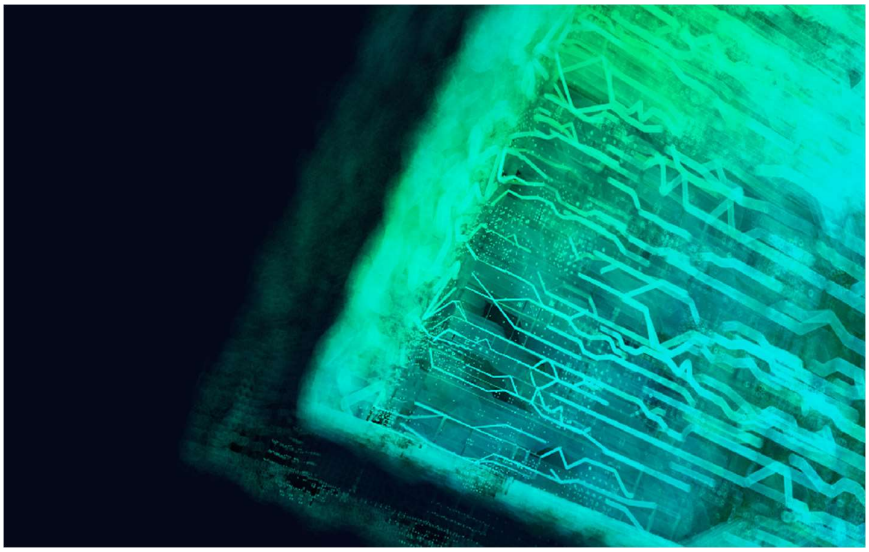
BlackBerry
Intelligent Security. Everywhere.

データシート

CylancePROTECT

未来を見据えたエンドポイントセキュリティ



長年にわたり、エンドポイントセキュリティ製品の主要な脅威防御はシグネチャを基にしていました。シグネチャは、最初の被害者が影響を受け、損害が発生した後に作成されるものです。すべての攻撃が以前に確認されたものであるなら、シグネチャを使用するのは意味のあることです。しかしながら、現在ではマルウェアは数時間で形を変えることさえあるため、シグネチャベースの防御ツールは時代遅れになりつつあり、エンドポイントセキュリティには、より強力な予防ベースのアプローチが必要になってきています。

BlackBerryは、自動化された予防ファーストのアプローチを活用することによって、エンドポイント保護ソリューションが組織に対して実行できること、実行すべきことを再定義しました。その結果、高度で執拗な脅威やマルウェアが組織のエンドポイントで実行されるのを阻止するための効率的かつ効果的で、正確なソリューションが開発されました。CylancePROTECT® は、セキュリティ侵害を阻止し、スクリプトベース、ファイルレス、メモリ、外部デバイスベースなどの各種攻撃を防御する追加のセキュリティコントロールを提供します。CylancePROTECTは、ユーザーや管理者の介入、クラウド接続、シグネチャ、ヒューリスティック、サンドボックスを必要とせずにこれを実現します。

機能

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制御
- リムーバブルメディアを使用したデータ盗難の防止

役割ベースのアクセス制御（RBAC）

- カスタム RBAC を使用したきめ細かな役割管理を通じてリスクを最小化
- 個々のユーザーの役割に基づいてネットワークアクセスの制限を改善
- 業務に必要な情報のみに従業員のアクセス権を制限
- 既存のユーザーに影響を与えないという利点

アプリケーション制御

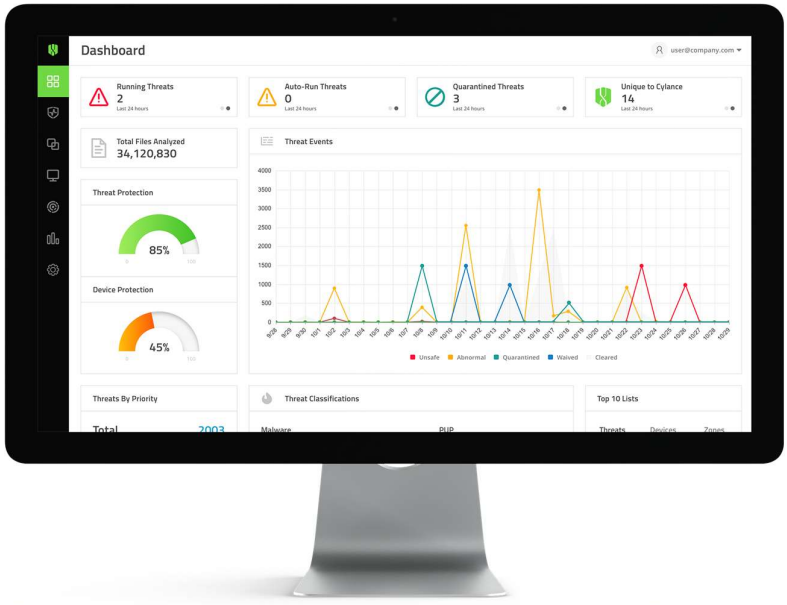
- 固定機能デバイスのロックダウン
- 不正なバイナリまたはバイナリ改変の阻止
- 指定したシステムのロックダウンと変更の制限

CylancePROTECT

デスクトップ向け CylancePROTECT®

CylancePROTECT® 内で利用されるアルゴリズムモデルでは、シグネチャ、パッチ、システムスキャンが使用されません。また、エンドポイントでセキュリティソリューションを実行することによるエンドポイントの速度の低下が生じません。従来のシグネチャベースの事後対応型アンチウイルス製品から乗り換えたお客様は、最大 99%の ROI を達成し、マシンの再イメージ化を 97% 削減し、ハードウェアとバッテリーのパフォーマンスを高め、ソリューション管理に要するスタッフの作業時間を90%削減しています[1]。

CylancePROTECTのアーキテクチャは、単一の軽量エージェントで構成されています。このエージェントはBlackBerry 独自の SaaS ベースのクラウドコンソールを使用して管理されます。このクラウドコンソールは、既存のソフトウェア管理システムやセキュリティツールと簡単に統合できます。また、エアギャップ環境向けにハイブリッド管理オプションとオンプレミス管理オプションが用意されています。エンドポイントエージェントは、クラウド接続や継続的な更新を必要とせずに、ホスト上でマルウェアを検知し、実行を阻止します。CylancePROTECTは、オープンなネットワーク、隔離されたネットワーク、仮想ネットワークでマルウェアを検知し、隔離することができます。事前の知識がなくても、未知の難読化手法が使用されていても、BlackBerry の機械学習をベースにしたアプローチによって悪意のあるコードの実行が防止されます。CylancePROTECTの精度、管理の容易さ、有効性に匹敵するアンチマルウェア製品は存在しません。



CylancePROTECT のアーキテクチャは、単一の軽量エージェントで構成されています。このエージェントは、BlackBerry 独自の SaaS ベースのクラウドコンソールを使用して管理されます。

機能

メモリの保護

- 悪意のあるメモリの使用を事前に特定・防止
- 権限昇格などのメモリベースの攻撃を阻止
- きめ細かな除外機能、高度なトラブルシューティングとレポートの機能

スクリプト制御

- 不正なスクリプトの実行を防止
- きめ細かなホワイトリストとセーフリストの機能
- MacOS®、Microsoft®、Linux® をサポート
- PowerShell ワンライナーの実行を阻止

IOS® サイドロードアプリケーション検知

- アプリケーションのサイドロードを即座にスキャンして検知

CylancePROTECT の特長

真のゼロデイ防御

回復力に優れた AI（人工知能）モデルがゼロデイペイロードの実行を阻止します。

デバイス使用ポリシーの適用

環境内で使用できるデバイスを制御し、外部デバイスを潜在的な攻撃ベクトルとして排除します。

AI（人工知能）を活用したマルウェア

実際の現場で実証された AI（人工知能）が、エンドポイントでの実行を試みるあらゆるアプリケーションを、実行前に検査します。

メモリエクスプロイトの検知と防御

悪意のあるメモリの使用（ファイルレス攻撃）を防御するために迅速かつ自動的に対処して、未然に識別します。

スクリプト管理

環境内でスクリプトを実行できる場所やタイミングを完全にコントロールします。

固定機能デバイス向けのアプリケーション制御

特定業務用途のデバイスが常に正常な状態に保たれるよう、実行できるアプリケーションを限定するホワイトリスト運用を実現します。

モバイル向け CylancePROTECT®

急速に発展している市場で競争し、従業員に常に接続を提供するために、モバイルデバイスを活用する組織がますます増加しています。史上初めて、モバイルデバイスは、インターネットに接続されている全デバイスの 50% を超えました[2]。その一方で、モバイルマルウェアがかつてないほどに拡散しており、昨年だけで攻撃が 50% 増加しました[3]。従来、企業のセキュリティソリューションはデスクトップデバイスに重点を置いていましたが、モバイルデバイスを標的としたマルウェアフィッシング攻撃、特にアプリケーション内の攻撃による脅威の高まりを認識している企業が増加しています。

これらの攻撃によって多額の損害が生じることがあり、個人情報（PII）やその他の重要なデータが漏洩するケースがますます増えています。これに対応するために、多くの組織が、悪意のある攻撃を防御するためにディープパケットインスペクション（DPI）などの機能の採用を進めています。

したがって、モバイル脅威防御（MTD）の市場が急速に成長していることは驚くに当たりません。MTD は、組織内のモバイルデバイスとアプリケーションのすべてのレベルにおける防御、検知、修復、全体的なセキュリティ体制の向上によって、追加のセキュリティレイヤーを提供します。

CylancePROTECT® MTDソリューションは、モバイルデバイスを標的とした悪意のある高度な脅威に対処することで、BlackBerry® UEM によって提供されるセキュリティの基準を高めます。CylancePROTECTは、デバイスレベルとアプリケーションレベルで攻撃をモニタリングし、BlackBerryの基本的なアプリケーションコンテナのセキュリティをさらに強化します。

機能

Android™ マルウェアスキャン

UEM アプリストア Android および APK マルウェアスキャン

- お客様のアプリケーションやカスタムパートナーアプリケーションを含め、BlackBerry の UEM アプリストアにあるすべてのアプリケーションをスキャンし、マルウェアから保護します。

フィッシングおよび悪意のある URL の検知

- AI を活用して、フィッシング要素が埋め込まれた URL を含む悪意のある URL を自動的に検知し、アクセスを防止します。

安全なアプリケーションの作成

- パートナーと企業が、企業全体でアクセス可能なデバイス向けの安全なカスタムアプリケーションを構築できるようにします。

BlackBerry Dynamics SDK アプリ向けの IOS アプリ妥当性チェック

- 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妥当性を確認します。
- 安全なアプリのみがデバイスにロードされるようにし、BlackBerry® アプリケーションの改ざんを防止します。

- デバイスレベルで、モバイルデバイス向け CylancePROTECTは、OS の更新、システムパラメータ、デバイス構成、システムライブラリをモニタリングすることによって、セキュリティの脆弱性や悪意のある活動の可能性を特定します。
- アプリケーションレベルで、モバイルデバイス向け CylancePROTECTは、アプリケーションサンドボックス、コード分析、アプリのセキュリティテストを使用して、マルウェアやグレイウェアを特定します。

また、モバイル向けCylancePROTECTは、サイドロードされたアプリケーションを通じて侵入することがあるマルウェア、独特なシグネチャベースのマルウェア、シミュレーションを特定し、BlackBerry Dynamics SDK プラットフォームにセキュリティレイヤーを追加します。これにより、パートナーと企業とは、企業全体でアクセス可能なデバイスにロードされる、カスタマイズされた安全なアプリケーションを構築できるようになります。

CylancePROTECTの一般的な使用事例

CylancePROTECTはすべての領域にわたって脅威防御を提供し、以下のような事例を解決することによって、エンドポイントのセキュリティ侵害を防ぎます。

- 頻繁な更新やクラウド接続を必要とせずに、悪意のある実行可能ファイルを特定してブロックします。
- OS の更新、システムパラメータ、デバイス構成、システムライブラリをモニタリングすることによって、セキュリティの脆弱性や悪意のある活動の可能性を特定します。
- 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します。
- USB デバイスの使用法を管理し、不正なデバイスの使用を防止します。
- ファイルレスマルウェア攻撃を防ぎます。
- キオスク、POS端末などの固定機能デバイスをロックダウンします。
- ゼロデイ攻撃やランサムウェア攻撃を阻止します。
- メモリベースの攻撃やエクスプロイトを防ぎます。
- アプリケーションサンドボックス、コード分析、アプリのセキュリティテストを使用して、マルウェアやグレイウェアを特定します。
- サイドロードされたアプリケーションを通じて侵入することがあるマルウェア、独特なシグネチャベースのマルウェア、シミュレーションを特定します。
- ユーザーがオンライン、オフラインのいずれの場合でもエンドポイントを保護します。

より詳しい情報

CylancePROTECT 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。CylancePROTECT に関する詳しい製品情報や、その他の資料については以下をご覧ください。

当社製品:

CylancePROTECT

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** をご覧ください。また、**@BlackBerry** をフォローしてください。*

BlackBerry
Intelligent Security. Everywhere.

BB20-0250 | 200518