BlackBerry. Intelligent Security. Everywhere.

CylanceGATEWAY

AI を活用し、プライバシーに配慮したゼロトラストネットワークアクセスソリューション

データシート

在宅勤務や個人所有デバイスの持ち込み（BYOD）といった方策が広く受け入れられている時代には、強固なネットワークセキュリティが欠かせません。リモートワークは便利さをもたらしますが、それと同時に組織の攻撃対象領域を大幅に増加させます。新たなデバイス、アプリケーション、ユーザーがビジネスリソースに接続するたび、新たなセキュリティリスクが発生します。リモートワーカーがさまざまなホームオフィステクノロジーをビジネスネットワークに接続する場合、こうしたリスクは急速に高まります。

最近の予測 [1] では、2021 年にはリモートワーカーの数が 2 倍になり、2025 年までには働く人の 70% が部分的にリモートで働くようになるとされています。このような労働形態の変化は、より多くのビジネスリソースが従来のネットワーク境界の外へと移動し、同時にネットワーク境界の外からアクセスされるようになることを意味します。リモートワーカーは多種多様なデバイスから仕事関連の SaaS（Software-as-a-Service）製品、そして組織のデータにより多くのアクセスを試みるようになり、これがセキュリティリスクを生じさることになります。

CylanceGATEWAY™ は、モバイルワーカーとリモートワーカーをサポートすることで生じる新たなセキュリティ上の脆弱性を軽減する、ゼロトラストネットワークアクセス（ZTNA）ソリューションです。ホームオフィステクノロジーのありとあらゆる組み合わせについて、それらをビジネスネットワーク上で許可する前に検証し、保護しようとするのは現実的ではありません。AI を活用したゼロトラストフレームワークを実装することで、CylanceGATEWAY は連続認証を行い、安全で信頼できるデバイスだけがビジネスリソースにアクセスできるようにします。ホームオフィスのデバイスやアプリのすべてが安全であるとは限りません。ビジネス環境に接続するデバイスやアプリはそれぞれ、アクセスの許可を受けるために自らの信頼性を証明する必要があります。

CylanceGATEWAY の機能

CylanceGATEWAY は、複数の高度なテクノロジーを 1 つにまとめ、ネットワーク環境を保護された状態に維持します。堅牢な TCP/IP スタック上に構築されており、モバイルデバイスとリモートデバイス向けに最適化されていて、暗号化されたパケット内の脅威を検知することが可能です。また、AI を用いて環境全体の疑わしい行動を検知し、アクセスをリアルタイムで調整するとともに、従来型のソリューションでは見過ごされることの多い脅威情報を相互に関連付け、コンテキストに応じて理解できるようにします。

[1] https://www.forbes.com/sites/carolinecastrillon/2021/12/27/this-is-the-future-of-remote-work-in-2021/?sh=5d30aff11e1d

CylanceGATEWAY は、ネットワークではなくアプリへのアクセスを制限し、IP を固定できるようにすることで、生産性を損なうことなく従業員を保護します。

AI を活用した、信頼に基づく、適応型の保護されたアクセス

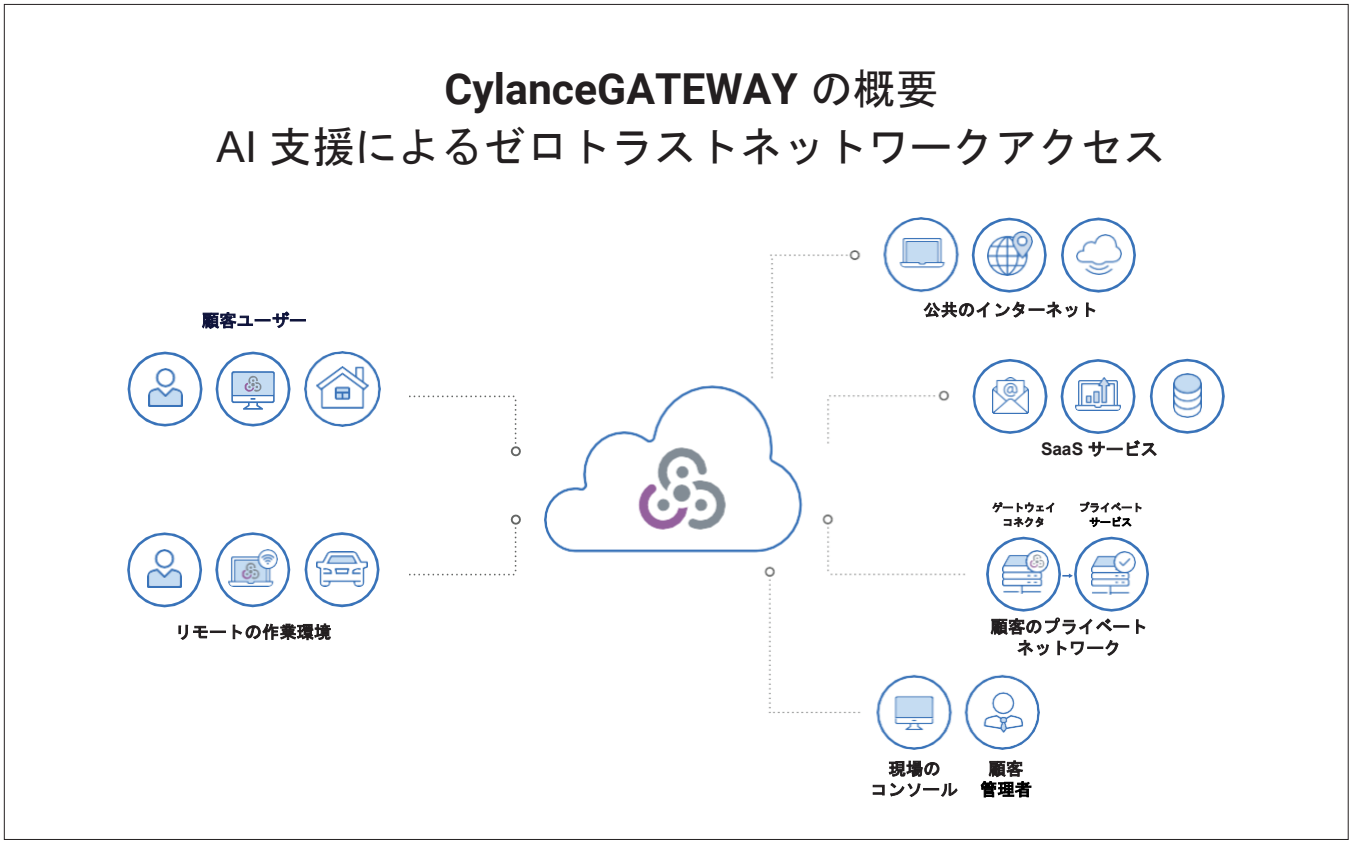
CylanceGATEWAY は、リモート参加者の信頼性とアクセス権限を決定する際、Cloud AI を用いてさまざまな要素を継続的に分析します。この参加者とは、ユーザーに限らず、環境にアクセスしようとするアプリケーションやボットの場合もあります。アクセスを評価する際、Cloud AI は以下の変数に基づいて信頼レベルを調整することができます。

- 参加者はリスクの高い場所から操作していないか。
- 参加者はなりすましをしていないか。
- 参加者は正常な行動を示しているか。
- 参加者は予測されるリソースにアクセスしているか。
- ユーザーの行動は、本人の過去のアクティビティや、同様の役割を持つ他のユーザーと一致しているか。

信頼スコアが大きく変化する際、Cloud AI はさまざまなアクションを取ることができます。信頼スコアがプラス方向に変化する場合、参加者は見返りとしてアクセスの継続またはアップグレードを受けられることがあります。信頼スコアがマイナス方向に変化する場合は、アクセスの制限、再認証のリクエスト、またはセキュリティアラートの表示と修正手順の実行につながることがあります。

フル/スプリットトンネルネットワークサービス

CylanceGATEWAY は、リモートユーザーまたはモバイルユーザーとビジネス環境との間の安全な通信トンネルを提供します。このトンネルは、組織のニーズに応じてフルアクセスモードまたはスプリットアクセスモードで動作します。



Cloud AI

CylanceGATEWAY の Cloud AI は、接続されているエンティティそれぞれについてネットワークのリスク要因を継続的に分析し、その信頼性に応じてアクセスレベルを動的に変更します。

フルモードでは、ユーザーとビジネスネットワークの間のすべての通信が保護されます。スプリットモードでは、管理者が指定したリソースについてのみ保護された通信を行い、その他のトラフィックはオープンなままにすることができます。スプリットトンネルのアプローチは、同一の BYOD またはホームオフィスデバイスからアクセスしているアプリを、個人用と仕事用に分けるのに役立ちます。

ソース IP の固定

Web サービスやクラウドアプリケーションの中には、組織が明示的に登録した IP アドレス以外からのネットワークトラフィックを拒否するものがあります。一部の組織では、IP アドレスを変更したり非表示にしたりするサイバーセキュリティ対策を単に省略することで、この制限に対応しています。こうした組織はトラフィックをサービスプロバイダに直接送信しており、これがセキュリティ上の脆弱性を生じさせます。

ソース IP の固定により、組織はセキュリティ対策を省略することなく、サービスプロバイダにデータを送信するデバイスの IP アドレスを管理できます。さらに、ネットワークに侵入して水平展開する手段を探っている外部の扇動者から内部リソースを見えなくすることもできます。

ネットワークアクセスではなくアプリアクセス

CylanceGATEWAY では、ビジネスリソースへのアクセスを許可する方法が VPN と異なります。VPN はネットワークに対して認証を行うため、攻撃者が攻撃に成功すると、その環境の広範囲にわたるアクセスを与えてしまいます。一方、CylanceGATEWAY はアプリへのアクセスを許可し、ネットワークについてそれ以上の可視性を与えないため、攻撃対象領域を大幅に削減できます。

また、CylanceGATEWAY の連続認証機能も VPN アプローチとは異なります。VPN は認証と承認に静的なアプローチをとります。VPN では、エンティティが最初の検証プロセスを通過すると、接続している間、そのエンティティは安全であると見なします。CylanceGATEWAY は外部のアクターを継続的に認証します。

ユーザーの行動、デバイスの信頼性、エンゲージメントの過程でのネットワークとアプリのアクセスパターンなど、複数の要素を調べます。Cloud AI が疑わしい点を感知すると、検知の重大度に応じて、環境を保護するための措置をただちに講じます。

強力な TCP/IP セキュリティ

CylanceGATEWAY は、モバイルデバイスや低消費電力デバイス向けに最適化された IP セキュリティレイヤーを備える堅牢な TCP/IP スタック上に構築されており、VoIP をはじめとした幅広いプロトコルのサポート、クラウドネイティブアーキテクチャ、フルトンネル/スプリットトンネルアクセスモードを提供します。CylanceGATEWAY を利用する組織は、SaaS アプリの識別を使用して、O365 などのサービスでエラーが発生しないようにできます。また、CylanceGATEWAY の IP レピュテーション機能で悪意のあるドメインと場所を特定し、危険なネットワークエンティティとのやり取りから従業員を保護することもできます。

ネットワーク脅威の検知

CylanceGATEWAY は、暗号化されたパケット内を含めてネットワークトラフィックに存在する脅威を検知し、ネットワーク全体で特定された脅威情報をコンテキストに応じて理解できるようにします。環境全体の情報を分析して関連付ける機能により、他の分析形式では可視化できない、複雑かつ多段階の脅威を識別することができます。CylanceGATEWAY のアプローチはパフォーマンスが高く、パケットの復号/再暗号化が不要なため、結果としてネットワークリソースへの負担が少なくなります。暗号化されたパケット内の脅威を検知することで、ネットワーク上の参加者のプライバシーを損なうことなく環境を保護します。

CylanceGATEWAY の一般的な使用事例

CylanceGATEWAY は、ネットワークセキュリティに対して AI を活用したゼロトラストアプローチをとることにより、今日の組織が直面する多くの現実的な問題を解決します。

ビジネス環境を強化する CylanceGATEWAY の機能には、以下のようなものがあります。

AI を活用した ZTNA

公共のインターネット、SaaS アプリケーション、オンプレミスアプリケーションに対するあらゆる場所からのアクセスを保護します。VPN を用いることなく、忠実度の高い VVoIP と安全なブラウジングを実現します。

動的なネットワークアクセス制御

ユーザーまたはグループの行動分析に基づくリアルタイムのネットワークリスクスコアを用いて、ネットワークアクセス制御を調整します。

AI を活用したネットワーク脅威の検知

ネットワークパケットの復号を必要とせずに、AI を用いてネットワークの脅威と異常を検知します。

ソース IP の固定

承認されていないユーザーがビジネスリソースやネットワークリソースにアクセスすることを制限します。ソース IP の固定により、組織はセキュリティ対策を省略するなどの手法を使用することなく、SaaS プロバイダにデータを送信するデバイスの IP アドレスを管理できます。

ワンクリック構成

Microsoft 365 などの主要な SaaS アプリへのアクセスを構成できます。

カスタマイズ可能なダッシュボード

SecOps では、ネットワークのトラフィックパターン、侵害、アラートを分析できます。NetOps では、コネクタの状態、アクセス履歴、上位の宛先を分析できます。

もっと詳しく

CylanceGATEWAY は、AI を活用した、防御型の、BlackBerry が提供する世界的なセキュリティソリューションの 1 つです。CylanceGATEWAY に関するその他の情報や組織のサイバー攻撃に対する準備、防御、検知、

対処を支援するために設計されたスイート製品全般につ
いては、以下をご覧ください。

詳細はこちら：

CylanceGATEWAY

BlackBerry® Cyber Suite

BlackBerry Intelligent Security. Everywhere.

BlackBerry（NYSE：BB；TSX：BB）は、インテリジェントなセキュリティソフトウェアとサービスを世界中の企業と政府機関に提供しています。BlackBerry のソリューションは、1 億 9,500 万台の自動車をはじめ、5 億以上のエンドポイントを保護しています。BlackBerry はカナダのオンタリオ州ウォータールーに本拠を置き、AI と機械学習を活用してサイバーセキュリティ、安全、データプライバシーソリューションの分野に革新的なソリューションを提供しています。また、エンドポイントセキュリティ管理、暗号化、組み込みシステムの分野におけるトップクラスの企業です。BlackBerry のビジョンは明確です。つながる未来に信頼性あるセキュリティを確保することです。

*詳細については、**BlackBerry.com** にアクセスし、**@BlackBerryJPsec** をフォローしてください。*