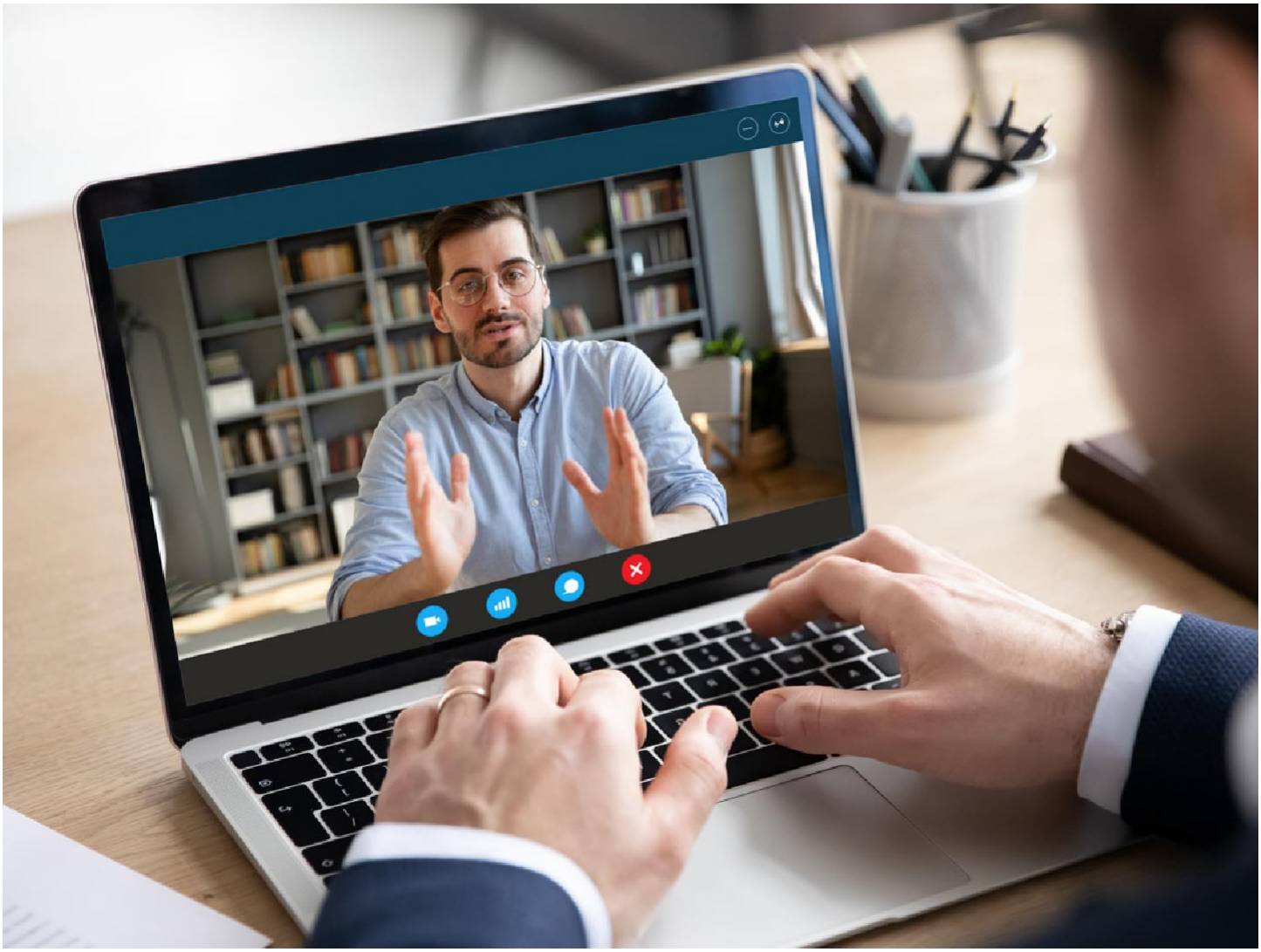
BlackBerry
Intelligent Security. Everywhere.

ホワイトペーパー



新たな現実

カオスに秩序をもたらす統合エンドポイントセキュリティ

概要

新型コロナウイルス感染症（COVID-19）のパンデミック以前にも、企業のサイバーセキュリティの状況はカオスと混乱に支配されていました。企業内でのエンドポイントの数と種類の増加に加え、増え続けるサイバーセキュリティ脅威により、IT部門は極めて大きなプレッシャーにさらされてきました。企業が手間のかかるセキュリティソリューションを導入すると、従業員が代替手段やシャドーITを利用するようになる場合がよくありました。パンデミックにより、このような問題がすべて悪化し、リモートワークに対する企業の備えが極めて不十分であることが露呈しました。

専門家は、ニューノーマルではデジタルトランスフォーメーションとリモートワークが加速すると予想しています。同様に、あらゆる種類のエンドポイントを保護し、企業の機密データを守る必要性も高まります。新たな現実の中で成功するために、ソリューションはITリーダーの厳格なセキュリティ要件を満たす一方で、使いやすさとモビリティに対するユーザーの要求にも応える必要があります。

統合エンドポイントセキュリティは、このような最新の課題を解決するための最新のソリューションです。AI、機械学習、自動化を活用することにより、統合エンドポイントセキュリティは、ユーザーの生産性を低下させることなく、デバイス、ネットワーク、アプリ、ユーザーに次世代のサイバー脅威予防／修復機能を提供します。ゼロトラストとゼロタッチをつなぐ統合エンドポイントセキュリティは、将来の働き方に向けて設計されています。

目次

3 新たなサイバーセキュリティの状況

4 サイバーセキュリティの状況における重要な要素

6 サイバーセキュリティのカオスに対するユーザーの反応とそれが危険な理由

7 人間向けに設計されたセキュリティ

8 ゼロトラストとゼロタッチ

9 新たな現実に対する新たなアプローチ：統合エンドポイントセキュリティ

10 現代の総合ソリューション： BlackBerry Spark® Unified Endpoint Security（UES）Suite

11 サイバー脅威を減らすために連携する6つのテクノロジー

12 BlackBerry Spark UES Suiteの主要な利点

13 将来の働き方に向けた準備

新たなサイバーセキュリティの状況

COVID-19のパンデミックにより、世界中の企業がかつてないほどテクノロジーに依存するようになりました。パンデミック以前も、企業は次第に脅威を増すサイバーセキュリティ環境と脆弱なエンドポイントの急増にすでに直面していました。現在、多くの企業が100%近いリモートワークに向けて突然舵を切り、世界中のサイバー犯罪者がこの危機に付け込もうとしているため、ITリーダーは前例のない課題に直面しています。

サイバー脅威に対抗する従来のアプローチはもはや役に立ちません。この危機の間だけでなく、それ以降も、従業員、顧客、機密データ、評判を守るために、企業には最もスマートな最新のソリューションが必要です。Gartner社によれば、CIOは既存のセキュリティインフラストラクチャを見直し、特にデバイスのエンドポイントセキュリティに重点を置いて、従業員が安全に自宅から仕事するには何が必要かを見極める必要があります。[1]

統合エンドポイントセキュリティ（UES）は、増え続ける現在のサイバーセキュリティ要件を満たすための新たな総合的アプローチです。AI、機械学習、自動化を活用することにより、UESは、ユーザーの生産性をサポートする一方で、ITリーダーの厳しいセキュリティ要求にも応えるように設計されています。

世界中での攻撃対象領域の拡大

攻撃ツールキットへのアクセスが容易になったことに加え、接続されているエンドポイントが急増したことにより、世界中でサイバー脅威が増大しています。2020年に、AIと機械学習は、ますます複雑になる攻撃の継続的な学習と予防的な脅威モデリングを通じて実現される優位性のために、脅威の予防戦略と修復戦略に不可欠になります。[2]

サイバーセキュリティランドスケープの状況における重要な要素

近年、サイバー環境はますます混沌とした状況になり、企業は執拗で巧妙なサイバー脅威に直面しながら、エンドポイントの急増に対応しようと努めてきました。この状況で、パンデミックにより、不慣れなことが多い膨大な数のリモートワーカーが短期間に生じました。ほとんどの企業は、セキュリティを確保しながらリモートワーカーが社内データにアクセスできるようにするためのソリューションを導入していませんでした。このような状況が重なり、企業は深刻なリスクにさらされることになりました。

サイバーカオス

以下のような複数のトレンドが重なることにより、サイバーカオスに拍車がかかっています。

- **技術革新の加速**
  新たなテクノロジーが絶え間なく生じており、企業は競争力を維持するために新しいツールを絶えず採り入れる必要があります。
- **攻撃対象領域の拡大**
  接続されているエンドポイントも含め、企業では、テクノロジーへの依存度が高まっています。
- **脆弱性の急増**
  エンドポイントが増えるほど、脆弱性も増大します。
- **攻撃者と攻撃タイプの急増**
  攻撃者は多面的なアプローチを利用して、無防備なエンドポイントを標的にしています。
- **攻撃的なサイバー投資**
  個人の攻撃者に加え、利益または国益のために攻撃的なサイバー兵器に投資する国家が増えています。
- **地政学的緊張**
  世界の地政学的状況により、すでに複雑なサイバーセキュリティ環境がさらに複雑になっています。
- **ガバナンスの欠如**
  インターネットガバナンスによりセキュリティを向上させる必要性についてはコンセンサスが得られていますが、その方法については合意に至っていません。

エンドポイントのカオス

企業がラップトップとデスクトップのみをセキュリティで保護すればよかった時代が終わってから、すでに長い時間が経過しています。携帯電話、タブレット、ウェアラブルデバイス、あらゆる種類のIoTデバイスとクラウド接続デバイスを含むエンドポイントの数と種類の増加により、ITのコストと複雑性が高まりました。企業は、攻撃者に対する脆弱性の増加は言うまでもなく、増え続けるセキュリティベンダー、ツール、コンソール、脅威アラートにも対処しようと奮闘しています。

パンデミック中には、世界中でBYOD（Bring Your Own Device）モデルの真価が問われました。すでにBYODに対応していた企業は優位に立つことができましたが、全面的なリモートワークを実現できたのは一部の企業に過ぎませんでした。現在、ITリーダーは膨大な数のエンドポイントだけでなく、管理対象となっていなかったデバイスの管理にも苦戦しています。

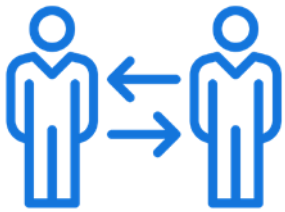
リモートワークに対する準備の欠如

COVID-19のパンデミックに伴って発生した大規模な混乱とリモートワークの必要性に対して、十分な準備ができていた企業はほとんどありませんでした。多くの企業は、従業員全体に支給するために十分な数の社内デバイスを所有していませんでした。また、従業員がファイアウォールの内側の社内データおよびリソースにアクセスできるようにするためのソリューションも導入していませんでした。最も重要な点は、データ、デバイス、アプリのセキュリティを確保するためのインフラストラクチャがなかったことです。

あらゆる地域のITリーダーは、サイバー攻撃の増大が世界中で報道されている中で、サイバーセキュリティ戦略の見直しを迫られました。パンデミックの初期に米国国土安全保障省は、サイバー犯罪者がCOVID-19関連の詐欺、マルウェア攻撃、兵器化されたWebサイト、フィッシングメールで、個人、中小企業、大企業を標的としていると警告しました。[3]また、Wall Street Journal誌は、こうした攻撃とそれに伴うカオスと混乱によって、損害が大きく、長期にわたるセキュリティリスクが生じていることに注意を促しました。[4]

パンデミック初期に実施された世界中の金融リーダーに対するPwC調査において、回答者は「リモートワーク能力の欠如による生産性の低下」が最大の課題となると答えています。[5]

サイバーセキュリティのカオスに対するユーザーの反応とそれが危険な理由



パンデミック以前も、混沌としたサイバー環境に対して、多くの従業員が不満を抱えていました。面倒な認証プロセス、使い勝手の悪いインターフェイス、繰り返し表示されるアラート、非効果的でコストのかかるシグネチャベースのセキュリティ対策などに対する不満から、従業員はセキュリティに対して代替手段やシャドーITを利用するようになりました。作業を簡略化し、生産性を維持するという意図は理解できますが、その結果発生するデータ漏洩は、企業に損害を与え、時には壊滅的な被害をもたらす可能性があります。

COVID-19の感染拡大に伴うリモートワーカーの急増により、データセキュリティに対する脅威はこれまでになく高まっています。パンデミック初期にCNBCが実施したハイテク企業幹部に対する短期調査では、従業員の大半が在宅勤務に移行したことにより、サイバー脅威が増大したという回答が36%を占めました。[6]

同様に、National Law Review誌は、人々の不安と、健康、安全、経済に関する情報への欲求に付け込んだフィッシング攻撃の急増を報告しています。[7]従業員は過去に経験がなくても自宅から仕事をしなければならないというプレッシャーにさらされており、セキュリティの代替手段や詐欺の被害を受けやすい状況への対処が、企業にとって緊急の課題となっています。

ハイテク企業幹部の36%が、従業員のリモートワークによりサイバー脅威が増大したと考えている。[6]

人間向けに設計されたセキュリティ

パンデミック中だけでなく、その前後にも、カオスを制御しようとするセキュリティソリューションでは、人間の性質と人的エラーも考慮する必要があります。新たなセキュリティの状況において、サイバー脅威は外部と内部の両方で発生する可能性があります。

世界中のIT専門家に対する最近のIDG調査では、回答者の95%が、従業員のミスにより企業でデータセキュリティのリスクが発生していると答えています。大半の回答者はセキュリティの強化が生産性に悪影響を及ぼしていると考えていますが、それでも58%は、従業員の使いやすさや利便性よりも厳密なセキュリティ制御が優先されると回答しています。[8]

企業は、ソリューションが以下の点を考慮して設計されているかどうかを検討する必要があります。

- 簡便さ、効率性、使いやすさに対するユーザーの要求に対応している
- 故意でないミスを軽減する
- 不満を抱いている従業員による悪意のある行為を阻止する

最新世代の高度なセキュリティソリューションは、企業ITの主要なステークホルダーである次の2者の優先事項を共に満たします。

- 最大限のセキュリティを求めるITリーダーとビジネスリーダー
- 最大限の使いやすさ、機能、モビリティを求めるユーザー／従業員

IT専門家の58%は、従業員の使いやすさや利便性よりも厳密なセキュリティ制御を優先させる。[8]

ゼロトラストとゼロタッチ

ゼロトラストはサイバーセキュリティ業界で流行語となっていますが、セキュリティチームにとってのゼロトラストの真価は、ユーザー／従業員によるゼロタッチも実現されるかどうかにかかっています。ゼロトラスト環境の構築によって、セキュリティのハードルが上がり、ユーザーにとって不便なものになると、ユーザーはシステムの利用を回避しようとします。継続的な脅威防御とユーザーの生産性の間で、バランスを取ることが重要です。

ゼロトラストとは

ユーザーは、本人であること、アクセスが許可されていること、悪意のある行動を起こしていないことを証明しない限り、いかなるデバイス上のデータにもアクセスできません。ユーザーは、すべてのエンドポイントで、このトラスト（信頼）を継続的に獲得しなければなりません。

ゼロタッチの利点

パスワード、タイムアウト、特別な権限、複数の認証などの面倒な手順なしで社内リソースにすぐにアクセスできるため、ただちに生産性が高まります。

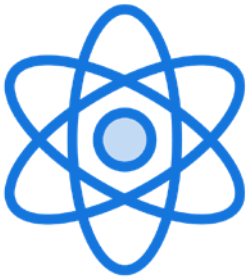
ゼロトラストソリューションでゼロタッチを実現することにより、企業は、新たに発生するサイバー脅威の防御として信頼できるセキュリティと生産性を高める優れたユーザーエクスペリエンスの両方を最大限にすることができます。

人間の処理速度での防御とコンピューターの処理速度での防御：AIの強み

過去のサイバーセキュリティツールは、人間の処理速度で動作しました。新たなサイバー攻撃が発生すると、ベンダーが脅威を解析し、サブスクリプションを通してウィルス定義を発行することにより、事後対応の防御ソリューションとして既知のマルウェアを特定していました。これは時間のかかるプロセスであり、ますます進化する脅威の急増に対応できませんでした。

現在のサイバー犯罪者は、攻撃の範囲と影響を最大化するためにAIを利用しているため、今日のソリューションも機械学習と自動化のパワーを活用する必要があります。高度なAIベースのセキュリティツールのみによって、企業に必要な予測による時間的な優位性が得られます。

新たな現実に対する新たなアプローチ：統合エンドポイントセキュリティ



最新の課題には最新のソリューションが必要です。次世代のサイバーセキュリティでは、あらゆるタイプのエンドポイントに対する脅威の検知、防御、修復のために利用できる最善のAI駆動型ツールが統合されます。統合エンドポイントセキュリティでは、混沌としたサイバーセキュリティ環境を制御するために総合的なアプローチを採用しています。

Gartner社の「Predicts 2020 Mobile and Endpoint Technologies」（2020年の予測モバイルおよびエンドポイントテクノロジー）レポートでは、エンドポイント検知／対処（EDR）およびエンドポイント保護とモバイル脅威防御（MTD）製品との統合に向けたトレンドに言及しています。[9]また、セキュリティ機能を根本的に変更するのではなく、MTDなどのセキュリティツールを採用して、既存のセキュリティインフラストラクチャ機能の隙間を埋めることを、企業に対して推奨しています。さらに、2020年にMTDを導入している企業は20%未満ですが、2023年までに50%の企業が導入すると予測しています。

パンデミック以前のIDC調査によると、60%以上の企業が、従業員の柔軟性（リモートワークの増加、機敏性、消費者製品のようなデジタルエクスペリエンス）とセキュリティ要件のバランスを取ることに苦心しています。IDC社は、パンデミックの経験により、多くの企業では、リモートワークに関連するポリシー、プロセス、テクノロジーの綿密な検証と更新が促進されると予測しています。[10]

50%の企業が2023年までにモバイル脅威防御を導入する。[9]

現代の総合ソリューション: BlackBerry Spark UES Suite

BlackBerry Spark® Unified Endpoint Security（UES）Suiteは、新たな現実向けに設計されたセキュリティソリューションです。他のベンダーがサイバー脅威の課題の一部にのみ対処しているのに対して、BlackBerry Spark UES Suiteはあらゆるデバイス、ネットワーク、アプリ、ユーザーを網羅して、ゼロトラストのための真のAI駆動型ソリューションを提供します。このゼロトラストアプローチの成果として、ユーザーの生産性を妨げることなくセキュリティを向上させるゼロタッチエクスペリエンスが実現されます。

BlackBerry Spark® Suite

BlackBerry Spark Suiteは、統合エンドポイントセキュリティ（UES）と統合エンドポイント管理（UEM）の両方を提供します。これは、あらゆるデバイスタイプとオーナーシップモデルをサポートしています。

AI、機械学習、自動化を活用するBlackBerry Spark UES Suiteでは、すべてのエンドポイントに対する可視性の改善と簡素化された管理を提供する一方で、サイバー脅威の予防と修復が改善されます。

ゼロトラストからゼロタッチへ

BlackBerry Spark UES Suiteは、現在のサイバーカオスに対処している企業の最も厳しいセキュリティ要件だけでなく、ユーザーの要求も満たすように設計されています。BlackBerry Spark UES Suiteでは、ユーザーに何度も再認証を求める代わりに、AIを利用して、デバイス、ネットワーク、データ、ユーザー、アプリに対する動的なトラスト（信頼）を維持します。

新たなモバイルワーカー向けの信頼性の高い生産性アプリ

BlackBerry Spark UES Suiteの中核であるAI駆動型の脅威防御は、BlackBerryモバイルアプリに直接組み込まれているため、ユーザーや管理者はモバイル脅威検知専用に作成されたサードパーティアプリをインストールまたは管理する必要はありません。

これは、モバイル脅威防御（MTD）ソリューションであり、モバイルアプリでマルウェアを絶えずスキャンし、攻撃を開始前に阻止します。企業は、リモートワーカーが使用している重要なビジネスアプリと、各アプリに含まれる大切なデータが保護されていることに安心感を抱くことができます。

サイバー脅威を減らすために連携する6つのテクノロジー

BlackBerry Spark UES Suiteは、相互に接続される6つのテクノロジー（柱）によって、非常に広範なセキュリティ機能と可視性を提供します。これらの柱は連携して、リスクを算出し、データを共有し、ポリシー制御を改善にします。

たとえば、エンドポイント検知／対処（EDR）ソリューションでは、エンドポイント保護とモバイル脅威検知（MTD）テクノロジーを活用して、*PC Magazine*誌により世界中の企業で増加していると報告されている[11]マルウェアとフィッシング攻撃をブロックします。また、連続認証により、EDR、EPP、MTDからのデータを使用して、行動プロファイルを改善し、ゼロトラストとゼロタッチを橋渡しします。

1. エンドポイント保護

AIを活用した自動マルウェア予防、アプリケーションとスクリプトの制御、メモリ保護、デバイスポリシーの適用を組み合わせることにより、サイバー攻撃を予測／予防します。

2. エンドポイント検知／対処（EDR）

AIベース、予防ファーストのエンドポイント検知／対処により、実行される前に攻撃を阻止し、プレイブックに基づくワークフローで調査と対処を自動化します。

3. モバイル脅威防御（MTD）

AIを活用して、モバイルデバイスと実行されているアプリで、新規または既知の脅威（悪意のあるURLとフィッシングなど）を監視し、修復のために適切な処置を実行します。

4. 連続認証

（モバイルとデスクトップでの生体認証、アプリ利用率、ネットワークおよびプロセスの起動パターンを組み合わせて）デバイスとのユーザーの継続的なやり取りと行動を評価してユーザーを認証し、社内データへのアクセスを動的に許可することにより、管理の負担を大幅に減らします。

5. 情報漏洩防止（DLP）*

デジタル著作権管理（DRM）や機械学習などのBlackBerry®のコアテクノロジーを組み合わせて、ユーザーとデータ間のゼロトラストを確立します。

6. 安全なWebゲートウェイ*

あらゆるデバイスで、即時、セキュア、かつVPN不要のモバイルアクセスというゼロタッチの目的を実現するために、複数の機能を提供します。

- 連続認証とコンテキスト認証
- トラフィックのセグメント化
- 脅威の予防
- レポートと解析

BlackBerry Spark UES Suiteの主要な利点

サイバーセキュリティ脅威予防／修復の改善

BlackBerry Spark UES Suiteは、煩雑な複数ベンダーの管理、過剰なアラートのノイズ、新たな現実での企業のセキュリティに関する不確実性を排除します。最新のAI駆動型の脅威予防、検知、連続認証、対処を利用することにより、現在の攻撃者の巧妙さに追い付き、さらに一歩先を行くことができます。BlackBerry Spark UES Suiteは拡大する企業の攻撃対象領域全体を対象とすることにより、世界中のリモートワーカーの前例のない脆弱性に対処します。

ゼロトラストとゼロタッチを橋渡しすることによる生産性のサポート

BlackBerry Spark UES Suiteは、すべてのエンドポイントを継続的に監視することにより、ユーザーがデバイス、アプリ、ネットワークとどのようにやり取りしているかを学習します。AIはこの情報を使用して、デバイス、時間、場所、ネットワークに関わらず、社内リソースへの即時アクセスを許可するために、ユーザーを信頼できるか否かを自動的に判断します。このスマートなAI駆動型のアプローチでは、正規のユーザーのエクスペリエンスを最適化する一方で、攻撃を阻止し、データ漏洩を防ぎます。

包括的な保護の提供

あらゆるエンドポイントタイプに対応することによって、BlackBerry Spark UES Suiteは、包括的な保護を実現し、信頼できるユーザーの行動に関する洞察を深めます。これは、デバイス、ネットワーク、アプリ、ユーザーに対する連続認証とエコシステム全体の可視性を提供します。パンデミック下の企業の状況において、BlackBerry Spark UES Suiteは、拡大する企業の攻撃対象領域全体にわたって明確な視野を提供します。

時間の経過と使用によるスマート化

BlackBerry Spark UES Suiteは、数年および数世代にわたり脅威検知と脅威モデリングに利用されてきた実証済みのAI-ML（機械学習）エンジン上に構築されています。これは、新たなユーザー、デバイス、アプリケーション、テクノロジーによる環境の変化に伴って、継続的に学習します。したがって、企業が長く使い続けるほど、BlackBerry Spark UES Suiteはスマートになります。

管理の簡素化

パンデミック中とそれ以降の事業継続性を確保するために、想定外の財務上の課題と複雑な業務の再編成に直面している企業に対して、BlackBerry Spark UES Suiteはより強力で*シンプル*なサイバーセキュリティを提供します。これは、管理が容易であり、複数のベンダーに費やしていた時間と費用を節約し、IT部門の負担を減らし、より戦略的な優先事項のためにリソースを解放することができます。

これからの働き方に向けた準備

COVID-19のパンデミックによって、人々の働き方は急激に変化しました。いつ元の状態に戻るのか、そもそも戻ることがあるのかは不明であり、専門家はデジタルトランスフォーメーションとリモートワークが加速すると予想しています。残念ながら、世界中のサイバー犯罪者は、膨大なリモートワーカーが利用している多様なエンドポイントによって生じた攻撃の機会を悪用しています。

BlackBerry Spark UES Suiteは最新のAIでゼロトラストとゼロタッチを橋渡しすることにより、企業がデータを保護する一方で、従業員が場所、時間、デバイス、アプリにかかわらず業務を遂行できるようにします。これは新たな現実に対する包括的なソリューションです。

1 https://www.gartner.com/smarterwithgartner/coronavirus-cio-areas-of-focus-during-the-covid-19-outbreak/

2 https://www.blackberry.com/us/en/forms/cylance/gated-content/2020-threat-report

3 https://www.us-cert.gov/ncas/alerts/aa20-099a

4 https://www.wsj.com/articles/coronavirus-cybersecurity-fallout-might-not-be-felt-for-weeks-or-longer-11585128601

5 https://www.pwc.com/us/en/library/covid-19/pwc-covid-19-cfo-pulse-survey-global.html

6 https://www.cnbc.com/2020/03/20/phishing-spam-spike-as-hackers-use-coronavirus-to-hit-remote-work.html

7 https://www.natlawreview.com/article/working-remotely-and-cyber-security-during-covid-19-outbreak

8 https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/infogrfx-bb-human-nature.pdf

9 https://www.gartner.com/en/documents/3980406/predicts-2020-mobile-and-endpoint-technologies

10 https://blogs.idc.com/2020/03/16/remote-work-in-the-covid-19-era-are-we-ready/

11 https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine

BlackBerryについて

BlackBerry（NYSE: BB; TSX: BB）は、世界中の企業や政府機関向けに、インテリジェントなセキュリティソフトウェア／サービスを提供しています。現在、BlackBerryのソリューションは、1億5,000万台の自動車を含む5億以上のエンドポイントを保護しています。カナダのオンタリオ州ウォータールーに本社を置く当社は、AIと機械学習を活用して、サイバーセキュリティ、安全性、データプライバシーの分野で革新的なソリューションを提供しています。さらに、エンドポイントセキュリティ管理、暗号化、組み込みシステムなどの分野を先導する役割を果たしています。BlackBerryのビジョンは明確であり、相互に接続される将来の世界を信頼性の高いセキュリティで保護することです。

詳細については、BlackBerry.comにアクセスし、Twitterで@BlackBerryをフォローしてください。

BlackBerry
Intelligent Security. Everywhere.

BB20-0279 | 200618