BlackBerry®

統合エンドポイントセキュリティ

①BlackBerry Protect
②BlackBerry Optics

BlackBerry製品概要

BlackBerry 製品

ただ安全なだけでなく、スマートに機能する AI 駆動型のサイバーセキュリティ

アンチウイルス ソフト(EPP)

①BlackBerry Protect

AI（人工知能）で安全性を予測・判断するシグネチャレスの「次世代アンチウイルス(NGAV)」

BlackBerry® Protect は、数理モデルの人工知能（AI）を使ったエンドポイント保護プラットフォーム（EPP）ソリューションです。これにより、未知の脅威を予防し、高度なサイバー攻撃から主導権を取り戻し、防御することができます。

エンドポイントの検知と対応（EDR）

②BlackBerry Optics

予防、検出、対処。人工知能を使った予測防御するフルEDRソリューション

BlackBerry® Optics はすべての検知と対応方法をエンドポイントが担います。これにより、対応の遅延を回避することが可能になりました。つまり、軽微なセキュリティイベントと広範囲に及ぶ無制御のセキュリティインシデントとを区別して対応することが出来ます。

従来のアンチウイルスソフトの現状

マルウェアの急激な増加

容易に入手可能　**新種・亜種の増加**　**攻撃手法の巧妙化**

マルウェア攻撃の85%は対応困難

マルウェアの85%は、新種・亜種マルウェア
対応するシグネチャの作成時間は**平均20時間**
一方で、攻撃者は、**7時間以内に攻撃を終える**

マルウェアから守れる確率は4%

マルウェアの96%は使い捨て
次回の攻撃で利用されるマルウェアは、
新たな顔をして、攻撃を開始する

従来のシグネチャをベースとしたアンチウイルスだと・・・

ウイルスがすり抜ける	定期的に定義ファイルを更新	インターネット未接続だと検知力が低下	追加のウイルス対策が必要
50%以下の検知率	週次での定期スキャンが端末に負荷をかける	クラウドシグネチャを利用できず、検知率低下	別途、新種・亜種ウイルス対策ツールの導入が必要

シグネチャをベースとした対策は限界
従来型のマルウェア対策アプローチでは脅威に対応することが難しい

Secure Innovation
沖縄から日本全国　そしてアジアへ

BlackBerry

BlackBerry Protect について

人工知能のアルゴリズムを使って
エンドポイント上でマルウェアが実行される前に
予測をして止める、**実行前防御**が可能

ファイルの**DNA（構造）の特徴点**を
AI（人工知能）によってい静的分析し
安全性を予測・判断する、**シグネチャレス**な

次世代アンチウイルス（NGAV）

Next Generation Anti-Virus

マルウェア防御率は、驚異の・・・

99%以上

製品の特徴

ファイルの特徴点を抽出

- マルウェアを識別するための判断材料である、ファイル特徴点を抽出
- 大量の教師データと膨大な特徴点から導き出される数理モデルによって、高い検知精度を実現

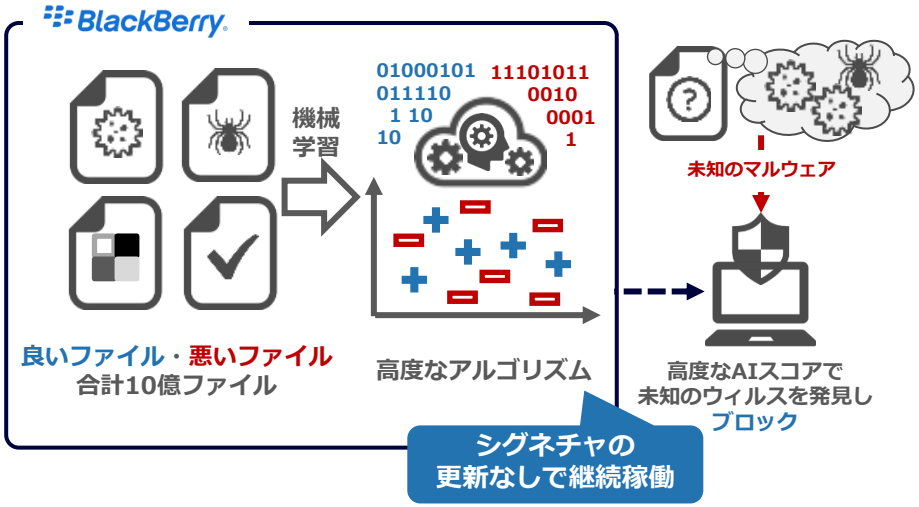
- DOSヘッダ
- NTヘッダ
- ファイルヘッダ
- セクションヘッダ
- エクスポートディレクトリ
- インポートディレクトリ
- リソースディレクトリ
- リロケーションディレクトリ
- デバッグディレクトリ
- パッカーの使用有無
- コンパイラの種類
- コンパイル言語
- ファイルサイズ
- PEサイズ
- イメージセクションヘッダ
- イメージインポート
- N-gram
- エントロピー値

⋮

700万点以上の特徴点から正確な判断を導き出す

Black Berry 人工知能

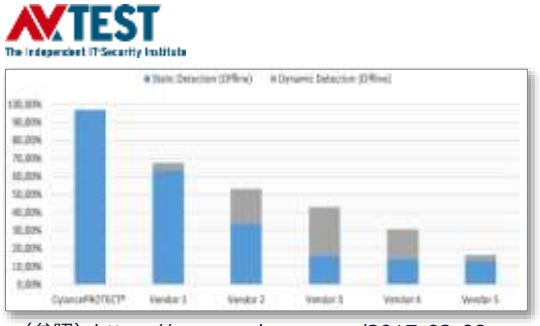
- 優秀なデータサイエンティストによる高度なアルゴリズムの構築
- AIに膨大（10億個以上）のファイルを学習させ、700万点以上の特徴点からマルウェアを分析
- 5億以上の悪いファイルと、それと同等の良いファイルを学習することで、誤検知を最小限に



検知率について

BlackBerry Protectの検知率について

- BlackBerry社自身で公表しているBlackBerry Protectの検知率は、**99%**
- 第三者評価機関（AVTESTによるBlackBerry Protectの有効性は、**97%**

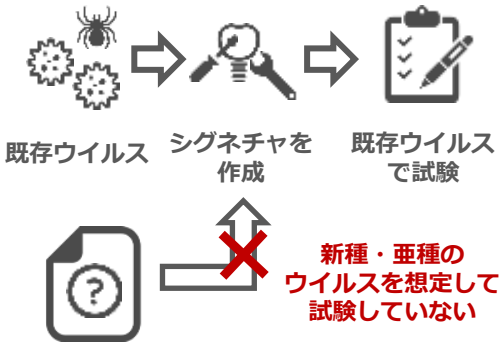


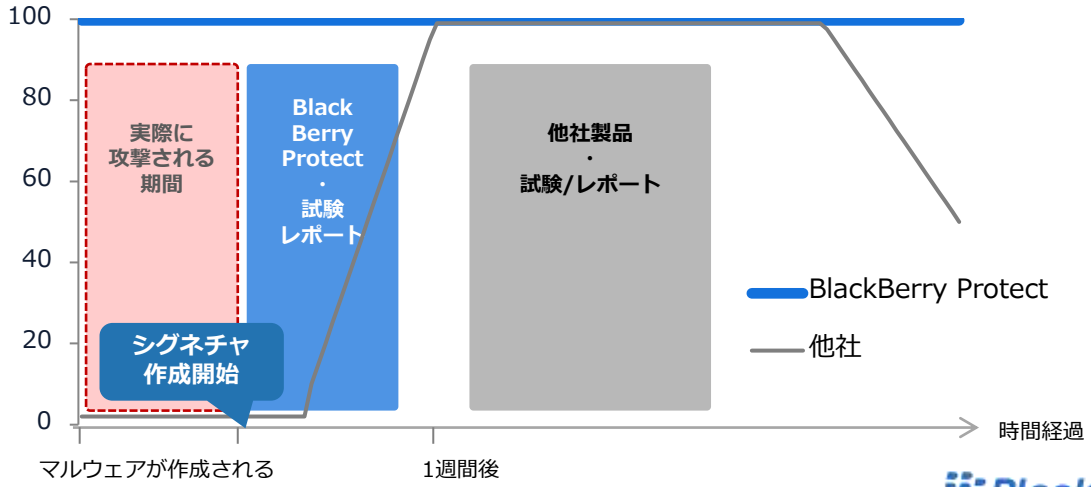
（参照）https://pages.cylance.com/2017-02-08-CNT-AV-TEST-Report-2017-2092.html

他社製品の検知率が100%になるカラクリ

- 他社が公表する検知率は**シグネチャを作成後、そのシグネチャを元に試験したデータに基づいている**ので、高い数値になるのは当然
- **実際の攻撃はシグネチャが作成されるより前に実施されている**ので、シグネチャベースであるということは攻撃が防げないということを意味する

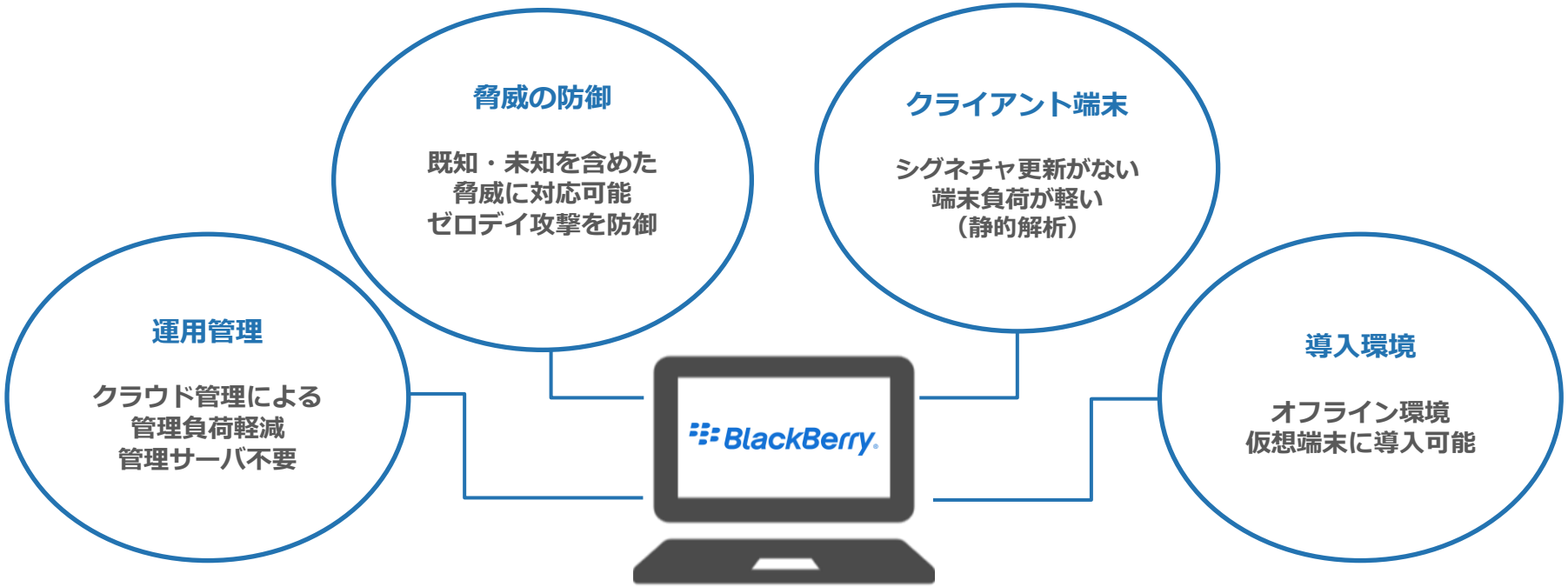
他社の製品アプローチ ----------→ **マルウェアに対する検知率の推移**





Secure Innovation
沖縄から日本全国　そしてアジアへ

導入メリット①



従来のエンドポイントセキュリティ

- シグネチャと照会することで防御
- フルスキャン運用が必要
- サンドボックスなどで動的検査(高負荷)を行う
- オフライン環境の場合検知率が低下

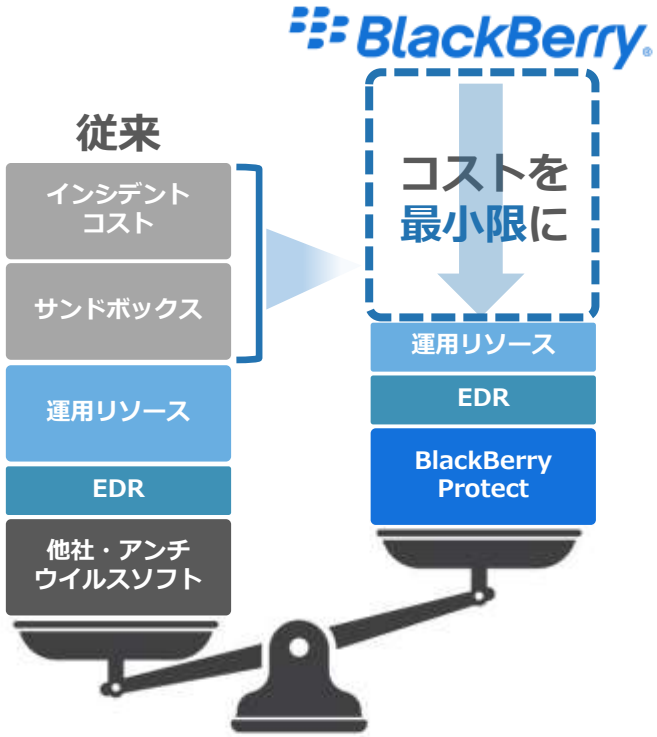
BlackBerry Protect

- ファイル特徴点をAIで分析し安全性を予測・判断
- 数理モデルを使用するためフルスキャン不要
- マルウェア実行前に静的(低負荷)に攻撃を予測
- オフラインでも変わらない検知率

導入メリット②

トータルコストで比較すると大きなメリット

- 一般的なセキュリティ体制と比べ簡潔で**管理が簡単**
- セキュリティ管理の**人員を削減が可能**
- 運用・製品を含めた**トータルコストは従来より軽い**



シグネチャの更新・PCフルスキャン、
PC負荷の増加による損失を
1日10分と仮定すると・・・

月間で約200分
＝**約3.4時間が消失・・・**

1日3.4時間×平均時給2,400円×12か月
＝**一人あたり97,920円が無駄に・・・**

※サラリーマン平均年収額を524万円、
年間平均労働時間を2136時間と想定した場合

従業員1,000人の企業の場合・・・

年間損失額

97,920,000円

BlackBerry Protect動作要件

エージェント動作対象OS

- Windows XP SP3
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 10 IoT Enterprise
- Windows Server 2003（R2）SP2
- Windows Server 2008（R2）
- Windows Server 2012（R2）
- Windows Server 2016
- Windows Server 2019

- OS X 10.9 Mavericks
- OS X 10.10 Yosemite
- OS X 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave

- RHEL / CentOS 6.6
- RHEL / CentOS 6.7
- RHEL / CentOS 6.8
- RHEL / CentOS 6.9
- RHEL / CentOS 6.10
- RHEL / CentOS 7.0
- RHEL / CentOS 7.1
- RHEL / CentOS 7.2
- RHEL / CentOS 7.3
- RHEL / CentOS 7.4
- RHEL / CentOS 7.5
- RHEL / CentOS 7.6

- SUSE (SLES) 11.4
- SUSE (SLES)
  12 including SP1, SP2, SP3

- Ubuntu LTS / Xubuntu 14.04
- Ubuntu LTS / Xubuntu 16.04
- Ubuntu LTS / Xubuntu 18.04

- Amazon Linux
- Amazon Linux 2

導入実績

増加を続ける導入企業

4,000社以上の導入実績（ワールドワイド）

国内導入事例（**560社以上 60万ライセンス**）

- 株式会社モスフードサービス 様
- 株式会社沖縄銀行 様
- 沖縄ツーリスト株式会社 様
- イー・ガーディアン株式会社 様
- 中央労働金庫 様

あらゆる業種・企業規模での導入実績

- 政府・公共事業
- 金融
- 流通・小売
- 病院
- 物流・運輸
- インフラ
- 製造・鉱業

BlackBerry Optics について

BlackBerry Opticsとは

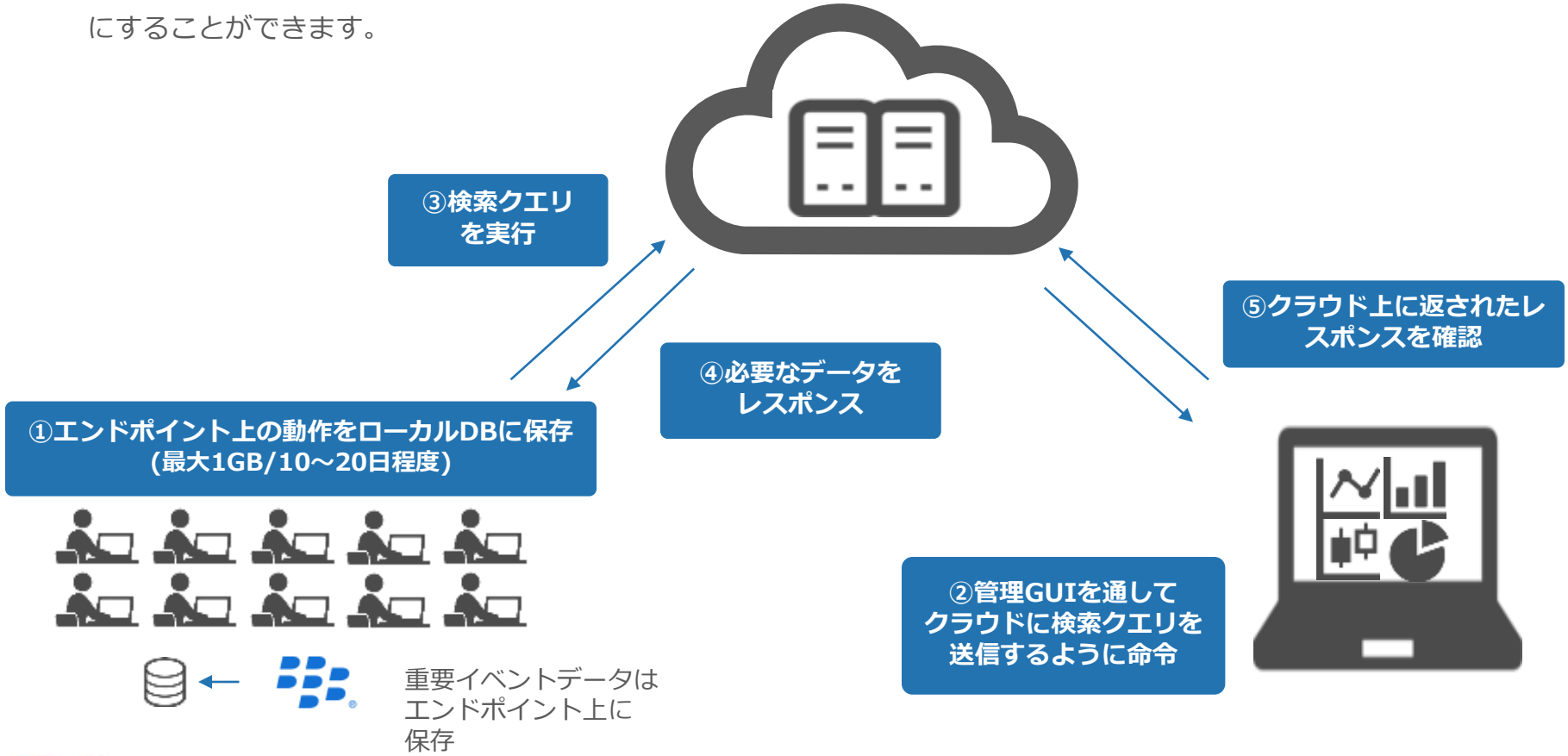
BlackBerry Protectが提供する防御機能におけるEDR(Endpoint Detection and Response)のコンポーネント

特徴

- 発生した脅威の分析が可能となるため、迅速な侵入経路の特定を実施し対策を立てられることで、被害リスクを最小限にとどめることができる
- シンプルなハンティング機能により隠れた脅威をいち早く特定することができる
- 独自のルールセットを作成できるため、不審な挙動に対してアラートを発生させることができる
- リモートからデバイスのロックダウンを実施できるため、感染拡大に対して即座の封じ込めが可能となる

機能と特徴　分散型アーキテクチャ

- オンプレミスでの管理サーバが不要です。BlackBerry ProtectのWeb管理コンソール”テナント”より統合運用管理が可能です。
- 端末に保存されるデータサイズは1GBまでなので、ストレージデータの増大を回避できます。
- クラウドへ常に情報を送信せず、必要なデータをクエリするため、通信帯域へのインパクトを最小にすることができます。



端末上で収集されるイベントデータ

収集されるイベントデータの例	
イベントタイプ	イベントの説明
BlackBerry Protect	- BlackBerry Protectの検知または検疫イベントからのバックトレースにより、ユーザデバイス上で観測された時系列イベントをたどれる「ブレッドクラムトレイル」を提供
ファイル	- ファイルの作成、変更、削除、名前変更イベントをメタデータおよびファイル属性とともにキャプチャ - それぞれのファイルとプロセスの関係を関連付け - 代替データストリームを識別 - リムーバブルデバイスのファイルを識別
プロセス	- プロセスの生成と終了のイベントをキャプチャ - モジュールロード - スレッドインジェクション - プロセスを、その所有ユーザおよびイメージファイルと関連付け - プロセスを、そのすべてのアクティビティ(ファイル、レジストリキー、ネットワーク接続など)と関連付け
ネットワーク	- IPアドレス - レイヤ4プロトコル - 送信元と送信先のポート
レジストリ	- レジストリのキーおよび値の作成、変更、削除イベントをキャプチャ - マルウェアがシステムの再起動後も存続するために使用する、120個以上の「パーシステンスポイント」を識別 - レジストリキー/値と作成したファイルプロセスとを関連付け - 専用のパーサーで永続レジストリキー/値を、存続しようとするファイルと関連付け
ユーザ	- 以前デバイスにログオンしたことのあるすべてのユーザをキャプチャ - ユーザと実行したアクション(作成、変更、削除イベントを含む)を関連付け - ユーザと悪意のあるアクティビティを関連付け
リムーバブルメディア	- リムーバブルメディアの挿入イベントを、コピー先/元ファイルおよび実行されたファイルとデバイスの詳細を一緒に収集 - リムーバブルメディアを変更したか、リムーバブルメディアからファイルをコピーしたプロセスを識別 - BlackBerry Protectで検知されたマルウェアがリムーバブルメディアから侵入したかどうかを識別

管理画面

根本的な原因分析と侵入経路調査(Focus Data)

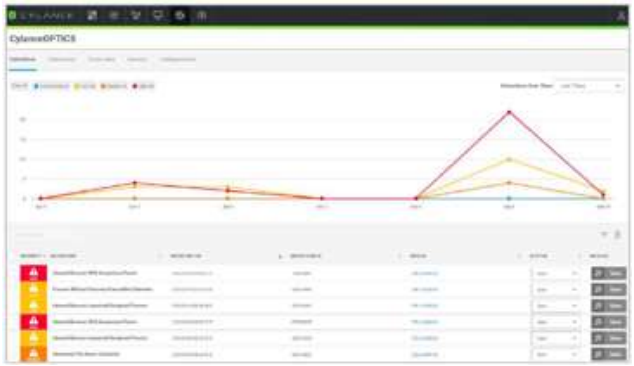
・脅威の動作や侵入経路等を確認することが可能
・発見したIoC情報に基づいて、さらにオンデマンド検索での調査を実施することが可能
  – 例えば接続されたC&Cサーバの接続IPを使用し、他に接続している端末がいないか等

脅威ハンティングと対処(Insta Query)

・以下のIoC情報に基づいて、組織内の隠れた脅威を検索することが可能
  – ファイル　　– ネットワーク
  – プロセス　　– レジストリキー
・対象端末に対するリモートからの迅速なアクションが実行可能

脅威の挙動検知と対処(Detections)

・検知ルール
  – プリセットされている多くの検知ルールを使用することも、カスタマイズすることも可能
  – 指定したアクションを自動で行うことが可能
・検知イベントに対してのアクション設定
  – リモートユーザのログオフ　　– プロセスの停止
  – 端末上への通知



BlackBerry
サービス全体の特徴

本製品の特長である EPR について

本製品は従来のEDRとは違い、新しい”EPR”としてご提供いたします。

EDRについて（既存製品）

- EDR(Endpoint Detection and Response)とは感染を検知し、拡散を防いだり、搾取された情報を調査したりといった感染後に対応するセキュリティのこと
- 既存のアンチウイルスでは防ぎきれない脅威に対して感染後に対応することを前提としている

EPRについて（本製品）

- EPR(Endpoint Prevention and Response)とは高度な事前防御機能を有する製品とEDRを組み合わせた新しいエンドポイントセキュリティのこと
- BlackBerry Protect の事前防御機能とEDR製品であるBlackBerry Opticsが揃って初めてEPRとなる

EPRとEDRの違いについて

- EDRはパターンマッチングの既存AV製品ですり抜けたものに関しての調査を前提としているので、既存AV製品を使用している限りは調査する件数は多くなる。結果として現在の分析班のリソースが足りず運用できないという事態が発生する。
- 一方で事前防御の強化を前提にしているEPRは、検知処理をすり抜ける絶対数が少ない。そのため調査する件数自体が少なく、結果として時間的効率が良くなったり、重要イベントに限定した対応が可能。

エンドポイントセキュリティの進化

EPP

- マルウェアの存在が多くない時代から活躍している実前・感染前防御のアンチウイルス
- 静的・動的検知防御機能をはじめとするさまざまな検知機能
- 端末上(エンドポイント)で動作

EDR

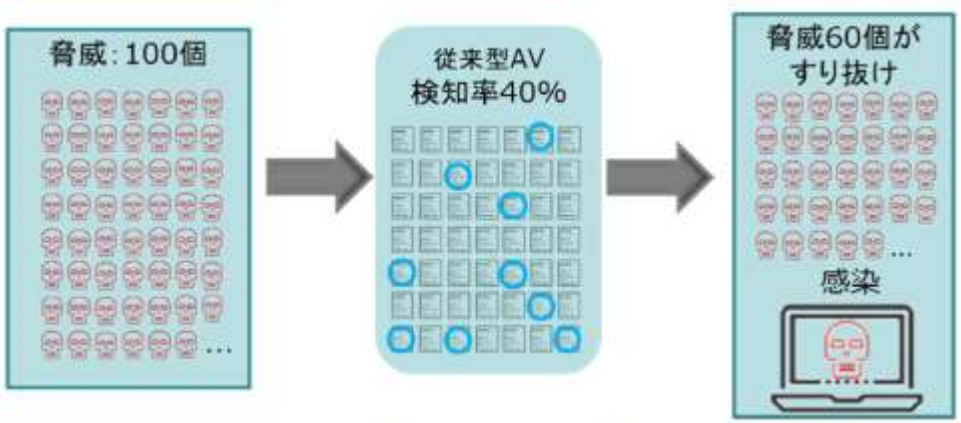
- 感染活動をいち早く発見して対処
- 検知・封じ込め・復旧の実施
- フォレンジック分析を実施

EPR

- 次世代アンチウイルスとEDRを統合した新しいエンドポイントセキュリティ
- AI(人工知能)とML(機械学習)の技術を活用
- 予防に焦点を当てた合理的なセキュリティ
- 情報の可視化と迅速なレスポンスも実施

導入メリット(運用の比較)

EPP＋EDR運用とEPR運用の違い



セキュリティの運用を行うために

セキュリティ運用における課題

- 多すぎるインシデントやアラートによって真に組織にとって致命的な脅威を把握することが困難となっている。
- 日々の業務を実施しながら、プロアクティブに脅威を発見することは時間的にも困難となっている。
- セキュリティ人材の不足から、脅威に対して十分な対策ができず運用が困難となっている。

実現可能な運用をするために

-上記の課題を解決する、高度な事前防御を前提としたEPRソリューション(BlackBerry Protect +BlackBerry Optics)が不可欠。

BlackBerry Optics
予防をベースとしたEDR(検知とレスポンス)ツール

BlackBerry PROTECT
AIによる高度なエンドポイント脅威防御

機能と特徴　要件と利用目的

BlackBerry ProtectとBlackBerry Opticsは以下の要件を満たすことができます。

利用目的	求められる要件	BlackBerry Protect	BlackBerry Optics
脅威活動の停止	悪意のある実行ファイルのエンドポイント上での実行を防ぐ	✓	
	許可されないスクリプトの実行を防ぐ	✓	
	ファイルレスマルウェアによるメモリの不正利用からの防御	✓	
	メールに添付された悪性ファイルの実行を防ぐ	✓	
	あらかじめインストールされたアプリケーション以外の実行を防ぐ	✓	
	感染端末へのインシデントレスポンスと封じ込め		✓
疑わしい活動の確認	悪意ある活動の調査や確認		✓
	侵入経路分析の実施や攻撃/脅威の発生元の特定		✓
脅威ハンティング	疑わしい活動のレビュー		✓
	現状および統計データからの状態のサーチ		✓
	IoC (Indicators of Compromise)情報に基づくチェック		✓
疑わしい活動の検知*	ルール及びAIベースでの脅威イベント検知		✓

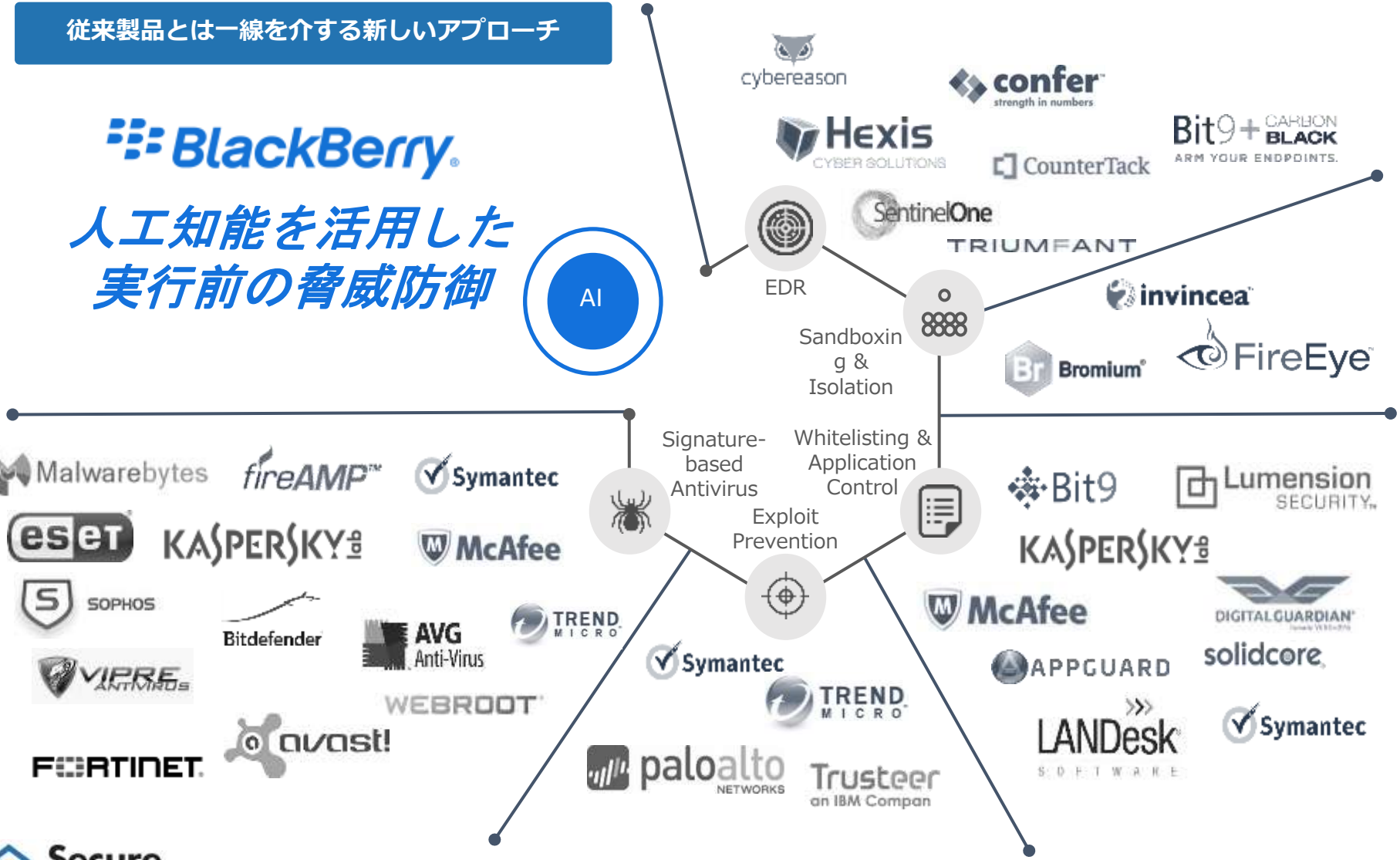
類似製品との差別化

従来製品とは一線を介する新しいアプローチ

BlackBerry

人工知能を活用した
実行前の脅威防御

AI



Secure Innovation
沖縄から日本全国　そしてアジアへ

BlackBerry

価格・サービスご案内

サービスに関する、お見積や詳細プラン等につきましては、ヒアリングをして状況を確認しながらお伝えさせていただきます。

まずは、お気軽に以下のお問い合わせ先からご連絡ください。

問い合わせ先

株式会社セキュアイノベーション
お問い合わせページ：https://www.secure-iv.co.jp/contact
セールス＆プロモーションチーム
（担当：高良・亀谷・伊勢）
TEL：098-943-2718
Mail：pr@secure-iv.com

Secure Innovation
沖縄から日本全国　そしてアジアへ

会社概要

会社名	株式会社セキュアイノベーション Secure Innovation Inc.（略称：SIV）
設立	2015（平成27）年 10月 21日
資本金等	1億1400万円（資本金9750万円、資本準備金1650万円）
主な出資者	株式会社セキュアヴェイル 、沖縄振興開発金融公庫 グローバルセキュリティエキスパート株式会社、株式会社ベリサーブ、栗田智明　他
代表取締役社長	栗田智明
取締役	金城夏樹 鉢嶺　光 米今政臣（株式会社セキュアヴェイル代表取締役社長）
本社	沖縄県那覇市上之屋一丁目18番36号 沖縄映像センタービル3F 098-943-2718
東京オフィス	東京都渋谷区広尾一丁目7番20号 TH広尾ビル 4F-N
名古屋オフィス	愛知県名古屋市中川区尾頭橋四丁目13番7号 名古屋ビジネスインキュベータ金山202-A
福岡オフィス	福岡県福岡市中央区渡辺通二丁目4番8号 福岡小学館ビル5F サービスオフィス福岡薬院18号室
事業内容	・情報セキュリティシステムの設計、構築、運用監視、診断、ログ分析 ・セキュリティ人材の育成、派遣事業 ・システム開発・サイト制作/運営・BPO事業 ・地域活性化事業

Secure Innovation
沖縄から日本全国　そしてアジアへ

会社概要

主な取引先	官公庁・行政機関、電力会社（東証プライム）、SIer（東証プライム） インターネット関連会社（東証プライム）、グループホールディングス（東証プライム） コンサルファーム、クレジット会社、システム開発会社 通信・インフラ会社、広告代理店、情報通信システム会社、リスクマネジメント会社 金融関連会社（銀行・保険会社・信用組合）、病院・クリニック、人材派遣会社 出版会社、学習塾、コンビニエンスストア、社団法人（公益・一般）他
所属団体	サイバーセキュリティ協議会 Center for Internet Security(CIS) 公益社団法人沖縄県情報産業協会 那覇商工会議所 ISCO(沖縄ITイノベーション戦略センター) 一般社団法人JASPAR　準会員 公益社団法人 自動車技術会　賛助会員
許可・認定等	JIS Q 27001:2014(ISO/IEC 27001:2013) ISMS認定(登録番号 IS127) JASA情報セキュリティサービス基準審査登録(セキュリティ脆弱性診断サービス) 労働派遣事業(許可番号：派47-300169)
主な保有資格 ※2022年1月現在	・IPA　応用情報技術者試験(AP) ・IPA　データベーススペシャリスト試験(DB) ・IPA　ネットワークスペシャリスト試験(NW) ・IPA　情報処理安全確保支援士(登録セキスペ) ・Splunk Core Certified Power User ・Splunk Enterprise Certified Admin ・CEH(Certified Ethical Hacker) ・CCDSサーティフィケーションプログラムレベル１ ・CISA(Certified Information Systems Auditor) ・CND3(Certified Network Defender) ・CHFI(Computer Hacking Forensic Investigator) ・SSCP(Systems Security Certified Practitioner) ・OSCP(Offensive Security Certified Professional) ・CISSP(Certified Information Systems Security Professional) ・AWSソリューションアーキテクト：アソシエイト ・AWSデベロッパー：アソシエイト ・SecuriST 認定ネットワーク脆弱性診断士 ・SecuriST 認定 Web アプリケーション脆弱性診断士