お客様成功事例

テクノロジー

Facebook

ソーシャルメディア大手がエンジニアのセキュリティを確保し、1万人を超えるユーザを保護するために導入したソリューション

CISCO

Duo Security is
now part of Cisco.

課題

Facebook 社は、自社のプラットフォームで 11 億 9000 万人の個人データを管理しており、顧客から預かった個人データの完全性が自社の成功に欠かせない重大要素であることを明確に示しています。

睡眠時間を削ることなく 10 億人のユーザを保護する

Facebook 社の開発者は、システム開発中に社内のネットワークやデータベースにアクセスします。その際、ソースコードとユーザデータへのセキュリティリスクを回避するため、悪意ある攻撃から開発者を保護しなければなりません。

Facebook 社のセキュリティ文化は、開発者が迅速に対応でき、セキュリティを簡単に確保できるようにすることに重点が置かれています。そのため、汎用性と効率が高く、コードを書くために開発サーバにログインするためのワークフロープロセスを合理化できるセキュリティソリューションを必要としていました。

1 日に数万の SSH セッションが、60 以上の対話型セッション、および 3,000 を超える非対話型認証が実行されるなか、現状よりも手間をかけることなくニーズをサポートするセキュリティが必要でした。

煩わしさのない強力なセキュリティが必要

Facebook 社では、すでにパスワードや公開キーと秘密キーのペアなどを使用していましたが、他の従業員にも容易に拡張できる、より強力な認証形式を探していました。そのとき、すでに利用しているもの（パスワード）とすでに所有しているもの（スマホなどのデバイス）を組み合わせる二要素認証というソリューションに注目しました。

Facebook 社のセキュリティチームは、最適な二要素認証ソリューションを選択するために幅広い調査を行いました。しかし、それぞれの方式にはいくつかの欠点がありました。時間ベースのトークン（RSA で提供しているもの）と Facebook 社のコードジェネレータを組み合わせた場合、開発者に与えられた認証時間はわずか 30 秒でした。また、同時に 2 台の端末を使用する必要がある場合にも、この方式は SSH での使用に最適ではありませんでした。さらにパスコードでしか認証が行えなかったため、この認証方式は面倒でした。

OTP（ワンタイムパスワード）では、同期エラーが発生してしまいました。誤ってトークンを何度も使用すると同期がとれなくなる可能性があり、使いやすさが大きく損なわれます。またトークンは、頻繁には使用されないという前提で設計されているため、1 つのセッションの VPN には適していますが、複数の SSH セッションを開く場合には適していません。

生体認証はデバイスのサポートが非常に限られており、他人受入率やリプレイ攻撃といった、セキュリティに関する独自の問題がありました。また、ユーザがローカルで各自のラップトップを使用しているときにリモートサーバでどのように生体認証要素を使用するのかという現実的な問題もありました。

PKI（公開キーインフラストラクチャ）はデバイスのサポートが不十分なうえ、認証形式としてスマートカードを使用するので、スマートカードプロキシ攻撃を受けやすいという欠点がありました。攻撃者がスマートカードの PIN を傍受すれば、ユーザの情報を得なくてもスマートカードを使用できてしまいます。さらに、スマートカードの管理は複数のプラットフォームで統一するのが難しく、多くのオーバーヘッドが必要になります。

Facebook 社のセキュリティチームが必要としていたのは、これらの方式より優れた二要素ソリューションであり、使いやすさ、柔軟なオプション、迅速な導入、そしてサポートのオーバーヘッドを最小限に抑えられるという特長を備えた、強力なセキュリティでした。

ソリューション

Facebook 社の情報セキュリティマネージャである John "Four" Flynn 氏は、Duo によって使いやすさが向上しただけでなく、認証も行いやすくなったと述べています。

Duo の二要素認証ソリューションは、Duo Mobile アプリケーションとしてスマートフォンにインストールできます。また、プッシュ、SMS、モバイル、音声など、固定電話やオフラインデバイスを使った数多くの認証方式もサポートしています。

さらに、Duo の二要素はクラウドベースであるため、ハードウェアの設置やソフトウェアのインストールが必要なく、迅速かつ簡単に導入でき、管理者のサポートのオーバーヘッドが削減されます。

カスタム セキュリティ ソリューションを可能にする汎用的な二要素認証

Duo の二要素認証では、数多くのソリューションを統合することができます。そのなかには、最も広く使用されているプラットフォーム、アプリケーション、およびデバイスが含まれています。Duo の認証サービスが提供する柔軟性と汎用性によって、さまざまなテクノロジーを組み合わせたカスタム セキュリティ ソリューションが実現できます。そこで Facebook 社は、サードパーティのハードウェアトークンを活用し、非常に迅速な認証を必要とする積極的なユーザに対して Duo による二要素認証のサポートを開始しました。

このような特定のユーザをサポートするため、Facebook 社は Duo Security の強力な二要素と USB ポート内で OTP トークンとして機能する Yubico 社の YubiKey Nano を組み合わせました。これら 2 つのソリューションを組み合わせることにより、SSH ログインを頻繁に使用するユーザはラップトップの側面をタップするだけで安全に認証されるだけでなく、移動中やデバイスを紛失した場合にもさまざまな認証方式を選択できるようになりました。

Facebook 社では、さらにエンジニアが使用するログイン方法をサポートする必要がありました。エンジニアは SSH クライアントとしてサードパーティのソフトウェアを実行しており、ログインに多くのカスタムスクリプトを必要としていました。また SFTP も頻繁に使用されていました。そこでエンジニアに対しては、対話形式で認証するのではなく、スクリプトを使った認証をサポートする必要がありました。

大多数のユーザが Kerberos、SSH 証明書、またはキーを使用してログインしたいと考えていたため、パスワードによる認証には多くの抵抗がありました。Facebook 社は Duo Security のサポートを受けて、認証入力を指示する独自のキーボード インタラクティブ ドライバとカスタムモジュールを作成しました。

最終的に Facebook 社に必要だったのは、エンジニアに究極の使いやすさと柔軟性をもたらす、迅速に導入できるうえにサポートのオーバーヘッドを最小限に抑えられるソリューションでした。もちろん強力なセキュリティが実装されなければなりません。Duo Security と Yubico 社は力を合わせ、Facebook 社のセキュリティのニーズに適合する強力な二要素ソリューションを実現したのです。

保護するユーザ数を 300 人から 1万人超にまで増強

当初 Linux サーバに導入された Duo の二要素認証は、Facebook 社内で利用が拡張され、現在では VPN、Windows Server、Splunk、OWA などにも導入されています。クラウドをベースとする Duo の統合モデルにより、Facebook 社は実稼働、財務、およびリモート VPN アクセスシステムへの導入を効率的に進めることができました。

現在、Facebook 社における Duo の利用状況はどのようになっているのでしょうか。Facebook 社は、RSA SecurID による時間ベースのトークンを完全に廃止し、組織全体に Duo を拡張して 1 万人を超える従業員をサポートするために Duo のエンタープライズ サイト ライセンス契約を締結しています。

Duo のユニファイド アクセス セキュリティ (UAS) で、すべてのユーザ、デバイス、およびアプリケーションを保護できます。

信頼できるユーザ

高度な二要素認証でユーザを確認し、ユーザアクセスポリシーを適用してアプリケーションへのアクセスを制限できます。

信頼できるデバイス

Duo により、ログイン時に従業員が所有するデバイスを含むすべてのデバイスのセキュリティ正常性がチェックされます。デバイスのリスクに基づいてアクセスポリシーをカスタマイズできます。

すべてのアプリケーション

ユーザと管理者の両方をサポートする Duo のセキュアなシングルサインオン (SSO) でクラウドとオンプレミスのアプリケーションを保護し、アクセスを簡素化できます。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

2020.06