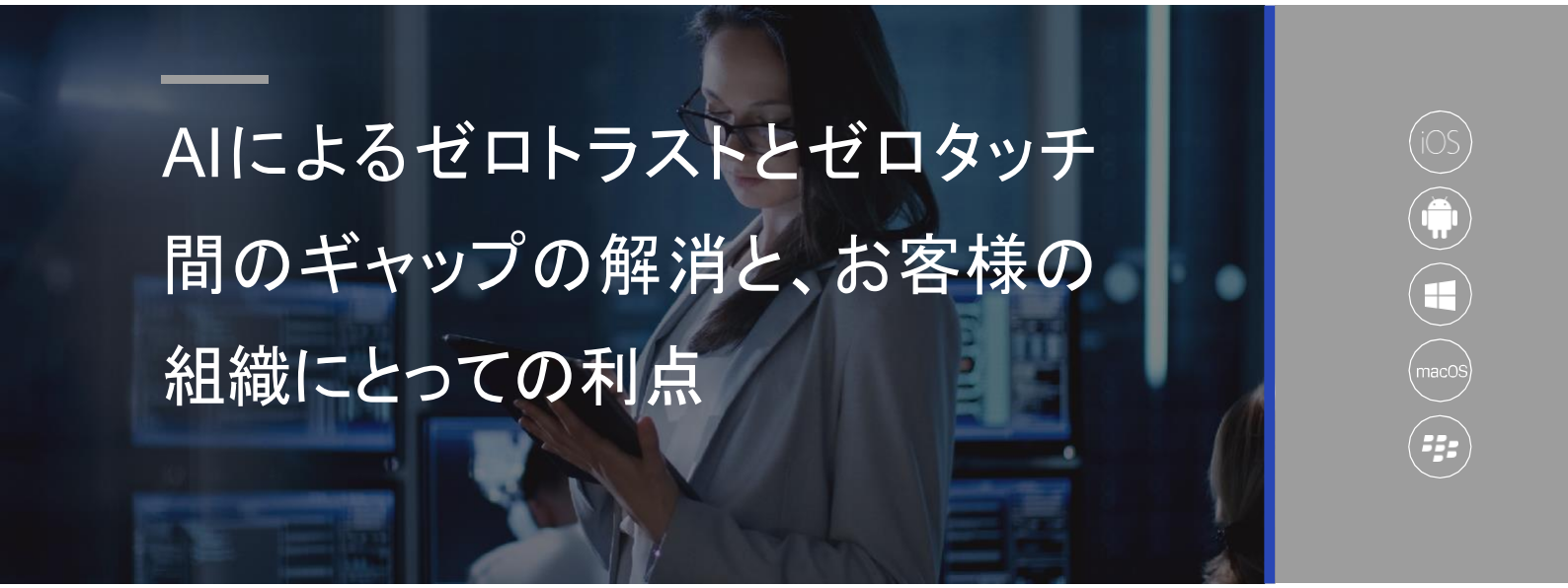
ホワイトペーパー



AIによるゼロトラストとゼロタッチ間のギャップの解消と、お客様の組織にとっての利点

ゼロトラストとは...

- 新たなユーザー、デバイス、アプリケーション、およびテクノロジーによる環境の変化に応じて進化し続ける多重セキュリティアプローチ
- プロセスとテクノロジーの組み合わせ
- 単一の製品または1回限りのチェックリストではない

基本原則:

- ユーザーは、あらゆる場所にあるデータにどこからでも任意の方法でアクセスできる
- ネットワークとエンドポイントには常に外部や内部の脅威が存在している
- あらゆるデバイス、ユーザー、およびネットワークフローを認証および承認する必要がある
- ポリシーはコンテキストに応じた動的、データドリブンなものである必要があり、静的ではない

ゼロトラストの基本要素

ユーザー – ゼロトラストはユーザーから始まります。まず、信頼できるユーザーかどうかを識別する必要があります。この識別は、断続的なログインイベントに基づいてではなく、アプリの使用ライフサイクル全体を通して継続的に行われます。その際には、今までどおり従来のIDおよびアクセス管理（IAM）テクノロジーが使用されますが、このようなテクノロジーは、単独ではユーザーの信頼性を継続的に監視、検証したり、断続的なログインイベント間でアクセスと特権を管理したりすることはできません。ユーザーはアクティブな再認証が頻繁に発生することに耐えられないため、アプリケーションにおける控え目かつ継続的な認証テクノロジーの必要が高まっています。

デバイス – ユーザーが使用するデバイスの信頼性は、適切に設計されたゼロトラストアーキテクチャのもう1つの基本的属性です。デバイスが侵害された状態ではないか、古いソフトウェアを使用していないか、十分に強力なパスワード制御を使用して整合性を確保しているかどうかなどを継続的に評価する必要があります。ネットワークに偏重したゼロトラストソリューションの皮肉な側面は、完全に信頼できるユーザーが完全に侵害されたデバイスからネットワークにアクセスすることを図らずも許可してしまう可能性があるということです。それによって、脅威に対する全体的な暴露を低減するのではなく逆に高めることになってしまいます。脅威の検知と防止は、モバイルとデスクトップもカバーすべきであり、どちらか一方を無視したり、サイロとして扱ったりするべきではありません。

ネットワーク – きわめて密接に接続されたネットワークの世界では、ネットワークの信頼はゼロトラストを確立する上での基盤となります。しかし、ネットワーク自体が動的で常に進化する存在であるため、クラウドや、ユビキタスなモバイル／Wi-Fiネットワークに移行するワークロードが増加してくると、ルールベースの静的な境界定義ではもはや不十分です。さらに、単にネットワークへのアクセス権にのみ基づいてユーザーとデバイスを信頼するという時代遅れの概念は、ネットワークセキュリティの最大の弱点であることが何度も明らかになっています。皮肉なことに、従来のVPNゲートウェイは、この問題を悪化させる可能性があります。BYOデバイスからクラウドに送信されたトラフィックを企業の境界内に持ち込み、社内ネットワークを横方向に移動する脅威にさらした挙げ句、再びトラフィックを送り返すためです。このより動的なネットワークの概念に適応し、クラウド、モバイル／Wi-Fi、およびBYOの組み合わせに内在する、常に変化するリスクを軽減するため、次世代のセキュアWebゲートウェイとサービスベースのネットワークセグメンテーションテクノロジーがゼロトラストアーキテクチャの基本要素となります。これは、ネットワークそのもののリスクのみならず、ネットワークにアクセスして使用するユーザー、デバイス、およびアプリのリスクにも動的に適応する能力に基づくもので、初期アクセス時だけでなく、アプリの使用ライフサイクル全体が対象となります。

アプリ – アプリレイヤーに加え、コンピューティングコンテナと仮想マシンを保護し適切に管理することは、ゼロトラストの採用の中核です。テクノロジースタックを識別、制御する機能を備えているため、よりきめ細かく正確なアクセス決定が可能になります。当然ながら、多要素認証は、ゼロトラスト環境でアプリケーションに適切なアクセス制御を提供する上でますます不可欠な要素になっています。

セキュリティ分析とAI – 見えない脅威とは戦えないのは真実ですが、脅威を何度も見てからでないと識別、予防できないようであれば、必然的に常に脅威にさらされ続けることになるのもまた真実です。そのため、適切に設計されたゼロトラストアーキテクチャでは、高度なAIベースの脅威の識別と防御、ユーザーとエンティティの行動分析（UEBA、User and Entity Behavior Analytics）、およびその他の分析ベースのアプローチを使用して、過去から学び、現在起きていることをリアルタイムで理解し、インテリジェントに予防措置を講じる必要があります。その目標は、事後に脅威と情報漏洩イベントを特定するだけでなく、脅威と情報漏洩がそもそも発生しないようにアクティブに防止することです。

自動化 – セキュリティアナリストが、要求時にすべてのアクセス決定またはそのごく一部にでも積極的に関わることは、単純に不可能です。コスト効果の高いゼロトラストでは、自動化とインテリジェンスベースの動的なポリシー適応と対応を必然的に最大限に活用し、ユーザーが望むリアルタイムのゼロタッチエクスペリエンスを提供すると同時に、セキュリティオペレーションセンター（SOC）が、的を絞った、洞察に基づく価値の高い方法で監視と対話を行うことができるようにします。

ゼロトラストのジレンマ...

ゼロトラストアーキテクチャ
これは、すべてのセキュリティチームが求めているものです。つまり自身の身元と、アクセスが承認されていること、悪意のある行動をしていないことを証明し、これらを継続して証明しない限り、誰も、いかなるものに対してもアクセスを取得または維持することはできません。

ゼロタッチエクスペリエンス
これは、ユーザー／従業員が求めているものです。面倒なパスワード、タイムアウト、特別な権限、多要素認証などを使用せずに、自身が必要だと思うものすべてに即座にアクセスできるため、すぐに満足感を得ることができます。

BlackBerryのゼロトラストアーキテクチャによってジレンマを解決

BlackBerryのゼロトラストアーキテクチャ（ZTA）には、必要な基本要素がすべて組み込まれており、強力なセキュリティAIと分析の専門知識を適用することでゼロトラストのジレンマを解決し、セキュリティチームが必要とするゼロトラストアーキテクチャと、エンドユーザーが望むゼロタッチエクスペリエンスを提供します。

図1：BlackBerryのゼロトラストアーキテクチャ

常時監視と脅威検知（MTD）

AIがモバイルデバイスとデスクトップデバイス、およびそこで実行されているアプリを監視して、新たな脅威や既知の脅威がないかを調べ、適切な修正措置を実行します。これには、悪意のあるURLへのアクセスをブロックし、フィッシング攻撃を阻止する「セーフブラウジング」のサポートが含まれます。BlackBerryのSecure Edge Frameworkにより、どのようなアプリにでも容易にMTDを統合できます。

コンテキストに応じた認証

ユーザー行動のAIモデリングにより、ユーザーの「マクロ」コンテキストが信頼済みの行動に一致しているかどうかを学習して、ネットワーク境界を動的に調整し、（i）行動が信頼でき、ポリシーに準拠している場合はアクセスを付与し、（ii）行動が新たな種類のものであるが、それ以外はポリシーに準拠している場合はユーザーにチャレンジし、（iii）行動がポリシーに準拠していないか、非常に特異なものである場合は、アクセスを即座にブロックします。

連続認証

初期アクセスの付与後は、連続認証によってユーザーの継続的な行動の「マイクロ」コンテキストを評価し、操作を続行するためにアクセスを許可すべきかどうかを決定します。連続認証は、モバイルとデスクトップにわたって生体認証、アプリ使用状況、プロセス呼び出しのパターンを組み合わせることにより、従来の2要素認証よりも強力な「N要素」認証を提供します。この認証方法は、ユーザーが「持っているもの」と「知っているもの」にとどまらず、さまざまな特徴と行動面からユーザーが「誰であるか」にまで及ぶため、悪意のあるユーザーによるなりすましは事実上不可能です。

動的なポリシー適応と対応

適切なポリシーを適切なタイミングで、動的かつインテリジェントに適用することで、ポリシーがユーザーの現在のコンテキストに合わせて最適化され、厳格過ぎることも消極的過ぎることもないようにします。AIベースによる防御ファーストのエンドポイント検知／対処（EDR）により、攻撃を実行前に阻止し、プレイブックベースのワークフローによって調査と対処を自動化します。

実世界の例

ある従業員が昼食時にスマートフォンを使って電子メールをチェックし、クラウドおよび企業イントラネット上のアプリにアクセスした後、それをレストランに置き忘れてしまいました。

一般的な静的なモバイルポリシー（30分のタイムアウトなど）と「ネットワークのみ」のゼロトラストアプローチの組み合わせの場合、このケースでは、正当なユーザーが既にアクセスを付与されており、直前にもアクセスが付与されているため、必然的にデータが危険にさらされます。この電話を拾った悪意のあるユーザーにとっては、これは以下のことを意味します。

- このモバイル／Wi-Fiネットワークからのアクセスは拒否されない

- アプリへのアクセスが付与されているため、再認証は実行されない
- そのうちタイムアウトが発生する可能性はあるが、アクティブな使用中には発生しない

よくありがちなこのケースの皮肉な点は、正当なユーザーの有益で生産的な行動がこの漏洩につながっているところです。しかし、誤解のないように言うと、これはユーザーの落ち度ではなく、コンテキストに対応しない静的なポリシーと、初期アクセスの付与に的を絞った過度に狭義の「ネットワーク中心」のゼロトラストの概念が原因です。

BlackBerryのゼロトラストアーキテクチャによるこのケースへの対応方法...

BlackBerryのZTAは、ソリューションを継続的に監視し、すべてのデバイスとアプリを継続的に監視し、強力なAIを適用することによって、ユーザーがデバイス、アプリ、ネットワークをどのように使用するかを把握して、情報漏洩をアクティブに防止し、正当なユーザーのエクスペリエンスを低下させるのではなく最適化します。

コンテキストに応じた認証

このレストランは、このユーザーにとって信頼性の低い場所として既に認識されています。デバイスやアプリのタイムアウトは、「置き忘れた」デバイスに関連する脅威の機会を減らすよう調整済みです。さらに、ユーザーがその後別の場所で別のデバイスからアプリにアクセスすると（たとえば、オフィスに戻って再度ラップトップにログインすると）、BlackBerryのZTAはそのイベントを検出し、「置き忘れた」電話／アプリをロックするというプロアクティブな措置を取ります。電話／アプリは、正規のユーザーが復旧させるまでロックされたままです。

*動的なポリシー適応：*タイムアウトはユーザーがレストランでデバイスとそのアプリを最初に使用するときに前もって動的に短縮され、次いでユーザーがオフィスに戻ったことが検出されたときにデバイスとそのアプリは明示的にロックされます。

連続認証

パッシブ生体認証と異常な使用の検出の組み合わせに基づいたAIベースの追加防御レイヤーにより、正当なユーザーのみがアプリとサービスに継続的にアクセスできるようにします。

*動的なポリシー適応：*悪意のあるユーザーは自動的にチャレンジされ、最初の生体認証によるパッシブチェックに失敗するか、正当なユーザーについて学習された信頼できる行動に合致しない異常な行動が取られると、アプリへのアクセスがブロックされます。これにより、短縮されたタイムアウトが発生する前に悪意のあるユーザーがアクセスを取得するようなことがあっても、残りの脅威はすべて排除されます。

BlackBerryのAIの手法

BlackBerryは、各種AI手法を組み合わせて使用し、これらを「集団」として連携動作させることにより、継続監視と脅威検知、コンテキストに応じた認証、および連続認証を提供します。

教師なし学習

個人、グループ、および役割について信頼できる通常の行動と場所を学習し、ユーザーのコンテキストと現在のリスクプロファイルに合わせて調整されたポリシーを動的に適用します。

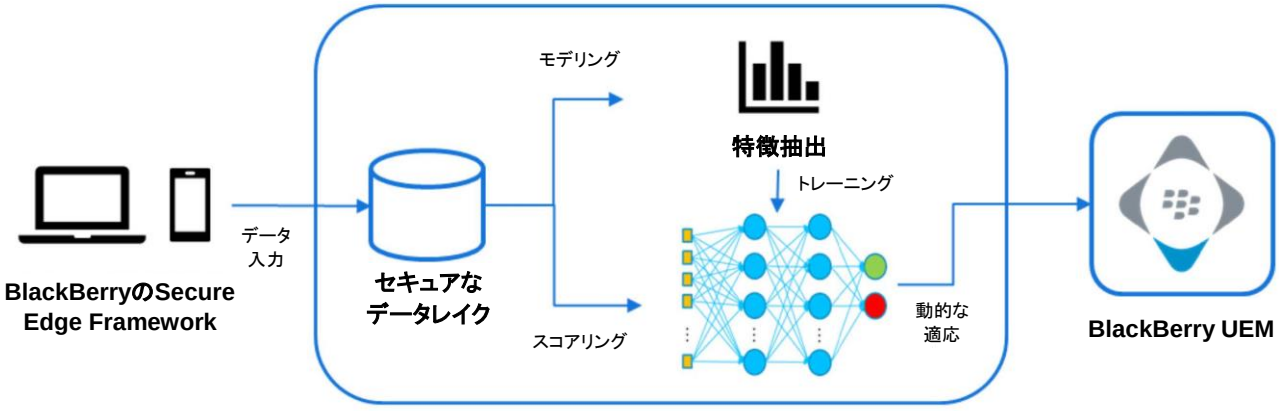
ディープラーニング

パッシブ生体認証やその他の行動およびセキュリティに関する分析を、正当なユーザーの連続「N要素」認証へと変えます。従来の「ログイン+タイムアウト」モデルには、最初にデバイス、ネットワーク、またはアプリへのアクセスが付与された正当なユーザーと現在のユーザーが今も同じであることが保証されないという現実的な問題がありますが、この問題が解決されます。

異常検知

アプリの使用とセキュリティの分析に教師あり手法と教師なし手法を適用し、悪意のある部外者と悪意のある内部関係者のどちらについても、通常の使用と異なる悪用パターンを識別します。

図2：全エンドポイントを対象にした、BlackBerryのインテリジェントなセキュリティAIベースのリスクモデリングとスコアリング



モデリングのインプット

コンテキスト

- 場所
- 日時
- 使用アプリ／サービス
- 使用ネットワーク

生体認証

- モーション／タッチ認証
- デバイスの方向角
- デバイスの揺れ
- マウスの動き
- キーストロークの速度

アプリの使用とセキュリティに関する分析

- 認証
- プロセスの開始
- 検索／ダウンロード
- 送信／転送
- 共有／開く
- コピー／貼り付け
- スクリーンキャプチャ

Secure Edge Frameworkがデータの整合性を確保

AIベースのセキュリティアプローチを成功させるには、モデリングおよびリスクスコアリングのプロセスで使用されるデータの整合性を確保する必要があります。システムに取り込むデータが侵害されていると、必然的にそれらのデータに基づくリスクスコアの検証と動的なポリシー適応も侵害されます。BlackBerryは、Secure Edge Framework（SEF）によってAIモデリングとスコアリングへのインプットの整合性を保護します。

セキュアブートストラップ | デバイスのコンプライアンス | モバイル脅威検知 | セキュリティ分析

このフレームワークは以下の4つの主要なコンポーネントで構成されます。これらのコンポーネントは、エンドポイントセキュリティと脅威検知における、BlackBerryとCylanceの実績あるベストオブブリードテクノロジーの組み合わせに基づきます。

セキュアブートストラップ

承認されたエンドポイントのみがデータを送信できるようにし、エンドポイントがその他のエンドポイントを「スプーフィング」し、侵害されたデータを悪意を持ってシステムに送信したり、「サービス拒否」型攻撃を実行したりするのを防ぎます。

デバイスのコンプライアンス

ルート化／脱獄の検知や他のコンプライアンスチェックを実行して、実行先のデバイスが侵害されている場合でもSecure Edge Frameworkを侵害から保護することで、デバイスのコンプライアンスを維持します。

モバイル脅威対策

未知の脅威を検知し、準拠したデバイスまたはアプリが侵害されるのを防止します。

セキュリティ分析

ターンキー型の分析ライブラリとサポートAPIを実装することで、BlackBerryのSecure Edge Frameworkを実装するアプリが、コンテキストに応じた連続認証を実行するのに必要な最も重要な分析のサブセットを簡単に装備し、安全に送信できるようにします。

セキュアインターネットゲートウェイ

前述のように、内部ネットワークと外部ネットワークを定義する境界はますます動的かつ曖昧になっており、その結果、従来のVPNゲートウェイやファイアウォールの有用性が低下しています。それと同時に、ファイアウォールとWebゲートウェイの違いも曖昧になっており、クラウドベースのゲートウェイ製品では、これら2つの機能が融合されていることがよくあります。従来のネットワークファイアウォールがこの役割を果たすことができるのは、送受信トラフィックがすべてそのファイアウォールを通過し、脅威の大半がパケットレベルの攻撃（サービス拒否攻撃、バッファオーバーフローの悪用、不正な形式のパケットの悪用など）であった場合です。これらの種類の脅威は今なお存在していますが、攻撃の拡大と高度化はアプリレベルにまで進んでおり、そこではハイジャッキング、フィッシング、データ抽出などの攻撃に重点が置かれています。

このようなネットワークの状況の進化に対処するには、ゼロトラストアーキテクチャにセキュアインターネットゲートウェイ（SIG）を組み込む必要があります。SIGは、VPNレスアクセスを可能にするだけでなく、以下のような追加機能を提供することにより、ユビキタス、セキュア、VPNレスのモバイルアクセスというゼロタッチの目標を実現し、その能力をあらゆるデバイスに拡張します。

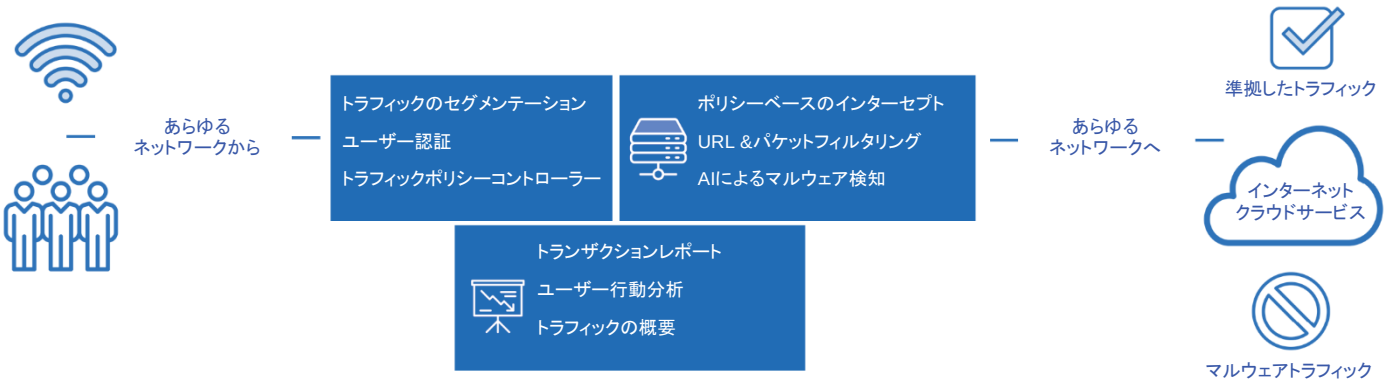
コンテキストに応じた連続認証

前述のように、ゼロトラストアーキテクチャにおける認証は、コンテキストに応じた連続的なものであり、アプリの使用ライフサイクル全体を通して行われる必要があります。これには、SIGを使用してユーザーが連続的に認証されるようにし、いずれかの時点で認証ステータスが疑わしくなった場合は、必要に応じてネットワークとアプリへのアクセスを動的にブロックすることが含まれます。

トラフィックのセグメンテーション

ゼロトラストネットワークの目標の1つは、トラフィックをセグメント化して効率的にロックダウンできるようにする一方で、信頼が確立されていて継続している場合は即座でユビキタスなアクセスを提供することです。主な課題は、新しいユーザー、デバイス、およびアプリが随時オンラインになる可能性があるような常に変化するネットワーク環境において、動的な権限モデルを維持することです。複雑な多層データセンターの展開環境においては、大量のネットワークアプライアンスやファイアウォールルールが機能している場合があり、それらを可視化または管理することはほとんど困難です。そのため、「誰が何に対してアクセスを持っているか」という最も基本的な質問に答えることさえ驚くほど困難である場合があり、より多くのサードパーティのホスティングおよびクラウドサービスプロバイダーがアプリの提供に加わるにつれ、ますます困難になっています。また、苦労して初期構成をまとめたとしても、構成ミスや人的エラー、プロセス関連エラーの可能性があるゆえに、継続的なメンテナンスはコストがかさむ、リスクを誘発する問題になります。

図3：セキュアインターネットゲートウェイ



SIGは、構成ポリシーによってソフトウェア定義ネットワークを有効化することで、これらの課題に対処します。構成ポリシーを使用することで、より一元的かつ動的に、特権に基づいてトラフィックをセグメント化でき、変更を行う必要はありません。また、大量の物理ネットワーキングコンポーネント全体にわたって、正確かつ一貫した方法で変更を行うことができます。さらに、BlackBerryのAIベースのモデルでは、ユーザー、グループ、および役割について学習したトラフィックアクセスパターンに基づいて必要なセグメンテーション構成を自動化することができます。その上、リアルタイムで異常を検知し、アクセスを拒否することで即座に修正することもできます。

脅威防御

認証とセグメンテーションに加え、SIGでは、ポリシーベースのインターセプトと標準のURL／パケットフィルタリングが、他のZTAコンポーネントを利用した先進的でプロアクティブなAIベースのマルウェア検知と脅威防御と組み合わされます。SIGでは、ゼロタッチの目標に従ってネットワークとアプリに動的かつ柔軟にアクセスできるようにすることにより、全体的なセキュリティを弱体化させて企業を悪意のあるサービス妨害や情報漏洩にさらす可能性のある、デバイスやネットワークに起因する脅威から企業を保護します。

レポートと分析

可視性を提供し、対象を絞った管理を実現するために、SIGは、トランザクションとトラフィックのレポートだけでなくユーザー行動分析をも含むレポートおよび分析機能を提供します。これにより、SOC担当者はユーザーとデバイスがどのようにネットワークとアプリを使用しているかを完全に把握し、ゼロトラストの目標とゼロタッチの目標のバランスが取れた、より最適なポリシーと管理策を実装することができます。

BlackBerryのゼロトラストアーキテクチャ – トータルソリューション、すべてのエンドポイントを完全にカバー

他のソリューションは問題に部分ごとに対処するのに対し、BlackBerryのZTAは、デバイス、ネットワーク、アプリ、ユーザーの全範囲を完全にカバーする、ゼロトラストのトータルソリューションを提供します。

- 強力なAIを利用して、ゼロトラストアーキテクチャからゼロタッチエクスペリエンスへのパスを提供
- あらゆるタイプのエンドポイントで動作して完全にカバーし、信頼できる動作への洞察を向上
- 継続的な監視と脅威検知を提供し、データとAIの整合性を確保
- デバイス、ネットワーク、アプリ、ユーザーにわたり、コンテキストに応じた連続認証を提供
- オープンプラットフォーム上に構築され、既存のソリューションとシームレスに統合可能

BlackBerry について

BlackBerry（NYSE：BB；TSX：BB）は、高い実績を誇るセキュリティソフトウェア・サービス会社で、企業や政府機関向けに、IoTのセキュリティ保護に必要なテクノロジーを提供しています。BlackBerryはオンタリオ州ウォータールーに本社を置き、安全性、サイバーセキュリティ、およびデータプライバシーに妥協することなく取り組んでおり、人工知能、エンドポイントセキュリティと管理、暗号化技術、組み込みシステムなどの主要分野をリードしています。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。