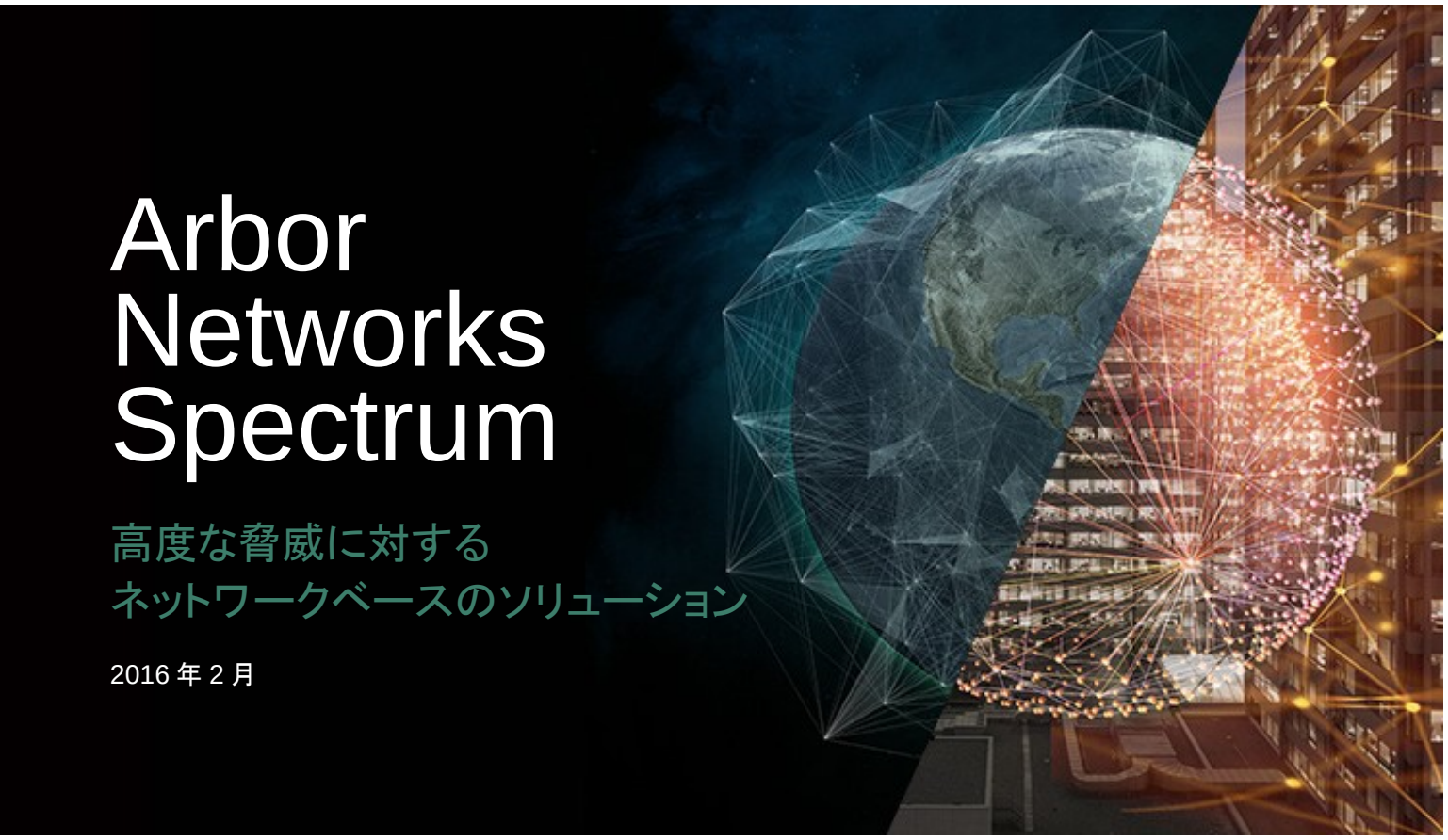
Arbor ホワイトペーパー



Arbor Networks Spectrum

高度な脅威に対するネットワークベースのソリューション

2016 年 2 月

ARBOR NETWORKS

The Security Division of NETSCOUT

Arbor Networks について

Arbor Networks は、NETSCOUT のサーバーセキュリティ部門で、DDoS 攻撃や高度化する脅威から世界の大手企業および大手サービスプロバイダーのネットワークを安全に守ることを支援しています。Arbor は全世界のエンタープライズ、キャリア、モバイルの市場において DDoS 保護ソリューションを提供する世界をリードする主要ソリューション・プロバイダーです（Infonetics Research 社調べ）。Arbor の高度なソリューションは、パケット・キャプチャと NetFlow テクノロジーを組み合わせることにより、完璧なネットワークの視認性を実現し、マルウェアや悪意のあるインサイダーの迅速な検出とミティゲーションを可能にしています。また、Arbor Networks は、動的なインシデント・レスポンス、履歴分析、視認性、およびフォレンジクスに関する市場をリードする分析サービスを提供しています。Arbor は、ネットワークおよびセキュリティチームが専門家になることを支援する「フォース・マルチプライヤ」（戦力倍増チーム）であることを目指しています。Arbor の目標は、ネットワークの現状に関して、セキュリティに重点を置いて豊富な情報を提供することにより、お客様がセキュリティ問題を迅速に解決し、事業リスクを低減できるようにすることです。Arbor Networks の製品およびサービスについて詳しく知りたい方は、Arbor Networks の日本語サイトまた、ATLAS グローバル脅威インテリジェンスのデータに基づく調査、分析および知見については、ATLAS セキュリティポータル（英文）をご覧ください。

概要

巧妙化する今日の連携・混合型攻撃キャンペーンに対抗するために、セキュリティチームはネットワーク全体にわたってリアルタイムに脅威データを監視すると同時に、脅威インジケータとトラフィックデータの両方のアーカイブに瞬時にアクセスすることが求められます。

現在あまりにも頻繁に、インシデント対応ツールが企業のセキュリティチームの役に立っていないという状況が発生しています。インシデント対応のソリューションを実装したにもかかわらず、ネットワーク全体を広範囲にカバーする深度の深い情報を提供しきれていないために、ユーザーは結果を得るまでに数時間待たされています。また、このようなソリューションには、インシデント対応のエキスパートも必要とされています。そして、多くの場合、脅威解析に必要なデータが提供されるものの、その時点では、データはすでに古いものとなっているという問題も発生しています。

Arbor Networks がこの現状から考えていることは、高度な脅威を調査し、対応するセキュリティチームにとって必要なことは、思考するのと同じ速度で、リアルタイムと過去の履歴の両側面から脅威データとトラフィックデータにアクセスすることです。Arbor Networks Spectrum™ は、セキュリティチームが必要とする視認性およびアクセスを提供しています。新たな脅威を検出し、セキュリティチームがいかなる脅威でも検証し、調査することをわずか数分で実現する革新的なワークフローおよび視覚化を可能にしています。もう、数時間待つ必要はありません。

Arbor Networks Spectrum は目的に特化したプラットフォームによってインシデント対応への新たなアプローチを提供:

他のソリューションがデータ・ソースのログまたはイベントに依存しているのに対して、Arbor Spectrum はネットワークを使用しています。ネットワークは現代のビジネスの中核であり、攻撃者たちは、検出／防御ソリューションを回避する手口において、ネットワークへの物理的アクセスなしでこれを達成することはできません。適切な方法で監視すれば、ネットワーク上の境界で発生するあらゆる侵入を可視化することが可能です。

- ネットワークの脅威およびトラフィック・アーカイブの全体に、高速で容易にアクセス。トラフィックおよび脅威インジケータの可視化で、ユーザーがホストの挙動を速やかに捉えることができる。
- 脅威発見からインシデント調査、フォレンジクスまで、セキュリティチームがすべて同一のインターフェイスで容易に実現することを可能するワークフロー。
- 検出のための複数の脅威インテリジェンス・ソース：Arbor ATLAS® インテリジェンス・フィード、Emerging Threats Pro、サードパーティー提供のユーザー指定ポリシー。
- 容易にコスト効率良く全ネットワークをカバーすることを可能にする柔軟な実装オプション。
- ストレージの効果的な利用（過去数ヶ月のレイヤー7 の各種のトラフィックデータを保存）。

Arbor Spectrum の主な特徴:

パケット+ フロー

Arbor Spectrum は、1 つのソリューションにパケットとフローの分析およびアーカイブを組み込んだ革新的なアーキテクチャを使用しています。パケットの分析およびアーカイブがネットワーク上の重要なポイントにおける脅威インテリジェンスを提供すると同時に、NetFlow などのフロー・データによってネットワーク全体を俯瞰するのに必要な広範な視認性を効果的に提供します。Arbor Spectrum では、パケットのみの実装、フローのみの実装、または 2 つを組み合わせた実装が可能です。

パケットおよびフロー・データの両方の分析とアーカイブを組み合わせることで、Arbor Spectrum は、単なるデータだけではない、他に例を見ないインサイト（知見）をセキュリティチームに提供します。これによって、脅威や挙動が企業内ネットワークのどこで発生しても、調査が可能になります。

リアルタイムのトラフィック分析および脅威検知

Arbor Spectrum は、ハイパフォーマンスなパケットおよびフロー分析を提供し、リアルタイムに攻撃キャンペーンの脅威を検知することを可能にします。Arbor Spectrum では、パケットおよびフロー分析の両方に Arbor 自社開発のインテリジェンスおよびユーザー提供のインテリジェンスを適用し、ネットワークにおける脅威の兆候を特定します。ATLAS インテリジェンス・フィードは、ASERT によって強化されています。

ASERT は、世界のインターネット・トラフィック全体の 3 分の 1 以上を活用した Arbor のグローバルな分析、高度なマルウェア調査、ボットネット侵入、ハニーポットの組み合わせにより、グローバルな脅威データの高精度なフィードを生成します。パケット分析では、ATLAS インテリジェンス・フィードは、URL、ドメインおよび IP レピュテーションと組み合わせることで、既知の犯罪者グループや現行の攻撃キャンペーン・インフラの照合をもとに脅威の兆候を特定します。フロー分析では、ATLAS インテリジェンス・フィードは、IP レピュテーションを消費されているフロー・レコードに適用します。

ATLAS インテリジェンス・フィードに加えて、Arbor Spectrum は、Emerging Threats Pro LLC 社が提供する業界最先端の Snort および Suricata のセキュリティ・ポリシーも使用しています。このポリシーは、ディープ・パケット・インスペクションや、マルウェア、脆弱性の悪用およびその他の痕跡を特定するのに適しています。また、ユーザーは、独自にカスタマイズした Snort ポリシーを分析に適用することもできます。Arbor Spectrum は、このようなポリシーを内部の Suricata エンジンに適用します。

さらに、Arbor Spectrum には、組み込みのシステム・ルールも内蔵されています。これによって、ポート・スキャン、ホスト・スキャンおよび長時間のセッションなど、ネットワークベースの脅威インジケータについてフローおよびパケットを分析します。

2016 年に、Arbor は、サードパーティーおよびユーザー定義のセキュリティ・インテリジェンスをさらに追加することで、パケットおよびフロー分析のプラットフォームを引き続き強化していきます。たとえば、ユーザーは Structured Threat Information eXpression（STIX）の基準 [1] に従って、セキュリティ・コンテンツをインポートすることができるようになります。また、各企業に固有のポリシーを定義することもでき、これによって異常または不適切なネットワーク通信が検出可能になります。

独自の可視化およびワークフロー

Arbor Spectrum のユーザーインターフェイスは、インシデント対応プロセスの主要部分をスピードアップするワークフローをセキュリティアナリストやインシデント対応担当者に提供できるよう設計されています。このユーザーインターフェイスを利用することで、脅威の発見、調査および対応に必要な視認性が提供されます。これによって、ユーザーは、脅威インジケータとトラフィックデータの両方を介して、移動、検索およびピボット操作をインタラクティブに行うことができます。ユーザーインターフェイス（リリース 2.0）には、以下の 3 つのモジュールが含まれています。継続的にネットワーク全体で検出された脅威兆候へ視認性を提供する「ハンティング」、ホスト脅威およびトラフィック・アクティビティの全体像を提示する「ホスト・ドシエ」、特定のフィルタと一致するネットワーク通信についての詳細表示を提供する「コネクション」です。

スケーラブルでハイパフォーマンスなトラフィック・アーカイブ

Arbor Spectrum を使用することで、セキュリティチームは、日々発生するパケットおよびフローを蓄積する膨大なトラフィック・アーカイブへ高速でアクセスすることができます。数百テラバイトもの複雑なストレージを実装することは一切必要ありません。Arbor Spectrum のプラットフォーム・アーキテクチャは、膨大なトラフィックデータを長期にわたって保持することができます。

従来のネットワークフォレンジクス製品に比べて、多くの場合、数週間から数カ月長期にデータを保存することが可能になります。Arbor Spectrum の革新的なネットワークフォレンジクス・アプローチは、アーカイブを超高速に検索できるよう設計されています。これによってセキュリティアナリストは、長期間にわたる複雑な調査を数秒で行うことが可能になります。もう、数時間の調査は必要ありません。フローの分析およびアーカイブには、64 TB AT-2300 アプライアンスが、1 秒あたり最大で 100,000 フローを収集すると同時に、6 カ月以上にわたってトラフィック・アーカイブを保持します。

パケット分析およびアーカイブのために、Arbor Spectrum では、AIF、ET Pro またはカスタマイズした Snort ポリシーによって特定された脅威の兆候が示されるすべてのセッションに対して完璧な PCAP（パケット・キャプチャ）を保存します。Arbor Spectrum プラットフォームに保存された PCAP は、Spectrum のユーザーインターフェイスから容易にアクセスすることができます。ユーザーは Wireshark のような外部ツールを使用して、Arbor Spectrum のインターフェイス内部で提供された自動生成のデコードとともに、PCAP の共有および表示を行うことが可能です。

キャプチャされたパケットが脅威兆候を示さない場合、Arbor Spectrum はストレージを効率的に使用して、トラフィックの必須要素をアーカイブします。このアーカイブには、各セッションの最初の 1,000 バイト、主レイヤー3/4 のトラフィックデータとレイヤー7 のメタデータが格納されます。リリース 2.0 では、抽出および格納されるデータは以下となります。

- 接続の開始時刻および期間
- サービス品質の値
- プロトコル
- トラフィック・ストリームのサイズ（パケットおよびバイト単位）（単一方向ごとに）
- 送信元および宛先の、IP アドレス、ポートおよび TCP フラグ
- トラフィックを受信したコレクターの IP アドレス
- 要求された DNS ホスト名
- HTTP URL
- 完全な HTTP ヘッダー
- セッションの最初の 1,000 バイト

[1] サーベンス・オクスリー法の遵守にあたっての免責条項：本ドキュメントに記載されている機能および特長は、利用可能な際にのみ提供され、Arbor Networks の側で確約するものではありません。

Arbor Spectrum：トラフィックの分析およびアーカイブ

Arbor Networks は、Arbor Spectrum プラットフォームを継続的に機能強化し、ユーザーが各セッションの最初の 1,000 バイトへ直接アクセスすることを可能にすると共に、将来、トラフィックの PCAP ダウンロードを可能にするオプションをユーザーへ提供していきます。

Arbor Spectrum プラットフォームの機能拡張により、次の豊富なトラフィックデータのアーカイブが付加されます

- ファイル・ハッシュ
- ストリームのエントロピー
- TLS/SSL サーバー認証
- TLS/SSL 共通名、サブジェクト名、発行者名
- TLS/SSL 証明書のフィンガープリント
- FTP ユーザー名およびパスワード
- FTP データ・チェックサム [2]
- SMTP メタデータ

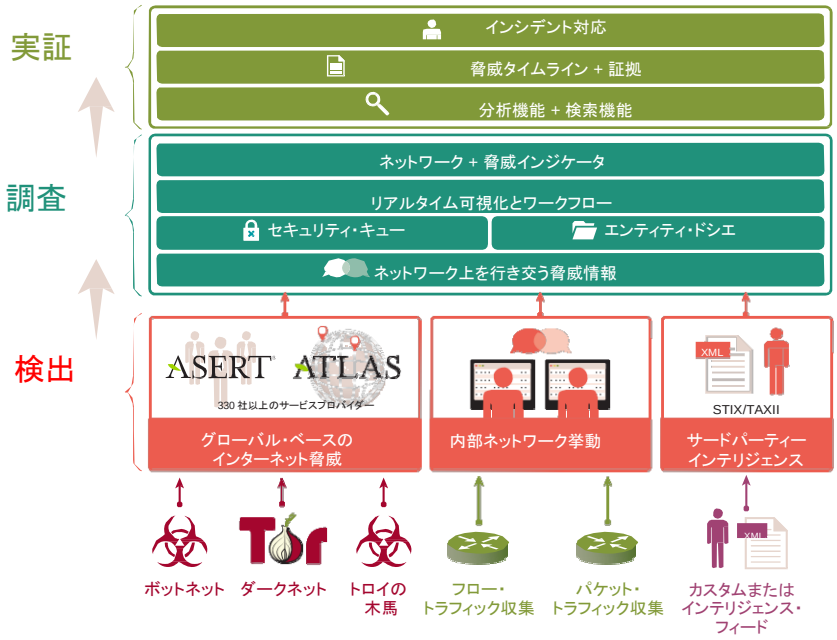
ネットワークフォレンジクスへのこの効果的なアプローチによって、5 Gbps 超えるトラフィックを処理する場合、単一の AT-2300 アプライアンスで 1 カ月以上にわたるアーカイブ情報を保持することが可能になります。また、Arbor のアプローチは、他社のネットワークフォレンジクス製品に比較して、脅威データの検索および結果の取得を最大で 10 倍高速に行うことを可能にします。

新たな脅威（新しいポリシー）に関してアーカイブされたトラフィックを分析する際に、Arbor Spectrum ではすべてのパケットを再現する必要はありません。ポリシーに該当するデータのみに的が絞られます。ペイロードの分析を必要とする多くの Snort および Suricata のシグニチャーの場合、セッションの最初の 1,000 バイト（Arbor Spectrum によって格納済み）が、この遡及分析に必要なトラフィックを提供します。

将来の PCAP オプション

2016 年に、Arbor は Arbor Spectrum プラットフォームを機能強化し、PCAP 全体の分析およびアーカイブを行うための追加のワークフローをサポートしていきます。最初に可能になることは、トラフィックがリアルタイムで収集および分析されるのと同様に、分析およびアーカイブのために、PCAP をパケット・コレクターにアップロードできるようになります。[3]

次に、ネットワーク全体においてリアルタイムでの脅威の追跡を可能にするために、Arbor は、選択したホストまたは接続に対して、既存のパケット・コレクターを介して、完全なパケット・キャプチャを起動するワークフローと機能を提供します。さらに、PCAP の完全なデコードも提供する予定です。また、Wireshark のような外部ツールでの分析のために、PCAP を速やかで容易にダウンロードする手段も提供する予定です。



[1] サーベンス・オクスリー法の遵守にあたっての免責条項：
本ドキュメントに記載されている機能および特長は、利用可能な場合にのみ提供され、Arbor Networks の側で確約するものではありません。

[3] 同上。

スケーラブルな実装アーキテクチャ

Arbor Spectrum は、ネットワーク全体に対して、セキュリティ全体に関する視認性を迅速かつコスト効率良く提供することを実現します。この視認性によって、長期にわたるネットワークトラフィックおよび脅威言インジケータの情報を、思考するのと同じ速度で、アクセスすることが可能になります。ユーザーは脅威を素早く容易に調査することができるため、攻撃キャンペーンのタイムラインの迅速な決定や、ネットワーク内部の脅威に関するラテラルムーブメント（マルウェアの侵入拡大ステップ）の把握が可能になり、攻撃者が目標に達する前に、的確な対応を取ることができます。

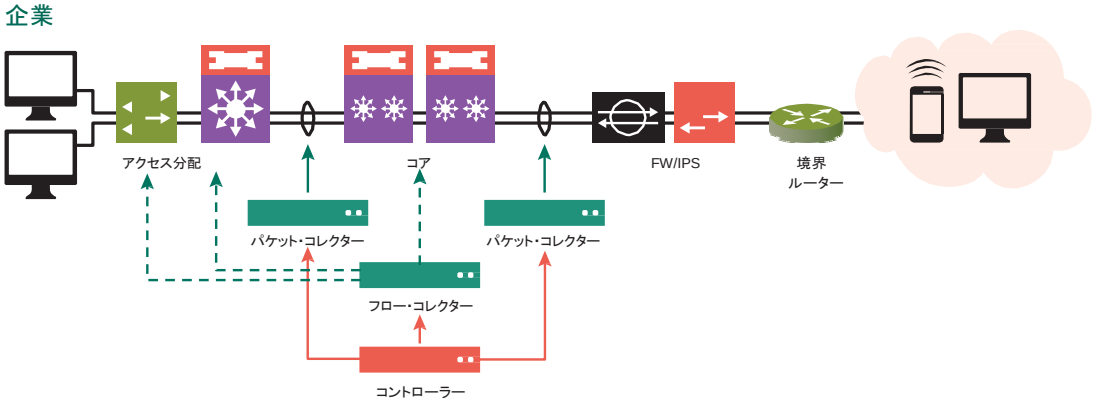
中・大規模企業のために

Arbor は、ネットワーク全体のパケットおよびフローの両方を分析する、広範囲にわたる実装を推奨します。パケット・コレクターは、ネットワーク・コアに加えて、インターネットおよびデータセンターのエッジにも実装する必要があります。フローは、ネットワークに対する広範な視認性を獲得するためのコスト効率良い方法を提供します。フローはインターネットのエッジ・ルーター、コア・ルーターおよび集約エッジ・ルーターで生成され、Spectrum フロー・コレクターにエクスポートされます。次の図は、企業における実装の一例です。

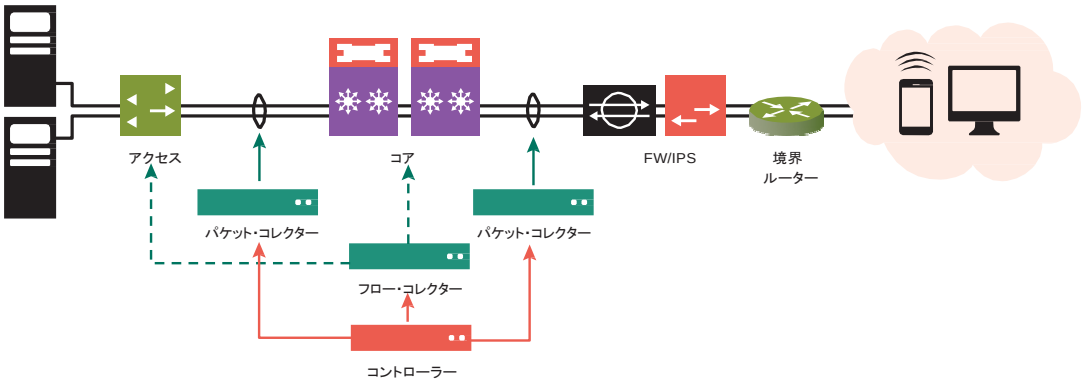
データセンターのために

上記と同じ手法を適用します。パケットは、インターネットのエッジ、コア／集約エッジでキャプチャされます。また、TOR（Top of Rack）または EOR（End of Row）からもディープ・パケット・キャプチャを行うことができます。フローについては、可能な限り幅広い視点を提供するために、この機能をサポートするすべてのルーターおよびスイッチからエクスポートすることができます。次の図は、この一例です。

企業



データセンター



コントローラー・アプライアンスは、Web ベースのグラフィカルインターフェースを提供し、パケット・コレクターおよびフロー・コレクターを管理します。リリース 2.0 では、1 つのコントローラーで、最大 5 つのパケット・コレクターおよび最大 5 つのフロー・コレクターをサポートすることができます。各コレクターは、単一の用途のために存在します（例：パケット・コレクターやフロー・コレクター）。

各コレクターにおける複数のキャプチャ・インターフェイス（1 ギガビット・イーサネット／10 ギガビット・イーサネット）が、 監視対象となるネットワーク内の送信元からのパケット・トラフィックまたはフロー・トラフィックを受信します。パケット・トラフィックの送信元は、ネットワーク・タップまたはミラー・ポートです。フローの送信元のデバイスは、ルーター、スイッチまたはプローブです。

フローはネットワーク全体で広範な視認性を確保するための非常に費用効果の高い手段となりうるため、フローベースの視認性から開始し、ソリューションの拡張にしたがって、より深いパケットの視認性を追加することができます。このアーキテクチャによって、ネットワーク全体における包括的なパケット・キャプチャに対して、最も費用効果の高い実装戦略を実現可能です。パケット・キャプチャは、主なネットワーク・ポイントに、位置を正確に指定して実装されます。

2016 年後期に、Arbor は、Spectrum のコントローラーおよびコレクターの機能に仮想ソフトウェアのライセンスを提供する予定です。これによって、柔軟性が向上し、NFV（Network Function Visualization）環境で Spectrum をさらに容易に使用できるようになります。リリース 2.0 では、Spectrum コントローラーおよびコレクターのライセンスは Arbor アプライアンスでのみ使用可能です。

まとめ

思考するのと同じ速度でのインシデント対応を可能に

Arbor Spectrum は、柔軟な実装オプションを活用し、企業ネットワーク内外にセキュリティに関する広範かつ深度の深い視認性を提供します。このような視認性によって、セキュリティチームは、思考するのと同じ速度で、リアルタイムと履歴の両方の脅威データおよびトラフィックデータにアクセスし、脅威に対する調査および対応を実施することが可能になります。Arbor Spectrum は、ネットワークの「あるがままの」姿を捉えることで、新たな脅威を発見して、革新的なワークフローおよび可視化を実現します。ここに、セキュリティチームが求めるネットワークでの脅威の検証および調査を迅速に実現する現実解があります。

本社
76 Blanchard Road
Burlington, MA 01803 USA
米国内通話料無料：+1 866 212 7267
TEL：+1 781 362 4300

北米販売担当
米国内通話料無料：+1 855 773 9200

欧州
TEL：+44 207 127 8147

アジア・パシフィック
TEL：+65 6299 68096226

日本
〒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
お問い合わせ japan@arbor.net

www.arbornetworks.com

ARBOR NETWORKS
The Security Division of NETSCOUT

©2016 Arbor Networks, Inc. All rights reserved.Arbor Networks、Arbor Networks ロゴ、ArbOS、Cloud Signaling、Arbor Cloud、ATLAS はすべて Arbor Networks, Inc. の商標です。その他の製品名はすべて各々の所有者に帰属する商標です。

WP/PROTECTENT/EN/0915-LETTER