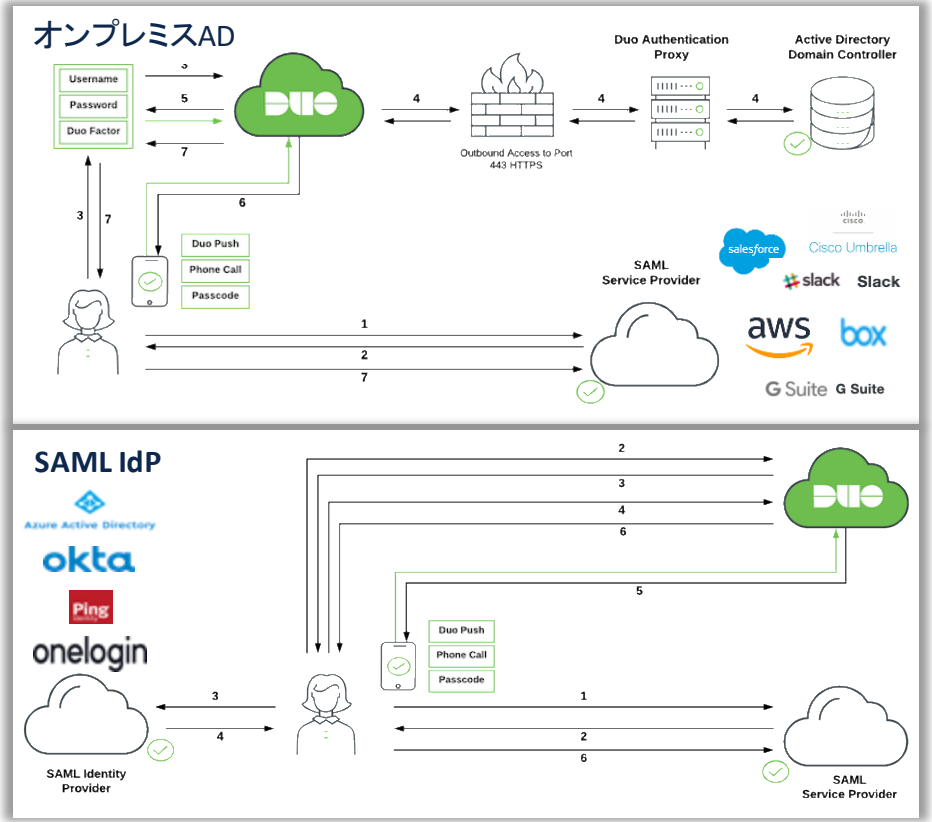
新機能紹介

ベータ

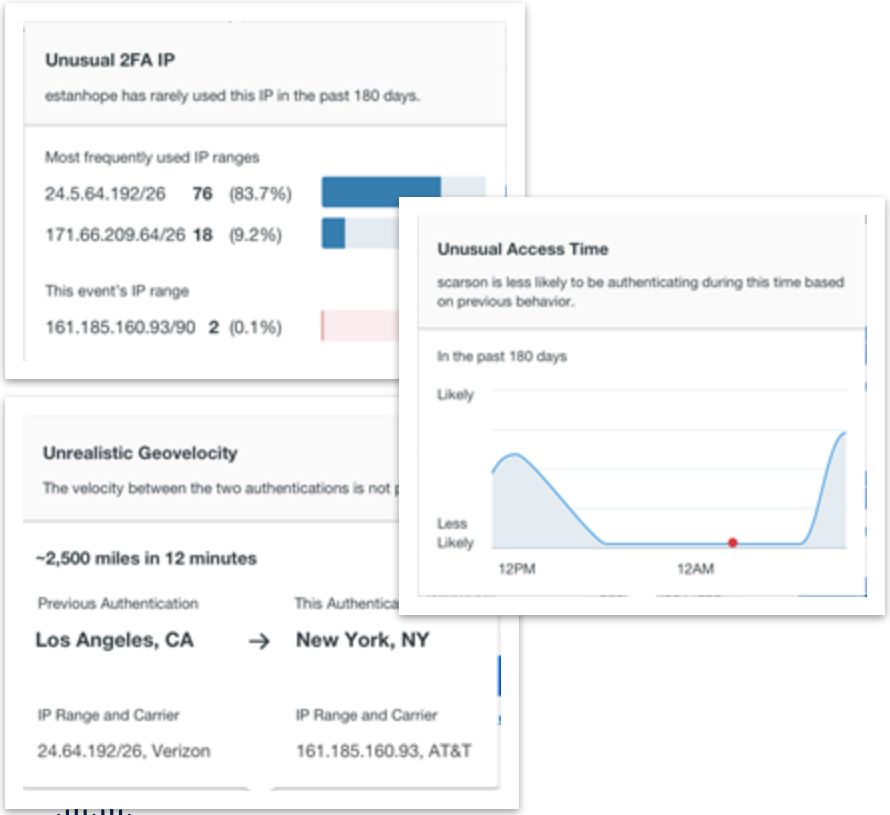
Duo Cloud SSO サポート

- SSO機能提供の拡張

  (Duo Access Gateway or Cloud SSO)
- すぐに、SSOを利用できる
- プライマリ認証のためのオンプレミスADとクラウドベースのSAML IDPの両方を　サポート
- 全てのSAML対応アプリに SSO を提供



Trust Monitor (UEBA)



Duo Trust Monitor は、企業/組織環境でアクセスアクティビティの調整されたベースラインを作成：

- 通常アクセスする**人**
- どの**アプリケーション**
- どの**デバイス**から
- いつ（時間）
- どこから（場所）

Trust Monitor機能により、異常または危険なユーザー認証の試みをハイライトし、アクセスポリシーを修正または更新することができる。

Duo を採用したお客様の声

Over 20,000 Customers

- 3000+ Technology
- 500+ Higher Education
- 600+ Healthcare
- 1500+ Financial Services
- 350+ Government
- 80+ Fortune 500

Duo Security is now part of Cisco.

お客様事例

FINANCIALFORCE

ファイナンシャルフォース様（ソフトウェア開発）

設立：2009年　　従業員数：750人

主業務：SFDC上にPSA及びERPのソフトウェア提供

業務環境：BYOD端末も利用して業務。クラウドベースのシステムを中心に利用。セキュリティを強化するため、PCを暗号化、ウィルス対策ツール、Umbrellaを利用して環境構築

【利用システム】
Salesforce, Google Suite、LucidChart、Docusign等

お客様の課題

・企業のPCから一連の**クラウドアプリケーションへの安全なアクセスを実現**すること

・社員の役割に応じて**きめ細かいアクセスポリシーを提供するSSOを実装**すること

・デバイスの状態を監視し、**OSとブラウザの更新を簡単に要求**できること

改善効果（お客様の声）

•管理するデバイスのみがアプリケーションにアクセスできるようにする**強力なアクセスポリシーを実装**できた

•DuoのSSO内でアプリケーションをグループ化し、**安全かつ簡単なアクセスを実現**できた。

•自己修復ツールにより、新しいバージョンのブラウザーやソフトウェアのリリースされたときの更新までの**時間の測定基準が劇的に改善**された。

お客様事例

レベルワンバンク様（金融）

設立：2007年　従業員数：約200人

環境：新しい金融機関として、小さい企業とともに成長していく環境。常に攻撃対象となっており、一日に数百～数千の攻撃を受けている。BYODの端末を利用しており、より簡単で便利な多要素認証の仕組みを検討していた。

【利用システム】
Office365、社内システム全て等

お客様の課題

・銀行とクライアントのシステムに対して、多くのハッキングの試みを経験しており、**セキュリティを強化し、資金の喪失を止める**必要がある。

・トークンベースの多要素認証を利用していたが、最適な方法ではないと考えており、**より簡単かつ安全な対策を実施する**必要がある。

・BYODを利用しているため、**場所によるアクセス制限とデバイスの可視化をする**必要がある。

改善効果（お客様の声）

•オンラインの脅威から保護し、Duoの2要素認証で**銀行システムを保護すると同時に、BYODポリシーとユーザーおよびデバイスの可視性を実装**できた。

•**場所に基づいたアクセスポリシーを設定**できた。また、DuoPushにより、長いパスワードを覚えなくて良く、**より簡単なアクセスを実現**できた。

•**簡単に登録作業が完了でき、簡単に開始できた**。サポートの対応が良く、**導入から稼働後までしっかりとしたサポート**が受けられている。

•最も重要な**Microsoftアプリケーションにさらに多くのアクセス制限を適用**している。

お客様事例

バランス様（農業用肥料製造・販売）

設立：2001年　従業員数：約690人

幅広い範囲の農業用肥料製品及び農場システムソフトウェアの製造および販売。企業ファミリーには異なる設備、製品、サービスのため複数の部門があり、製品と設備は、製造プラントからソフトウェアをサポートするIT環境まで多岐にわたる

【利用システム】
Office365、NetScaler、Palo Alto等

お客様の課題

・リモートユーザのアクセス制限と可視化ができていなかったため、**ユーザ及びデバイスの可視化が必要**。

・ファイアウォールとOffice365の分析結果から、**会社はリスクにさらされており、脆弱性があることが確認され、対策が必要**

・ADFSの分析結果から、世界各国からブルートフォースがあり、ブロックされていることが確認され、**ユーザのクレデンシャルを守る必要**がある。

改善効果（お客様の声）

•他のMFAソリューションを実装して比較検討した結果、**Duoが圧倒的に使いやすい**との評価となった。

•ビジネスに必要な**きめ細かいポリシーの作成とコントロールが可能**になった。請負業者のBYODデバイスのタイプ別のアクセスやユーザ別のアクセスを実現できた。

•Duoが**様々なソリューション（NetScaler、Palo Alto等）の保護に使用できる**ことは、ポジティブな差別化要因だった。

•ゼロトラストを達成することは不可能に思えるかもしれないが、**Duoはゼロトラストの道のり示してくれた**。

お客様事例

デューク大学様（教育）

Duke University

設立：1838年

従業員数：約8,800人　学生数：14,850人

大学のシステムには、行動やニーズが異なる 54,000 人を超えるユーザがアクセスする。その環境下で安全かつ柔軟な多要素認証を検討していた

【利用システム】
OWA、RDP、VMWare、Shibboleth、リモートデスクトップ、等

お客様の課題

・ハッキング事件によるコストが約3,500万ドルと見積もられ、**セキュリティ対策が急務**　（2015年、教員がフィッシング攻撃され、10人の給与が攻撃者の口座へ送金）

・侵害された可能性がある**アカウントの検出を強化する**

・IT チームが管理している**システムにアクセスするための手順を増やさない**

改善効果（お客様の声）

•Duoを採用するにあたっては、何を統合できるか、またどのようにコミュニティがそれを使用できるかという点で、この**テクノロジの柔軟性が重要**でした。（CISO）

•IT部門とセキュリティ部門が連携して、**多要素認証（Duo）の環境とフィッシング攻撃に騙されないための教育をすることで、セキュリティ強化**を実現

•既存の**VPN、インフラ、リモートアクセス、SSOの環境と連携して多要素認証を実現**

•認証に3秒～5秒を追加することだけで、**攻撃者からのハッキングを心配する必要がなくなった**

Duo を採用したお客様の声（提供価値）

簡単に利用できる

*“Our clinicians **loved the simplicity** of Duo Push to their phone or smartwatch to approve prescriptions.”*
Dr. CT Lin, CMIO

uchealth

TCOを削減できる

CONNECTRIA HOSTING

*“We have reduced the number of help desk requests by **more than 75%** since deploying Duo’s MFA.”*
Steve Grzybinski, Dir. of Security

大人数・豊富なアプリへ柔軟に対応できる

*“We have **over 300K employees** enrolled with Duo accessing hundreds of apps. It has been one of the most successful projects at Ohio State.”*
Helen Patton, CISO

THE OHIO STATE UNIVERSITY

すぐに開始できる

Anchorage School District

*“We went from identifying a solution to users authenticating with Duo in **less than 1 week**. From start to finish, the entire process was incredibly easy.”*
Mike Fleckenstein, CIO

まとめ

まとめ

- Duoは各アクセスにプライマリー認証と切り離した2要素目の認証を提供し、デバイス検疫も同時に提供：Zero trust
- Duoはユーザ及び管理者の双方にとって、シンプルで簡単に利用でき、短期間に開始可能（提供価値）
- Duoは多くのお客様がTrialにてDuoの機能を体感してから本格導入を検討。まずはTrialをご検討ください！
- Duoはセキュリティを強化し、組織に安心とシンプルさを提供することで、スピードのある組織を作ることが目標

Duoの情報

- Duoのトライアル（Duo Accessライセンスで30日間）
  - https://www.cisco.com/c/m/ja_jp/duo/trial.html

- Duo アプリケーション連携・構築マニュアル
  - https://duo.com/docs

- Duo demo サイト
  - https://demo.duo.com/


cisco
Secure