自宅のデバイスを保護しリモートワークの生産性を上げる5つのステップ

目次

リモートワークの特徴

最新のセキュリティは、従業員や企業のリモートワークを成功に導く強い味方です。

世界の急激な変化により、リモートワークは現代の企業にとって必要不可欠な要素となりました。リモートワークをうまく機能させるためには、会社のデータやリソースへの迅速かつ安全なアクセスの確保が必須です。セキュリティの整備が生産性とコラボレーション強化につながるため、こうした新しい働き方のサポートには、時代遅れではない革新的なセキュリティ対策が重要です。

リモートワークのメリット：
勤務時間の柔軟性
勤務地の柔軟性
ワークライフバランス
生産性

オフィスワークと
リモートワークの比較

オフィスからリモートワークへの移行により、企業リソースへのアクセスといった特有の課題が生まれました。

従来のオフィスワーク

企業ネットワーク境界内でのみデータにアクセスできる。

ネットワーク境界の内側かもしくは外側かに基付いて、リソースへアクセス。

企業データのほとんどがオンプレミスにある。

簡単に漏えいする可能性のあるユーザ認証に基づくアクセス権の付与。

企業ネットワーク外のリソースにアクセスする場合、従来のVPNが必要で、ネットワークエクスポージャーのリスクがある。

VPN経由で企業ネットワークに接続してリソースにアクセスする場合、速度が遅く、信頼性が低い。

アクセスに失敗した場合、修復手順が提供されず、IT部門からのサポートが必要で追加コストが派生する。

会社から提供されたセキュリティ対策が実施されている。

リモートワーク

企業ネットワーク境界外からデータへアクセスできる。

どこからでもリソースにアクセス可能。

企業データはクラウドとオンプレミスにある。

ユーザIDやアクセスポリシーに基づいたアクセス権の付与により、セキュリティを強化する。

リソースへのアクセスに従来のVPNを必要とせず、ネットワーク露出のリスクを軽減する。

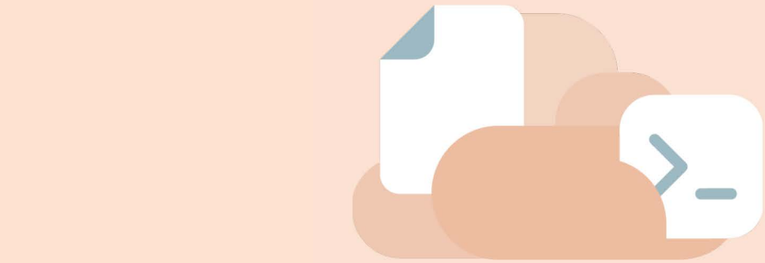
企業ネットワーク上の企業リソースへの迅速かつ信頼性の高いアクセスが可能。

アクセスに失敗した場合、アクセスに関する問題を即座に解決するための改善手順が追加費用なしで提供される。

BYOD、ホームネットワーク、セキュリティ知識不足により、セキュリティ対策が不十分である。

リモートワークのセキュリティとユーザビリティに関する5つの課題

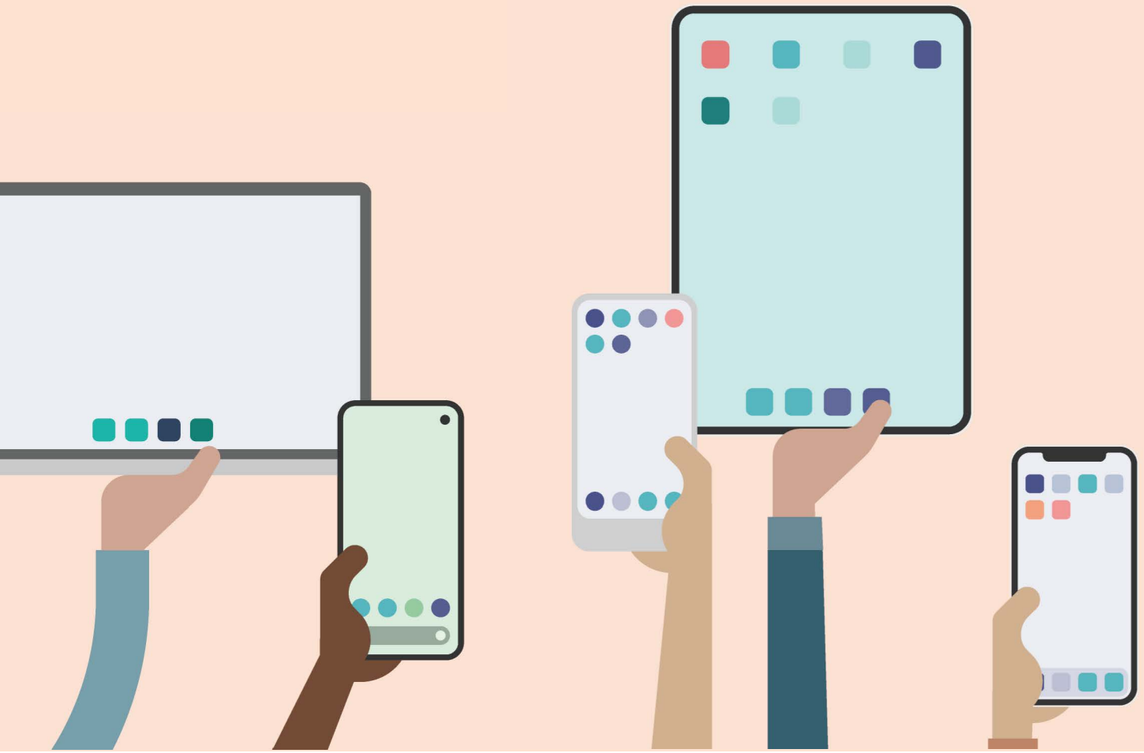
リモートワークにはさまざまなメリットがある一方で、セキュリティ上の課題も存在します。その課題は、使用する技術や、ユーザのセキュリティ知識や意識不足、増え続けるサイバー攻撃など、多岐にわたります。多くの場合、攻撃者がフィッシング攻撃やパッチが適用されていない脆弱性を利用してたった1台のデバイスを危険にさらすだけで、社内ネットワークの重要なリソースにアクセスできます。このような事象は、社内ネットワークの露出、ひいては情報漏えいにつながる可能性があります。



1.
オフィス
ネットワーク
への接続

社内ネットワーク露出の
可能性（不正なデバイス
と知らずに接続した場合）。

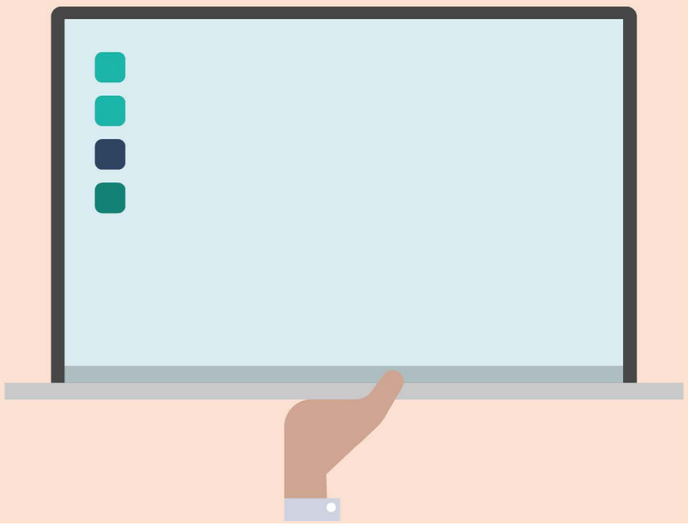
接続性や接続速度の問
題により、生産性が低下。



2.
デバイスの
セキュリティの
課題

デバイスのOSバージョンが
古く、既知の脆弱性が悪用
されやすくなる。

脱獄ジェイルブレイク済も
しくは侵害されたデバイス。



3.
ネットワーク
セキュリティの
課題

誰が、どのデバイスで、どこ
から、どのくらいの時間、ど
のリソースにアクセスして
いるのかが可視化されて
いない。

侵害されたデバイスはネッ
トワークに「テレポート」す
ることが可能

アクセス失敗時の修復手順
が整備されていない。

リソースにアクセスするため
のマルチクラウド接続に対
するサポートにおける課題

4.
フィッシング
などの
サイバー脅威

個人情報、会社の認証情報や
金融機関の口座情報、その他
の貴重なデータの窃盗を狙う。

信頼できる送信元からの送信
に見せかけ、悪意のあるリンク
や添付ファイルが通常含まれ
ている。

上記の結果、アカウント情報を
盗むリンクをクリックしたり、不
正なソフトウェアをインストー
ルしたりしてしまう。

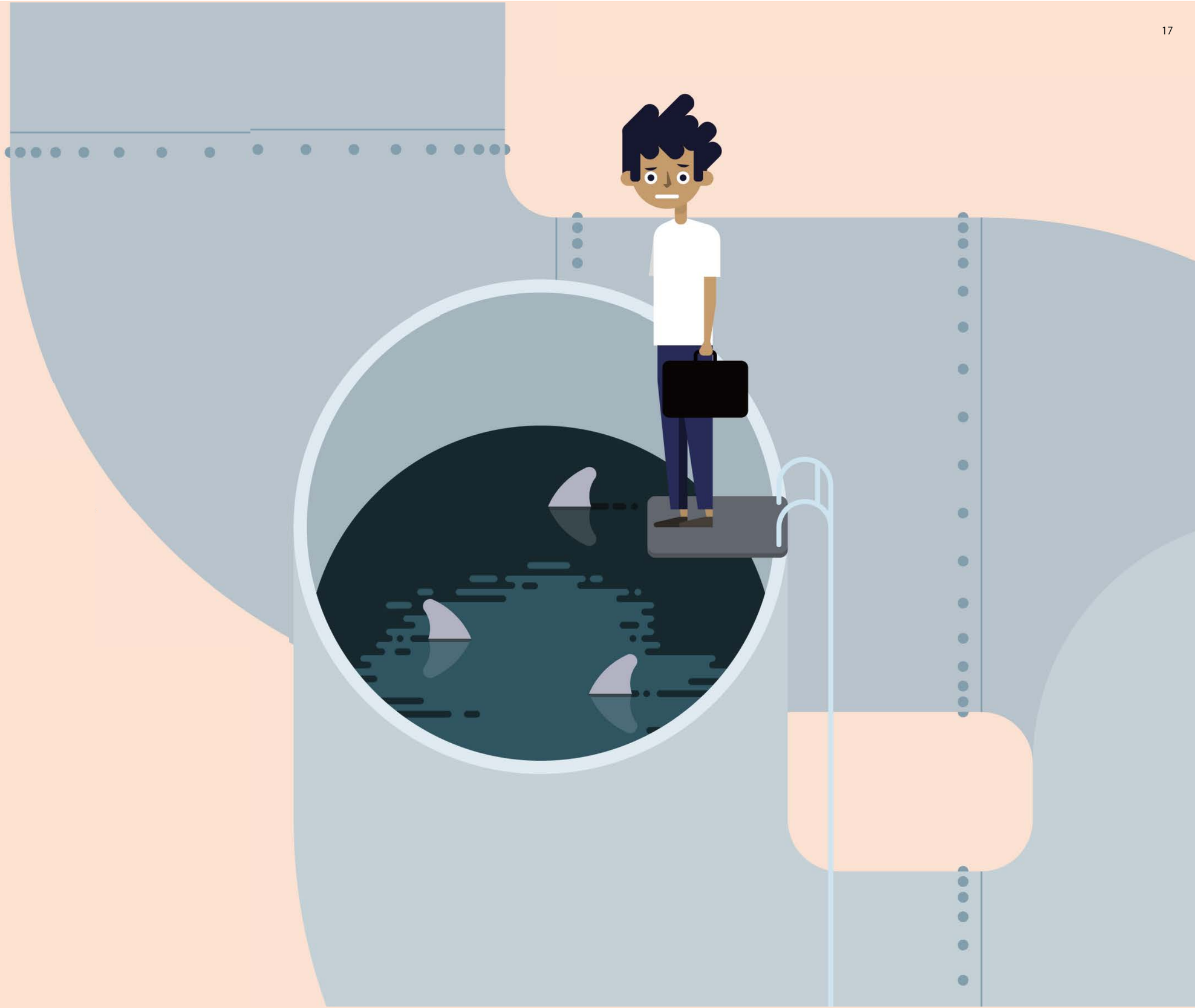
5.
VPNの課題

VPNは企業のデバイスのセキュリティやコンプライアンス要件を強制するものではない。

VPNは意図したリソースへのアクセスだけでなく、社内ネットワーク全体へのアクセスを提供することで社内ネットワークを露出してしまう。

VPNはロールベースのアクセスをサポートしない。

VPNでは認証情報の盗難、フィッシング、ドライブバイダウンロード、不正広告などのWebベースの攻撃から保護できない。



デバイスを保護し生産性を上げる5つのステップ

安全で生産性の高いリモートワークを実現するためには、従業員が所有するデバイスや共有のホームコンピュータを正しく設定し、これらの管理されていないデバイスを安全に企業のネットワークやアプリケーションに接続しなければなりません。

Barracuda CloudGen Accessは、オンプレミス、クラウド、またはハイブリッドのアプリケーションとワークロードへのアクセスを保護・簡素化し、あらゆるデバイスや場所から安全に企業データへアクセスできるようにします。

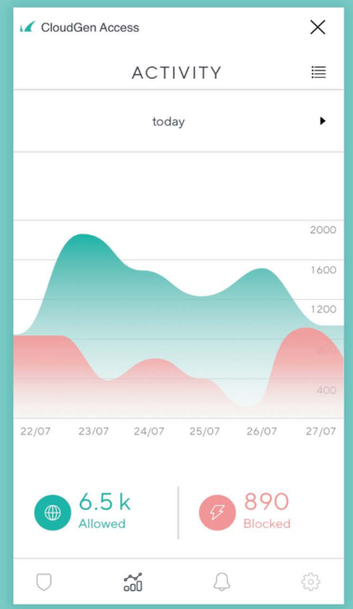
従来のVPNと比較してBarracuda CloudGen Accessで実現できること：

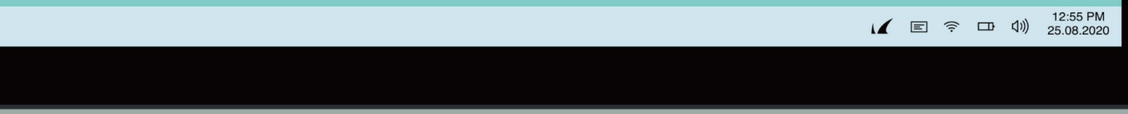
70 %
アクセス
レイテンシの
短縮

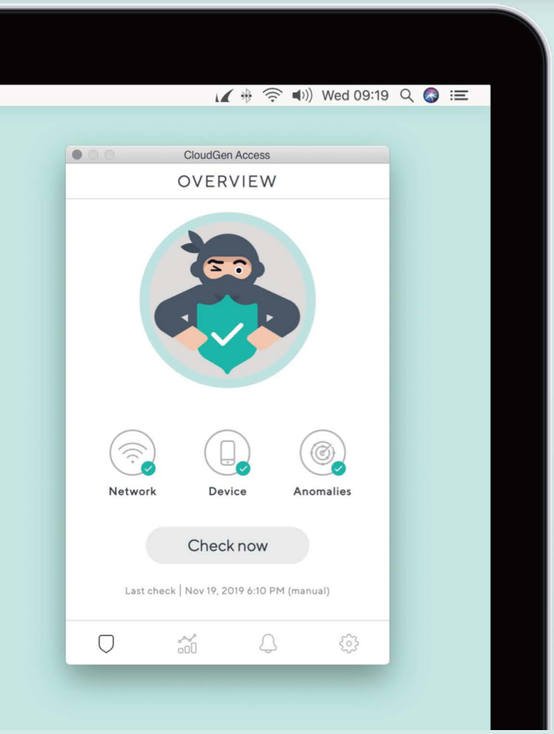
20 %
アクセスフロー
の改善

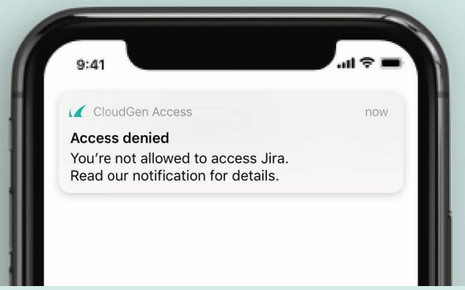
5 min
たった5 分で
デプロイ可能

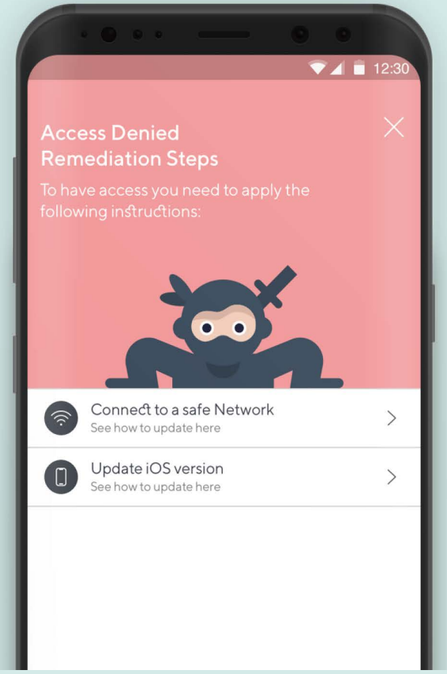
すべての
リモートアクセス
リクエストを
可視化

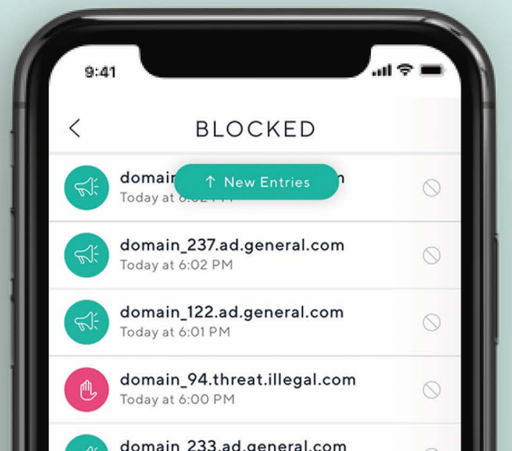












1.
デバイスを
セキュアにする

デバイスのセキュリティ強化のため必ずデバイスを最新のOSバージョンへアップグレードする。

フィッシング、マルウェア、ランサムウェアなどのWebベースの攻撃をブロックする。

2.
ネットワークを
セキュアにする

誰が、どのデバイスを使って、どのリソースにアクセスしているかを把握する。

侵害されたデバイスから、社内ネットワークを保護する。

アクセスポリシーやポスチャポリシーに違反した場合、簡単な修復手順を提供する。

リソースにアクセスするためのマルチクラウドインフラに対して、容易なサポートを提供する。

3.
アクセスをセキュアにする

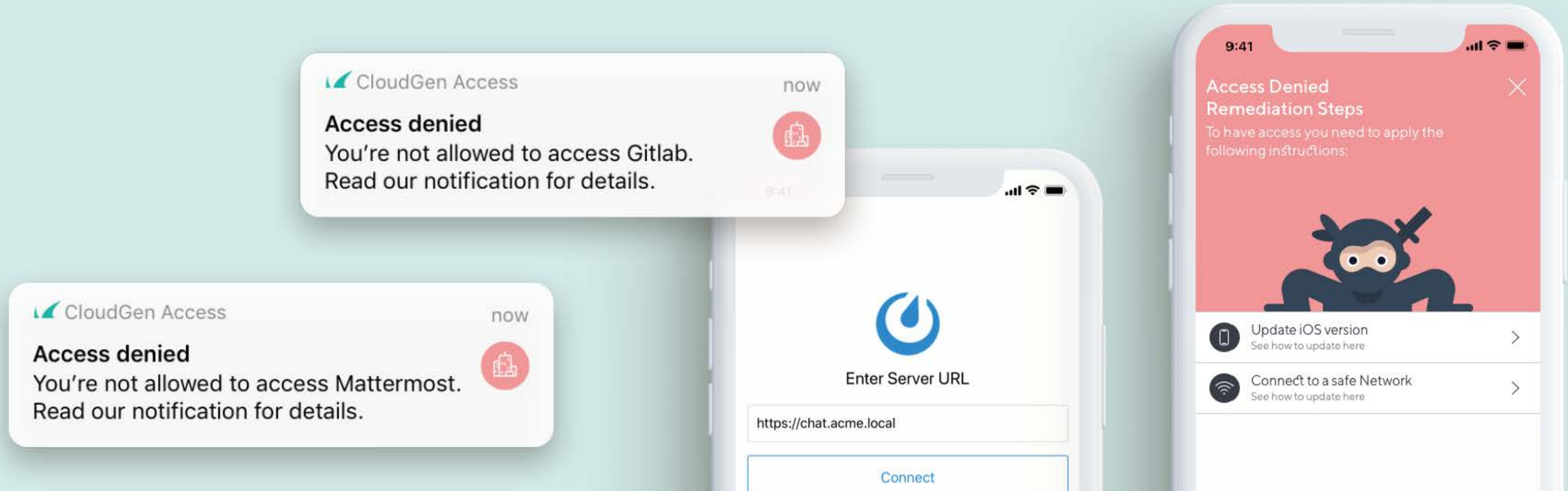
オンプレミスの
アプリケーション

ロールベースと属性ベースに基づく制御を設定し、信頼できるユーザとデバイスにコンテキストに基づくアクセスを許可する。

アクセス状況を可視化し、リスクを軽減する。

データプライバシーの確保：データプレーンがインフラから外れることがないようにする。

ネットワーク遅延のないアクセスを確保する。



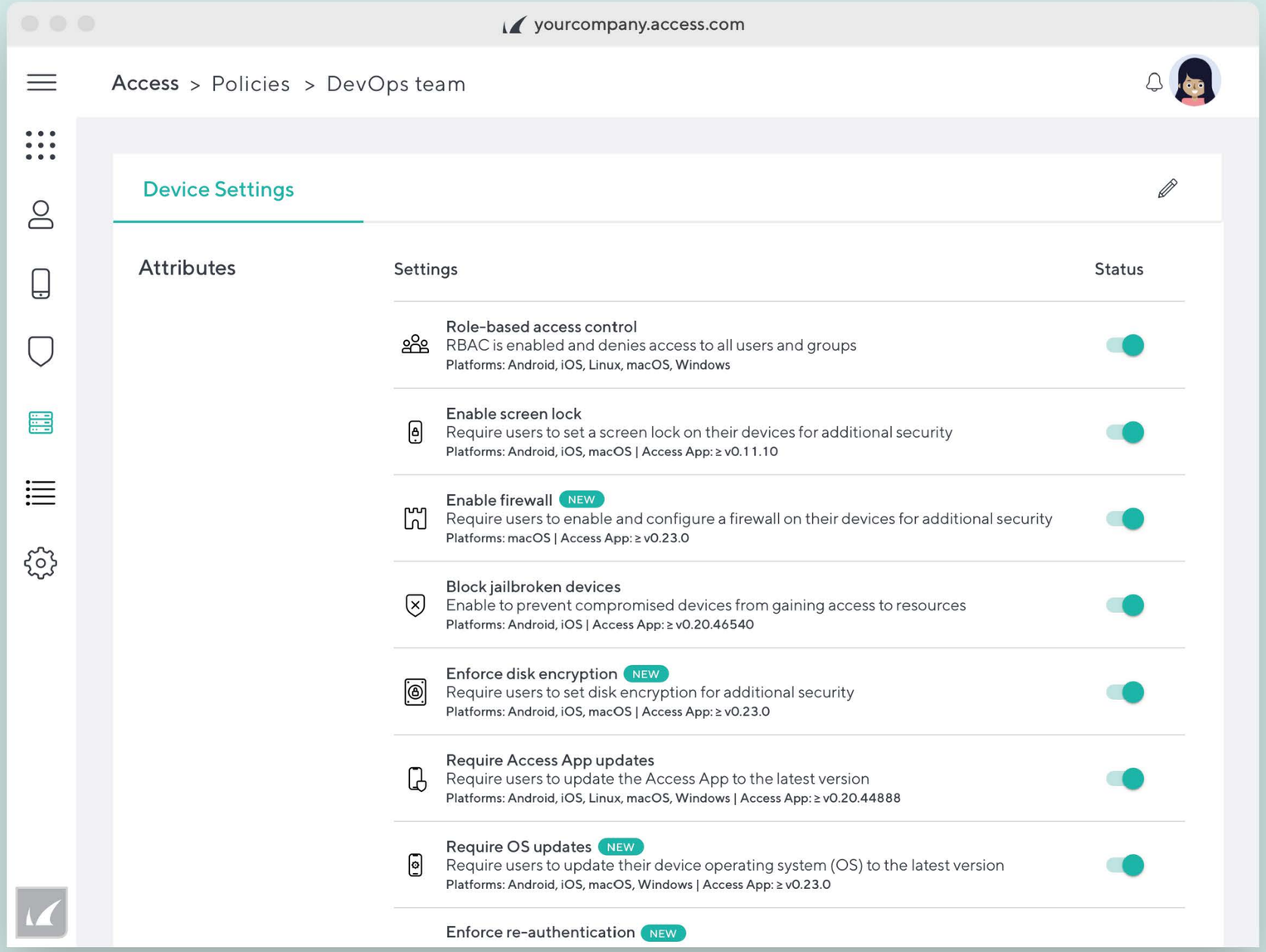
3.
アクセスをセキュアにする

ポリシーの徹底と
ユーザへの権限付与

ユーザとデバイスのアイデンティティとセキュリティポスチャを継続的に評価し、セキュリティを維持する。

ディスクの暗号化や、デバイスの画面ロックなどのグローバルポリシーを管理し侵害されたデバイスのアクセスを自動的にブロックする。

ブロックされたユーザに対してセルフ式のシンプルな修復手順を提供することで、煩わしさを排除し、生産性を向上させる。



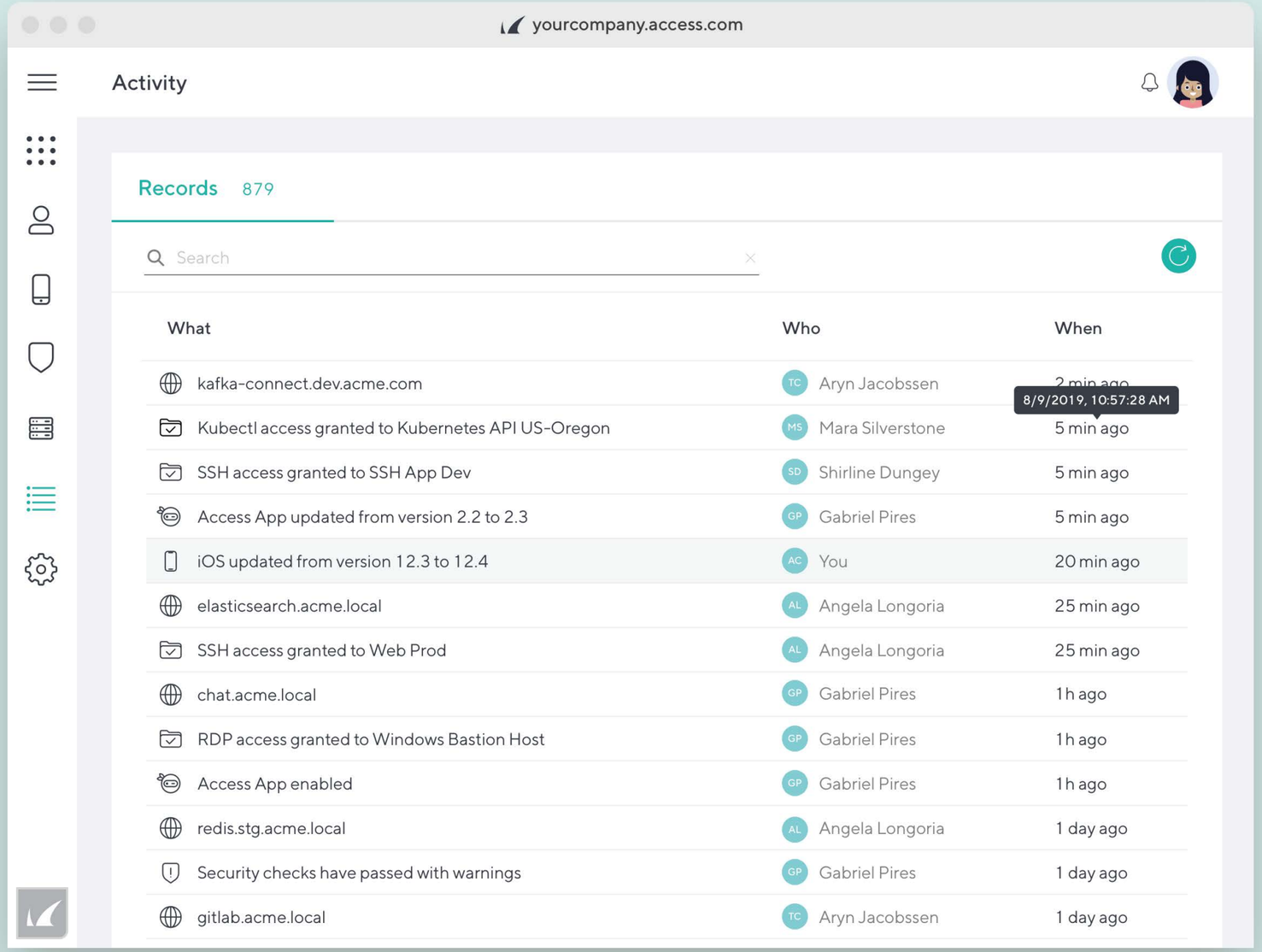
3.
アクセスをセキュアにする

アプリケーションと
ワークロードのアクセスに
関する記録システム

監査とコンプライアンスに関する報告を合理化する。

オンプレミスのアプリケーションにアクセスするユーザとデバイスを追跡・観察する。

エンドポイントの遠隔測定、アクセスポリシーの定義、デバイスのセキュリティ体制の継続的な監視など、有益なインサイトを得る。



4.
サイバー攻撃から身を守る

フィッシング、マルウェア、ランサムウェア、認証情報の盗難、Wi-Fiネットワークの侵害など、さまざまなサイバー脅威から保護する。

5.
生産性を上げる

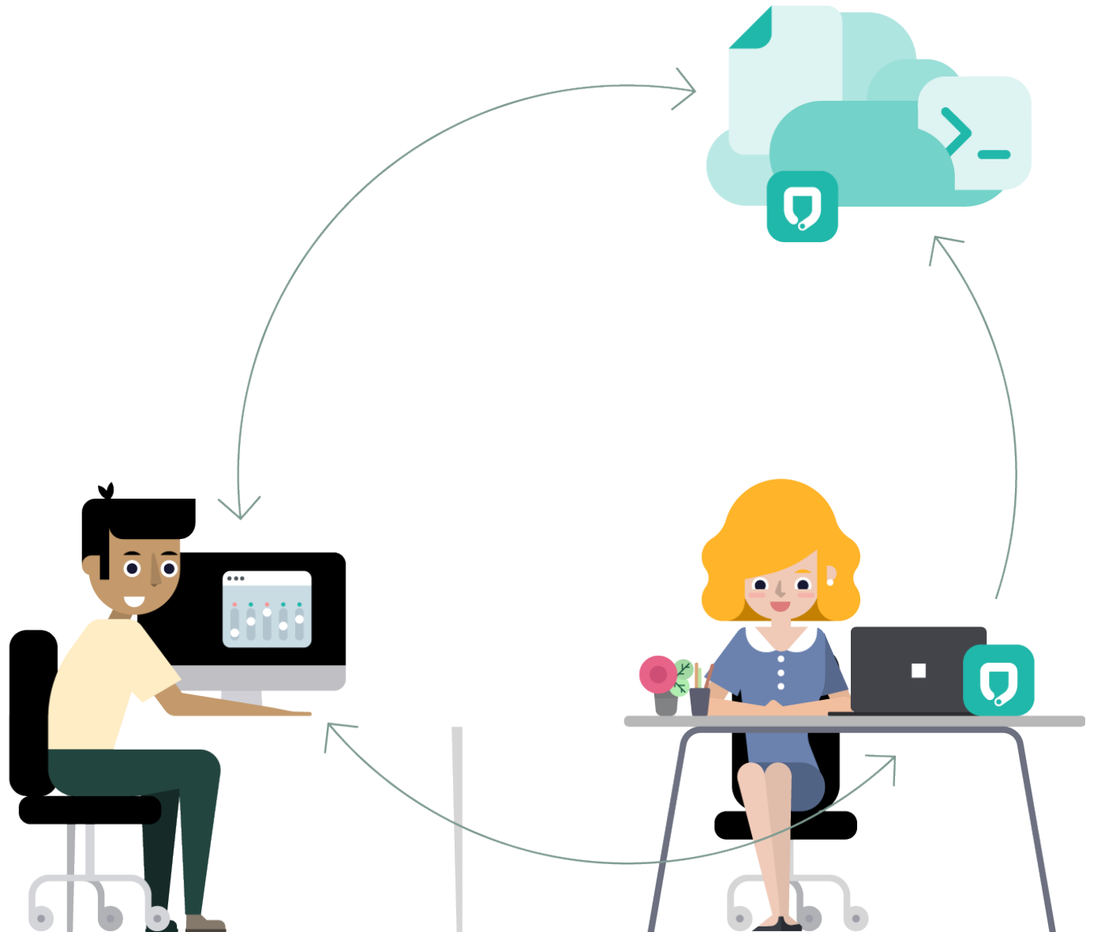
楽しいオンライン体験を邪魔する押しつけがましい広告や、プライバシーを侵害するトラッカーをブロックする。

通常のVPNによる遅延なしに、素早く企業リソースにアクセスして仕事に集中できるようにする。

ますます分散化が進む世界ではデジタルトランスフォーメーションが推奨され、現状に対する課題が突きつけられています。そんな中、Barracuda CloudGen Accessはゼロトラストセキュアアクセスの新基準となっています。

Barracuda CloudGen Accesssは、組織が新たな働き方やITの在り方に対応する中で直面するリスクを軽減し、ゼロトラストアーキテクチャへの道のりを後押しします。特許取得済みの技術による当社のアプローチは、オンプレミス、クラウド、ハイブリッドのアプリケーションやワークロードへの安全で信頼性の高い高速なアクセスを可能にします。

Barracuda CloudGen Accesssは従来のVPNアクセスに関連するセキュリティリスクを排除し、アカウント乗っ取り攻撃からユーザIDを保護します。



Barracuda CloudGen Accessで
デバイスを保護し、生産性を向上

Barracuda CloudGen Accessによる、
セキュリティと生産性を向上するゼロトラストの実装について、さらに詳しく知りたい方はこちらをご覧ください。

Barracuda

barracuda.co.jp

jsales@barracuda.co.jp