データシート

ARBOR NETWORKS SPECTRUM™

ネットワークの詳細なマイクロビューとインターネット・トラフィックのマクロビューを関連付けることにより、これまでにはない速さで迅速な脅威対応を実現

利点

従来のフォレンジックス・ツールや SIEM に比べて、10 倍の速さで脅威を調査・実証

- スマートなワークフローと検索機能によって、脅威を検証
- ネットワーク内外のあらゆるエンティティに対する完璧な可視化の提供

スケーラブルなリアルタイムのパケット分析・フロー分析で、現在および過去において脅威にさらされているポイントを検知

- かつてないレベルの可視化とパフォーマンスを実現するパケット分析・フロー分析
- インタラクティブなズーム／ピボット・ツール
- アクセス可能なパケット・キャプチャ
- ネットワーク上のすべての情報を検索可能（日単位、週単位、月単位）

インターネットから内部ネットワークまでのネットワーク全体にわたって脅威のやりとりを検知し、関連付け

- ATLAS® インテリジェンス・インディケーター
- 個別のサードパーティ脅威インテリジェンス
- ネットワーク挙動学習とポリシー

容易な設定と運用

- 導入とトレーニングが 1 日で完了

高度な脅威に対する防御ソリューション

セキュリティ脅威の状況は大きく変化しています。企業や組織にとっての最大のリスクは、従来の防御策で見落とされている高度なマルウェアだけではもはやではなく、高度な脅威へと拡大しています。

過去 2 年間で成功した高度な脅威の攻撃の大半は、攻撃可能な重大な脆弱性に仕掛けられたものではありません。その多くは、標的の防御策を擦り抜けるためにマルウェア以外の方法を使用しています。

Arbor Networks は、高度化する脅威に対抗するために、セキュリティ・チームのための新しいプラットフォームを開発しました。このプラットフォームにより、セキュリティ・チームはこれまでは不可能であった広範な脅威の可視化および調査を実現し、ネットワーク内およびネットワーク間にわたって脅威を検知し、実証することができます。

- **グローバルで組織的な攻撃をネットワーク全体にわたってリアルタイムに把握：**
  Arbor Networks のサービスプロバイダー・ネットワークからリアルタイムに収集されたグローバル脅威インテリジェンスを内部トラフィック・パターンと関連付けすることで、損害を与える危険な脅威をいち早く検知することを可能にします。
- **ネットワーク内のすべてを監視し、ネットワーク脅威を視認化：**
  現在および現在のすべてのネットワーク活動に対して、わずかなコストで完璧な視認化を実現します。現行のセキュリティ・フォレンジックス・モデルを刷新するイノベーションをもたらします。
- **ネットワーク上の脅威を迅速に調査し、実証：**
  セキュリティ担当者のために開発されたスマートでリアルタイムのワークフローと分析機能により、セキュリティ・チームは今日市場で提供されている既存のソリューションの 10 倍の速さと効率性で脅威を調査し、検証することができます。

7 つ以上のツールキット
が 2015 年に仕掛けられた高度な攻撃に使用されたが、重大な脆弱性を利用したものは半数に満たない。

40%
ほどしか、2015 年に発生した高度な攻撃のうちで、マルウェアを利用していない。

ARBOR NETWORKS
The Security Division of NETSCOUT

「われわれは、7分以内に、コマンド&コントロールを検知し、すべての攻撃タイムラインと影響を受けたホストを追跡しました。われわれの既存のフォレンジックス・ツールを使用していたら、数日はかかったでしょう。」

セキュリティ・オペレーション責任者
(北米多国籍企業)

Arbor Spectrum 概要

Arbor Spectrum は、リアルタイムのフロー分析とパケット分析に加えて、過去数ヶ月の活動を迅速かつ容易に検索する機能によって、ネットワーク上のあらゆる活動に対して完璧な可視化を実現します。この一線を画す Arbor Spectrum のアプローチは、インターネット上のグローバルな攻撃の視認性を内部ネットワーク上の活動とリアルタイムに関連付けし、ネットワーク全体の状況把握と迅速な調査を可能にします。

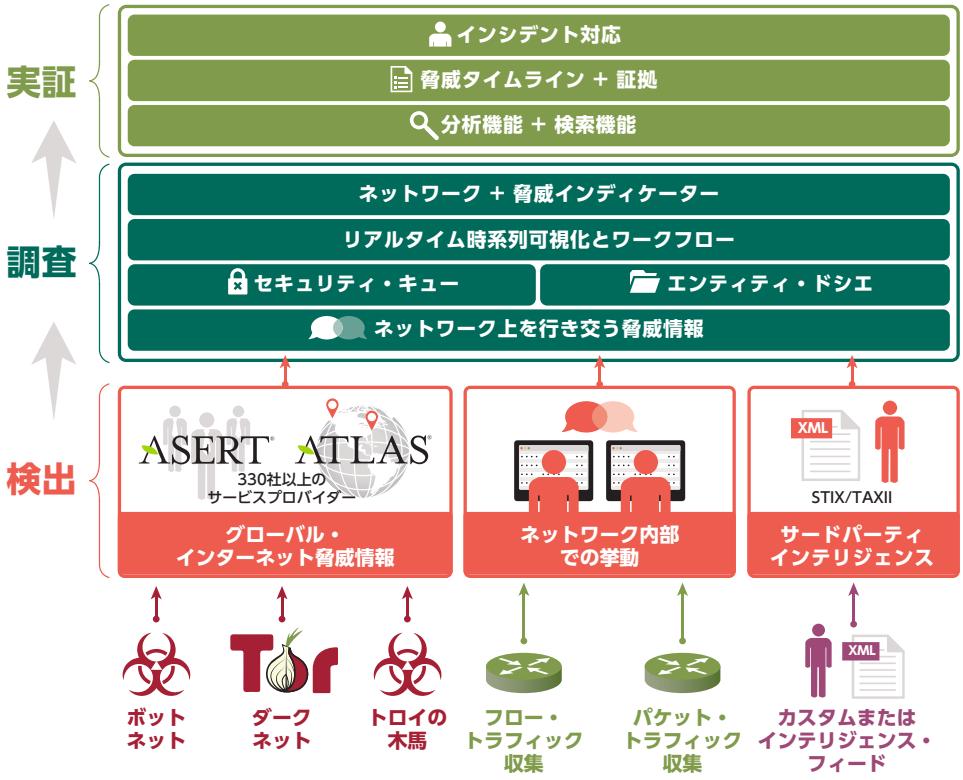

図 1: Arbor Spectrum

主な機能

検出

- **脅威特定ワークフロー**

  攻撃の兆候を示す関連性のあるインディケーターのリアルタイム・ビューを提供します。このリアルタイム・ビューから、インタラクティブなズーム／ピボット・ツール、ライブ・トレンド分析機能を使って、脅威を特定するための調査を開始できます。

- **ATLAS® インテリジェンス・インディケーター**

  Arbor Networks が他のベンダーと異なる点は、世界の大手サービスプロバイダーや企業との連携を通して広範囲にトラフィック・データをリアルタイムに収集して、これをお客様へ提供していることです。Arbor Networks の ATLAS® は、匿名のトラフィック・データを Arbor Networks と共有することに同意していただいた 330 社を超えるお客様との共同プロジェクトであり、全インターネット・トラフィックの約 3 分の 1 に相当するデータを収集しています。この一線を画す独自の情報網から、Arbor Networks はリアルタイムで発生している攻撃に関する攻撃インテリジェンスを提供することを可能にしています。

  ATLAS インテリジェンスは Arbor Spectrum と統合され、高度化するさまざまな攻撃に迅速に対処するためのポリシーと防御対策を提供します。ATLAS インテリジェンスと ASERT（Arbor Security Engineering and Response Team）の組み合わせにより、Arbor Networks が誇る専門的なリサーチ力を活用して、高度化する脅威からネットワークを守ることができます。

調査

- **ホスト・ドシエ**
  エンティティについての関連データを迅速に統合し、業務への影響を回避するために攻撃の発生を特定します。
- **リアルタイム情報検索**
  攻撃活動の検知と調査の迅速に実行することで、攻撃方法、発生場所、内容を数分で確認できます。
- **リアルタイムでの脅威トレンド分析**
  新たな兆候（攻撃標的およびソース）など脅威トレンドをリアルタイムに可視化します。

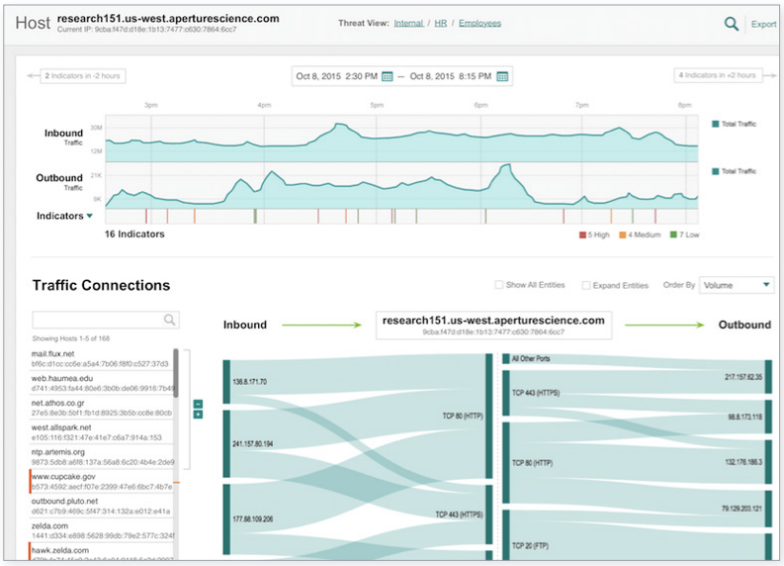

図 2: ホスト・ドシエ・モジュールを使用して、特定のホストに関連するすべての活動を調査

実証

- **アクセス可能なパケット・キャプチャ**
  ネットワーク内で検知された 3 ～ 6 か月にわたる脅威を従来のセキュリティ・フォレンジックス・ツールの数分の 1 のコストで実証します。
- **容易な導入と運用**
  導入とトレーニングが 1 日で完了し、ROI の迅速な達成を可能にします。

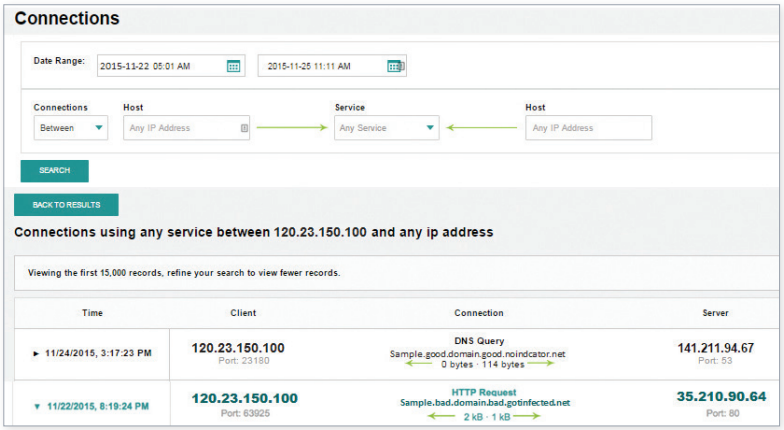

図 3: コネクション・モジュールを使用して、他ホストから、または他ホストへの接続状態またはホスト間の接続状態を表示

「Arbor Spectrum の優れた点の 1 つとして、専門家レベルのネットワーク・フォレンジックス・スキルがなくても容易に使用できることが挙げられます。インターフェイスは単純明快であり、調査に必要な関連情報を容易に抽出できます。」

セキュリティ・アーキテクト
（北米大手小売会社）

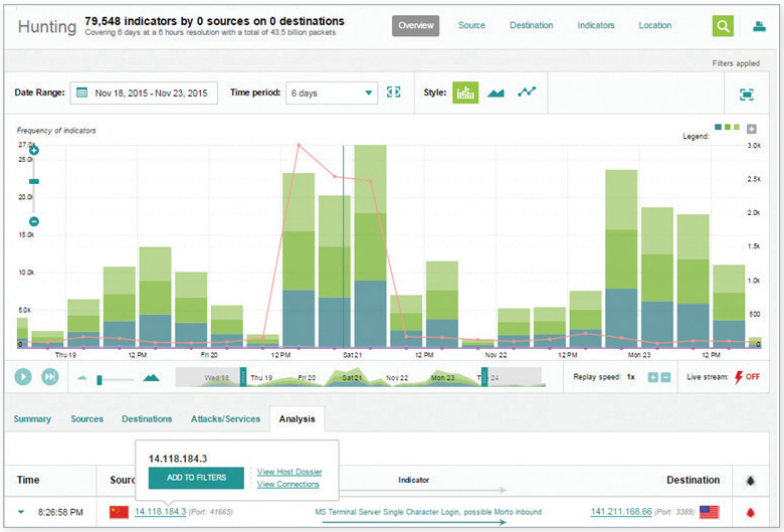

図 4: ハンティング・モジュールを使用して、脅威インディケーターの変化を表示

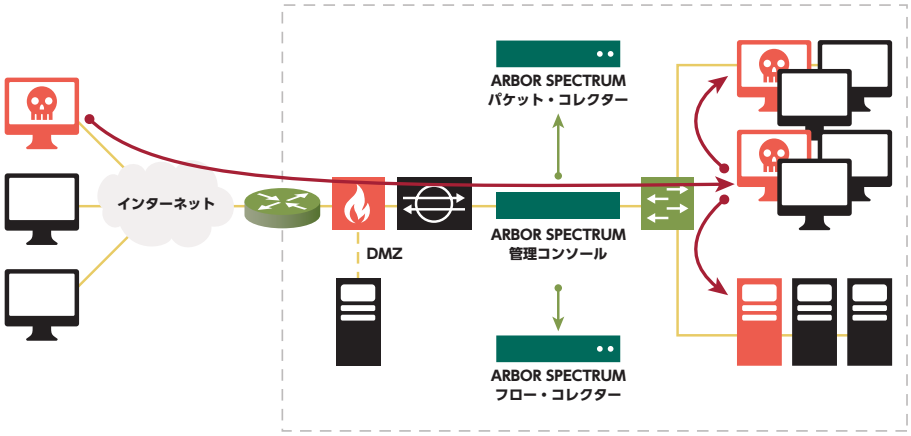

図 5: Arbor Spectrum 導入イメージ

アプライアンス・モデル

	2200	2300
導入	プラットフォーム・コンソール、パケット・コレクターまたはフロー・コレクター	パケット・コンソールまたはフロー・コレクター
メモリー	64 GB	64 GB
ハード・ドライブ	2 TB SATA 7200 RPM x 8	4 TB SATA 7200 RPM x 16
トラフィック・アーカイブ	9.1 TB	44 TB
最大フロー／秒（プロー・コレクターとして）	25,000	100,000
最大パケット・インスペクション（パケット・コレクターとして）	1.5 Gbps	5 Gbps
キャプチャ・インターフェイスのオプション	4 ポート SFP または 2 ポート SFP+	
管理インターフェイス	10/100/1000 銅線 x 2	
プロセッサ	XEON ES-2658 (2.1 Ghz/20 MB, 8 コア・プロセッサ) x 2	
サイズ	2 RU	3 RU
電源	デュアル AC または DC **AC ユニット：** 100 – 240 VAC、47/63 Hz **DC ユニット：** -40 – -72 V / 20 -12ADC	デュアル AC または DC **AC ユニット：** 100 – 127 –200 – 240VAC、 10 – 5A、50/60 Hz **DC ユニット：** -40 – -72VDC、31 – 15A
相対湿度	8 – 90%（結露なきこと）	8 – 90%（結露なきこと）
放熱	1365 BTU/ 時（400 ワット）	1791 BTU/ 時（525 ワット）
環境仕様	IEC 60950-1:2005 2nd Edition、Am 1:2009 CAN/CSA-C22.2 No. 60950-1-07、2nd Ed.Amendment 1:2011 ANSI/UL Std No. 60950-1-2011、2nd Ed FCC 47 CFR Part 15、Subpart B – Verification ICES-003 EN 55022: 2010 + AC:2011 EN 55024:2010 CISPR 22:Edition 6.0 2008-09 AS/NZS CISPR 22:2009 EN 61000-3-2:2006 + A1:2009 + A2:2009 EN 61000-3-3:2008	IEC 60950-1:2005 2nd Edition、Am 1:2009 CAN/CSA-C22.2 No. 60950-1-07、2nd Ed.Amendment 1:2011 ANSI/UL Std No. 60950-1-2011、2nd Ed FCC 47 CFR Part 15、Subpart B – Verification ICES-003 EN 55022: 2010 + AC:2011 EN 55024:2010 CISPR 22:Edition 6.0 2008-09 AS/NZS CISPR 22:2009 EN 61000-3-2:2006 + A1:2009 + A2:2009 EN 61000-3-3:2008

ARBOR NETWORKS
The Security Division of NETSCOUT

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
米国内通話料無料：+1 855 773 9200

ヨーロッパ
TEL：+44 207 127 8147

アジア・パシフィック
TEL：+65 6664 3140

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

DS/ADVANCEDTHREAT/EN/1115-LETTER