Arbor Cloud DDoS攻撃防御ソリューション

あらゆるDDoS攻撃に対するインテリジェントな自動防御を包括的に提供

主な機能と特長

グローバルなDDoS攻撃対策

ワールドクラスのセキュリティインテリジェンス、そして業界をリードするDDoS攻撃防御製品を組み合わせることにより、通信事業者に依存しないグローバルなDDoS攻撃対策が1つのソリューションで実現します。

Tbpsクラスのクラウド上の防御能力をグローバルに提供

複数のグローバルなスクラビングセンター間に攻撃のミティゲーション基盤を分散することで、攻撃の発生源に近い場所で迅速なミティゲーションが可能となります。データのプライバシーを考慮して、データの保管地域におけるミティゲーションもサポートします。

インテリジェントな多層型防御

Arbor独自のCloud Signaling™技術により、オンプレミスのArbor APS、またはArbor SP/TMSを、クラウド上の防御機能と統合します。

グローバル脅威インテリジェンスの活用

オンプレミスの防御対策と組み合わせたArbor Cloud DDoS攻撃防御ソリューションは、Arbor Security Engineering & Response Team(ASERT)が提供するリアルタイムのグローバル脅威インテリジェンスを自動的に取得し、最新の防御機能を提供します。

マネージドAPS(mAPS)サービス

Arborの業界をリードする専門技術を駆使して、APSによるオンプレミスのDDoS防御の管理と最適化を行います。

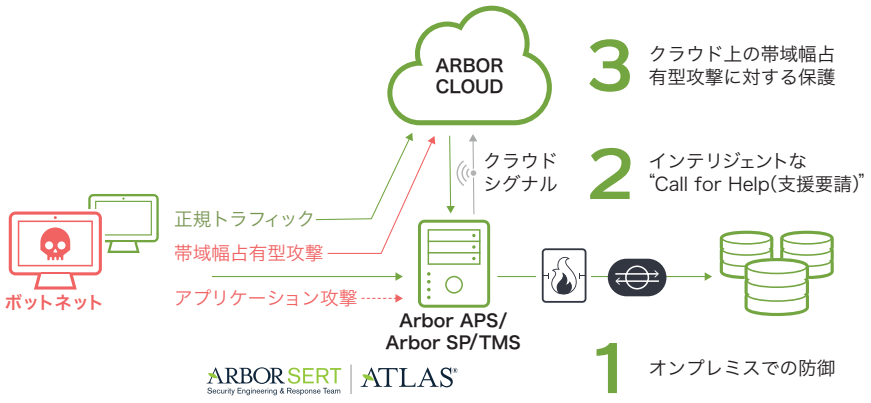
深刻度が高まるDDoS攻撃の脅威は、企業にとって頭の痛い問題です。帯域幅占有型攻撃が増加傾向にあり、増幅/反射攻撃の普及も加わって、問題はますます複雑化しています。最近のDDoS攻撃は、帯域幅占有型、TCP状態枯渇型、アプリケーションレイヤー攻撃型など、複数の攻撃ベクトルを組み合わせたものに進化しています。エンタープライズ向けのArbor Cloud™ DDoS攻撃防御ソリューション(Arbor Cloud)は、オンプレミスのDDoSミティゲーションと密接に統合されたクラウドベースのトラフィックスクラビングサービスを提供します。DDoS攻撃対策におけるこの多層型アプローチは、最新の動的なDDoS攻撃の脅威をミティゲーションする企業にとってベストプラクティスとなります。

最新のDDoS攻撃に対する多層型防御

Arbor Cloudは、DDoS攻撃対策における多層型アプローチの一角を占めており、アプリケーションやサービスへのアクセスを妨げることなく、高度で大規模なDDoS攻撃に対してクラウド内で防御機能を提供します。DDoSセキュリティに関するArborのエキスパートが提供するArbor Cloudのオンデマンドトラフィックスクラビングサービスによって、オンプレミスでのミティゲーションでは対応不可能な規模の帯域幅占有型攻撃に対する防御が実現します。

Arbor Cloudのオンプレミスコンポーネントであるarbor APSは、DDoS攻撃に対して常時稼働のインライン型パケットベースの検知とミティゲーションを実現します。Arbor APSは、あらゆる種類のDDoS攻撃を検知し、阻止します。しかしながら、インターネットへの接続経路やローカルでの防御を圧倒する大規模な帯域幅占有型DDoS攻撃が発生した場合、Arbor APSは「Cloud Signaling™」という強力な機能を活用してArbor Cloud のスクラビング実行場所に自動通知するとともに、攻撃トラフィックを再ルーティングし、攻撃をミティゲーションします。オンプレミスのArbor APS、Cloud Signaling、Arbor Cloudを組み合わせることで、今日のあらゆるDDoS攻撃に対する極めて包括的な防御対策を実現します。

またCloud Signalingは、通常サービスプロバイダーや大規模なエンタープライズネットワーク環境に配備されているArbor SP/TMSと連携し、機能します。オンプレミスの自動DDoS攻撃防御ソリューションであるArbor APSおよびArbor SP/TMSの両方を組み合わせて配備することも可能です。



以下の機能を完全統合し、ATLAS/ASERTのグローバル脅威インテリジェンスによって、すべてのコンポーネントが常に最新の防御機能を装備することで、DDoS攻撃に対する業界トップクラスの包括的な保護を実現します。

1) オンプレミスのArbor APSまたはSP/TMS
2) インテリジェントなCloud SignalingをArbor Cloudへ送信
3) Arbor Cloudが大規模攻撃を阻止

Arbor Cloudの技術仕様

Arbor Cloudセキュリティオペレーション＆スクラビングセンター

- オペレーションセンター：北米（バージニア州スターリング）
- スクラビングセンター：米国、ヨーロッパ、アジアに9ヶ所、7.6 Tbpsのネットワークスクラビング能力

パッケージオプション

- クリーンなトラフィックベースの価格設定
- ミティゲーション：72時間の利用枠
- 標準的なプロビジョニングの設定は無料
- 別途指定がない限りすべての価格は月額制

サービス提供オプション

- Arbor Cloud Connect：攻撃発生時に予備のクラウドミティゲーションサポートを提供
- Arbor Cloud Essentials：リアルタイムのミティゲーションサポートを年間12回まで提供
- Arbor Cloud Essentials+：クラウド上でのリアルタイムのミティゲーションサポートを無制限に提供

柔軟なサービスパッケージ

クリーンなトラフィックベースのオプション

- 100Mbps
- 500Mbps
- 1Gbps
- 2Gbps
- 4Gbps
- 8Gbps
- 10Gbps

パッケージ内容

- 年間12回のミティゲーションサポート
- BGP：1ヶ所のリターン先ロケーション（GRE）で1日に1時間の保護
- DNS：5件までのホスト名を保護
- Cloud Signalingによるアラートと監視
- ASERTの脅威レポート、攻撃分析、アラート
- レベル1、2、3のサポートサービス（24時間365日対応）
- 「攻撃のミティゲーションに要する時間」に関するArborのSLA

リテナー形式のサービスパッケージ

クリーンなトラフィックベースのオプション

- 100Mbps
- 500Mbps
- 1Gbps

パッケージ内容

- 低価格の月額制サブスクリプション
- 年間1回のミティゲーションサポート（2回目以降は別途料金が発生します）
- BGP：1ヶ所のリターン先ロケーション（GRE）で1日に1時間の保護
- DNS：5件までのホスト名を保護
- Cloud Signalingによるアラートと監視
- ASERTの脅威レポート、攻撃分析、アラート
- レベル1、2、3のサポートサービス（24時間365日対応）
- 「攻撃のミティゲーションに要する時間」に関するArborのSLA

追加オプション

DNSオプション

- 保護するホストの追加
- SSL証明書（証明書1件毎）
- 緊急の設定/変更（1回毎）

BGPオプション

- 追加のGREトンネルエンドポイント
- 1日の保護時間の追加
- 1ヶ所またはそれ以上のArbor Cloudスクラビングセンターとの直接接続

オンプレミス向けオプション

Arbor APS

- 常時稼働のインライン型パケットベースの検知とミティゲーション
- 最大40Gbpsの攻撃ミティゲーション能力を備える2Uサイズのアプライアンス
- 1G未満の攻撃を阻止可能な仮想アプライアンス
- サポートするハイパーバイザー：VMware、KVM
- オーケストレーションをサポートするVNF：Cloud-Init、Openstack

Arbor SP

- Arbor SPによるフローベースの検知機能を利用する場合、Arbor SP 8.2およびSP Cloud Signaling実装のSKUが必要

クラウドベースの強力なトラフィックのオンデマンドスクラビング

攻撃が発生した場合、ビジネスの継続性を確保するためにはスピードと俊敏性が極めて重要になります。帯域幅占有型攻撃を受けた際には、まずオンプレミスのArbor APSあるいはArbor SP/TMSが防御の最前線で攻撃を検知します。攻撃の強度が、インターネットの帯域幅やローカルのミティゲーション能力に関して事前設定されたしきい値に近づくと、Arbor APSまたはArbor SP/TMSはArbor Cloudにシグナルを送信して支援を要請します。Arbor Cloudは、グローバルスクラビングセンターの1つでクラウドベースのミティゲーションを実行するために、インバウンドのトラフィックを再ルーティングします。複数のグローバルなスクラビングセンター間にTbpsクラスのミティゲーション能力を分散することで、攻撃の発生源に近い場所で迅速なミティゲーションが可能となります。厳格化の進むデータのプライバシーを考慮して、データの保管地域におけるミティゲーションもサポートします。24時間365日対応のArbor Cloudセキュリティオペレーションセンター(SOC)は、お客様のセキュリティ/IT部門と緊密に連携し、悪意のあるDDoSトラフィックを迅速にブロックすると同時に、正規トラフィックをすべてお客様のデータセンターに戻します。

Arbor Cloudは、IPv4およびIPv6のグローバルなスクラビング能力を備えており、クリティカルなリソースや資産の可用性を脅かす、大規模で多様化した今日の攻撃にも対処できます。

ASERT:Arbor Security Engineering & Response Team(Arborのセキュリティ、エンジニアリング&レスポンスチーム)

世界水準のセキュリティ研究者チームであるASERTは、140Tbpsを超えるグローバルなリアルタイムのインターネットトラフィックにアクセスし、分析を行います。ASERTは、攻撃データの収集、パートナーからの情報、分析ツールの高度な組み合わせを活用します。これにより、インターネット上の新たな脅威を特定して分析し、的を絞った防御対策を講じることで、最先端の巧妙な攻撃からお客様を保護します。

ASERTは、Arbor Cloudポータルで Threat Briefs(脅威概要レポート)を毎週公開し、お客様にグローバルな脅威インテリジェンスを提供しています。

Arbor Cloudポータルでは、下記の情報を参照できます。

- グローバル脅威マップ
- Arbor Cloud Threat Briefs(脅威概要レポート):インシデント発生後、お客様固有の状況に当てはめたインテリジェンスをレポートとして提供
- 脅威発生源の上位リスト
- 脅威指標
- インターネット上の攻撃の上位リスト

NETSCOUT

米国本社
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
TEL:+1 978-614-4000
www.netscout.com

アーバーネットワークス株式会社
101-0063 東京都千代田区神田淡路町2-105
ワテラスアネックス13階
TEL:03-3525-8040
EMAIL:japan@arbor.net
WEB:jp.arbornetworks.com

NETSCOUTは、世界32カ国以上の国々で製品、サポート、サービスを提供しています。各国の事業拠点所在地、電話番号などのお問い合わせ先は、NETSCOUTのWebサイトでご参照ください。
www.netscout.com/company/contact-us

SECPDS_007_JP-1801 10/2018