データシート

ARBOR NETWORKS SPECTRUM™

With NETSCOUT ISNG

攻撃活動の状況は変化しています。マルウェアなどの攻撃ツールは、通常はネットワークへ不正アクセスするための最初の武器として使用されもはや選択肢の一つではありません。今日の攻撃者は、従来のエッジセキュリティの防御を迂回して、ユーザーアカウントにアクセスし、著名なITアプリケーションやオペレーティングシステムを操ります。攻撃を検出するのに掛かる平均期間は通常150日を超えますが、攻撃者がネットワークを侵害するのには、10分以下しか掛かりません。Arbor Networks Spectrum™は、攻撃者がすでに内部にいるときに、セキュリティチームが攻撃を認知するまでの時間を全体を劇的に増加させ、すばやく排除したり閉じ込めることができます。重要なインシデント対応やセキュリティ運用のワークフローを自動化および連携統合することで、セキュリティチームはスケールアップすることができ、既存のスタッフやリソースでさらに多くの成果を上げることができます。

エピック・レンジ

Arbor Spectrumは、世界中のすべてのインターネットトラフィックの3分の1から要約され実情を正確に表したATLAS™ (Active Threat Level Analysis System) 脅威インテリジェンスを利用してネットワークの正確な可視性を提供します。最新の脅威情報によって絶えず更新されるATLASの可視性とATLASのインテリジェンスポリシーを組み合わせることで、ネットワーク内、またはその周辺で起こっている脅威を最高の正確性で確認できます。

より速い実証

Arbor Spectrumのリアルタイムで高性能のトラフィックアーカイブを使用して、業界トップクラスを誇るNETSCOUTのネットワークおよびアプリケーションのメタデータ収集および分析テクノロジーであるASIテクノロジを搭載したISNGとを統合することによって、前例のない広範な可視化とプロトコル、アプリケーション、およびネットワークデータ分析を可能にします。 ビルトイン調査ワークフロー、高速検索、過去数ヶ月のネットワークとユーザーの活動を簡単にピボットすることよって、従来、数時間～数日間を要していた作業をたった数秒の作業にすることができます。

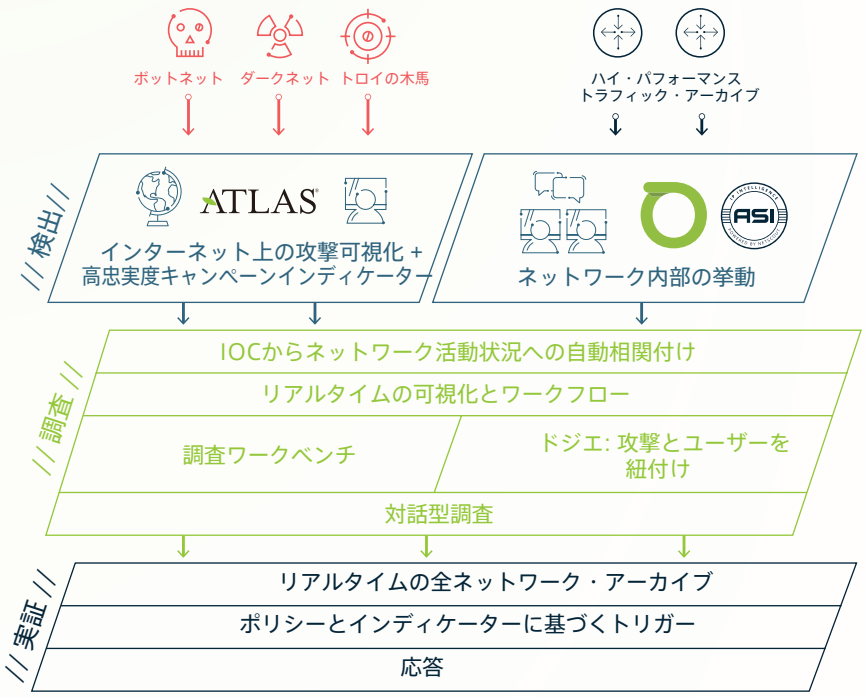
「セキュリティー製品は銀でできた銃弾ではありませんが、Arbor Spectrumはこれまでにない真のエンドツーエンドの可視性を私たちに与えてくれました。Arbor Spectrumのソリューションとサービスに非常に満足しています。」 & Benefits

大手金融機関 セキュリティーマネージャー

ARBOR NETWORKS
The Security Division of NETSCOUT

Arbor Specrtumの仕組み

Arbor Spectrumは、Arborのユニークな脅威インテリジェンスと独自の脅威データとトラフィックパターンを使用したArborのグローバルな可視性を活用し、有害な脅威を検出、調査、証明します。 Arbor Spectrumは、ASIテクノロジーおよび/またはArbor Spectrum Flow Collectionを使用したNETSCOUT ISNGと、Active Directoryを使用してネットワーク内部のアクティビティーを表面化します。



検出

- 調査開始する関連指標
- ATLAS Intelligenceインジケータによる新しい脅威
- 共有脅威情報を適用するためにSTIXフィードをインポート
- 新しく識別された指標のアーカイブ検索のための遡及分析

ATLASインテリジェンスインジケーター

ATLASは、ライブインターネットトラフィックテレメトリー（全インターネットトラフィックの約3分の1）の世界最大のデータセットです。 ATLASはArborにインターネット上の攻撃活動レベルを監視させ、さらにその攻撃トラフィックパターンを高度に検査された情報インジケータに1時間ごとにArbor Spectrumに抽出します。

調査

インジケーターの優先順位付け

新しい指標やネットワーク活動の動向をリアルタイムで視覚的に表現 グループ（ユーザー、ビジネス機能、場所など）にマップ可能です

調査モジュール

関連インジケータ、ホストプロファイル、ネットワーク接続などの手がかりを高度な脅威の単一のビューにまとめます

ユーザーID /アクティビティのディレクトリ統合によるホスト文書

- ユニークなワークフローは、ネットワーク内の横方向の動きを識別し、追跡します
- ホストと目的の接続ポイント間のネットワークの会話の詳細な表示

証明

セキュリティー侵害の兆候を自動でパケットキャプチャー

特定された各インジケーターのPCAPを保存することにより、破壊的かつ自動化されたフォレンジクスを可能にし、フォレンジクスの拡張性と費用対効果を高めます。

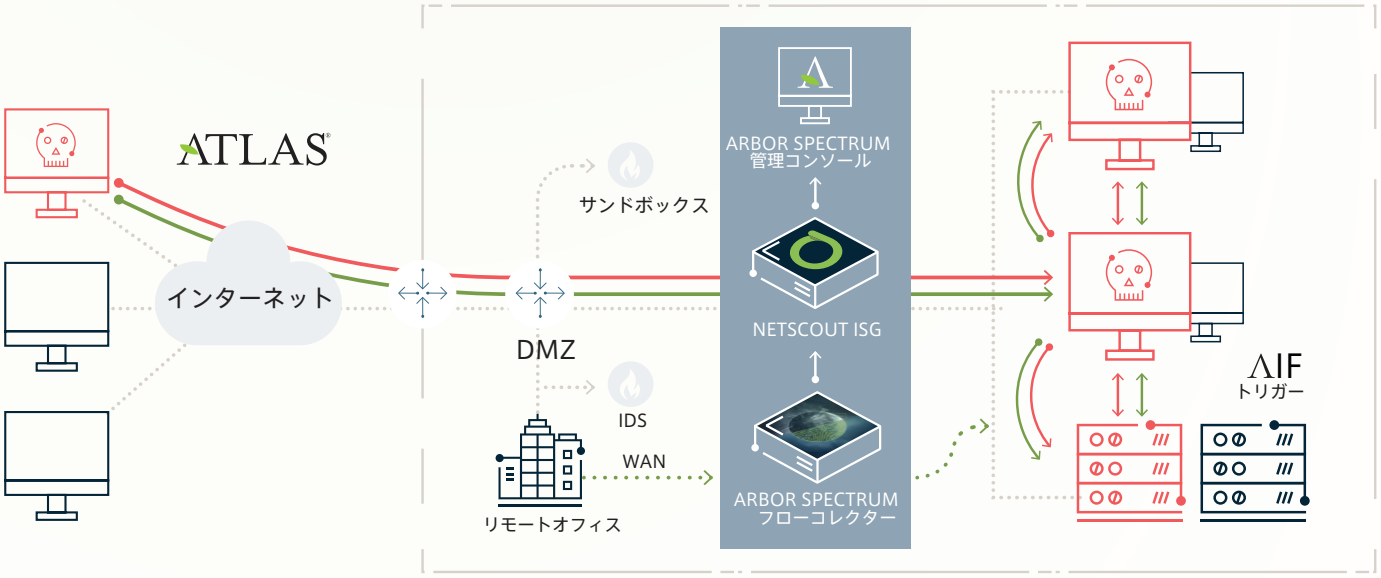
任意のホストまたは会話の手動パケットキャプチャー

PCAPをアップロードしたり、追跡もしくは調査によって発見されたホストや通信のPCAPを起動する機能を提供します

主要なSIEMプラットフォームとの統合

キャプチャしたデータをHP Arcsight、IBM QRadar、Splunk Enterprise SecurityなどのSIEMプラットフォームへ送信します

ARBOR SPECTRUM展開例 with NETSCOUT ISNG



図：AIF スタンダード・フィードを使って特定された脅威の例すべての防御策およびポリシーは常時アップデートされるため、上記のリストは随時変更されます。

主な特長

攻撃活動傾向を高性能に表示

ALTASインテリジェンスとの連携

特徴的なワークフロー

疑わしい活動をすばやく発見し、攻撃指標へ反映

高性能ネットワーク・トラフィック・アーカイブ

NETSCOUT ISNGと連携して指先一つで数ヶ月におよぶデータへ簡単にアクセス

サーチとピボット

数ヶ月間におよぶデータへ即座にアクセス

一日以内で導入が完了

アプライアンスおよび仮想マシンを提供

推奨NETSCOUT ISNGモデル

ISNGモデル	インタフェース数	インタフェースタイプ	ストレージ	コア数	RAM
ISNG9895	4	4ポート 10G/1G	96TB	36	256GB
ISNG9795	4	4ポート 10G/1G	64TB	24	128GB
ISNG4895	4	4ポート 10G/1G	32TB	36	256GB
ISNG4795	4	4ポート 10G/1G	24TB	24	128GB

ARBOR SPECTRUM管理コンソール & フローコレクター

	2200	2300
導入方式	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·コレクターまたは フロー·コレクター
ハード·ドライブ	2TB SATA 7200 RPM x 8	4TB SATA 7200 RPM x 16
ストレージ容量	15TB	64TB
トラフィック·アーカイブ	9.1TB	64TB
最大フロー/秒 (フ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)	1.5Gbps	5Gbps
キャプチャー·インタフェース·オプション	4 ポート SFP または 2 ポート SFP+	
管理インターフェース	10/100/1000 銅線 x 2	
プロセッサー	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
相対温度	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)

ARBOR SPECTRUM VM 推奨ハードウェア仕様

VM展開形態	コンソール	パケット·コレクター	フロー·コレクター
サポートVMwareバージョン	vSphere Hypervisor software (以前の「ESXi」), version 5.5		
コア アロケーション	8 - 32	8 - 32	8
メモリー アロケーション	16 - 64GB	16GB	16GB
ディスク アロケーション	**OS:** 150GB / **Data:** 1 - 4TB	**OS:** 150GB / **Data:** 1 - 40TB (検証済み最大値、仕様上は40TB以上)	
ネットワークインタフェース	1 - 2	3 - 15	1 - 15
最大フロー数/秒	—	—	250,000 FPS
最大パケットインスペクション	—	最大 2GB	—

この表に記載された要件とパフォーマンスは実運用時に向けたな内容となっています。小規模なPOC向けのオプションも別途用意しています

ARBOR NETWORKS
The Security Division of NETSCOUT

arbornetworks.com

DS/SPECTRUM/JA/1117-A4

米国本社
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA: +1 866 212 7267
T: +1 781 362 4300

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