

BlackBerry Spark UES スイート

ゼロトラストとゼロタッチの隙間を埋める





データおよびエンドポイントのセキュリティを確保・保護するといった課題は新しい要件ではありません。ただ、その重要性はかつてないほど高まっています。モバイルからモノのインターネット(IoT)に及ぶ新しいタイプのエンドポイントの普及、そして世界的なりもネットワークの高まり。このような動きが重なることで新たな攻撃対象領域が急速に拡大しつつあり、状況は混乱を極めています。データおよびエンドポイントのセキュリティ確保と保護がゼロトラストと密接に関連するようになるにつれて、ゼロトラストフレームワークの概念と具体化がかつてないほど重要になっています。

ゼロトラストが作られたのは、脱境界化、または企業ネットワーク境界の浸食に対応するためです。テクノロジーの普及とクラウドベースアプリの台頭により、CISO は、外部から入ってくるトラフィックより組織内のトラフィックのほうが信頼性が高いという考えを変えざるを得ませんでした。ゼロトラストの目的は、信頼を築くこととアクセスを制限することに尽きます。つまり、信頼できるユーザーが信頼できるデバイスを使うことを徹底させながら、そのユーザーのアクセスを仕事に必要なデータとアプリに制限します。2020年3月までは、ゼロトラストの要件と作業者の生産性とのバランスを取ることが非常に困難でした。しかし、この時期を境に組織が全世界の従業員の勤務形態を在宅勤務モデルへと一夜にして移行したことで、状況は変わりました。その結果として、今度はゼロトラストと事業継続性が、優先的に解決すべき課題の筆頭となっています。

BlackBerry による課題への対応:

BlackBerry® Unified Endpoint Security(UES)スイートは特定の目的をもって設計されたセキュリティ制御のセットであり、ゼロトラストのフレームワークを提供し、必要な作業を最小限に抑える(ゼロタッチ)ユーザーエクスペリエンスを実現します。BlackBerry UES スイートは、最新式のセキュリティ制御とプロセスの統合セットです。従来のエンドポイントからモバイル、IoT デバイスへと広がるセキュリティ制御に加え、ゼロトラストのセキュリティアーキテクチャの基盤を提供します。







AI セキュリティ



BlackBerry Unified Endpoint Security のコンポーネントは、ゼロトラストのエンタープライズセキュリティアーキテクチャの基盤として連携します。あらゆるセグメントの高度なゼロトラストの専門家によると、このアーキテクチャを採用した結果、次のように、複数のメリットがあったとのこと。

- 可視性の向上によるセキュリティ体制の強化、および制御性の向上による優れたリスク緩和策の実現
- ラップトップやサーバーからモバイルおよび IoT デバイスにわたるすべての攻撃対象領域の保護および管理
- 導入と管理が容易な統合プラットフォームの使用による、時間とコストの節約

BlackBerry UES を使用することで、セキュリティチームのスピードとアジリティが促進されるとともに、多様な IT インフラストラクチャ全体に優れた可視性が提供されます。

コンポーネント	説明
 エンドポイント保護	人工知能(AI)と機械学習の機能の活用により、BlackBerry® Protect では自動マルウェア防御、アプリケーションとスクリプトの制御、メモリ保護、デバイスポリシー適用が提供されます。また、サイバー攻撃を予測し、防止します。その効果は桁外れで、使いやすく、システムへの影響は最小限です。
 エンドポイント検知/対応(EDR)	業界をリードする防御型の EDR でシステムおよびユーザーの行動を監視します。自動的に反応することによってリアルタイムの保護を提供します。BlackBerry Spark® プラットフォームの AI ベース対応テクノロジーを使用するプレイブックベースのワークフローを用いて、調査と対応を自動化します。
 モバイル脅威対策(MTD)	モバイル向け BlackBerry Protect は、デバイスおよびアプリケーションレベルで悪意のある高度な脅威を防止、検知、修正します。BlackBerry® UEM のモバイルエンドポイント管理機能と高度な AI 駆動型の脅威防御との組み合わせにより、ゼロトラスト環境での悪意のあるサイバー攻撃に先手を打ちます。
 連続認証	BlackBerry® Persona は、生体認証、アプリ使用率、ネットワークおよびプロセスの起動パターンに基づいて、信用を生み出します。モバイルデバイス全体で適応リスク評価と動的なポリシー適用を用いて、連続認証を提供します。
 情報漏洩対策(DLP) <i>将来リリース予定</i>	監視、フィルタリング、ブロックなどの修正機能を使用して、不注意による、あるいは偶発的なデータの消失を含むデータ関連の脅威に対処します。
 セキュア Web ゲートウェイ <i>将来リリース予定</i>	ユーザーの Web 閲覧から不要なソフトウェアおよびマルウェアをフィルタリングすることによって、Web サイトの閲覧ができるエンドポイントを感染から保護し、会社および規制上のポリシーへの準拠を強化します。

BlackBerry® Enterprise Identity は、共通サービスとして含まれます



エンドポイント保護

BlackBerry Protect は自動化された防御優先のアプローチを用いて、組織のエンドポイントでマルウェアが実行されるのを阻止します。多様な形態のランサムウェア、ゼロデイ攻撃、その他のマルウェアを含むセキュリティ侵害を防止します。また、スクリプトベースの攻撃、ファイルレス攻撃、メモリ攻撃、および外部デバイスベースの攻撃を阻止する予防手段も含まれています。このような保護を実現するのに、ユーザーまたは管理者の介入、クラウド接続、シグネチャ、ヒューリスティック、サンドボックスは必要ありません。

機能:

- ④ **マルウェア防御**
 - 人工知能と機械学習を用いた核となる防御テクノロジーで、マルウェアを検知および阻止
 - Microsoft® Windows®, macOS®, Linux® の環境を保護
- ④ **デバイス使用ポリシーの適用**
 - USB マスストレージデバイスの使用を制御
 - リムーバブルメディアを介したデータ窃取を防止
- ④ **アプリケーション制御**
 - 固定機能デバイスをロックダウンし、変更を制限
 - 新しいアプリケーションの追加を防止
- ④ **メモリ保護**
 - 事前にメモリベースの攻撃を特定し、阻止
 - きめ細かい除外処理と強化されたトラブルシューティングおよびレポートを許可
- ④ **スクリプト制御**
 - 不正スクリプトの実行を阻止
 - きめ細かいホワイトリストおよびセーフリストの機能により、管理者制御を強化
 - 特定のアプリケーション内で実行されない限り、PowerShell のようなスクリプトのブロックを可能にするペアレンティング制御を含む。

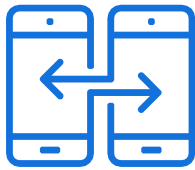


エンドポイント検知/対応(EDR)

BlackBerry® Optics は一種の EDR ソリューションであり、人工知能を用いてセキュリティインシデントを防止することによって、BlackBerry Protect で提供される脅威防御を拡張します。BlackBerry Optics は真の AI インシデント防御、根本原因分析、スマートな脅威ハンティング、自動化された検知/対応/修正を提供します。他の EDR 製品と異なり、BlackBerry Optics では、オンプレミスのインフラストラクチャにそれほど多くの投資を行う必要がありません。保管および分析の目的でクラウド環境に連続的にデータをストリーミングすることも、技術的な専門知識を使用することも不要です。BlackBerry Optics とその真の AI インシデント防御機能は、エンドポイントで実行できるように設計されています。この軽量のアーキテクチャが意味するのは、シンプルなユーザーインターフェイス、自動化された対応と修正を特徴とする EDR 機能を組織が手頃な値段で導入できるということです。

機能:

- ① **分散型の検索と収集**
弊社独自のデータ収集アプローチにより、データ収集、検索、分析を最適化します。
- ② **クロスプラットフォームでの一貫した可視性**
Microsoft Windows、macOS、Linux のエンドポイントへのサポートにより、1つのソリューションで組織の環境全体の状況を常に把握できます。
- ③ **根本原因分析**
BlackBerry Protect によってブロックされた攻撃、およびエンドポイントで特定された他の注意を要するアーティファクトに関する、Web ベース、オンデマンドの根本原因分析です。
- ④ **企業全体での脅威ハンティング**
エンドポイントデータを即時に検索し、エンドポイントに隠れている潜在的な脅威を見つけます。
- ⑤ **迅速なインシデント対応**
検疫、疑わしいファイルの取得、セキュリティ侵害を受けたエンドポイントのネットワークからの隔離など、インシデント対応アクションを迅速に実行します。
- ⑥ **動的な脅威検知**
カスタムおよびキュレーションされた検知ルールを使用して、潜在的な脅威のリアルタイム検知を自動化します。
- ⑦ **クラウド依存ではなくクラウド対応**
各エンドポイントにローカルインテリジェンスが提供されるため、接続性または人的介入に依存しません。
- ⑧ **リモート対応**
直観的および対話的にスクリプトを実行し、従来またはネイティブのコマンドをシステムに対して実行するためのインターフェイスを提供します。これにより、ほぼリアルタイムで、これらのコマンドの結果にすばやく優先順位を付けて表示できます。
- ⑨ **回避**
インフラストラクチャ全体で悪意のあるイベントの修正を自動化します。
- ⑩ **自動化された対応**
ルールセットに関連する自動化された対応アクションをカスタマイズして、滞留時間を減らします。



モバイル脅威対策 (MTD)

モバイル向け BlackBerry Protect は、BlackBerry UEM で提供されるセキュリティ基準を強化するモバイル脅威対策 (MTD) ソリューションです。デバイスおよびアプリケーションレベルで悪意のある脅威を防止、検知、修正します。BlackBerry UEM のモバイルエンドポイント管理機能と高度な AI 駆動型の脅威防御が統合されます。モバイル向け BlackBerry Protect により、モバイルデバイスは、ゼロトラスト環境で悪意のあるサイバー攻撃より優位に立つことができます。

機能:

- ④ **iOS® サイドロードアプリケーション検知**
サイドロードアプリケーションのすばやい検知とスキャンが実行されます。
- ④ **Android™ マルウェアスキャン**
- ④ **UEM アプリストアの Android および APK マルウェアスキャン**
BlackBerry UEM アプリストアのすべてのアプリケーション (カスタムパートナー、カスタマーアプリケーションを含む) がスキャンされ、マルウェアから保護されます。
- ④ **フィッシングおよび悪意のある URL 検知**
BlackBerry Protect の AI が絶えず稼働して、マルウェアまたは悪意のある URL がどのような様子で、どの URL にフィッシング要素が埋め込まれているのかを判断します。
- ④ **Android および iOS 用のオフライン防御**
- ④ **BlackBerry® Dynamics™ SDK アプリ用の iOS アプリ完全性チェック**
BlackBerry Protect は、BlackBerry Dynamics SDK プラットフォーム上に構築されたアプリケーションの完全性を保証し、セキュアなアプリだけがデバイスにダウンロードされるよう徹底します。BlackBerry® アプリケーションの改ざんも防止します。
- ④ **統合ダッシュボードレポート**
BlackBerry UEM のダッシュボードおよび通知を利用したエンドユーザーの監視およびアラートにより、アナリストがマルウェアおよびハッキングイベントをリアルタイムで迅速に修正できます。



連続認証

BlackBerry® Persona は機械学習と予測 AI を用いた連続認証を提供して、ユーザーの場所、デバイス、その他の要素に基づきセキュリティポリシーを動的に適応させます。また、モバイルデバイス全体で適応リスク評価と動的なポリシー適応を用いて、連続認証を提供します。ユーザー認証のエクスペリエンスを向上させることによって、BlackBerry Persona は人的ミスおよび善意による回避策から環境を保護します。

機能:

① 適応リスク評価

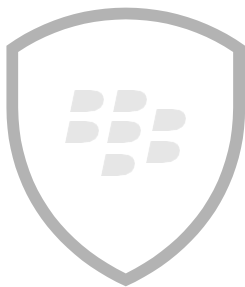
- 行動の位置: ユーザーの頻度とパターンに注目し、匿名化された位置データの予測分析に基づいて位置情報ベースのリスクスコアを求めます。
- ネットワークトラスト: ネットワーク利用の頻度を測定し、そのプロファイルに基づいて動的にセキュリティを調整します。たとえば、初めてパブリック Wi-Fi にアクセスすると、それに伴ってリスクスコアが調整されます。
- 時間および使用率の異常: 他の ID プロバイダおよびシステムとシームレスに統合します。BlackBerry の実績あるセキュリティインフラストラクチャにより、すべてのデータをセキュアかつ容易に共有できます。
- デバイスおよびアプリの DNA: デバイスおよびアプリが準拠し、最新であるかどうかを判断する機能です。BlackBerry Persona を使用すれば、デバイスおよびアプリの DNA プロファイルに基づきセキュリティポリシーを調整できます。

② 動的なポリシー導入

- アクセス権の付与
- ポリシーの導入
- 認証チャレンジの発行
- アラートと修正

③ 連続認証

- パッシブ生体認証など使用率に基づくパターンを利用して、存在を感じさせず継続的にユーザー ID を検証します。
- 異常な行動を示した悪意のあるユーザーは、アクセスしようとしているアプリから自動的にブロックされます。
- セキュリティ体制を強化し、それと同時に、静的なタイムアウトを設ける場合よりもエンドユーザーのエクスペリエンスが向上します。



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エンタープライズと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 5 千万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ローに本拠を置き、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。

BlackBerry のインテリジェントなセキュリティをあらゆる場所に。

詳細については、BlackBerry.com にアクセスし、[@BlackBerry](#) をフォローしてください。