

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

- 03 リモートワークの特徴
- 04 オフィスワークとリモートワークの比較

- 10 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
- 12 オフィスネットワークへの接続
デバイスのセキュリティ
ネットワークセキュリティ
- 14 フィッシングなどのサイバー脅威
- 16 VPNの課題

- 18 デバイスを保護し
生産性を上げる5つのステップ
- 20 デバイスをセキュアにする
ネットワークをセキュアにする
- 22 アクセスをセキュアにする
- 28 サイバー攻撃から身を守る
生産性を上げる

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

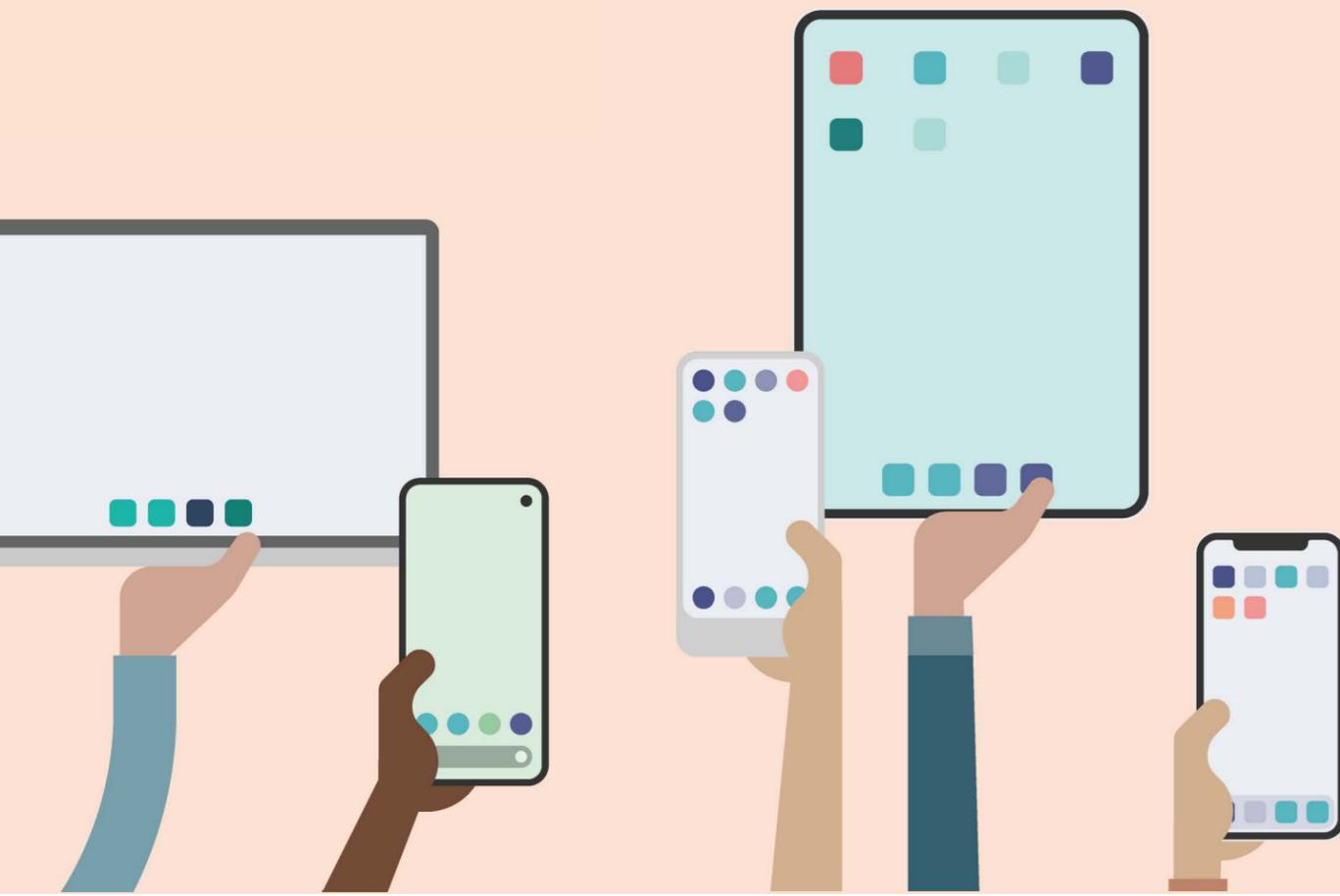
リモートワークにはさまざまなメリットがある一方で、セキュリティ上の課題も存在します。その課題は、使用する技術や、ユーザのセキュリティ知識や意識不足、増え続けるサイバー攻撃など、多岐にわたります。多くの場合、攻撃者がフィッシング攻撃やパッチが適用されていない脆弱性を利用してたった1台のデバイスを危険にさらすだけで、社内ネットワークの重要なリソースにアクセスできます。このような事象は、社内ネットワークの露出、ひいては情報漏えいにつながる可能性があります。



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)。

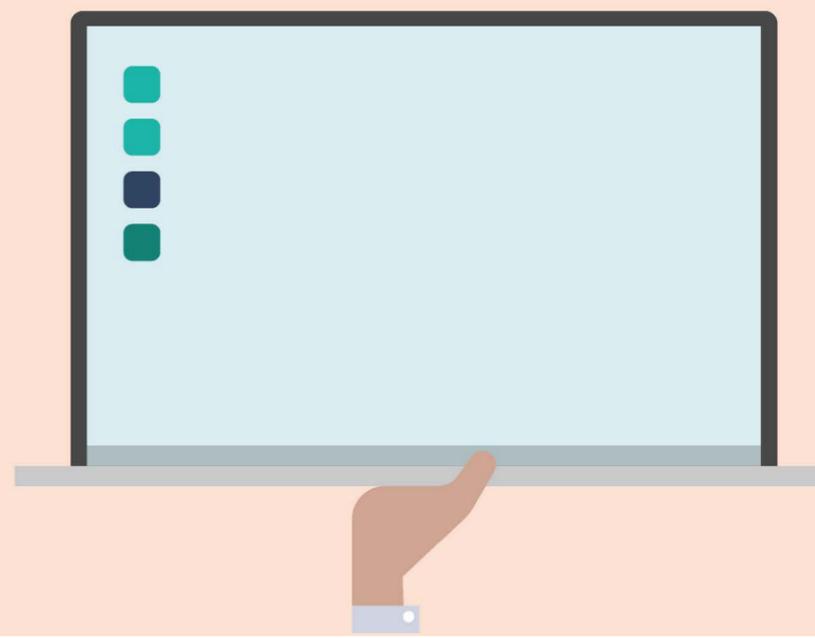
接続性や接続速度の問題により、生産性が低下。



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み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。

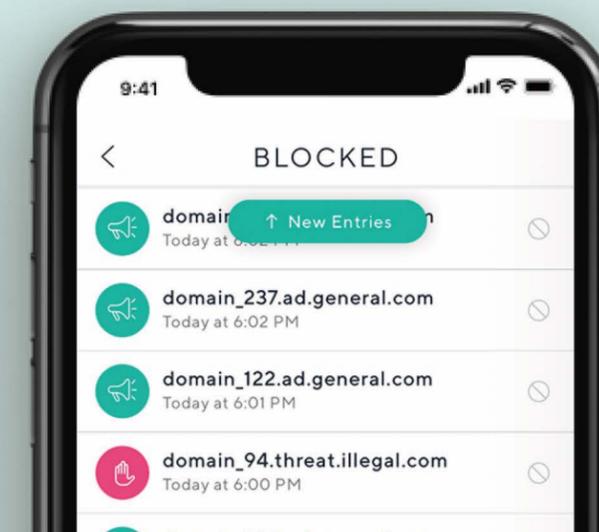
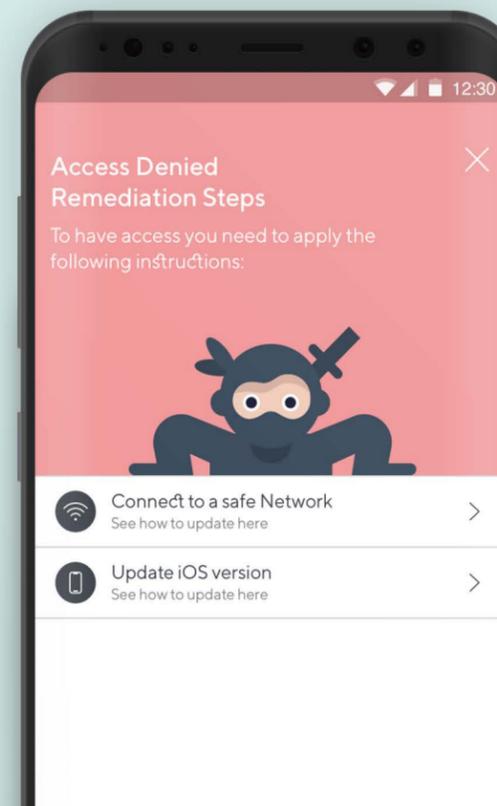
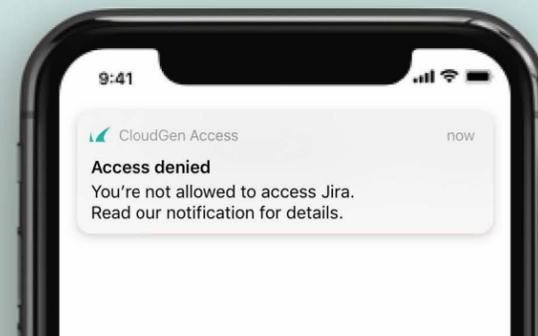
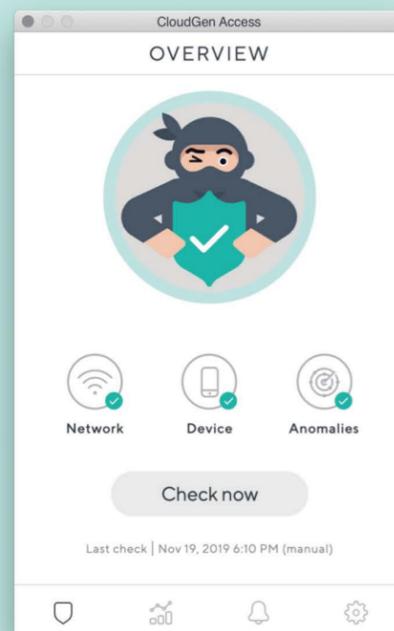
2. ネットワークをセキュアにする

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

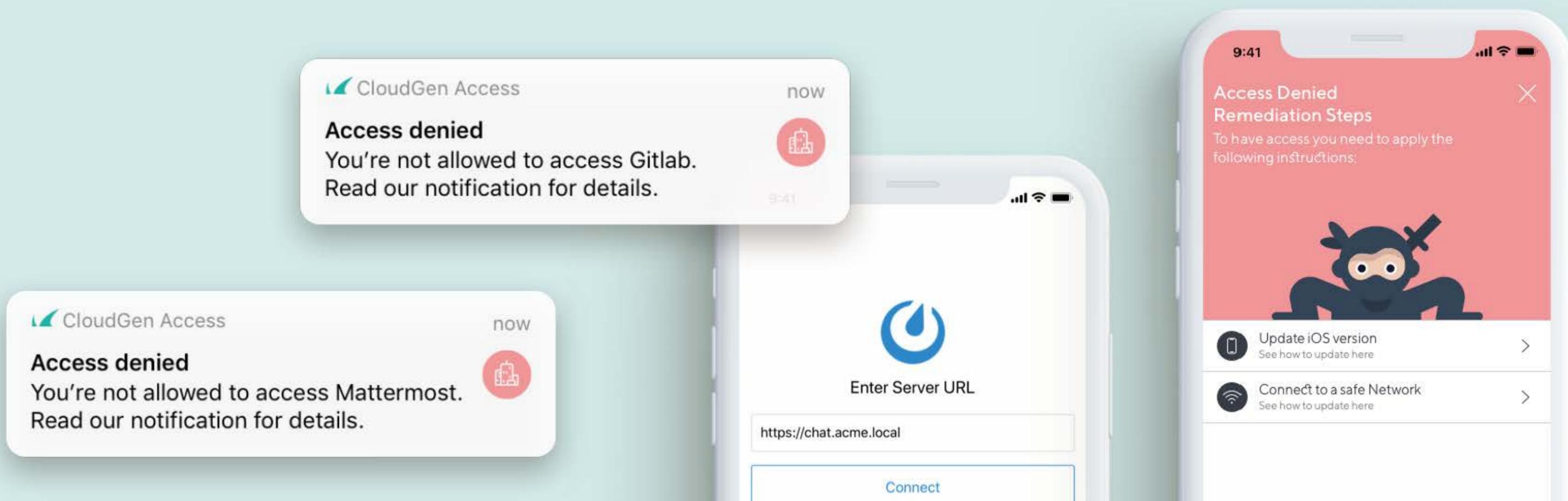
オンプレミスの アプリケーション

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。

The screenshot shows a web interface for managing access policies. The breadcrumb navigation is 'Access > Policies > DevOps team'. The main content area is titled 'Device Settings' and contains a table of security settings, all of which are currently enabled (indicated by green toggle switches).

Attributes	Settings	Status
	Role-based access control RBAC is enabled and denies access to all users and groups Platforms: Android, iOS, Linux, macOS, Windows	On
	Enable screen lock Require users to set a screen lock on their devices for additional security Platforms: Android, iOS, macOS Access App: ≥ v0.11.10	On
	Enable firewall NEW Require users to enable and configure a firewall on their devices for additional security Platforms: macOS Access App: ≥ v0.23.0	On
	Block jailbroken devices Enable to prevent compromised devices from gaining access to resources Platforms: Android, iOS Access App: ≥ v0.20.46540	On
	Enforce disk encryption NEW Require users to set disk encryption for additional security Platforms: Android, iOS, macOS Access App: ≥ v0.23.0	On
	Require Access App updates Require users to update the Access App to the latest version Platforms: Android, iOS, Linux, macOS, Windows Access App: ≥ v0.20.44888	On
	Require OS updates NEW Require users to update their device operating system (OS) to the latest version Platforms: Android, iOS, macOS, Windows Access App: ≥ v0.23.0	On
	Enforce re-authentication NEW	On

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。

The screenshot shows a web interface for 'yourcompany.access.com' with an 'Activity' section. It displays a list of records with columns for 'What', 'Who', and 'When'. A search bar is present at the top of the records section. A tooltip shows the date and time '8/9/2019, 10:57:28 AM' over the 'When' column of the first record.

What	Who	When
kafka-connect.dev.acme.com	TC Aryn Jacobssen	2 min ago 8/9/2019, 10:57:28 AM
Kubectl access granted to Kubernetes API US-Oregon	MS Mara Silverstone	5 min ago
SSH access granted to SSH App Dev	SD Shirline Dungey	5 min ago
Access App updated from version 2.2 to 2.3	GP Gabriel Pires	5 min ago
iOS updated from version 12.3 to 12.4	AC You	20 min ago
elasticsearch.acme.local	AL Angela Longoria	25 min ago
SSH access granted to Web Prod	AL Angela Longoria	25 min ago
chat.acme.local	GP Gabriel Pires	1 h ago
RDP access granted to Windows Bastion Host	GP Gabriel Pires	1 h ago
Access App enabled	GP Gabriel Pires	1 h ago
redis.stg.acme.local	AL Angela Longoria	1 day ago
Security checks have passed with warnings	GP Gabriel Pires	1 day ago
gitlab.acme.local	TC Aryn Jacobssen	1 day ago

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。

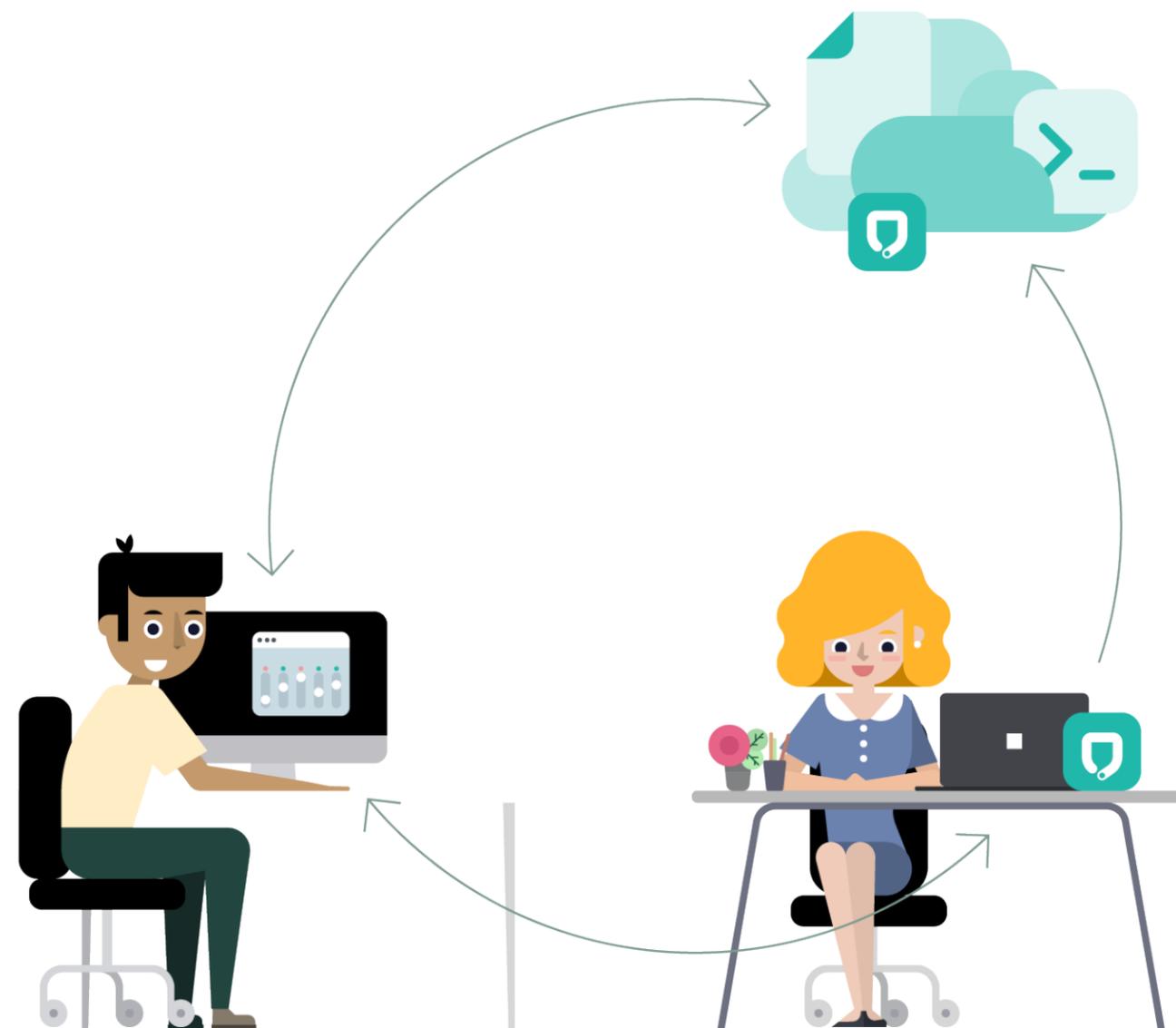
通常のVPNによる遅延なしに、素早く企業リソースにアクセスして仕事に集中できるようにする。



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 Access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 Access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。