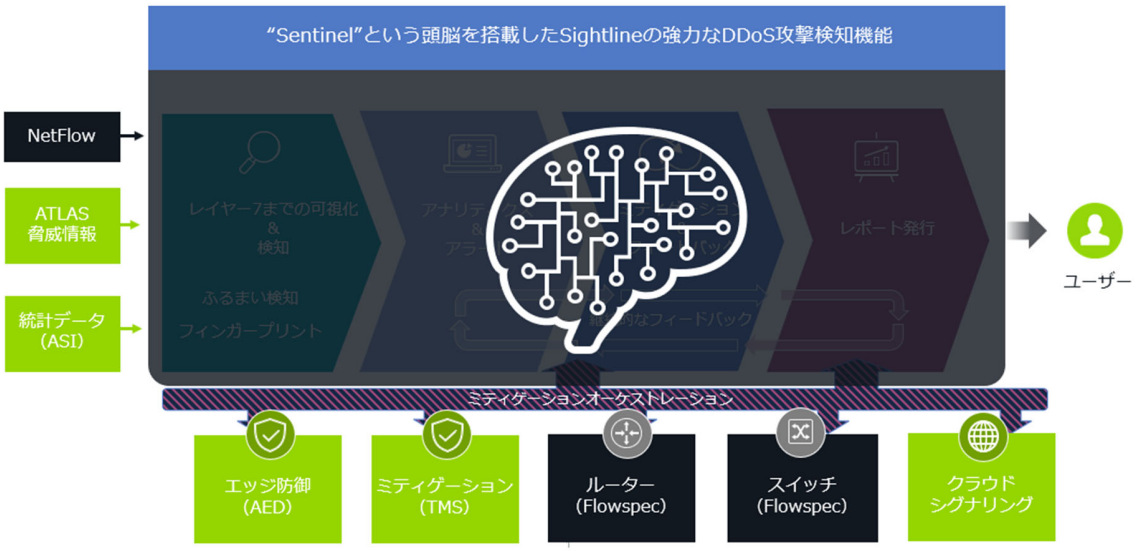
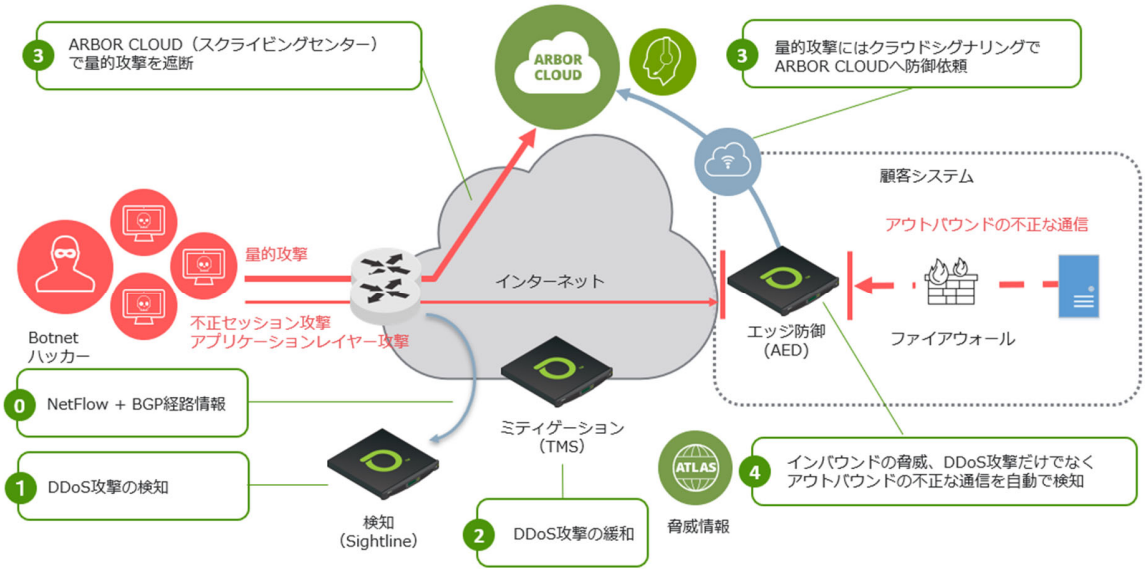

“Sentinel”という頭脳を搭載したSightlineの強力なDDoS攻撃検知機能
NetFlow
ATLAS
脅威情報
統計データ
(ASI)
レイヤー7までの可視化
&
検知
ふるまい検知
フィンガープリント
レポート発行
ユーザー
ミティゲーションオーケストレーション
エッジ防御
(AED)
ミティゲーション
(TMS)
ルーター
(Flowspec)
スイッチ
(Flowspec)
クラウド
シグナリング

DDoS 攻撃の検知から緩和（ミティゲーション）までの流れ



DDoS 攻撃の検知から緩和（ミティゲーション）までの手順

	説明	ネットスカウト製品名	ネットスカウト製品の特徴
0　フロー情報の連携	NetFlow	-	-
1　DDoS攻撃の検知	NetFlow + BGP	Arbor Sightline (※統計フローデータ)	BGP経路情報も連携可能
		+ Insight (※生フローデータ)	多角分析が可能
		+ Sentinel	OTTの分析が可能
2　DDoS攻撃の緩和	ミティゲーション	Arbor TMS	最大400Gbpsまで対応
3　DDoS攻撃の緩和	ミティゲーション (オフロード)	Arbor Cloud	最大11Tbpsまで対応
	ミティゲーション (オフロード)	Arbor Cloud	クラウドシグナリング
4　DDoS攻撃の緩和	エッジ防御	AED	出口対策も可能
*　脅威情報の連携	ATLAS	+ AIF	-
*　パケットデータの連携	ASI	+ ISNG or vSTREAM (※統計パケットデータ)	DNS情報の連携可能
•　ツールチェーンの可視化	インラインバイパスタップ	+ EPT	-
*　ツールチェーンの集約	集約スイッチ	+ PFS	-

ネットスカウト製品の出来る事製品種別

	Sightline			TMS	Arbor Cloud	AED	AIF	ISNG or vSTREAM	EPT + PFS
	Sightline のみ	+ Insight	+ Sentinel						
DDoS攻撃の検知	✓								
フローデータの統計化	✓								
生フローデータの参照	✓	✓							
生フローデータの分析	✓	✓							
OTTの分析	✓	✓	✓				✓		
DNSの参照	✓	✓	✓					✓	
パケットデータの統計化	✓	✓	✓					✓	
DDoS攻撃の緩和	✓			✓					
DDoS攻撃のオフロード	✓				✓				
クラウドシグナリング					✓	✓			
エッジ防御						✓			
入口(DDoS攻撃)対策						✓			
出口(内部不正)対策						✓			
脅威情報の連携							✓		
ツールチェーンの可視化・集約									✓

製品ラインナップ

Sightline

NetFlowなどのフロー情報を集約し解析するコレクター製品
アプライアンス版とソフトウエア版をご用意
＋ Insightで生フローデータの参照、＋ SentinelでOTTの分析が可能

TMS

1台で最大400Gbpsの緩和が可能なミティゲーション装置
アプライアンス版のみの提供
量的攻撃に対応

Arbor Cloud

最大11Tbpsの緩和が可能なミティゲーションクラウド
CDN事業者提供のクラウドと異なり、HTTP/HTTPS以外のトラフィックも処理可能
クラウドシグナリング機能でエッジ防御（AED）とのシームレスな連携が可能

AED

上位のISPでは緩和出来ない不正セッション攻撃やアプリケーションレイヤー攻撃に対応
脅威情報（AIF）と連携し入口（DDoS攻撃）対策だけでなく出口（内部不正）対策にも対応
セッションレスのアーキテクチャを採用しワイヤレートでの処理が可能

AIF

グローバルに脅威情報を解析するモニタリングシステム
約400社のISPと契約しインターネット全体の4割にあたる140Tbpsのトラフィックデータを収集
これらのデータは自社脅威研究チーム（ASERT）が分析

ISNG or vSTREAM

1Gbpsから100Gbpsまでのキャプチャポートに対応した専用パケットキャプチャアプライアンス
アプライアンス版と仮想版をご用意
パケットデータから抽出したDNS情報などを統計データ（ASI）としてSightline Sentinelに連携可能

EPT + PFS

セキュリティツールチェーンの可視化が可能なPower Safe機能を持ったTAP（EPT）
セキュリティツールチェーンの集約が可能なアグリゲーションスイッチ（PFS）
1Gbpsから100Gbpsまでのインターフェイスに対応

Worldwide Infrastructure Security Report

年に一度米国内で開催されるユーザー向け年次イベント

参加費は無料（※宿泊費、交通費は自己負担）

各種製品のデモや多数のワークショップを開催

https://www.netscout.com/engage20

自社作成のセキュリティの年次報告書

ダウンロードは無料

DDoS攻撃のトレンドや種類、検知や防御手段の分布を要約

https://www.netscout.com/report/

ENGAGE 20

ネットスカウト・システムズ・ジャパン株式会社

〒105-0022 東京都港区海岸1-2-3 汐留芝離宮ビルディング 21F

TEL: 03-5403-6979

http://www.netscout.com/

mailto:jp-enterprise-sales@netscout.com