cisco Secure

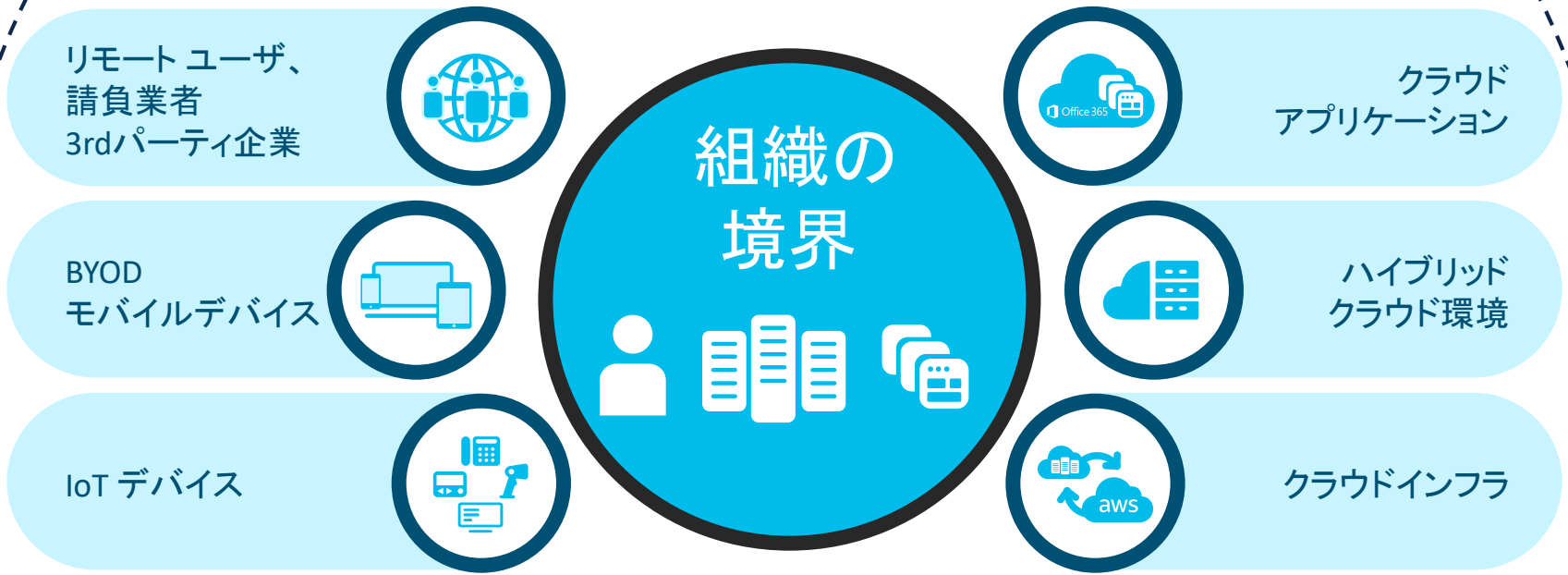
30分でわかる最新の多要素認証

Duo Securityで、セキュアなリモートワーク

村上　英樹
Duo セキュリティ コンサルティングシステムズエンジニア
2020年6月4日

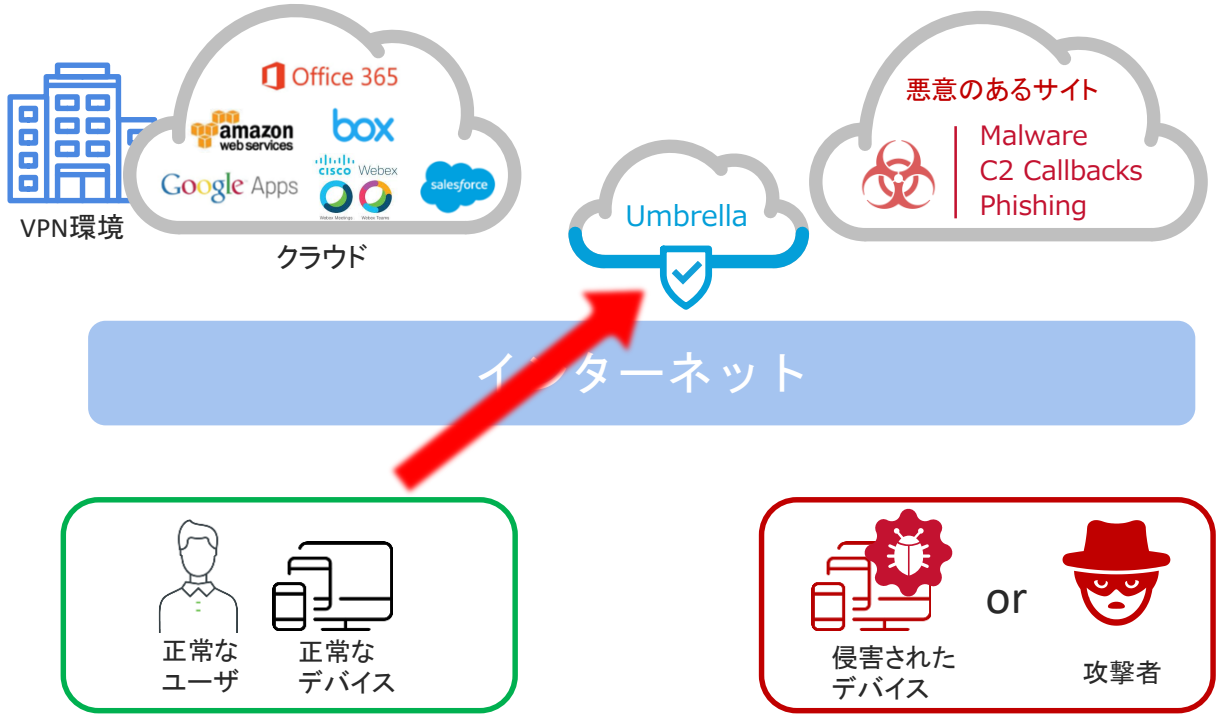
デジタル化によって起こるIT環境の変化

- あらゆる場所にあるユーザ、デバイス、アプリケーション



企業境界の拡大による、脅威と複雑性の増大に直面している

悪意のあるサイトへの誘導は、Umbrellaで防御



Umbrella
正常なユーザとデバイスが、悪意のあるサイト（Malware/C2/Phishing）へ誘導されのをDNSレイヤおよびWebプロキシで防御する。

盗んだパスワードを使った攻撃や侵害されたデバイスからのアクセスは、Duoで防御

Duo Security
フィッシングやクラッキングで盗んだクレデンシャルを利用した攻撃者やマルウェアに侵害されたデバイスがVPN接続やクラウド環境に侵入することを防御する。

テレワーク(オンライン授業)のセキュリティ対策

テレワークを行う際のセキュリティ上の注意事項

掲載日：2020年 4月 21日
独立行政法人情報処理推進機構
セキュリティセンター

1. はじめに

新型コロナウイルス感染症(COVID-19)の影響により、ICTを用いて自宅でも業務が行えるような環境を整えて、社員等を出社させずに事業継続を図る動きが急速に進んでいます。このような環境で働くテレワーク勤務者に向けたセキュリティ上の注意事項をご案内します。

テレワークには様々な利用環境があります。代表的なのは、自宅のパソコン等を用いてリモートデスクトップや仮想デスクトップで社内での業務用端末と同じ利用環境（テレワーク環境）を実現する方法です。

一方でそのような本格的な環境が提供されていない状況で自宅勤務を実施されている場合もあると思います。このページでは、そのような場合における注意事項も説明します。

https://www.ipa.go.jp/security/announce/telework.html

警視庁　安全な暮らし　交通安全　相談・お悩み　手続き

トップページ → 安全な暮らし → 情報セキュリティ広場 → 注目情報 → テレワーク勤務のサイバーセキュリ

テレワーク勤務のサイバーセキュリティ対策！

更新日：2020年4月16日

テレワークで勤務をされる方へ

サイバーセキュリティ対策

テレワークで使用するパソコン等（タブレット、スマートフォン）

サポートが終了しているOS（オペレーティングシステム）のパソコンを使用しない。

Windows7、WindowsVista、WindowsXPは、すでに脆弱性等に対するサポートがされていないため、マルウェア（ウイルス）に感染するリスクが高くなります。

ウイルス対策ソフトを必ず導入する。

マルウェア（ウイルス）の感染防止のために必ず導入しましょう。

https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/telework.html

National Security Agency | Cybersecurity Information

Selecting and Safely Using Collaboration Services for Telework

Criteria to Consider When Selecting a Collaboration Service

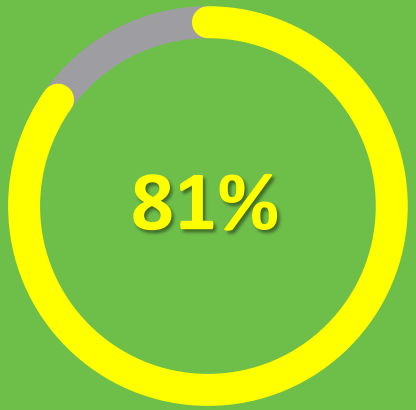
1. Does the service implement end-to-end encryption?
2. Are strong, well-known, testable encryption standards used?
3. Is multi-factor authentication (MFA) used to validate users' identities?
4. Can users see and control who connects to collaboration sessions?

https://media.defense.gov/2020/Apr/24/2002288653/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-SHORT-FINAL.PDF

現実の脅威：不正侵入は、ID/パスワード漏洩から
セキュリティの新しいアプローチが必要とされる

Targeting Identity

81%のハッキングによる侵害は、パスワード漏洩や弱いパスワードなど、クレデンシャルに関連している
*2017 Verizon Data Breach Investigations Report



Duo Security による最新の認証方法

- 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 が提供する機能

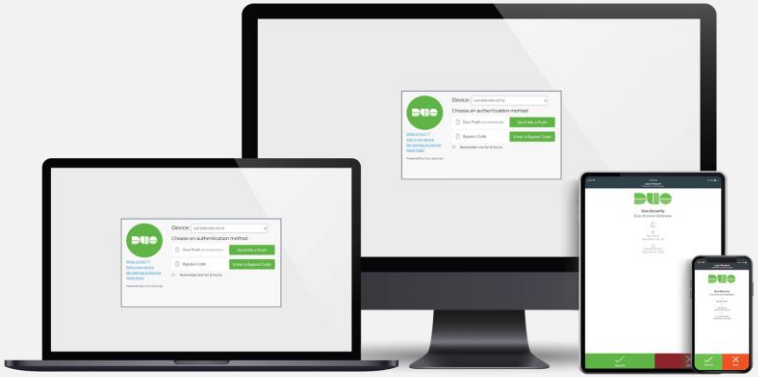
多要素認証によるユーザーの信頼

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



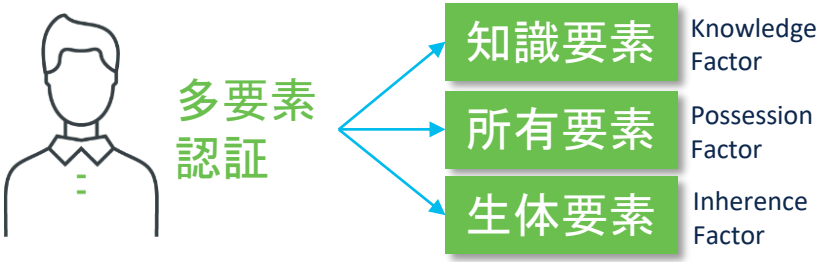
- ✓ デバイス可視化
- ✓ 危険なデバイスを監視
- ✓ 古いバージョンのOSやブラウザの通知
- ✓ Anti-Virus/Anti-Malwareの検査

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)



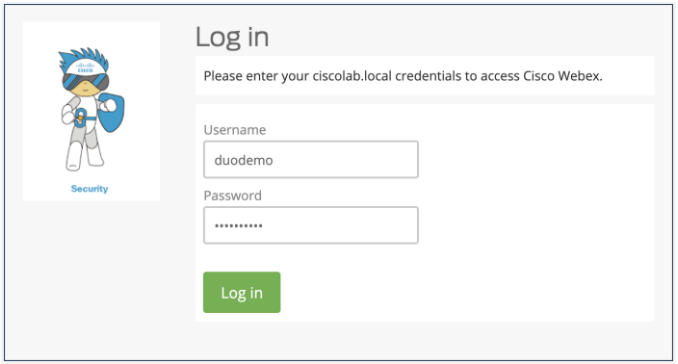
Duo MFAによって

- ✓ 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

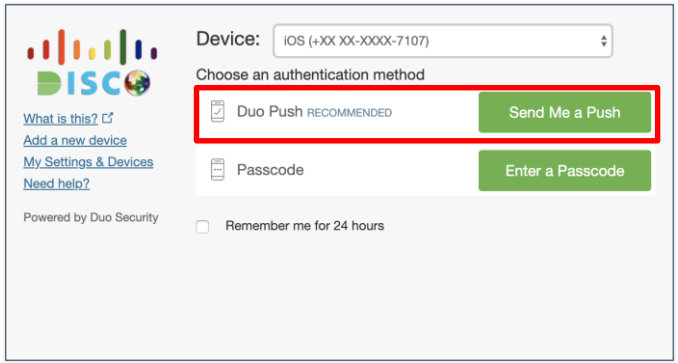
多要素認証の例 - Webexログイン時のSAML認証

1 Webexログイン – メールアドレス入力

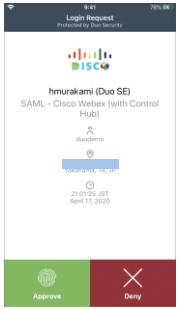
2 Duo DAG (SAML IdP) へリダイレクトし、プライマリ認証



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

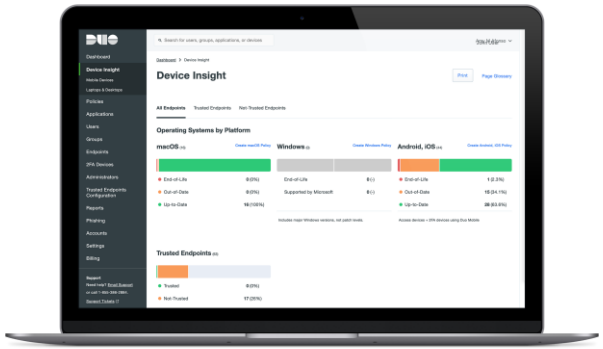

Biometrics


Phone Callback

Hardware Token


U2F Token

デバイスのトラストと可視化



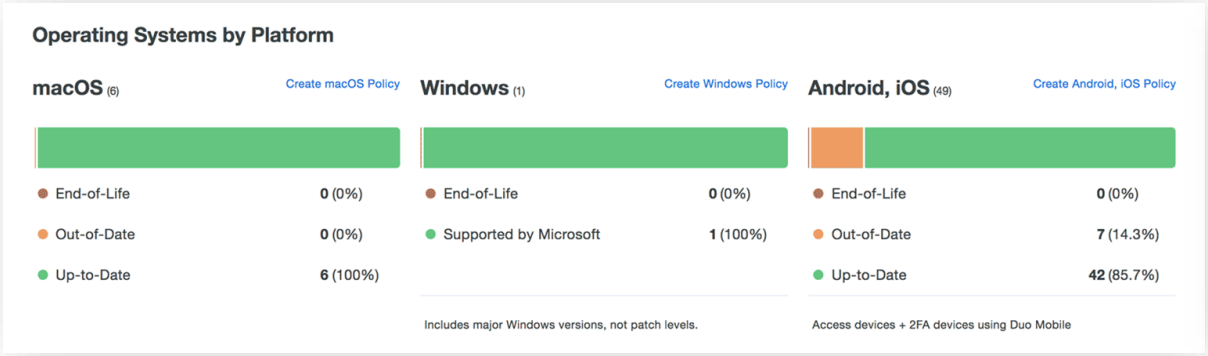
デバイスインサイト

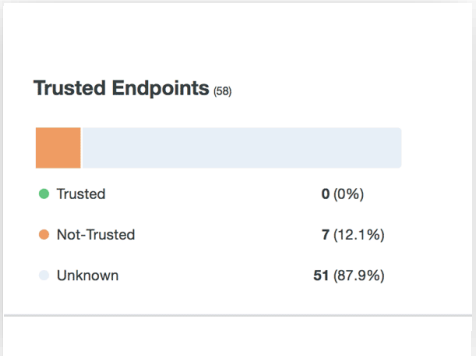
Duo の Unified Endpoint Visibility は、ログイン時にユーザのデバイスを検査（エンドポイントのエージェントインストールは不要）

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

- 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
- Out-of-date/End-of-life デバイスを迅速に識別できる

OS	Browsers	Security Warnings	User	Last Used (JST)	Trusted Endpoint
Windows 10.0.17134.1365	IE 11.0 Flash 32.0.0.330 Java enabled Firefox 75.0	Windows end-of-life	testwebex1.2020janact	Apr 30, 2020 9:13 PM	No
Windows 10.0.17134.1365	Chrome 80.0.3987.163	encryption disabled Windows end-of-life Chrome out-of-date	duodemo	Apr 14, 2020 1:06 AM	No
Windows 10.0.17134.1365	Firefox 75.0	Windows end-of-life	testwebex2.2020febact	Apr 14, 2020 11:30 AM	No
Windows 7	Chrome 77.0.3865.120	Windows end-of-life Chrome out-of-date	duodemo	Apr 15, 2020 10:55 PM	No

Timestamp (JST)	Result	User	Application	Access Device	Second Factor
9:49 AM MAY 1, 2020	Granted User approved	duodemo	SAML - Cisco Webex (with Control Hub)	Mac OS X 10.14.6 (18G4032) Chrome 80.0.3987.149 Flash Not installed Java Not installed Device Health Application Installed Firewall On Encryption On Password Set Security Agents Running: Cisco AMP for Endpoints Yokohama, 14 [redacted] Trusted Endpoint has a valid Duo certificate	WebAuthn & U2F Touch ID (WebAuthn) W[redacted]1
9:23 PM APR 30, 2020	Denied Device health data is missing	testwebex1.2020janact	SAML - Cisco Webex (with Control Hub)	Windows 10 Unknown 11.0 Flash 32.0.0.330 Java enabled Device Health Application Installation status unknown Firewall Unknown Encryption Unknown Password Unknown Security Agents Unknown Edogawa, 13 [redacted] Not a Trusted Endpoint doesn't have a Duo certificate or the Duo certificate has expired	Unknown
9:21 PM APR 30, 2020	Denied Endpoint is not healthy	testwebex1.2020janact	SAML - Cisco Webex (with Control Hub)	Windows 10.0.18362.778 Unknown 11.0 Flash 32.0.0.330 Java enabled Device Health Application Installed Firewall On Encryption Off Password Set Security Agents Unknown Edogawa, 13 [redacted] Not a Trusted Endpoint doesn't have a Duo certificate or the Duo certificate has expired	Unknown

適応型ポリシー

カスタマイズ可能なアクセスポリシー設定により、セキュリティリスクを削減

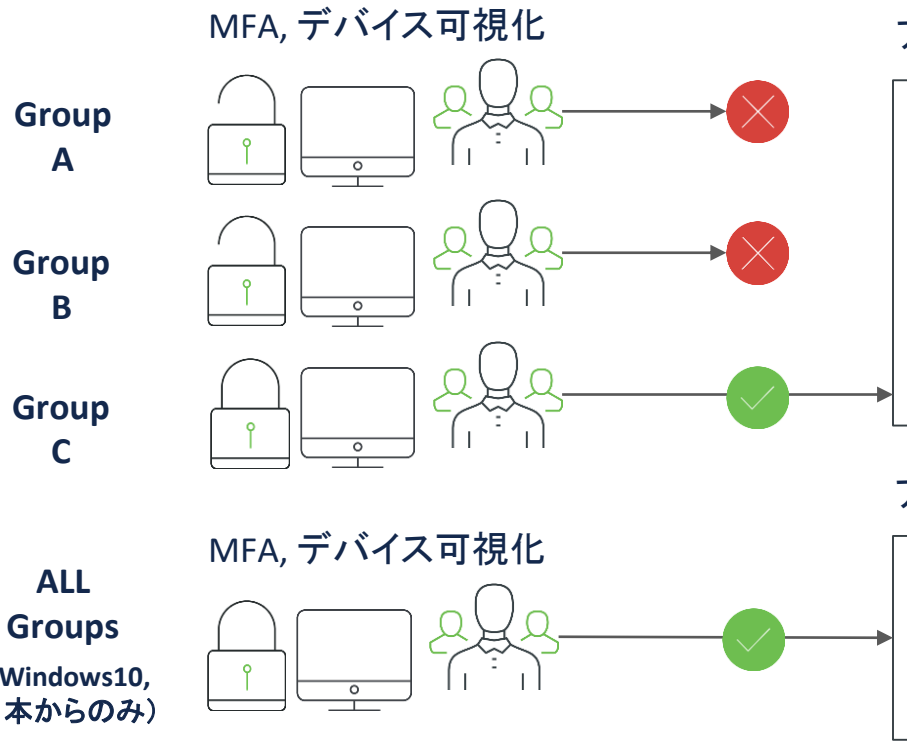
Role-Based Policy
個々のユーザやグループに基づき、誰がアプリケーションにアクセスできるかを決定するためのポリシーを実行

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



AWSの利用は、Group C のみに限定

Webexの利用は、全ての Group が利用を許可
（ただし、Win10で日本からのみアクセス可能）

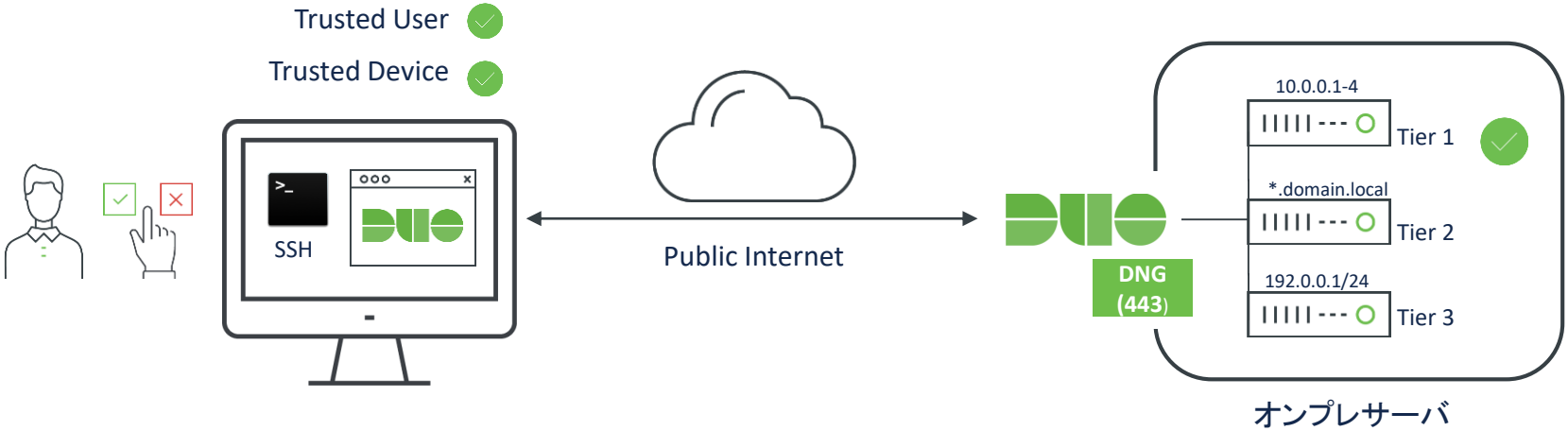
シンプルなセキュアSSO

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

Duo Network Gateway: リバースプロキシ

VPNレスによる内部HTTP/S と SSH サーバへのゼロトラスト アクセス



内部ネットワークとパブリッククラウドへのアクセスをセキュアにするために、
Duo Beyond (Duo Network Gateway) を利用する

amazon web services™ Google Cloud Platform Microsoft Azure

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

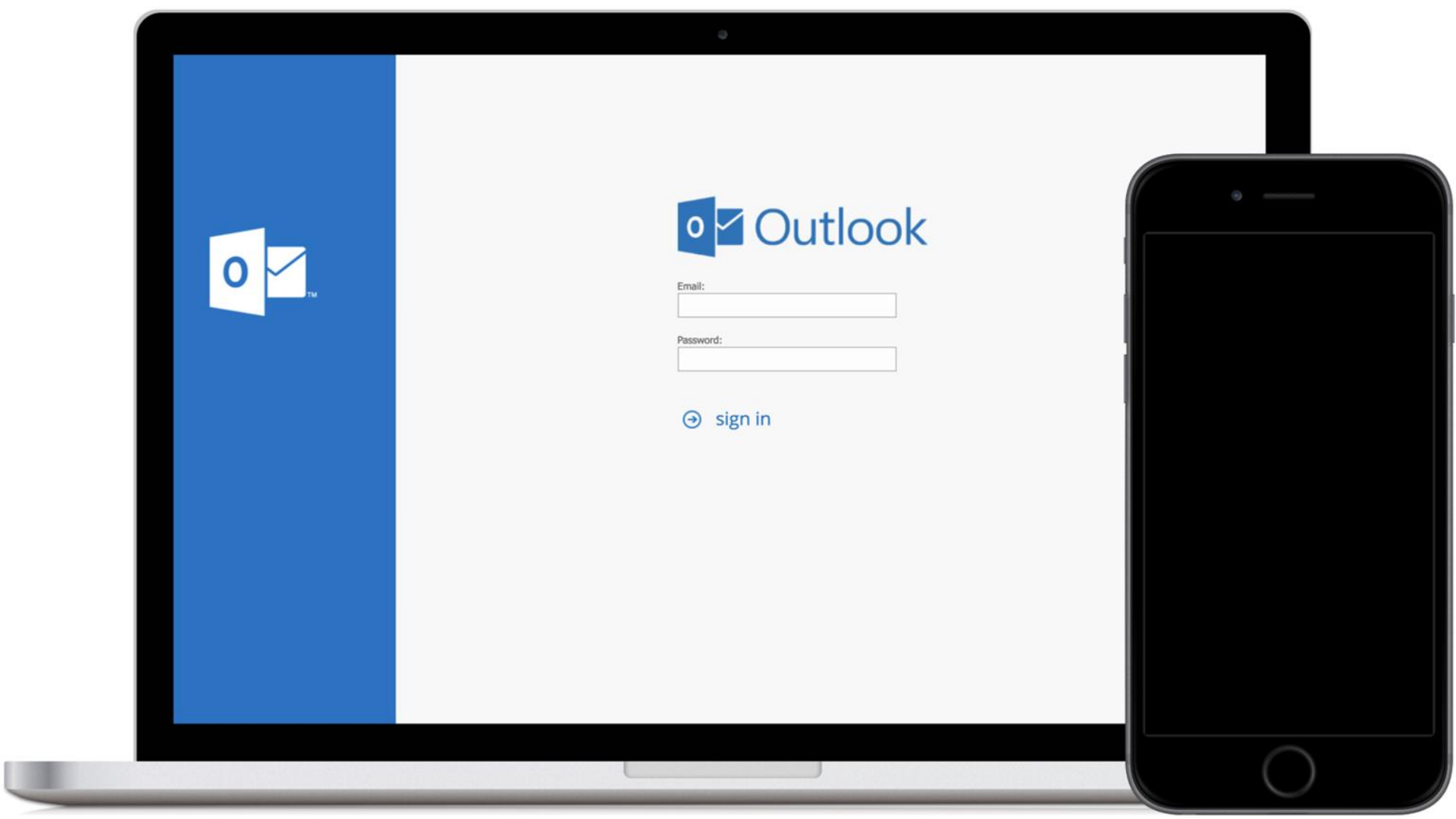
Duo Beyond

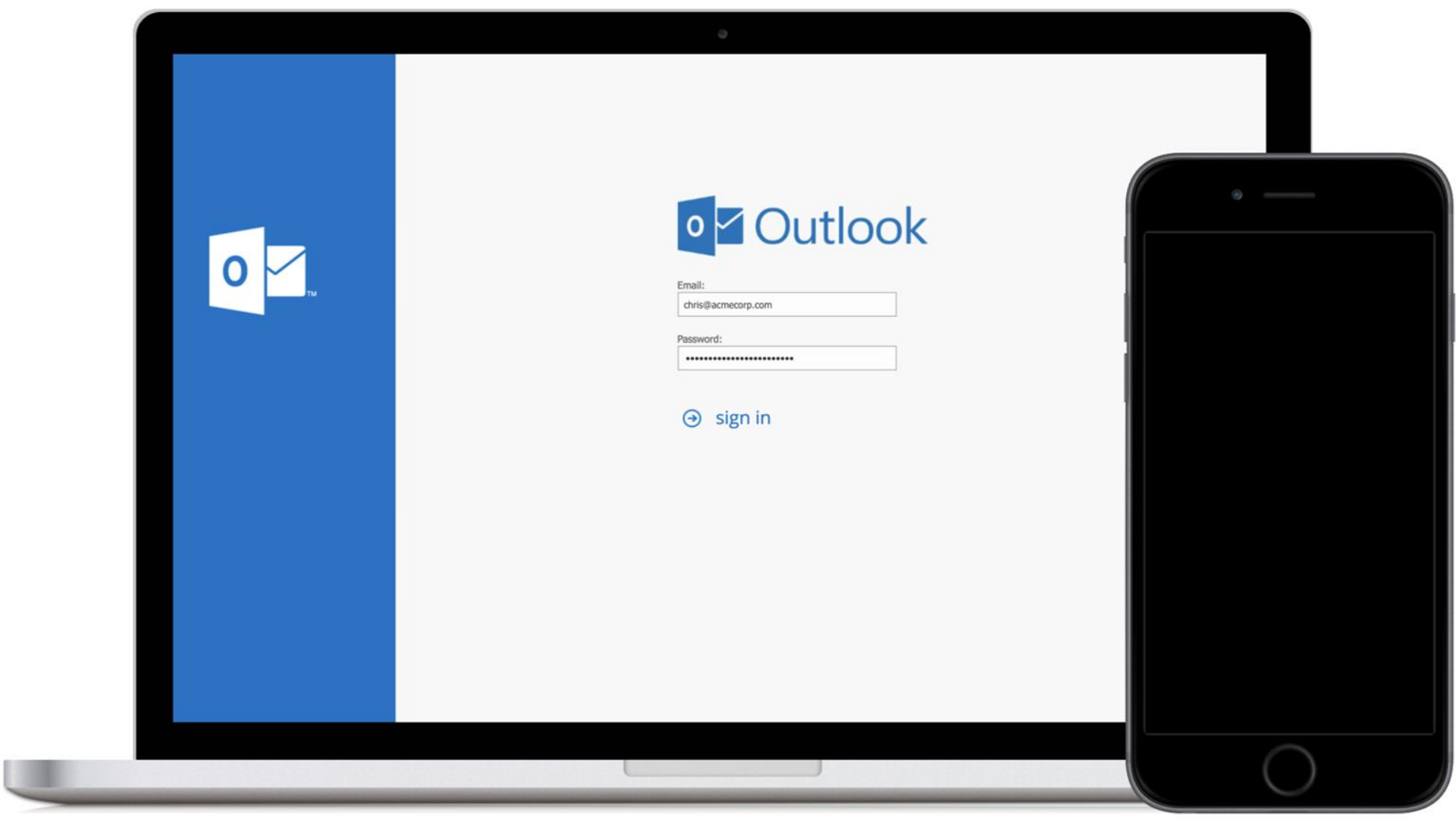
Duo Access機能を含む

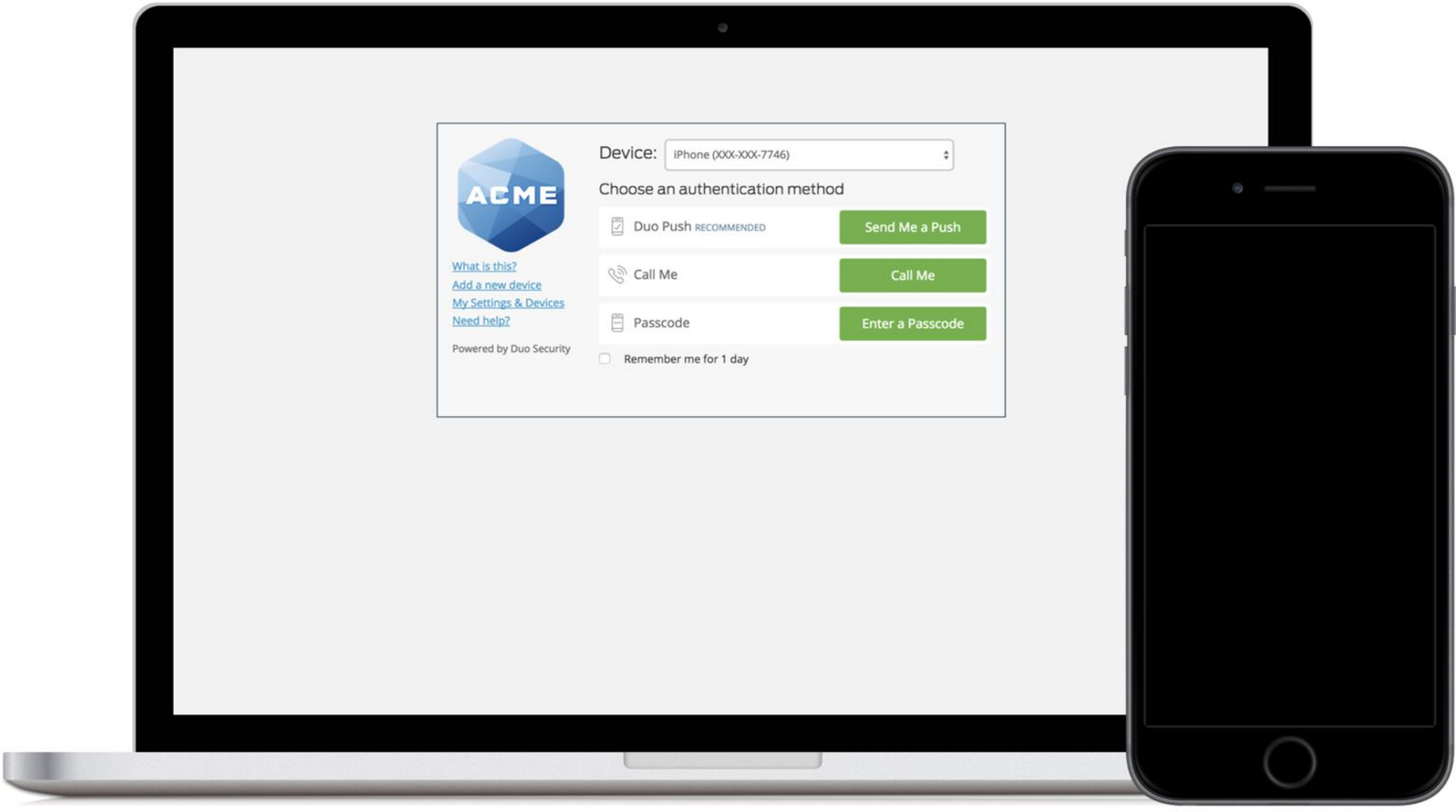
- 信頼されるエンドポイントの検出
- Duo Network Gateway（リバースプロキシ）
- Anti-Virus/Anti-Malwareの検知

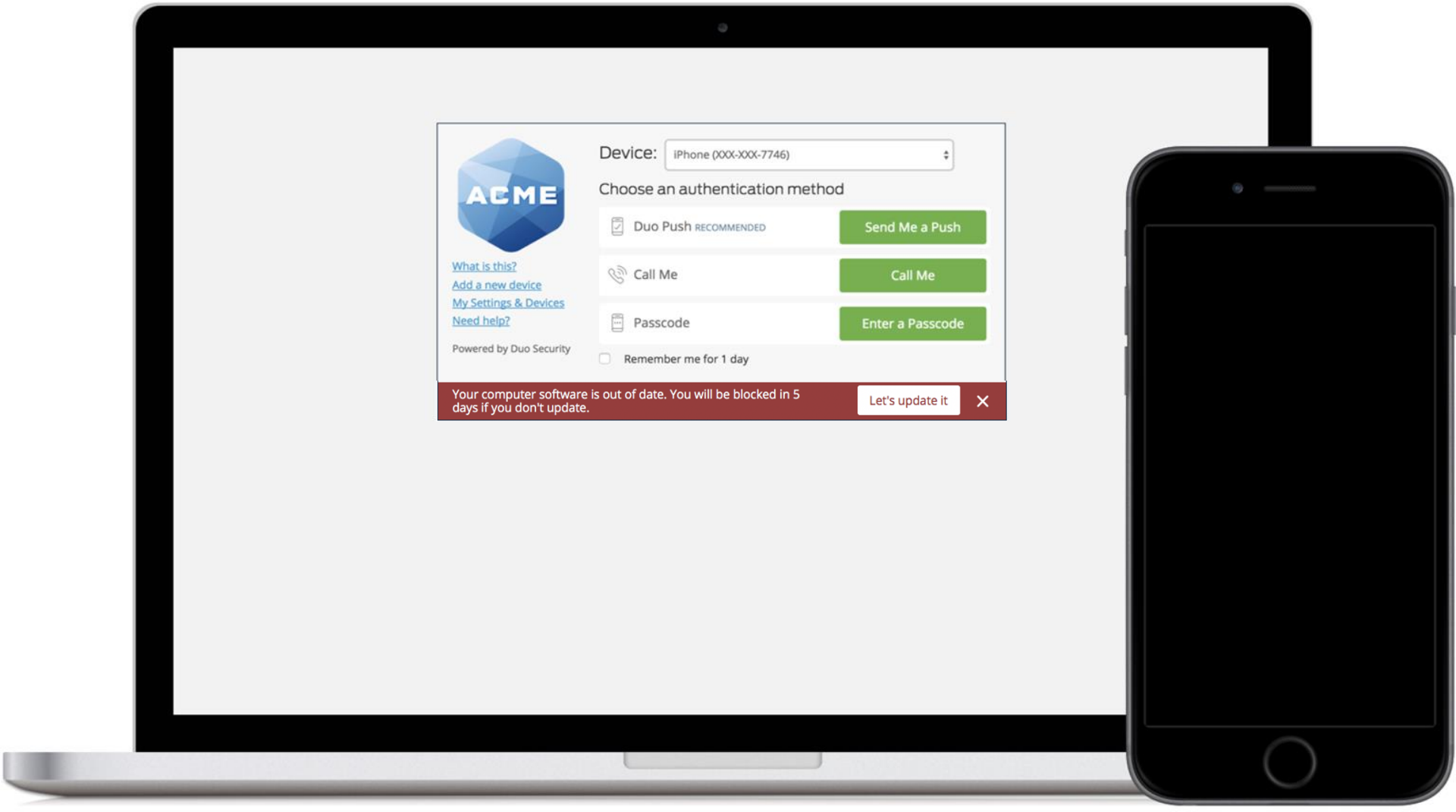
詳細情報: https://www.cisco.com/c/dam/global/ja_jp/products/catalog/pdf/cisco-duo-security-brochure.pdf

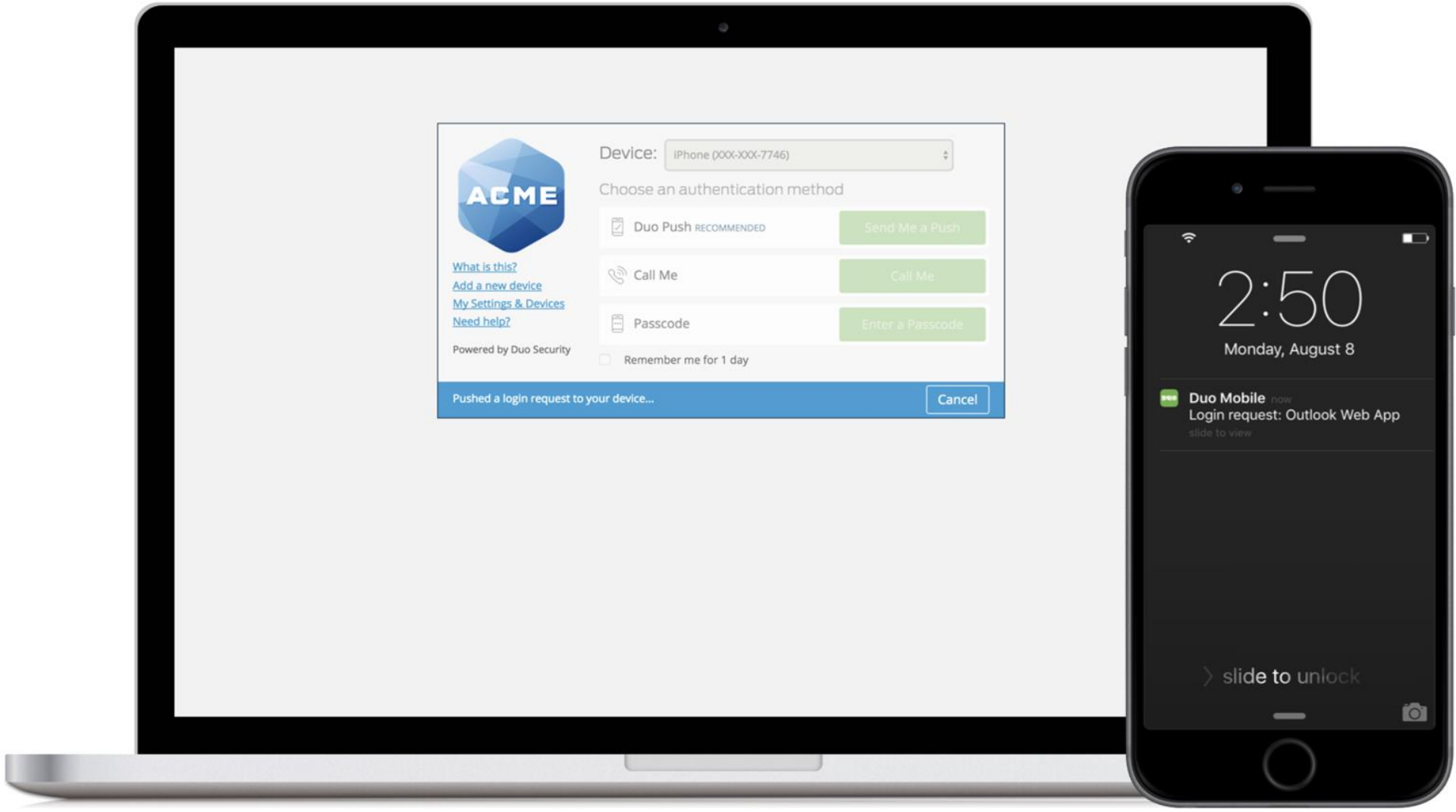
動作イメージ

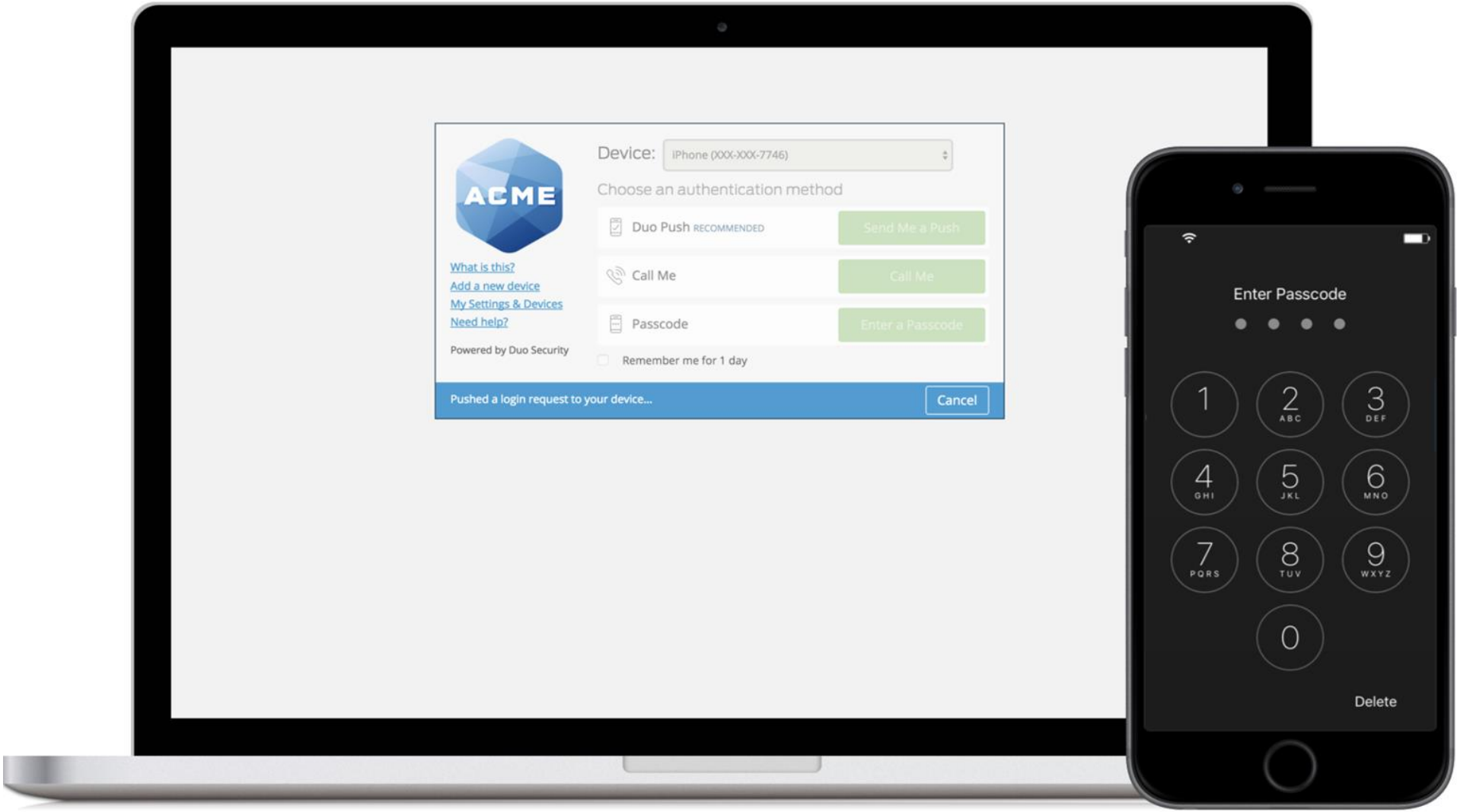

Outlook
Email:
Password:
sign in

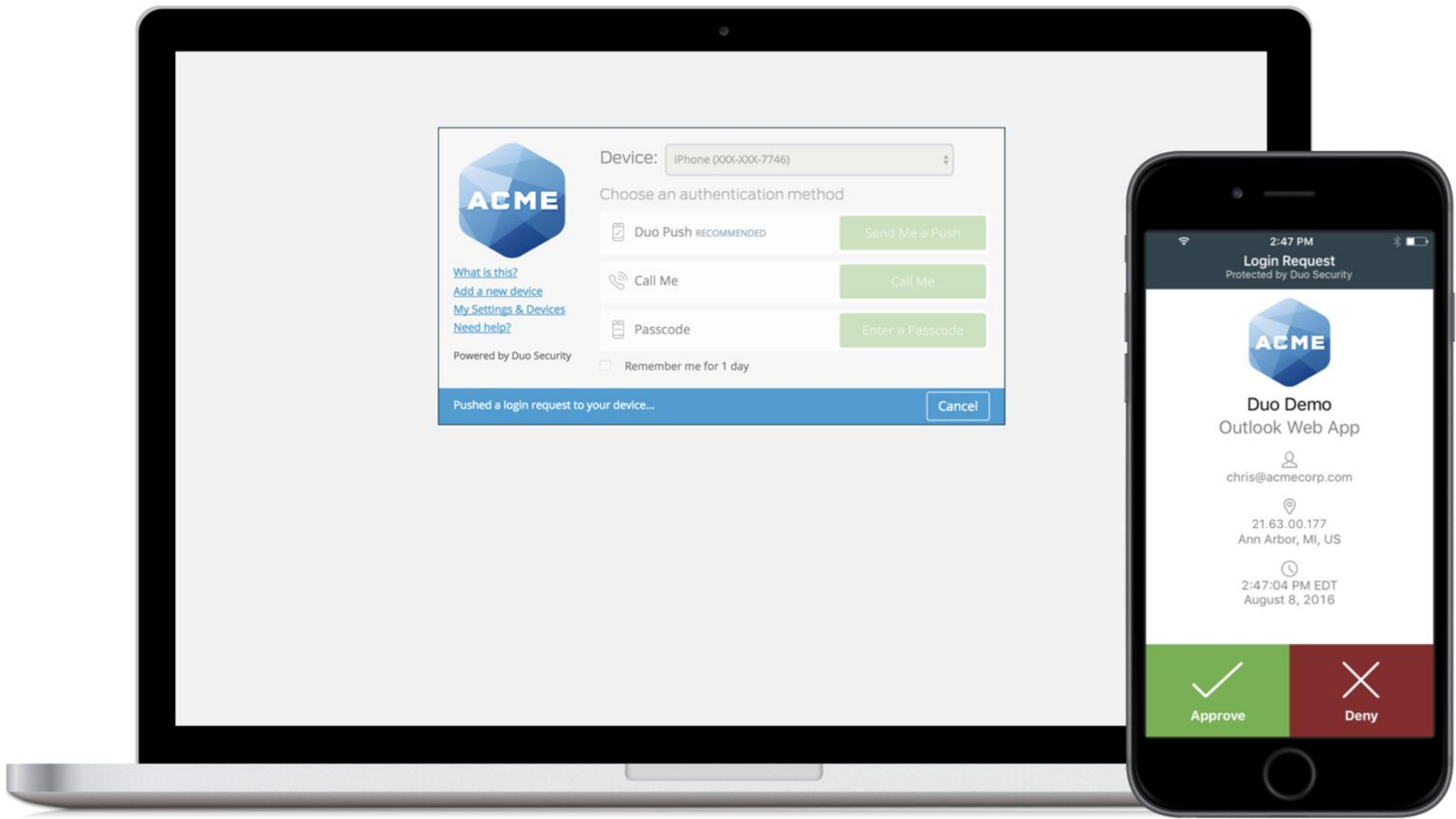

Outlook
Email:
chris@acmecorp.com
Password:
sign in

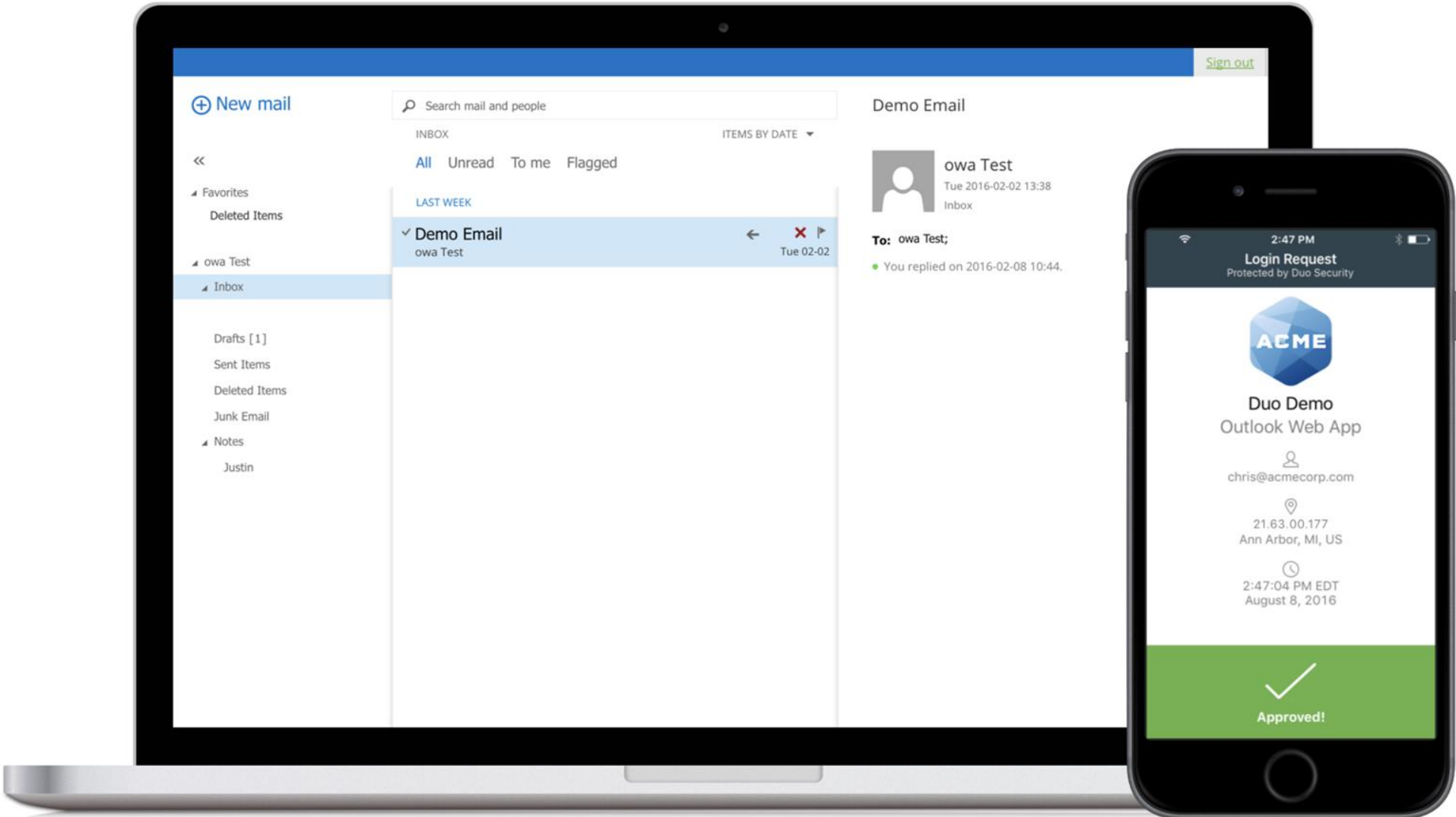

ACME
Device:
iPhone (XXX-XXX-7746)
Choose an authentication method
Duo Push RECOMMENDED
Send Me a Push
Call Me
Call Me
Passcode
Enter a Passcode
Remember me for 1 day
What is this?
Add a new device
My Settings & Devices
Need help?
Powered by Duo Security


ACME
Device:
iPhone (XXX-XXX-7746)
Choose an authentication method
Duo Push RECOMMENDED
Send Me a Push
Call Me
Call Me
Passcode
Enter a Passcode
What is this?
Add a new device
My Settings & Devices
Need help?
Powered by Duo Security
Remember me for 1 day
Your computer software is out of date. You will be blocked in 5 days if you don't update.
Let's update it


ACME
Device:
iPhone (XXX-XXX-7746)
Choose an authentication method
Duo Push RECOMMENDED
Send Me a Push
Call Me
Call Me
Passcode
Enter a Passcode
What is this?
Add a new device
My Settings & Devices
Need help?
Powered by Duo Security
Remember me for 1 day
Pushed a login request to your device...
Cancel
2:50
Monday, August 8
Duo Mobile now
Login request: Outlook Web App
slide to view
slide to unlock


ACME
Device:
iPhone (XXX-XXX-7746)
Choose an authentication method
Duo Push RECOMMENDED
Send Me a Push
Call Me
Call Me
Passcode
Enter a Passcode
What is this?
Add a new device
My Settings & Devices
Need help?
Powered by Duo Security
Remember me for 1 day
Pushed a login request to your device...
Cancel
Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Delete


ACME
Device:
iPhone (XXX-XXX-7746)
Choose an authentication method
Duo Push RECOMMENDED
Send Me a Push
Call Me
Call Me
Passcode
Enter a Passcode
What is this?
Add a new device
My Settings & Devices
Need help?
Powered by Duo Security
Remember me for 1 day
Pushed a login request to your device...
Cancel
2:47 PM
Login Request
Protected by Duo Security
ACME
Duo Demo
Outlook Web App
chris@acmecorp.com
21.63.00.177
Ann Arbor, MI, US
2:47:04 PM EDT
August 8, 2016
Approve
Deny

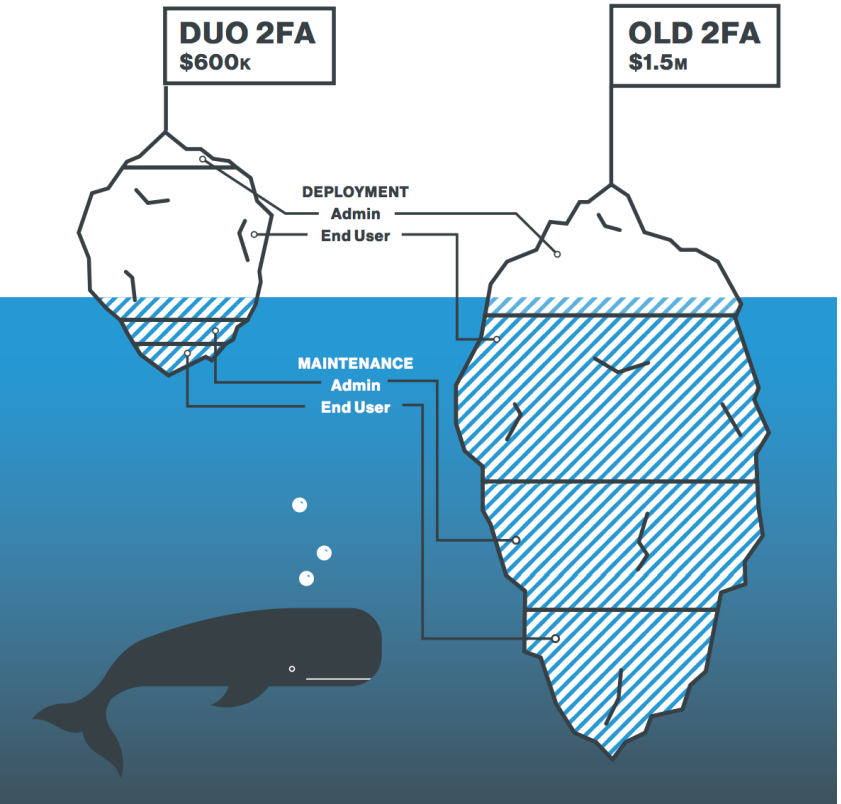

Sign out
New mail
Search mail and people
INBOX
ITEMS BY DATE
All
Unread
To me
Flagged
Favorites
Deleted Items
owa Test
Inbox
Drafts [1]
Sent Items
Deleted Items
Junk Email
Notes
Justin
LAST WEEK
Demo Email
owa Test
Tue 02-02
Demo Email
owa Test
Tue 2016-02-02 13:38
Inbox
To: owa Test;
You replied on 2016-02-08 10:44.
2:47 PM
Login Request
Protected by Duo Security
ACME
Duo Demo
Outlook Web App
chris@acmecorp.com
21.63.00.177
Ann Arbor, MI, US
2:47:04 PM EDT
August 8, 2016
Approved!

まとめ

Duoセキュリティが選ばれる理由

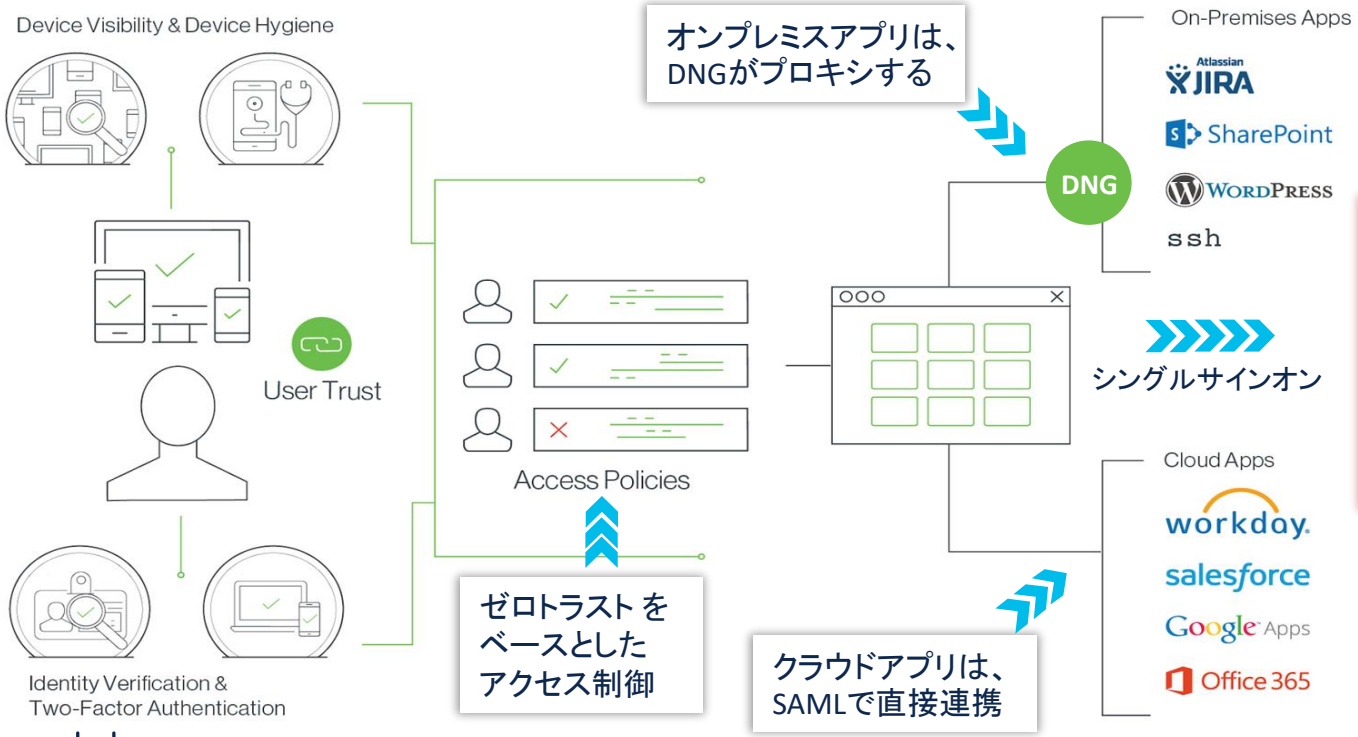
- **簡単に使える**
  - ✓認証は、ワンタップで承認
  - ✓シングルサインオン（SSO）
- **簡単にゼロトラスト環境を構築できる**
  - ✓ ユーザの信頼（多要素認証）
  - ✓ デバイスの信頼（デバイス可視化）
- **豊富なアプリケーションとVPN環境をサポート**
  - ✓ クラウドとオンプレミスアプリケーション
  - ✓ マルチベンダーのVPN環境

Duo 2FA vs. OLD 2FA
コスト比較



	Duo	OLD 2FA
導入	専門技術を必要としない	インストールには専門技術が必要
インテグレーション	VPN, RDP, クラウドアプリなど豊富なアプリを追加コスト無くサポート	インテグレーションごとにカスタムコネクタのコストを要求される
トークンの導入	トークンは必須ではないほとんどのユーザがスマホで Duo Mobile を使用	トークンの発送から展開まで時間を要する
トークンの紛失、盗難、破損による交換	トークンの利用は必須では無い。多くのユーザは Duo Mobileを利用	毎月一定数のトークンの紛失などが発生する
システムメンテナンス	基本的にサービスダウン無し	メンテナンス中のサービスダウンあるいは縮退
2FA デバイスのパッチやアップデート	クラウドからの自動アップデート	手動によるIT管理者のサポートが必要
新しいユーザの登録 （２FAデバイス含む）	2-3 分 ユーザ自身で登録可能	1 時間 エンドユーザのトレーニングも必要
認証にかかる時間	2 秒 Duo Push でワンタップ	15-30 秒 ワンタイムパスワードを入力する時間
デバイス可視化 PC, Mac, モバイルデバイス, BYODなど	Duoの機能に含まれる	別の製品が必要
ユーザ/グループに基づいたセキュリティポリシー	Duoの機能に含まれる	別の製品が必要

Duo SSO Central をセキュリティのコンタクトポイントに
オンプレ、クラウドアプリのシームレスでセキュアな通信



Duo SSO Central

Duo 無料トライアル

- トライアルを申し込むと30日間無料でお試しいただけます。
  登録サイトはこちら↓
  https://www.cisco.com/c/m/ja_jp/duo/trial.html


cisco
Secure