Barracuda

Barracuda ATP (Advanced Threat Protection)

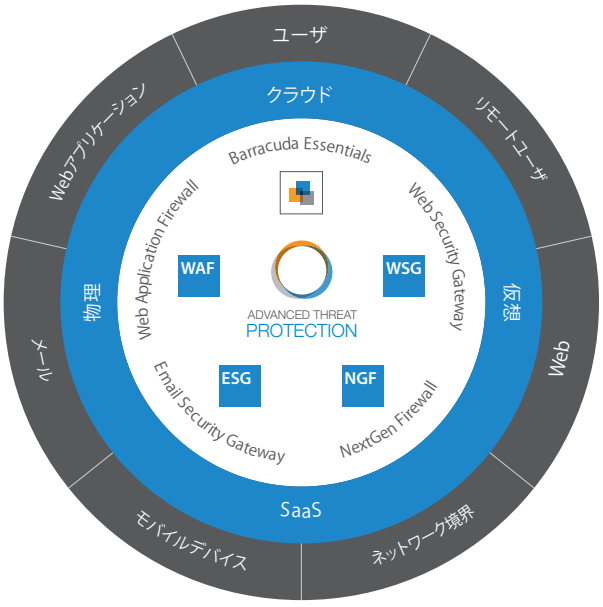
ホワイトペーパー

最新の脅威に効果的な階層型の保護対策

最新のサイバー脅威は多様な性質を持っているため、従来のシグネチャベースの対策では太刀打ちできません。一方、サンドボックスをはじめとする多層防御はコスト高であり、パフォーマンス低下の原因にもなります。ランサムウェアや標的型攻撃のようなサイバー攻撃に確実かつ包括的に対抗するには、精度と速度をバランスよく備えた高度な脅威検知機能を階層的に実装するアプローチが必要です。また、さまざまな脅威ベクタや複数の導入環境（物理／仮想インフラ、SaaSサービス、パブリッククラウドプラットフォームなど）を標的にした攻撃すべてに対抗できるアーキテクチャも不可欠です。

最も一般的な6つのインターネット脅威ベクタ

Barracuda Advanced Threat Protection（BATP）とは、ランサムウェア、マルウェア、高度なサイバー攻撃を複数の階層で防御するクラウドベースのサービスです。シグネチャ分析、静的解析、挙動解析から包括的なサンドボックスまで、複数の階層を備えることによって多様な攻撃を高精度で検知します。BATPをバラクーダネットワークスのセキュリティソリューションと統合することで、Web、ユーザ、ネットワーク、メール、アプリケーションなど、幅広い導入環境の脅威ベクタを保護することが可能になります。また、世界中のさまざまなソースから脅威データを収集する脅威インテリジェンスネットワークに自動接続し、あらゆる脅威ベクタをリアルタイムに保護します。



Barracuda Advanced Threat Protection (BATP)

従来の検知機能を迂回する高度な脅威

最新の攻撃は、急速に増大し、巧妙化しています。ランサムウェアのように、従来の検知機能をすり抜け、標的型のゼロアワー攻撃を使って感染を広げる新型マルウェアが登場しています。

業界アナリストによると、2023年までに、1四半期に200ものランサムウェアが登場すると予測されています。[1] ランサムウェアは攻撃者にとって大きなビジネスチャンスであり、しかも収益は増加し続けています。実際2017年には、ランサムウェアだけで10億ドルを超える被害額が発生しています。このような新型攻撃に対抗できる最善の方法を探しだそうと、さまざまな取り組みが進行しています。

複数の脅威ベクタを攻撃するランサムウェア

新型のマルウェアがこれまでの脅威と異なるのは、複数の脅威ベクタを標的にすることで、攻撃の効果を高め、効率化する点です。現時点では感染方法にメールが使用されることが多く、特にフィッシングやスピアフィッシング攻撃ではメールが多用されます。実際、IDCが見積もったところ、「ランサムウェアの感染方法の90%以上を悪意のあるメール添付が占めています。[2]

また、ソーシャルエンジニアリング、スプーフィング、Webサイトのハッキング、URLの改ざんといった方法で、悪意のあるペイロードのダウンロードを誘導する方法もあります。さらに、モバイルユーザが多い環境や分散ネットワーク環境では、ゲートウェイファイアウォールだけでは十分な効果を発揮できないケースもあります。

ここで重要なのは、「あらゆる脅威ベクタで発生する脅威すべてに包括的に対抗できるセキュリティ戦略が必要だ」という点です。また、効果的な脅威保護フレームワークを採用し、すべての脅威ベクタから収集された脅威インテリジェンスを共有する必要があります。

サンドボックスだけでは不十分

サンドボックスは、ゼロアワー攻撃を検知する有効な方法です。攻撃を受けやすいエンドポイント環境をエミュレートした仮想的な「サンドボックス」環境を構築し、そこで添付ファイルを「爆発（デトネーション）」させるのが一般的です。

サンドボックスは有効な方法であるものの（高い処理能力が必要）、添付ファイルを1つずつ処理していたら、非常に時間がかかってしまいます。コンテンツデリバリの遅延を回避するには、非常に大規模なサンドボックスアプライアンスが必要ですが、それにはコストがかかります。ところが、このようなアプライアンスがなければ、一部の添付ファイルのスキャンが完了しない状態で配信するリスクが発生してしまいます。高度な脅威の中には、仮想マシンのみをベースにしたサンドボックス環境を回避できるものがあります。悪意のある操作をマスクしてサンドボックスをすり抜けるので、サンドボックスは効果を発揮できません。

また、一般的に、オンプレミスベースのサンドボックスソリューションは企業の本社に導入されるので、サンドボックスに添付ファイルをバックホールするリモートやサテライトサイトが必要になります。ところが、オンプレミスのサンドボックスソリューションは、トラフィック、サイト数、ユーザ数の増加に合わせて拡張することはできません。また、インフラをクラウドに移行する企業の増加も、環境が複雑になる要因の1つになっています。セキュリティ機能もクラウドに移行されるため、オンプレミスのサンドボックスの負荷が増大します。

[1] *アナリストであるMichael Osterman氏、2016年*

[2] *IDC Analyst Connection：Why SaaS-Based Productivity Tools Require Additional Threat Protection – 2017*

BATP (Barracuda Advanced Threat Protection) による階層型防御

バラクーダネットワークスは、数十年にわたって培ってきたマルウェア対策の経験を活かして、パフォーマンス、カバレッジ、精度、セキュリティ強度を妥協することなく、あらゆるタイプのマルウェアに包括的に対抗できるクラウドベースのプラットフォームを構築しました。

階層型防御

Barracuda Advanced Threat Protection (BATP) は、脅威検知を行う複数の階層と機械学習技術を組み合わせたクラウドベースのサービスです。BATPでは、重大度／複雑さが異なる脅威を、各レイヤが段階的に排除していきます。脅威は、レイヤで事前にフィルタ処理され、次のレイヤへと進みます。この方法では、あらゆるタイプの攻撃に瞬時に対応し、データパスの遅延を最小限に抑えることができ、セキュリティポリシーの強度が損なわれることもありません。また、検知レイヤの解析結果は他のレイヤでも相互に共有されるので、サービス全体の品質が高まり、新しい脅威が出現しても迅速な対処が可能になります。その結果、出現頻度の高い脅威ほど低いレイヤで簡単に捕捉できるようになります。一方、サンドボックスのようなリソースを大量に消費する上位レイヤは、新種の脅威の検知に使用されます。

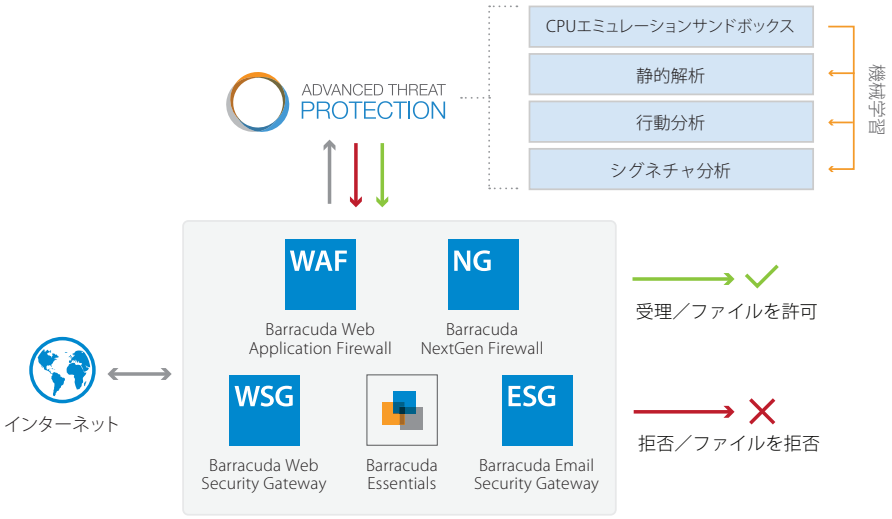
BATPは次のレイヤで構成されます：

1. **高度な脅威シグネチャ：** バラクーダネットワークスは、25万を超えるエンドポイント (Web上のアプライアンスとサービス) の脅威シグネチャに加えて、ハニーポット、クローラー、ダウンロード、ウイルス、マルウェア、スパイウェア、メール添付、ネットワーク、アプリケーションデータなどの情報を収集しています。収集したデータは、脅威インテリジェンスシグネチャデータベースに統合されます。バラクーダネットワークスが監視している領域で新たな脅威が登場すると、このデータベースをもとに、バラクーダネットワークスのセキュリティ製品とサブスクライバに対して脅威情報がリアルタイムで配信されます。

2. **挙動解析とヒューリスティック分析：** 挙動解析とヒューリスティック分析とは、不審なコードやスクリプトを含むプログラミングコマンドを管理された環境内で実行するプロセスを指します。このプロセスでは、レプリケーション、ファイルの上書き、不審ファイルの難読化といった挙動を解析します。他にも、過剰に長いタイマー、数日間実行を続けるプログラミングループ、レジストリやメモリにアクセスしようとするコードなどの検出も行います。

3. **静的コード解析：** 静的コード解析とは、実行可能ファイルを実際には実行せずに検証するプロセスです。悪意のあるコードは、難読化によってウイルス対策ソフトウェアなどの検知機能をすり抜けようとします。静的コード解析レイヤでは、不審なコードを検出すると、難読化を解除します。このレイヤは、非常に効果的なマルウェア高速プレフィルタとして機能します。フィルタ処理の後、不審だと判定されたファイルはサンドボックス階層に送信されます。

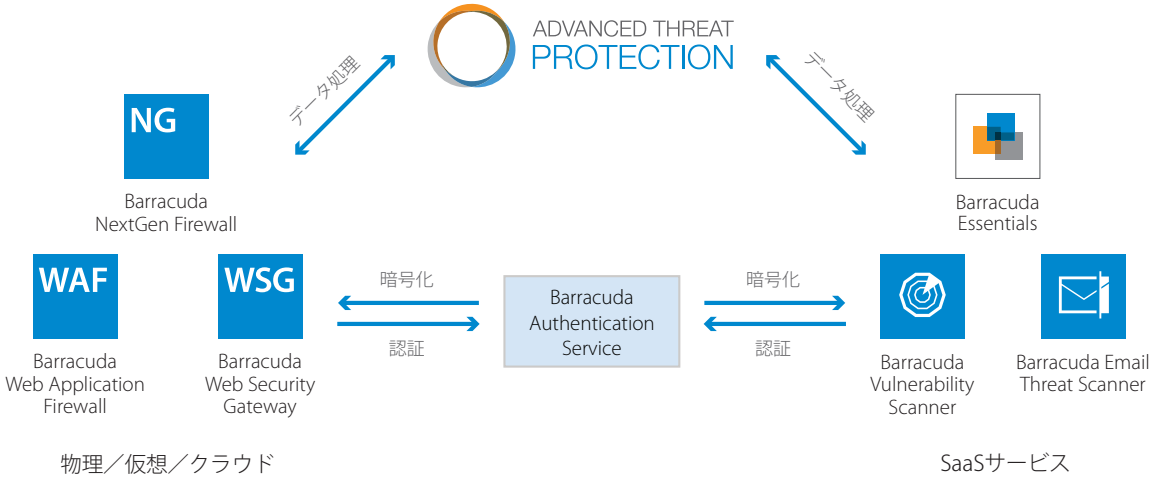
4. **CPUエミュレーションを使ったサンドボックス：** 脅威検知の最後のレイヤは、CPUエミュレーションを使った包括的なサンドボックスです。このレイヤでは、前のレイヤで解析できなかった添付ファイルを「爆発 (デトネーション)」します。CPUエミュレーションを採用することで、従来の仮想化をベースにしたサンドボックスをすり抜けていた脅威の検出が可能になっています。また、他のレイヤのプレフィルタを経たファイルが転送されてくるので、非常に複雑な脅威であっても非常に短時間で処理できます。



階層型脅威保護

スケーラブルな分散型クラウドサービス

BATPは、グローバル規模での分散と高度なスケーラビリティを特徴とするクラウドマイクロサービスアーキテクチャのメリットを最大限に活かすことできます。BATPは、ネットワーク、Webアプリケーション、メール、Webセキュリティなど、バラクーダネットワークスのセキュリティ製品ポートフォリオ全体で使用されています。ユーザが処理するトラフィックの増加に合わせてサービスは自動的に拡張されるので、必要なパフォーマンスを発揮できます。また、通信チャネルに強力なセキュリティを実装することで、プライバシー保護と安全なデータ転送を実現します。



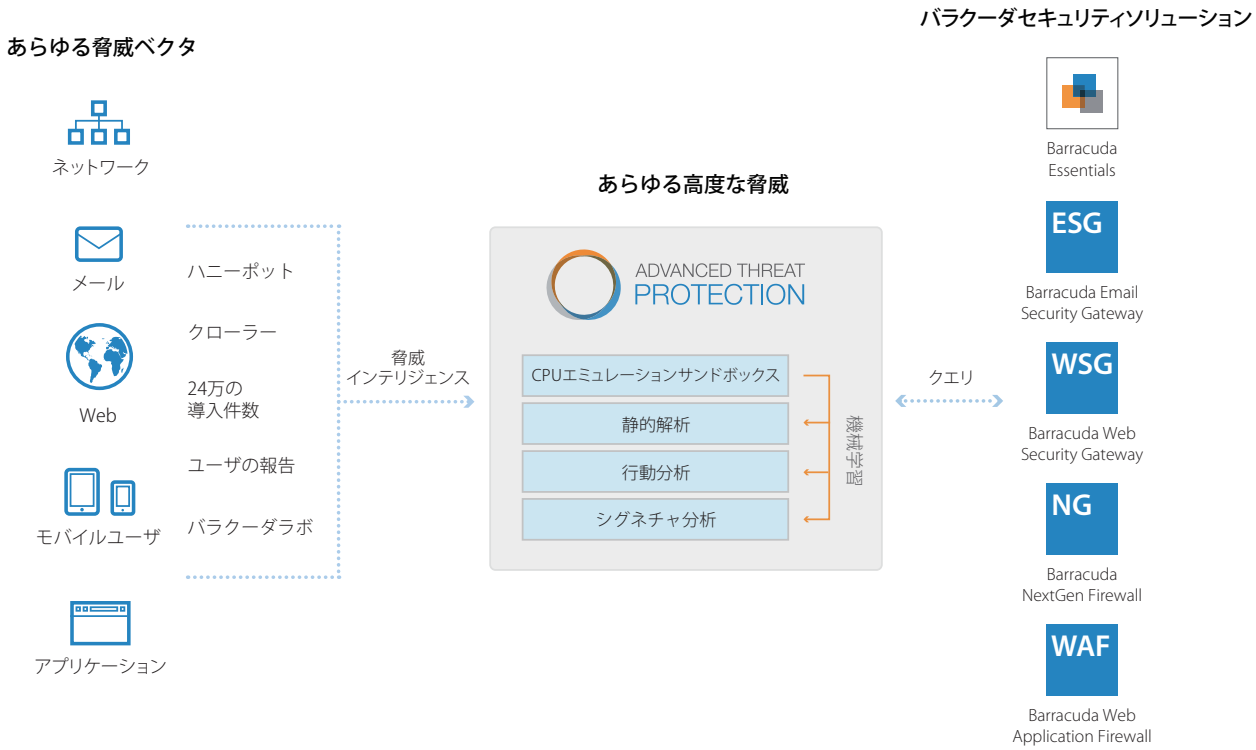
Barracuda BATPアーキテクチャ

グローバル脅威インテリジェンスネットワーク

BATPには、複数の脅威ベクタを保護する目的で、グローバル脅威インテリジェンスが実装されています。このデータベースには、世界中に配置された5,000万を超える収集ポイントから送信される大量の脅威情報が蓄積されています。バラクーダネットワークスのATPインフラにはハードウェアアクセラレーションを採用した機械学習ファームが搭載され、900を超えるアーチファクト属性をもとにデータ分析を行います。

BATPを使用するバラクーダネットワークス製品はすべて、この脅威インテリジェンスネットワークの一部として機能し、脅威ベクタのインテリジェンスを共有することでサブスクライバをリアルタイムで保護します。たとえば、BATPがメールを介して感染する脅威を検知すると、対策が他の脅威ベクタにも瞬時に適用され、セキュリティが確保されます。さらに、新たな脅威が特定されると、

シグネチャが生成され、その情報はレイヤ2にプッシュされます。これにより、ネットワークに同じ脅威が侵入してきた場合、瞬時にブロックできるので、サンドボックスに送信する必要はなくなります。2016年に第三者組織がATPテクノロジに関して行ったテストの結果、誤検出と検出漏れがいずれもゼロという100%の効果を達成できたのは、バラクーダネットワークスのみでした。



バラクーダ脅威インテリジェンスインフラ

結論

今日の高度な脅威に対して包括的なセキュリティ対策を講じるには、多元的なアプローチが必要です。BATP（Barracuda Advanced Threat Protection）とセキュリティ保護に特化したバラクーダネットワークスの製品ポートフォリオの統合は、優れたスケーラビリティと機能を備えたソリューションであり、高度な脅威にも簡単かつ経済的に対処できる防御策となります。

バラクーダネットワークスジャパン株式会社
〒141-0031 東京都品川区西五反田8-3-16
西五反田8丁目ビル 5階
Tel 03-5436-6235 • Fax 03-5436-5128
www.barracuda.co.jp • jpinfo@barracuda.com

販売代理店：