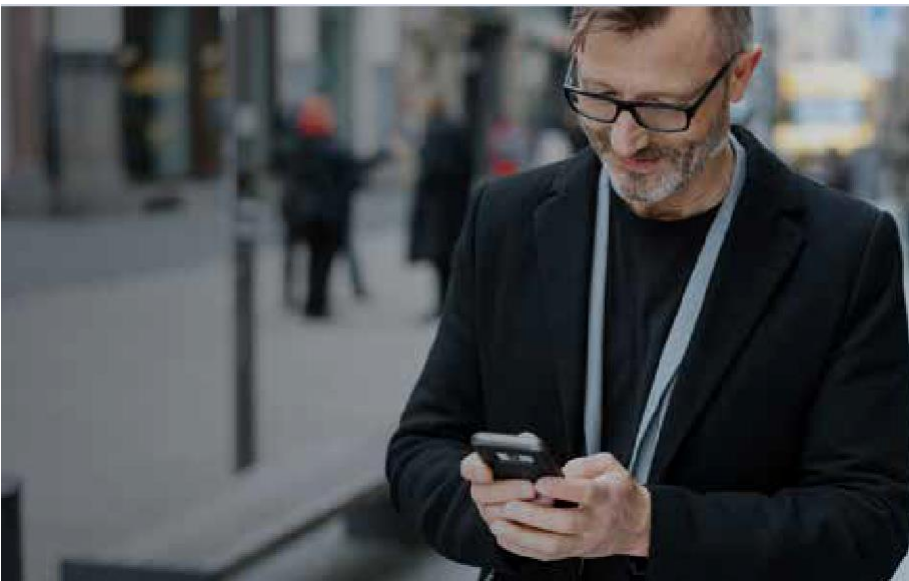


CylancePERSONA

AI 駆動の継続的な認証と行動分析



ゼロトラスト
アプローチによる
アイバーセキュリティポ
リシーの採用に努めて
いる組織は、デスクトッ
プデバイス向け
CylancePERSONA が
基礎をなす要素である
ことを認識しています。

デスクトップ用 PERSONA の概要

CylancePERSONA™ は、AI を活用した継続的な認証と行動分析のソリューションです。その目的は、疑わしいユーザーをリアルタイムで特定してセキュリティ侵害を防ぐことです。主な機能は次のとおりです。

- 行動分析と行為分析の両エンジンを使用して、盗まれた資格情報の悪用を防御。
- 悪意のある行為分析エンジンを使用して、内部関係者による脅威を防御。
- 二要素認証方式、ネットワーク削除、ユーザーアカウントの一時停止など、エンドポイントでのリアルタイムの軽減措置。
- 直感的で使い慣れた単一のクラウドコンソールに、すべてのエンドポイントイベントとユーザー信用スコアをほぼリアルタイムで表示。
- Ping、OKTA などのサードパーティプロバイダーと統合することで、Webアプリの継続的な認証を実現。

主なユースケース

ゼロトラストアプローチによるサイバーセキュリティポリシーの採用に努めている組織は、デスクトップデバイス向け CylancePERSONA が基礎をなす要素であることを認識しています。モバイルデバイス向け CylancePERSONA (BlackBerry Spark® Unified Endpoint Management Suite のコンポーネント)で実証されたように、デスクトップ向け CylancePERSONA は、行動分析と行為ベースの機械学習モデルを活用して、デバイスのユーザー信用スコアをリアルタイムで作成します。この情報は、ユーザーの資格情報に関連した攻撃を数分以内に阻止できる、自動化された軽減措置をトリガするために使用されます。CylancePERSONA を導入すれば、以下のような企業のセキュリティ問題を速やかに解決できます。

- **資格情報の盗難** – CylancePERSONA は、従業員の資格情報が漏洩したときに被る損害から組織を守ります。CylancePERSONA は、行動分析と行為のモデルを使用し、ユーザーとデバイスのやりとりをリアルタイムで分析して、ユーザーのリスクを判定します。ユーザーがリスクのしきい値を超えるとアラートがクラウドに送信され、二要素認証方式を促すなど、自動化された軽減措置が講じられます。
- **内部関係者による脅威** – CylancePERSONA は、従業員の行為を継続的に分析し、その行動に悪意があるかどうかを判定することで、不正を働く従業員がもたらす被害から組織を守ります。リスクのあるアプリケーションのダウンロードやデータの持ち出しなど、従業員の普段の行動が行動基準から逸脱している場合、そうした行為は CylancePERSONA により異常と見なされます。管理者が定義したポリシーに基づいて、アラートとプロアクティブな措置が実施されます。
- **物理的な不正アクセス** – CylancePERSONA は、デバイスが物理的な不正アクセスや盗難の被害を受けた場合に従業員と組織を攻撃から保護します。権限のないユーザーがエンドポイントにアクセスすると、行動分析モデル(キーストローク、マウス)が新しいユーザーを検知して、アラートの送信やデバイスのロックを行うことができます。デバイスのロックはエンドポイントで自動的に行われるため、ネットワーク接続やクラウドとのやりとりは不要です。

「...デスクトップ向け CylancePERSONAは、行動分析と行為ベースの機械学習モデルを活用して、デバイスのユーザー信用スコアをリアルタイムで作成します」



BlackBerry Persona の仕組み

CylancePERSONAの機械学習機能により、システムは複数ユーザーの行動と場所のパターンを特定し、場所のリスクを判定します。たとえば、同じ場所で大規模な従業員集団の反復パターンが特定された場合、そこは自動的に勤務場所と判定されます。または企業の判断により、その場所を既知の場所としてあらかじめ組み込むこともできます。

継続的な認証で CylancePERSONA は、行動分析を使用してデスクトップソフトウェアの標準的な使用パターンを認識し、どの行動が高リスクまたは低リスクであるかをリアルタイムで判定します。使用ベースのパターンには、時刻とユーザーによるソフトウェアの使い方（内部転送か外部転送か）などが含まれます。CylancePERSONA は他のさまざまな要因に基づいて、従業員または請負業者のプロファイルに許可するアクセスレベルをいつでも決定できます。主な例を以下に示します。

- **行動分析:** CylancePERSONA は、ユーザーの入力特性を評価して行動分析の基準を決定します。この基準により、ユーザーの資格情報の確実性が判定されます。
- **行動場所:** CylancePERSONA は、非特定化された場所データの予測分析に基づいてユーザーの頻度とパターンを考察し、場所に基づくリスクスコアを決定します。
- **ネットワークの信頼性:** CylancePERSONA は、ネットワークの使用頻度を特定し、そのプロファイルに基づいてセキュリティを動的に調整します。公共 Wi-Fi に初めてアクセスする場合は、それに応じてリスクスコアが調整されます。
- **使用状況の異常*:** CylancePERSONA は、アプリケーションの使用状況を評価し、異常な使用状況から許容できる使用状況を推測し、ユーザーの資格情報の信頼性を判定します。

リスクスコア分析:セキュリティ要件の動的な採用

CylancePERSONA は、リアルタイムのリスク分析に基づいてアクセスを許可し、認証チャレンジを発行する独自の機能を備えています。そのため、セキュリティポリシーを損なわずにエンドユーザーエクスペリエンスと生産性を高めることができます。リアルタイムのリスクスコア分析に基づいて、以下の処理を実行できます。

- アクセスの許可
- ポリシーの採用
- 認証チャレンジの発行
- アラートと修復

CylancePERSONA はセキュリティとポリシーの状態を動的に適合させ、必要に応じて修復を施します。そのため、ユーザーエクスペリエンスとセキュリティ/ポリシーの状態は動的かつ相互に最適化され、矛盾は起きません。

*保留中の機能

「継続的な認証で CylancePERSONA は、行動分析を使用してデスクトップソフトウェアの標準的な使用パターンを認識し、どの行動が高リスクまたは低リスクであるかをリアルタイムで判定します」

CylancePERSONA のメリット

処理のためにすべてのデータをエンドポイントからクラウドにまず送信しなければならない従来のソリューションとは異なり、CylancePERSONA では、信頼できる情報源であるエンドポイントの暗号化されていないクリーンデータを利用して処理します。さらに、CylancePERSONA のデータとロジックはエンドポイントにあるため、検知の時間短縮と、広範囲にわたるプロアクティブな軽減措置が可能になります。

検知の時間短縮



数日間のセキュリティ侵害で大量のデータが流出するおそれがあります。CylancePERSONA は、資格情報の悪用を制限することで、セキュリティ侵害に迅速に対処して保護を提供します。

正確性の向上



CylancePERSONA が際立っているのは、クラウドにデータを送らずに、エンドポイントでのローカルなユーザーの行動に基づくスコアリングを備えている点です。

コストの削減



CylancePERSONA はエンドポイントに存在するため、ユーザーのすべての分析とスコアリングをエンドポイントで継続的かつリアルタイムに行うことができます。そのため、クラウドに送信して保管する必要があるデータの量が大幅に減少します。

管理の強化



管理コンソールで生成されるアラートに加えて、二要素認証、ネットワークアクセスの制限、ユーザーアカウントの一時停止などのプロアクティブな措置を CylancePERSONA はエンドポイントで実施します。

BlackBerry について

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およびサービスを世界中の企業や政府機関に提供しています。現在セキュリティで保護しているエンドポイントの数は5億台を上回り、そのうちの1億9,500万台は道路を走行する車両です。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。

詳しい情報については、[BlackBerry.com](https://www.blackberry.com) をご覧ください。また、[@BlackBerry](https://twitter.com/BlackBerry) をフォローしてください。



 **BlackBerry**
Intelligent Security. Everywhere.