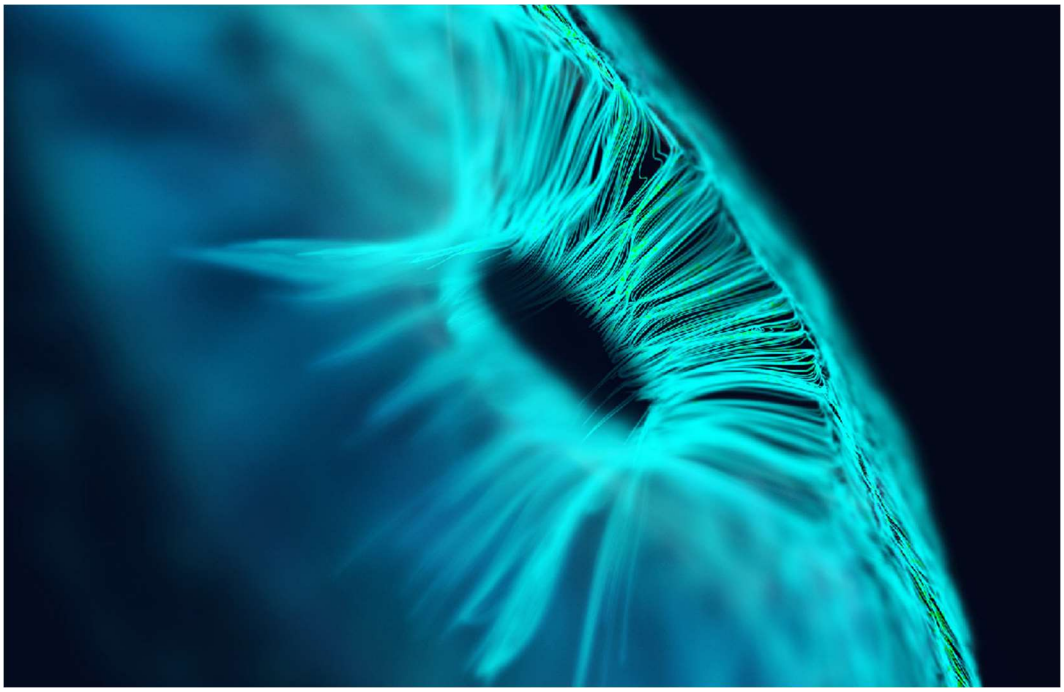
BlackBerry
Intelligent Security. Everywhere.

データシート

BlackBerry Optics

AIを活用したエンドポイント検知／対処



予防ファーストのEDR

シグネチャに依存する防御製品では、目まぐるしく変化する今日の攻撃に追従できず、セキュリティチームが日々大量のアラートの調査に追われる状況は変わりません。これではセキュリティ上の重大なリスクを見つけることはほぼ不可能であり、攻撃者は企業全体に蔓延したままです。

予防ファーストのセキュリティであれば、セキュリティスタックによって生成されるアラートの数を大幅に減らし、終わりのない無駄なアラート調査に伴う負担とフラストレーションを軽減できます。

BlackBerry® Protectがマルウェア、悪意のあるスクリプト、不正なアプリケーション、ファイルレス攻撃がビジネスに被害を及ぼすのを防止するのに対し、BlackBerry® Opticsは、データとビジネスのセキュリティ確保に必要な、AIを活用したEDR機能を提供します。

BlackBerry Opticsは、AIを使用して広範囲に及ぶセキュリティインシデントを特定、防止することによって、BlackBerry Protectが提供する脅威防御を拡張するよう設計されたエンドポイント検知／対処（EDR）ソリューションです。

AIの活用

BlackBerry Opticsは、広範囲に及ぶセキュリティインシデントをAIを活用して特定、防止することによって、BlackBerry Protectが提供する脅威防御を拡張するEDRソリューションです。BlackBerry Opticsの機能には次のものがあります。

- AI駆動型のインシデント防御
- コンテキストに基づく脅威検知
- 機械学習による脅威の特定
- 根本原因分析
- スマートな脅威ハンティング
- 自動化されたリモート調査
- 対応スクリプトに基づく動的な対処機能

特長

- 滞留時間を減らし、セキュリティ侵害によって生じる可能性のある影響を低下させる
- セキュリティスタッフのスキルレベルに関係なく、一貫性のあるセキュリティレベルを維持
- 攻撃からの回復にかかる時間と費用を大幅に削減

BlackBerry Optics

導入や維持管理が難しいだけでなく使いづらい他のEDR製品とは異なり、BlackBerry Opticsには次のような特徴があります。

- エンドポイントに数分でインストールでき、ハードウェアやネットワークインフラ増強は不要
- データをエンドポイントにローカルに保存、分析することで、定期的な更新が不要で、遅延のない検知と対処を実現
- 静的な検知ルールでは見つけにくい脅威を発見することを目的とした、機械学習による脅威検知モジュールと自動アクション機能を提供

BlackBerry Opticsは、BlackBerry Protectと連携して、攻撃者の一歩先を行くために必要な検知および防御機能を提供し、ビジネスのセキュリティを確保します。

BlackBerry EDRソリューションの2.4リリースでは、InstaQuery、FocusView、BlackBerry OpticsのContext Analysis Engine（CAE）ロジックで機能向上が図られており、より優れた可視性機能が提供されます。これらの機能向上のいくつかを以下に示します。

- レジストリ検査の向上
- DNSの可視性
- Windows®ログオンイベントの可視性
- RFC 1918アドレス空間の可視性
- Windows APIを通じたWMI検査の向上
- Windows APIを通じたPowerShell検査の向上

BlackBerry Opticsの2.4リリースには、EDR検索パラメータを幅広さと深さの両面で支援するためのいくつかの製品拡張が含まれています。これらの拡張は、

基盤となるBlackBerry ProtectのAIベースの保護機能とローカルに保存されるインテリジェンスに基づいて構築されており、CAEルールのトリガーが発生した場合に、それを調査、トリアージ、修復するための確実な情報をリアルタイムで提供します。これにより、セキュリティ担当者は脅威ランドスケープに応じた速度で調査と修復を行うことができます。クラウドへのクエリ、長期間のフォレンジック分析、その他の時間がかかるプロセスによって遅延が発生することはありません。セキュリティインシデント対処チームは、イベントのトリガーの前後に発生したすべてのアーティファクトを理解できます。その結果、次のようなメリットが得られます。

- InstaQuery、FocusView、CAEルール内の検索パラメータの柔軟性が向上
- インシデントへの対処が迅速化
- MITRE ATT&CKフレームワークとの整合性
- CAEルールによる自動対処の拡張

BlackBerry Optics EDRソリューション

エンタープライズ対応	検知	調査と対処
· 分散型の検索と収集 · クロスプラットフォームの可視性 · APIへのアクセス · Syslogとの統合	· コンテキストに基づく検知 · 機械学習モジュール · MITRE ATT&CKフレームワーク	· 第2世代 · クラウド拡張モデル

BlackBerry Opticsは、BlackBerry Protectと連携して、攻撃者の一歩先を行くために必要な検知および防御機能を提供し、ビジネスのセキュリティを確保します。

一般的なエンドポイント検知／対処の使用事例

- **悪意のあるアクティビティの阻止**：BlackBerry Opticsの基盤を提供するBlackBerry Protectは、エンドポイントを標的にした攻撃の成功を阻止することに特化して設計されています。これには次の要素が含まれます。
  - AIを活用して悪意のある実行可能ファイルや他のファイルを特定してブロックする
  - スクリプトを実行できる場所、方法、およびユーザーを制御する
  - USBデバイスの使用法を管理し、不正なデバイスを禁止する
  - 攻撃者がファイルレスマルウェア攻撃の手法を使用できないようにする
  - 悪意のある電子メール添付ファイルのペイロードのデトネーションを防止する
- **攻撃とアラートデータの調査**：あらゆるアラート関連アクティビティをわかりやすく可視化して、BlackBerry Protectを含む他のセキュリティコントロールからのアラートを調査し、エンドポイントから有益な情報を取得できます。
- **企業全体の脅威の探索**：ネットワークエンドポイント全体でファイル、実行可能ファイル、ハッシュ値、および他のIOCを素早く検索し、隠れた脅威を発見できます。
- **エンドポイントでの脅威検知**：疑わしい動作や、エンドポイントの潜在的な侵害を示す他の指標は自動的に発見されます。
- **対応スクリプトに基づいた、インシデントへの迅速で自動的な対処**：影響を受けたエンドポイントから重要なフォレンジック情報を自動的に取得できるほか、有害なエンドポイントが発見された場合は自動的に対処アクションを実行できます。

より詳しい情報

BlackBerry Opticsは、BlackBerryが提供するワールドクラスの幅広いセキュリティソリューションの1つです。インテリジェントなセキュリティをあらゆる場所に提供する完全なセキュリティスイートの詳細については、以下をご覧ください。

- BlackBerry Spark® Suite
- BlackBerry® Unified Endpoint Security Suite
- BlackBerry® Unified Endpoint Management Suite

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。

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。

BlackBerry
Intelligent Security. Everywhere.

お問い合わせ