リモートワークおよび事業継続ソリューション

製品

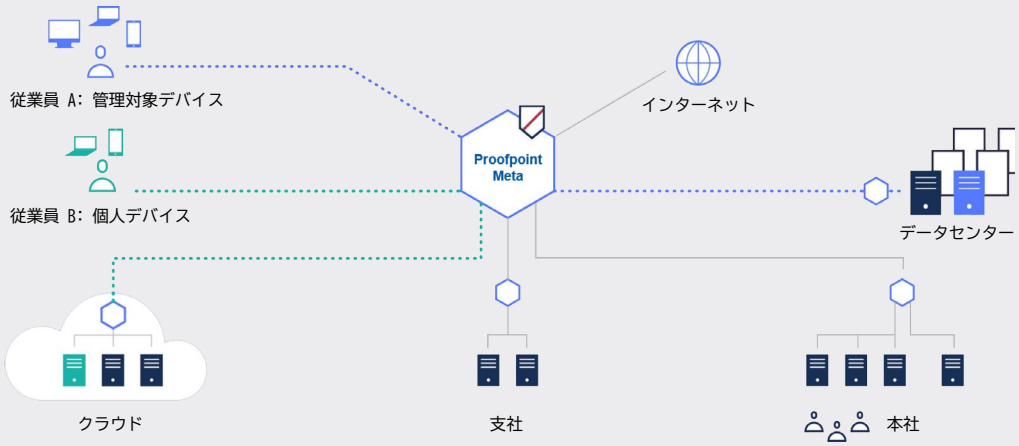
- Proofpoint Meta
- Proofpoint Browser Isolation
- Proofpoint Security Awareness Training
- Proofpoint Cloud Account Defense

主なメリット

- リモートワークでも、オフィスにいるときと同じレベルのセキュリティとアクセスを提供
- 従業員やコントラクターに、データセンターやクラウド上のアプリケーションへの安全なリモートアクセスを迅速かつ効果的に提供
- リモート ワーカーは悪意あるコードなどを心配することなく、会社支給のデバイスから Web の利用が可能
- リモートワークで直面するリスクについて従業員に教育
- 不審なクラウド アカウント アクティビティを識別して対処

従業員はオフィスよりもリモートで働くことが多くなってきましたが、変わらず攻撃のターゲットとして狙われ続けています。つまり、リモートからでも安全に仕事ができる環境は、これまでにないほど重要になっています。しかし従来のリモート アクセス方法ではセキュリティ上のリスクがあるため、高い確率で問題が発生します。加えてリモートワーカーは組織でセキュリティ コントロールをおこなえる領域外にいることもあるため、さらにリスクが高くなっています。プルーフポイントはリモートワークの迅速かつ安全な導入と、セキュリティ リスクの低減の両方を強力に支援します。

管理対象/管理対象外デバイス用のクライアント/クライアントレス アクセスでゼロトラスト ネットワークを提供します。アクセス管理を細分化し、ユーザーのロケーションに関係なく、必要なアプリケーションにのみアクセスできるようにします。そして Web トラフィックを分離し、悪意あるコードが会社支給のデバイス上で実行されないようにすることで、個人メール アカウントを経由して組織を狙う攻撃のリスクを低減します。



リモートワークの導入

ロケーションの制約なく アプリケーションに即座に接続

ユーザーだけでなくデータやアプリケーションも分散しています。Proofpoint Meta ではゼロトラストの手法を用いて、リモートの従業員、パートナー、顧客のデータセンター アプリケーションやクラウド インフラ へのアクセスを保護します。より高度なセキュリティ、優れたユーザー エクスペリエンスと同時に IT 管理負荷の低減を実現し、ユーザー タイプ別にアクセスをセグメント化し、検証し、監査します。これにより、従来の VPN の問題点であるユーザー ケーパビリティの制限、トラフィックのボトルネック、ソフトウェア クライアント要件、ハードウェア導入、過剰なアクセス権限の付与、アクセスの遅さ、管理作業の多さなどに悩まされなくなります。

アクセス ポリシーの細分化により、各ユーザーは必要なアプリケーションにのみアクセスできるようにすることで、不要なリスクを回避することができます。承認済みのアプリケーションであれば、ユーザーはどこにいても、単一の方法で常時接続することができます。またクラウド ネイティブの暗号化されたオーバーレイ ネットワークでは、グローバル PoP でパフォーマンスを最適化します。さらに、このアクセス ソリューションはクラウドで提供されるため、IT 部門は散在するアプライアンスでのルール管理やトラブル シューティングといった作業から解放されます。

悪意あるコンテンツによる 会社支給デバイスへの被害を防止

攻撃者は、リモート ワーカーが会社のセキュリティで保護されていないかもしれないということ、個人デバイスを使っているかもしれないこと、個人メール アカウントにアクセスしているかもしれないことを知っています。Proofpoint Browser Isolation は、こういったユーザーの行動によってもたらされるリスクを防止します。また同時に、信頼されていないサイトを訪問したり、個人 Web メールを使用するユーザーのプライバシーも守ります。Browser Isolation では URL 分離技術を使ってアクセスを処理します。これによりユーザーはリスクなく、安全に、かつ安心してインターネットを利用できるようになります。

安全なリモートワーク

会社の環境へのリスクについて従業員を教育

ユーザーは在宅勤務やリモートワークをしているとき、オフィスで勤務しているときにはなかったセキュリティ上の問題に直面することがあります。Proofpoint Security Awareness Trainingでは、リモートワークに特有の問題についてトレーニングをおこないます。トレーニングには、デバイスや Wi-Fi ネットワークの保護方法や、オフィス外で働くときに直面するセキュリティ上の問題の対処方法などが含まれます。

不審なクラウド アカウント アクティビティを識別して対処

攻撃者はさまざまな方法を使ってクラウド アプリケーションのアカウントに不正アクセスし、アカウントを乗っ取ろうとします。そして一度それが成功してしまうと、社外から攻撃が仕掛けられるようになってしまいます。そうなると組織の信頼が損なわれ、金銭的損失も被ることになります。

しかし Proofpoint Cloud Account Defense（CAD）を用いれば、Microsoft Office 365 や Google G Suite アカウントの乗っ取りを防ぐことができます。Proofpoint CAD は、機密データや信用されているアカウントを侵害しようとする脅威を迅速に検出、調査し、防御します。導入は簡単で、Office 365/G Suite ユーザーがどのネットワークやデバイスを使っていても保護できます。これにより、従業員やセキュリティ チームがどこにいたとしても、安心して仕事ができ、さらに、Office 365 や G Suite を最大限活用できるようになります。

「Webブラウジング、パスワード、メール、モバイル デバイスに関する4つのセキュリティ
トレーニングのモジュールをのべ 400,000 人が修了することができました。
そのうち、モバイル デバイスのセキュリティに関するモジュールは、任意のトレーニングにもかかわらず、
32,000人以上のユーザーが2週間以内に修了しました。これは驚くべき成績です。
わずか4つのモジュールで、トレーニング コストの適正化ができました。
この投資は正解でした。」

大手テクノロジー企業 セキュリティ意識向上・トレーニングディレクター

詳細

詳細は proofpoint.com/jp でご確認ください。