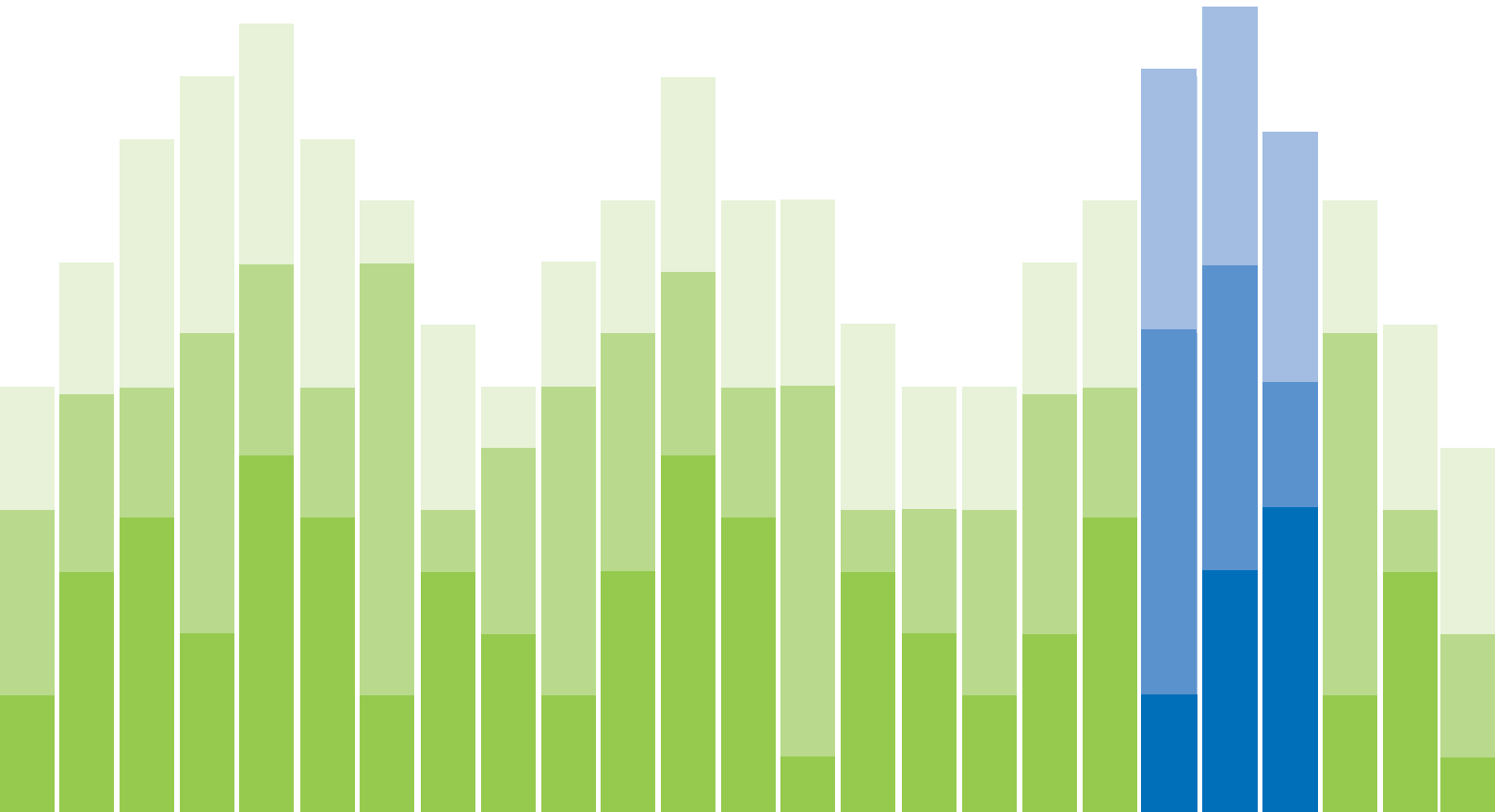
WEBROOT®
Smarter Cybersecurity™

2017年12月

四半期別脅威トレンド

Webroot BrightCloud® 脅威インテリジェンス：未来に向けて開かれた窓



未来を知りたいと願わない人はいないでしょう。サイバーセキュリティの世界は、他のいかなる業界よりもこの願いを強く持っています。それは将来の脅威がほんの少し垣間見れるだけで、破滅的で莫大な費用の掛かる侵害を防ぐことができるためです。セキュリティ業界では受け身の状態から抜け出し、脅威に対し積極的かつ自発的に反応すること、そして攻撃の前に防止できることを目指しています。この四半期別脅威トレンドレポートは、顧客がこういった予測能力を持ち、脅威や潜在的な攻撃を防ぐことについて、Webroot BrightCloud脅威インテリジェンスサービスが実際にどのように助けになるのかを説明しています。最初に、ウェブルートの専門家が立てた2018年の予想を見てみましょう。

将来を見据える

脅威インテリジェンスはより賢くなり、迫り来る攻撃を検知し、攻撃の対象者がその存在に気付くより前にそれを取り除くことが可能になります。2017年11月下旬、NotPetyaを元にしたランサムウェア攻撃がニュースで取り上げられた時、ウェブルートが目的としている行動の実行を、はっきりと見ることができました。ウェブルートは、顧客が誰もこの攻撃を受けていないことを、すぐに確認しました。機械学習とクラウドベースの分析が、既存の脅威の類似性を認識し、マルウェアの存在を予測することでネットワーク境界においてその拡がりを止め、エンドポイントに与える影響を防ぎます。

ウェブルートチームはBrightCloudの予測能力を利用して、近い将来に発生しうるセキュリティ関連の事象を未然に防ぎます。予測の例：

ゲイリー・ヘイスリップ最高情報セキュリティ責任者

» **人工知能：使用するのは、良い人たちだけではない**
私たちは、過去のアンチマルウェアソフトウェアに対し人工知能（AI）を使用したマルウェアが出現することを予測しています。DEF CONでの最近のデモストレーションでは、マルウェア作成者がGitHub上で利用可能なオープンソースのAIを使用していることが発表されました。彼らは当時で過去のウィルス対策ソリューションの16％に対応したマルウェアを作成することができました。どの技術でもそうであるように、ポイントは、どの企業がデータを調査しているか、そして誰がより優れた分析モデルを持っているかということなのです。

それについて言えば、ウェブルートは完璧なモデルを目指してからすでに10年以上を費やしているとともに、実社会の大量の情報を継続的に入手し続けており、とても強力なポジションを占めています。私たちは最先端の研究を続け、学んだことをパートナーのためのサービスのセキュリティプラットフォームに組み込み続けています。これによりウェブルートのパートナーはリスクへの露出を減らし自分たちの顧客を保護することができます。

» **破壊的ランサムウェア**
近々、暗号化目的ではなく、破壊を目的としたランサムウェアが出現することを予測しています。フィッシング攻撃は、ランサムウェアの中でも最も一般的な方法であり、その目的を遂行させないように攻撃を止めることはこれまで以上に重要になっていきます。

BrightCloudリアルタイムアンチフィッシングサービスは、フィッシング攻撃に関連のあるページやURLへのアクセスを妨害します。状況に応じた方法でセキュリティ侵害のサインをすべて点検し、潜在的な悪意のある活動の兆しをすべて見つけます。また、BrightCloudストリーミングマルウェア検知サービスは、境界やその他の技術からのアップストリームにおいて悪意のあるファイルをブロックします。

デイビッド・ケネリー脅威研究ディレクター

» **二次感染ベクトルとしてのランサムウェア**
ランサムウェアの作成者たちは、目的とする攻撃の実行中にトラックを隠すことが、より上手になってきています。悪意のあるURLやフィッシング攻撃から始まったランサムウェアの場合は特にそうです。こういった攻撃は、ハッカーが感じ取った特定の脆弱性をターゲットにしています。そういったターゲットは特定の会社に存在することが多く、その会社のアプリケーションポートフォリオ、ネットサークサイズやハッカーが気付くことのできるその他の要因を元にしています。一旦内部に入り込むと、ランサムウェアは二次感染を開始するためのペイロードを何にするかを決定できるようになります。その際、初期感染時に学んだこと及び成功した攻撃モデルを参考にします。

ニック・エマニュエル製品ディレクター

» **埋め込みリンクを利用した誘い**
今後もフィッシングやスピアーフィッシングは続き、埋め込みリンクを利用したフィッシングが増加します。EU一般データ保護規則（GDPR）の適用が開始し英国がEUから脱退することで、これらの話題に関連した内容を利用したフィッシングやスピアーフィッシングが企業に多く仕掛けられることを予想しています従来の脅威インテリジェンス製品は、2つのレベルで不十分だと言えます。一つは固定されたフィッシングリストに依存していることです。固定されたリストでは今日の攻撃ペースにとても追いつくことはできず、一瞬のうちに開いて閉じる新しいフィッシングサイトを、簡単に見つけることはできなくなっているのです。それに加え、セキュリティ侵害のサイトをひとつひとつ個別にみているため、コンテキスト分析ができず、点と点をつなぎ実際の攻撃を予測するということができません。

Webroot BrightCloud脅威インテリジェンスサービスは、リアルタイムのアンチフィッシングサービスを提供するだけでなく、豊かな機械学習モデルとコンテキスト分析を同時に利用することで、セキュリティ侵害を完全に異なるものとして表し、脅威全体を全く別の絵のように映し出します。より多くのフィッシング攻撃が埋め込みリンクに依存するようになるにつれて、BrightCloudは複数段階に及ぶ保護を提供します。

予測可能な脅威インテリジェンスに必要なもの

脅威インテリジェンスは、先に発生する脅威を予測することを約束してきましたが、多くの場合、不十分なレベルでしか達成していません。理由は簡単です。脅威インテリジェンスそのものが、今後何が起こるのかを予告するにはまだ不十分なのです。大抵は根拠データが不十分であり、機能を支える機械学習は堅牢でなく、データが古く、そしてリスクの表示も個別に確認しています。予測ツールとして本当に便利に使用するためには、脅威インテリジェンスは以下の項目を満たす必要があります。

» 正しい基礎の上に構築され、時間の経過の中での行動分析を元にした洞察ができること。
» 適切（かつ十分な）ソースを使用。
» 効果的な危険学習を採用し、定期的に予測能力が改善可能。
» コンテキスト分析を通して「全体像」としてみる事ができる。

Webroot BrightCloud脅威インテリジェンスの予測機能の独自性

Webroot BrightCloud脅威インテリジェンスは、そのプラットフォーム、ソース、機械学習、コンテキスト分析から、未来に対する独自の窓を提供します。

プラットフォーム

まずウェブルートはURL、IP、ファイル、モバイルアプリケーションで脅威インテリジェンスを実行する、高度なクラウドベースのセキュリティプラットフォームです。10年以上に渡り、プラットフォームは機械学習、クラウドベースの大量の基準データ、軽く高速な処理を効果的に実現してきました。世界的に広がったデータベースにより、処理の速度と深さを得ることができたのです。数字が物語る：Webroot BrightCloud脅威インテリジェンスサービスは、インターネットの95%の分類及びスコアリングを継続的に行い、同時にIPv4スペース全体と使用中のIPv6スペースの監視を行います。

情報源

次に、BrightCloudの情報源は、クローラー、ハニーポット、何かが発生するのを待つような受動的なセンサーだけを利用するのではなく、実世界の製品、システムやネットワークと相互作用を持つ人々から得ており、広く深いものとなっています。ウェブルートは世界中に存在する4千万個以上のセンサーと3千万個以上のコネクテッドエンドポイントを利用し、脅威インテリジェンスに情報を供給しています。過去10年間で、ウェブルートは270億以上のURLおよび6億以上のドメインのカテゴリ分析を行ってきました。

それぞれの入力ベクトルサイズは大量：BrightCloudは単一のウェブページ内の100万個以上の特性をキャプチャすることができる容量を持っています。

BrightCloudは40億以上のIPアドレス、5500万以上のモバイルアプリ、そして130億以上のファイル動作レコードのクラシフィケーションおよびカテゴリ分析を行ってきました。さらに、これらの大量のデータは、継続的にリアルタイムで分析されているのです。ウェブルートは毎秒5千個の速度でURLのクラシフィケーションを行っており、毎日2万5千個の新規の悪意のあるURLを見つけています。日々見つけられている10万個の新規の悪意あるIPアドレスと6千個の新規のフィッシングサイトを合せれば、ウェブルートがネットワークおよび情報セキュリティ産業における中心的な脅威インテリジェンスプロバイダーであることに疑いがありません。

効果的な機械学習

三点目として、機械学習は脅威インテリジェンスプラットフォームにおいて必要不可欠な構成要素です。それは、脅威の特性が絶え間なく変化するにもかかわらず、常に高い検知率を維持するためです。ウェブルートの機械学習は分散型システムで、Hadoopファイルなどのビッグデータ構造をしています。これにより実行可能な約100万個の未確定ファイルについて自動的に分類を行い、各ファイルが安全なものか悪意のあるファイルかを確認します。機械学習はまた、ゼロデイフィッシングサイトの検知を完全に自動化します。また、最大エントロピー原理（MED）、アクティブラーニング、アクティブフィードバックなど、多様な分類技術を同時に利用できるようになっています。

ウェブルートの自己学習プラットフォームは、これまで知られていない脅威を素早く正確に特定できるように連続的な入力が行われます。例えば、ネットワーク上でファイルの横断が開始するとすぐに、ウェブルートはファイルがユーザーのハードディスクに到達するより前にデータ要素を引き出します。ストリング、作成者、URL、埋め込みIPなどの情報に基づき、モデルが分析を開始します。ほんの少しの情報であっても、それを元にレピュテーションスコアが直ちに付けられます。顧客はそのスコアを元に閾値を設定し、その閾値より低いものはブロックし、高いものは許可するということが可能になります。つまりソフトウェアが、ファイルが悪意のあるものであることを予測しファイルのトラック中に停止させることが可能となります。同時に、レピュテーションの決定結果について学習し、アルゴリズムをより完璧なものにすることで、次回より正確な決定が可能となります。

多くの脅威インテリジェンスのベンダーが機械学習の採用を謳いますが、どのベンダーも例外なく、卓越したウェブルートの機械学習エンジンの有する長年にわたる継続的な学習データを持っていません。ウェブルートのアルゴリズムと数学モデルは独自のものであり、複数の特許により保護されています。ウェブルートが所有する、機械学習技術の最適化を目指した80件以上の特許（毎年平均8～10件の登録）の右に出る企業は存在しないのです。

コンテキスト分析

四点目に、非常に重要なことですが、コンテキスト分析を行うことでインテリジェンスの糸が紡がれ、大きな全体図を露わにすることが可能になります。ウェブルートのコンテキスト分析は、URL、IP、ファイル、モバイルアプリをそれぞれ別々に見るのではなく、実世界のエンドポイントから得たもともと特性の異なるデータを相互に関連付けることで、リスクスコアリングを予測します。「guilt-by-association（連座制）」モデルを利用することにより、コンテキストデータベースが、一見無害に見えても他のロケーションやアセットと結びつくと悪意ある行為を開始するURL、IP、ファイル、モバイルアプリを相互に関連付けます。

例えば、マルウェアとして働くと言われているURLがあります。これまで見たことのない新規のファイルがそのURLと関連付いた場合、過去に問題を発生させたことのないサイトと関連付けられたことのある未明のファイルと比較して、悪意のあるファイルである可能性がより高くなります。

別の例としては、人事部から来たとみられるフィッシング攻撃があるとします。他社の脅威インテリジェンスソリューションでは、最新情報に基づき、ソースIPアドレスを無害としてみるかもしれません。しかしながらウェブルートでは、以前有害であったことを確認することができるため、そのファイルは再び脅威と見なされるようになります。また、悪意のある活動が見られたURLへの内部リンクに注目することができ、それによりEメールは有害であると捉えることができます。

ユーザーとその顧客にとっての意味

ウェブルートを利用することで、ユーザーは浮かび上がってくるパターンを確認することができ、それに自動的に対処し、判断理由を理解することができます。

浮かび上がるパターンを見る

ウェブルートのプラットフォームでは、大量の情報を整理し、精査し、すべての雑音の中から信号を見つけます。それにより最も危険で検知することが難しいゼロデイ脅威の予測を可能にします。パターンを示すには少量過ぎる狭小なデータセットに依存した他の脅威インテリジェンスサービスと違い、ウェブルートはより広くさまざまな種類のデータソースを利用し、正確で一貫性があり、信頼できる脅威検知を行います。

機械学習は正しく実行できれば、未来の結果を予想できることが証明されています。BrightCloudの場合、機械学習とコンテキスト分析を行うことによりアクションに転化できる脅威インテリジェンスを実行し、未知のオブジェクトの動作を予想し、未特定の脅威を事前に見つけることができます。BrightCloudは、それまでの履歴と既知の悪意のあるオブジェクトとの関連性からインターネットオブジェクトを評価し、スコア付けを行い、オブジェクトが将来攻撃を行うかどうかの可能性を表示します。市場において長い歴史を持つため、ウェブルートはより強力な対応モデルと長い年月の中で変化するオブジェクトをトラックする能力を身に着けました。またウェブルートは、セキュリティを専門にしたデータサイエンティストと脅威研究者の献身的なチームを配置し、チームの何年にもわたる経験を利用し予想能力の継続的な強化に努めています。

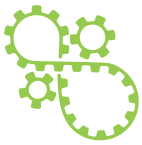
自動的に行動する

ウェブルートの高度なコンテキスト分析が作成した予想レピュテーションスコアは、顧客が決定し、自動的にアクションを取れるようにします。ウェブルートはグローバルなカバレッジと相互連結したインフラを持つため、ひとつのマシンに脅威が見られた場合、すべてのシステムが5分以内に保護されます。この機能は、1日経たない速さのスパンでフィッシングサイトが行ったり来たりしているこの世界ではとても重要です。

レピュテーションスコアへの信頼

ウェブルートの誤検知率は非常に低いため、そのこともまた、10年以上に渡る信頼性の高いトラックレコードの積み重ねと共に、予想に対する信頼性を高めています。これによりウェブルートは過去を振り返り、IPが有害なものから無害なものに変わり、また有害なものに戻る経過を正確に再現することを可能にしています。事実、Webroot BrightCloud脅威インテリジェンスサービスを信頼できるアドバイザーとしての立場に持ち上げたのは、このレピューテーションスコアです。顧客はこのレピュテーションスコアと実行中の脅威ステータスを元に、自信を持って行動することができるのです。

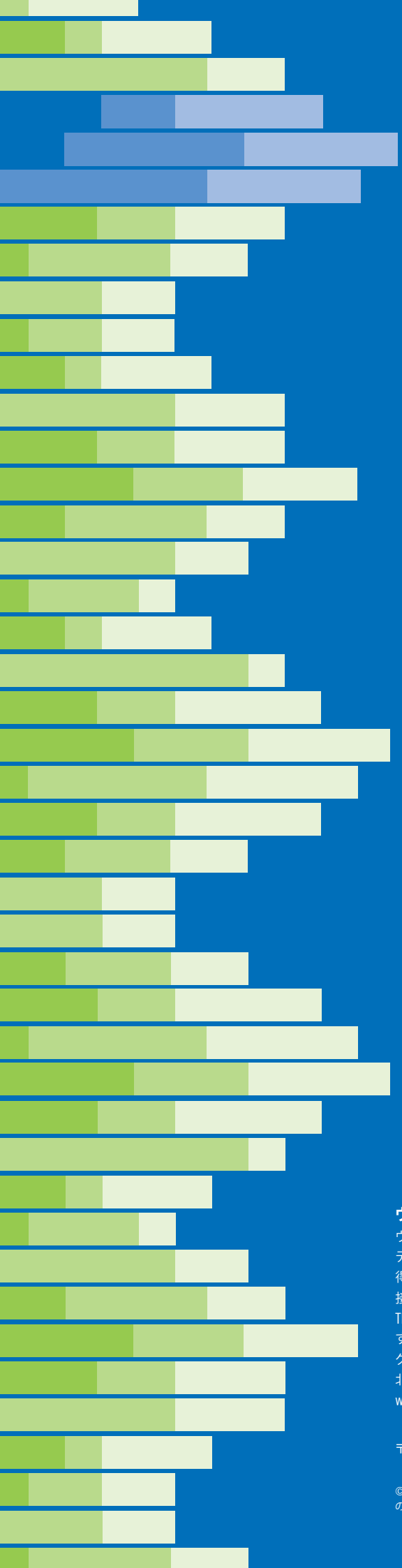
ウェブルートはまた、予測結果の信頼性を最大限に高めるため、完全な透明性を提供しています。BrightCloudコンテキスト脅威インサイトが決定の理由を明確に表します。脅威インサイトが「BrightCloudはなぜ特定のIP、URL、ファイル、モバイルアプリを悪意あるものとして判断したのか、どのくらいの期間、脅威であったのか、どのような種類の悪意のあるアクティビティが関与しているのか」といった質問への答えを提供します。これにより脅威に対するインサイト提供サービスを可能にし、BrightCloudがその決定において使用した可能な因子を明白にします。信頼性を植え付けるだけではなく、セキュリティオペレーションチームが脅威の重大性を理解し、事件対応やそれに続く調査を優先させることの助けになるのです。



まとめ

サイバーセキュリティにおいてひとつだけ不変なものは、変化です。犯罪者はより賢く、より洗練されてきており、犯罪者を事前に食い止めるには、私たちがより賢く動く必要があります。何が起こりうるか、そしてその最大の影響がいつになるのかを正確に予測する能力は、頑強なセキュリティを確実に実行するためのもっとも優れた賢い方法です。脅威インテリジェンス単独では、これら全てのタスクを実行することはできません。プラットフォームへの厳しい要件、インテリジェンスへの幅広いソース、機械学習、コンテキスト分析を実行できた場合に限り、未来に続く窓を開くことが実現します。

ウェブルートは操作可能な脅威インテリジェントの信頼できるプロバイダーであり、ネットワークと情報セキュリティのトッププロバイダーにサービスを提供しています。過去10年間、ウェブルートは自己学習プラットフォームの継続的な改善、これまで以上に幅広いインテリジェントソース一式、そしてより大きな視点で見るためのコンテキスト分析に努力を続けてきました。BrightCloudはこれらの努力の結果であり、攻撃の一歩先を行き、実効性が高くタイムリーかつ予測可能な脅威インテリジェンスを届けるためのスピード、規模、範囲、信頼性を提供します。



ウェブルートについて

ウェブルートは、世界中の企業や個人を保護するためのネットワークおよびエンドポイントのセキュリティと脅威インテリジェンスサービスを提供しています。ウェブルートの高度なアプローチでは、何百万台もの実際のデバイスから得られるクラウドベースの総合的な脅威インテリジェンスを活用して、脅威をリアルタイムで阻止し、ネットワークに接続された世界のセキュリティを確保します。定評あるSecureAnywhere®エンドポイントソリューション、BrightCloud® Threat Intelligence Services、およびFlowScape®ネットワーク動作分析は、企業、ホーム ユーザー、モノのインターネットのすべてにおいて、数百万台ものデバイスを保護しています。Cisco、F5ネットワークス、Citrix、Aruba、パロアルトネットワークス、A10ネットワークスなどの市場をリードする企業が信頼を寄せるウェブルートは、コロラド州に本社を置き、北米、欧州、アジアでグローバルに事業を展開しています。Smarter Cybersecurity™ ソリューションの詳細については、www.webroot.com/jp/ja/ にアクセスしてください。

〒 107-0062 東京都港区南青山 3-13-18 313 南青山 8F　電話: 03-4588-6500　webroot.com