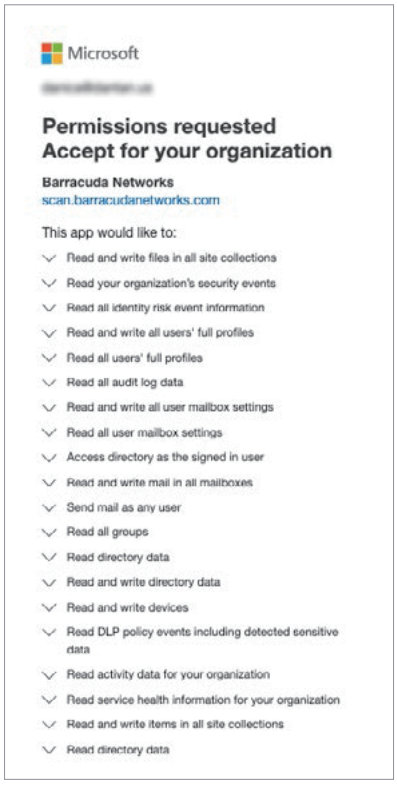
Barracuda Sentinelのデータプライバシー

Barracuda Sentinelはスピアフィッシングとサイバー詐欺を防止するリアルタイムのAI(人工知能)ソリューションです。Barracuda Sentinelは、クラウドサービスとして提供され、Office365の公式のパブリックAPI(アプリケーションプログラミングインターフェース)を使用して、アカウント内のメールを検証します。

Barracuda Sentinelのサインアッププロセスにかかる時間は5分未満です。サインアップすると、Office365をBarracuda Sentinelに接続するように指示されます。このプロセスでは、Barracuda Sentinelがアカウントにアクセスできる権限を付与するようにに許可するマイクロソフトのポップアップが表示されます *(右側のスクリーンショットを参照)*。

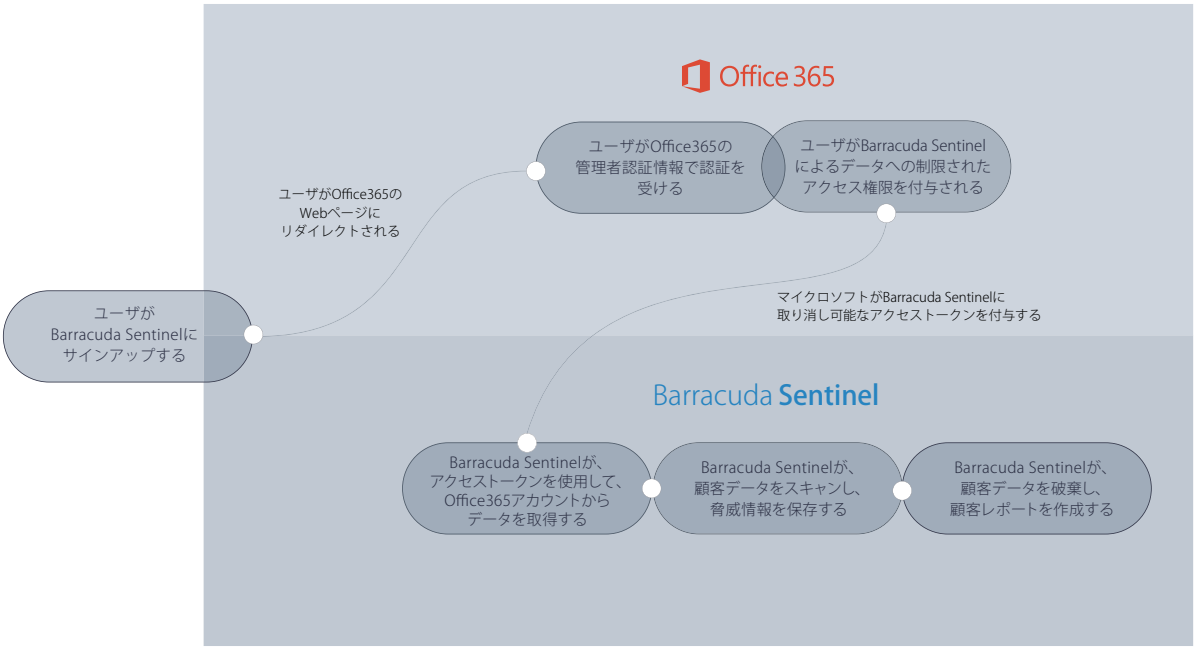
権限を付与すると、クラウドベースのAIが、バックグラウンドで実行され、Office365クラウドと直接通信します。Barracuda Sentinelは、APIを使用するため、ネットワークパフォーマンスとUX(ユーザエクスペリエンス)には影響しません。



Barracuda Sentinelがアクセスできるアカウント内の情報

Barracuda SentinelはOffice365の認証情報にアクセスできません。

- Barracuda Sentinelは、広く使用されているOAuthプロトコルによって、Office365の認証を受けます。
- Barracuda Sentinelによるアクセスはスピアフィッシングとサイバー詐欺を検出および修復するための情報に制限されています。
- Barracuda Sentinelはユーザ、メールフォルダ、およびメールに関するメタデータをダッシュボードに表示するために取得します。
- Barracuda Sentinelは、システムをデバッグし、パフォーマンスを最適化し、AIアルゴリズムを向上および再トレーニングするためだけに、メールデータを保存できます。このデータへのアクセスは厳重に制御および監査されます。



データプライバシーの保護方法

・Barracuda Sentinelは、アカウント内のスピアフィッシングとサイバー詐欺を検出するためにのみ、メールと添付ファイルにアクセスします。脅威情報は、Barracuda Sentinelダッシュボードに情報を表示するためだけに使用され、いずれの部外者とも共有されません。

・脅威分析はバラクーダがAWS(Amazon Web Services)上およびバラクーダのデータセンター内にホスティングしているセキュアなサーバ上で実行されます。

・すべてのサーバ、ストレージシステム、およびネットワーク通信は暗号化され、すべてのサーバは厳格なセキュリティ基準で厳重に制御および監査されます。

・デバッグまたはシステム最適化の作業が必要な場合は、必要最少人数のバラクーダエンジニアが作業に必要なデータにアクセスする権限を付与されます。

・バラクーダの慣習と手続きの詳細については、バラクーダサイトのプライバシーポリシーページをご参照ください。

FAQ (よくある質問)

Barracuda SentinelによるOffice365アカウントへのアクセスを取り消すことはできますか?

はい。いつでもAzure ADアプリケーションダッシュボードで権限を取り消すことができます。

・Azure ADダッシュボードにアクセスします。https://manage.windowsazure.com/

・Active Directoryに移動し、Barracuda Sentinelの接続先のディレクトリの名前をクリックします。

・「Applications」タブに移動し、「Barracuda Networks」をクリックします。

・下部のナビゲーションバーの「Manage Access」をクリックし、「Remove Access」を選択します。

Barracuda Sentinelにユーザメールボックスへの書き込みアクセス権限が必要である理由

Barracuda Sentinelは、スピアフィッシングを検出すると、リアルタイムに自動的に修復するため、書き込みアクセス権限が必要です。Barracuda Sentinelは、エンドユーザのメールボックスからExchange Onlineアカウント内の隔離フォルダに脅威を移動して、修復を実行します。

・エンドユーザは、Barracuda SentinelのUI(ユーザインターフェース)にアクセスせずに、隔離済みメールを表示できます。

・すべての隔離動作によって、通知がエンドユーザとアカウント管理者に送信され、メールが隔離されたことが可視化されます。

Barracuda Sentinelはユーザが付与した権限をどのように使用するか

Barracuda Sentinelには下記の情報が必要です。この情報は、ユーザがBarracuda Sentinelに権限を付与すると、自動的にアクセスされます。下記の権限を付与しないと、正確なML(機械学習)モデルを構築するための情報、およびユーザメールボックスから脅威を削除する機能を使用できず、Barracuda Sentinelは機能しません。

セキュリティとリスク情報

アカウント乗っ取りイベントを検出および修復するには、下記の権限が必要です。

・すべてのIDリスクイベント情報を読み取る

・すべての監査ログデータを読み取る

・自社のセキュリティイベントを読み取る

・検出済み機密データなどのDLP(データ損失防止)ポリシーイベントを読み取る

・自社のアクティビティデータを読み取る

・自社のサービス動作状態情報を読み取る

・すべてのユーザメールボックス設定を読み取る、書き込む

・すべてのグループを読み取る

・デバイスを読み取る、書き込む

メールとユーザ情報

社内のコミュニケーションパターン履歴をマッピングして、従業員のインパーソネーション、スピアフィッシング、およびBEC(ビジネスメール詐欺)を検出および防止するには、下記の権限が必要です。

・すべてのユーザの完全なプロファイルを読み取る、書き込む

・すべてのメールボックス内のメールを読み取る、書き込む

・ディレクトリにログインユーザとしてアクセス

・ディレクトリデータを読み取る

・ディレクトリデータを読み取る、書き込む

・すべてのサイトコレクション内のファイルを読み取る、書き込む

・検出済み機密データなどのDLP(データ損失防止)ポリシーイベントを読み取る

外部送信者への通知

アカウント乗っ取りが検出された後に、外部送信者に警告通知を送信するには、下記の権限が必要です。

・メールをいずれかのユーザとして送信

Barracuda
Your journey, secured.