Duo for...

cisco SECURE

サイバー賠償責任保険

Duo は多要素認証を手始めに、強力でプロアクティブなセキュリティ基盤の構築を支援します。

課 題 :

未知の脅威に対する防御

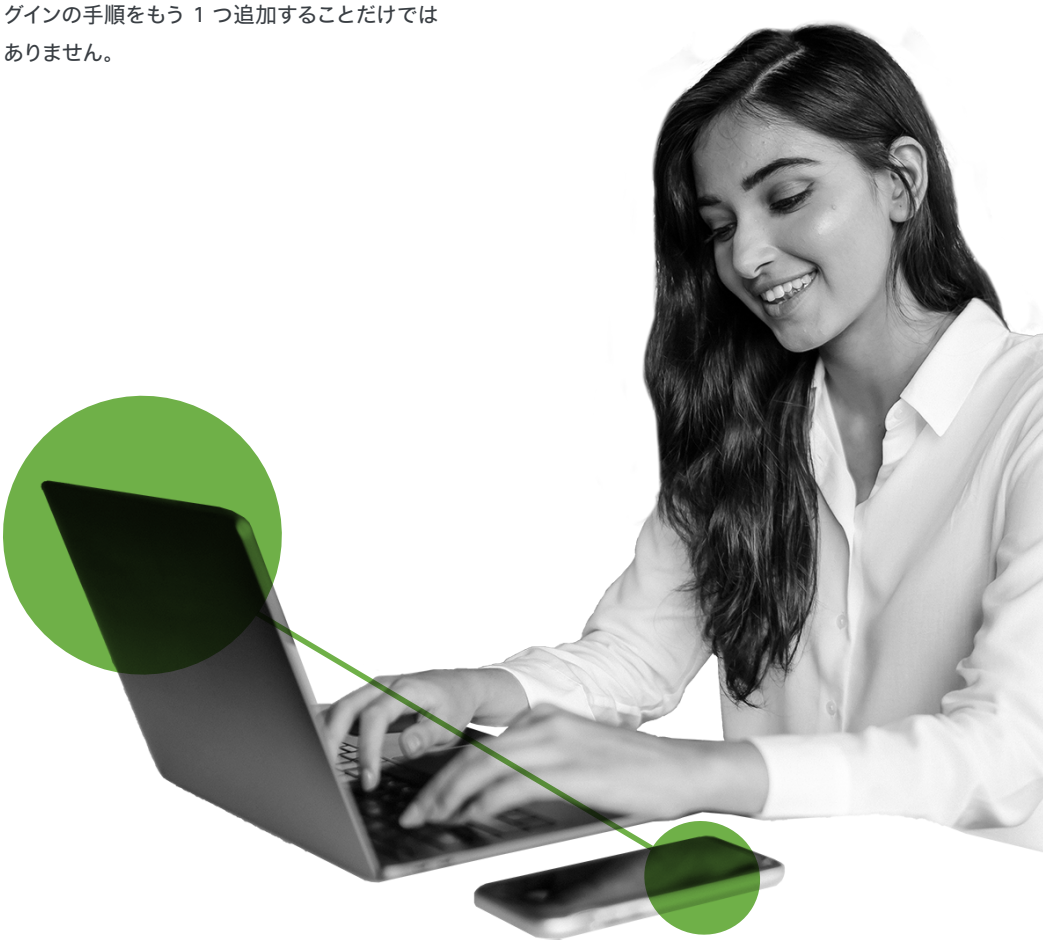
現代社会はフィッシング、ランサムウェア、リモートワークフォース、個人デバイスといった課題に次々に見舞われていて、必要なサイバーセキュリティ プラクティスも高度になる一方です。組織は、事前対応と事後対応のバランスを取りながら、未知の脅威や進行中の脅威からビジネスを守る必要があります。

サイバー賠償責任保険は、データ漏洩、ネットワークへのダメージ、およびその結果として生じるビジネスの中断など、さまざまなサイバーインシデントによって被る損失とコストを軽減することを目的とした一連の補償です。

保険料に影響を与える要因には、次のようなものがあります。

- 収益と従業員数で表される事業規模
- ビジネスの種類、アクセスされるデータの特性、およびアクセスするユーザー
- 補償の対象となる機密情報の量
- 過去の保険金請求と既存のサイバーセキュリティ対策

多要素認証 (MFA) は、盗まれたログイン情報よる攻撃や総当たり攻撃に対する強力な防御戦略であることが証明されていて、サイバー保険会社が要求する最優先の判断基準となっています。ただし、プロアクティブなセキュリティとは、ログインの手順をもう 1 つ追加することだけではありません。



ソリューション：

Duo のセキュアで信頼できるアクセス

Duo は、侵害された可能性のあるデバイスが貴重なリソースやデータにアクセスできないようにすることで、すべてのユーザー、デバイス、アプリケーションを保護します。Duo は、ユーザーの本人確認を行い、デバイスがポリシーに準拠し最新状態で安全であることを確認した後、アプリケーションへのアクセスを許可します。

01

使いやすく導入が簡単

Duo はクラウドベースのソリューションであるため、お客様のインフラストラクチャと連携して、数時間で企業全体に展開できます。

Duo のログインプロセスは、すべてのユーザーにとってシンプルになるよう妥協することなく設計されています。プッシュ通知、トークン、生体認証などの柔軟な認証方式を備えていて、ユーザーは自身のワークフローに最適なものを選択できます。

クラウドをベースとしているため、Duo は既存のテクノロジーと簡単に連携できます。管理者は、Duo のサポートチームや、導入に役立つリソースにアクセスできます。また、Duo には、ネイティブな連携機能、クラウドベースの簡単なセットアップ、メンテナンスが少なくて済むといったメリットがあります。

02

強力なセキュリティ習慣を構築

請負業者からエグゼクティブまで、組織のあらゆるレベルで強力なセキュリティ対策が不可欠です。MFA とともに、セキュリティに対するワークフォース全体の意識と行動がリスクを軽減するのに役立ちます。

Duo Mobile は、2 番目の認証要素として機能します。また Duo Mobile を利用することで、ユーザーがセキュリティの問題を自分で修正できるようになります。一方管理者は、デバイスのセキュリティ状態の全体像を把握できます。ラップトップとデスクトップに関しては、Duo Health アプリケーションがファイアウォールや暗号化の有無を確認し、オペレーティングシステムが最新の状態に更新されているかどうかをチェックします。

Duo を利用することで、個人所有か企業所有かに関わらず、すべてのデバイスのアクセスを制御できます。さらに、エンドポイントセキュリティ全体を可視化できます。

03

幅広いカバレッジがさらに拡大

Duo には 200 を超える連携機能が初めから備わっています。これらを利用して Office 365、Dropbox、Cisco VPN などのオンプレミスとクラウドベースのアプリケーションへのアクセスを保護できます。

さらに Duo は、企業のセキュリティニーズに合わせて拡張し、オフライン MFA や、コンプライアンスに利用できるレポートとログを提供できます。また、ユーザーとデバイスをいつでも追加できる機能も備えています。

MFA とシングルサインオンと組み合わせて、すべてのアプリケーションで一貫したログインワークフローを作成することができます。また、ディレクトリと同期することで、ユーザーベースが変更されてもポリシーを最新の状態に保つことができます。簡単に、すぐに使える。それが Duo なのです。

Duo のエディション

機能	利点	Duo MFA	Duo Access	Duo Beyond
MFA	ユーザーの信頼を確立	✓	✓	✓
SSO	複数のアプリに一度にログイン	✓	✓	✓
適応型認証	ポリシーに基づいてアクセスを許可		✓	✓
トラストモニター	異常なログイン試行を検出		✓	✓
デバイスの分析	デバイスの可視化		✓	✓
DHA	デバイスが正常であることを確認		✓	✓
信頼できるエンドポイント	アクセスを信頼できるデバイスに制限			✓
DNG	VPN なしで内部アプリケーションにアクセス			✓

「

Duo を利用すれば、KAYAK で管理している何百台ものラップトップを明確に識別し、従業員が社内の環境に持ち込んでいる個人用デバイスと区別できます。

これらのデバイスの状態をトラッキングして、オペレーティングシステムとブラウザが最新であることも確認できます」

Steve Meyes 氏

KAYAK 社 セキュリティ主任

サイバー賠償責任保険

まとめ

サイバーセキュリティはどこへ向かっているのでしょうか

ランサムウェアの懸念への対応や政府の義務化からサイバー保険の普及に至るまで、セキュリティは予防的な Zero Trust モデルの採用に向かっています。このモデルでは、セキュリティは境界を越えて今日のハイブリッドワークフォースの業務に拡張されます。Zero Trust モデルでは、環境全体にわたる問題の軽減、検出、対応が可能になるため、ID を基本としたアクセスなどがもたらすセキュリティリスクを防ぐことができます。

MFA は保険要件チェックリストの項目のように見えるかもしれませんが、事後対応ではなくプロアクティブなセキュリティ戦略の基礎となり得るものです。Duo は、あらゆる組織のニーズに合わせて成長や拡張が可能です。ワークフォースのセキュリティを対象に、現在や将来のリスクと規制に備える幅広いソリューションを提供します。不確実な世界でベストプラクティスの先例を構築できるように、Duo はあらゆる組織をサポートします。

「これが Duo の優れた点です。大多数の人は Duo の操作にほとんど時間を費やしていません。それは Duo が非常に高速かつシンプルで、使っていることを意識することがほぼないからです」

Ben Hughes 氏
Etsy 社ネットワーク セキュリティ マネージャ