ENEA

DATASHEET

Qosmos Probe as a DPI Sensor for Network Traffic Analysis

優れたネットワーク・トラフィック解析のためのリアルタイム・プロトコルとメタデータ・インテリジェンス

主な特長

実証済みのテクノロジー

- ベースエンジンは、サイバーセキュリティで最も広く導入されている Qosmos ixEngine®

独自の NTA サポート機能

- 極めてキメ細かい信頼性のあるデータにより強化されたマシン・ラーニング
- 暗号化トラフィックや回避型トラフィックを正確に可視化
- SCADA／IoT プロトコルおよびメタデータをサポート
- ネットワーク独自のカスタム・ルールをサポートするインテリジェンス性

業界一のクラシフィケーションとメタデータ抽出

- 幅広いプロトコルとアプリケーションに対応
- 3,300 以上のプロトコルを分類
- 5,300 以上のアプリケーション・メタデータを抽出
- 独自のリアルタイムなディープ・ファイル・インスペクション機能
- 正確なエンドポイント（デイバス、IP、ユーザー、ドメイン名など）を特定
- サイバーセキュリティ固有のプロトコル・メタデータを提供

スマートなアラート機能

- 効果の高いアラート優先度付け
- ディープなアラートのコンテキスト化
- Qosmos 独自の「誤検知なし」コミットメント

ビジネス・モデル

- 業界最先端の DPI テクノロジーを、低価格かつ容易なデプロイのSW センサーとしてパッケージ
- カスタム DPI の開発が不要
- 継続的でホットスワップ可能な更新を提供
- フルパケットキャプチャーの必要性を大幅に軽減
- コストのかかるエンドポイント・ベースや境界ベースのデータ収集要件を緩和

エンタープライズ SOC（セキュリティ・オペレーション・センター）や MSSP（マネージド・セキュリティ・サービス・プロバイダ）では、既存のエンドポイントや境界での防御では防ぎきれない疑わしい活動の特定に、NTA（ネットワーク・トラフィック解析）を活用することが増えています。

NTA は、マシン・ラーニング、高度なアナリティクス、ルール・ベースの検出により、ネットワーク・トラフィックのフローや接続で発生した異常なパターンを通じて脅威を特定します。

これは特に、APT（Advanced Persistent Threat: 高度かつ持続的な脅威）に対して有効であることがすでに実証されています。ビヘイビア・ベースの異常検出機能がなければ、APT は数ヵ月、あるいは数年もはびこる恐れがあります。

ただし、効果的なビヘイビア解分析には、膨大な量の高信頼性かつ詳細なトラフィックデータが必要です。つまり、NTA には、DPI（ディープ・パケット・インスペクション）センサーが提供するようなデータが欠かせません。

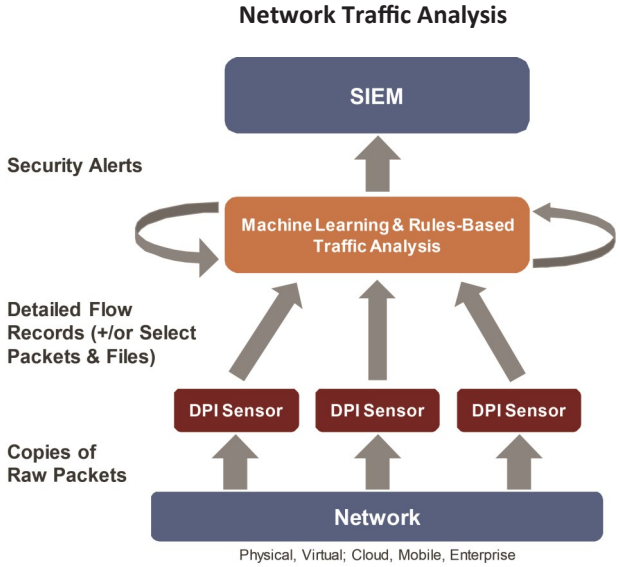
The Qosmos Probe

Qosmos Probe は、クラス最高の DPI センサーです。暗号トラフィック（APT トラフィックの多くがこれに該当）も含むテレメトリのロー・データを非侵入的に収集し、詳細なクラシファイド・トラフィック・データに変換します。

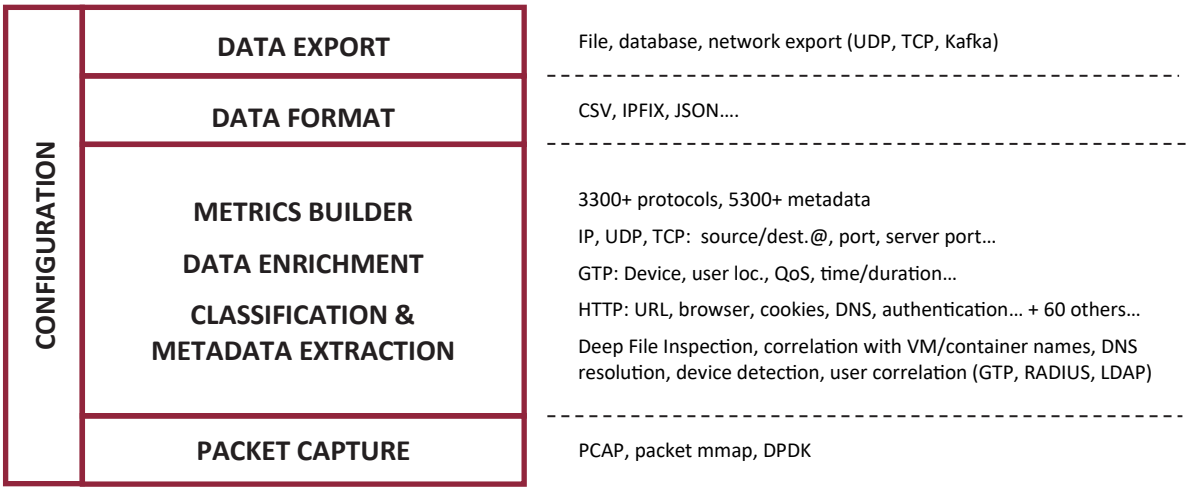
Qosmos DPI センサーを主要なネットワーク・アセットにまたがってデプロイすることで、次のようなデータを取得できます。

- 高信頼性： 極めて信頼性の高いソースに基づくテレメトリ・データ（非セキュアなログファイルではない）
- 包括的： OSI L2 から L7 まで（データ・リンクからアプリケーション・レイヤまで）を網羅するクラシフィケーション
- リアルタイム： パッシブな物理ネットワークまたは仮想ネットワークの TAP（トラフィック・フローに影響を与えない）を通じてオン・ザ・フライで収集

Qosmos Probe DPI センサーは、サイバーセキュリティで基も広く導入されている DPI ソフトウェアである Qosmos ixEngine をベースとしています。 抽出したプロトコルとメタデータの処理能力の高さ、幅広さ、深さは他に類を見ません。



Qosmos Probe アーキテクチャ



パフォーマンスとフローの処理

- プローブ当たり最大 20 Gbps までのトラフィックデータを単一エンティティとしてスタックし管理
- CPU1 コア当たり 1 Gbps、1 Gbps 当たり 4GB RAM
- トンネル内 (GTP、GRE、PPOE など) のカプセル化トラフィックを分類
- ホットスワップ可能な更新 (3 週ごとにリリース)

暗号トラフィックと回避型トラフィック

- 高精度 (97% 超の認識精度) で Skype を特定するトラフィック・パターンを使用
- 統計モデルとマシン・ラーニングを使用して、RC4 で暗号化される BitTorrent などの複雑なプロトコルを検出 (検出率 95% 以上)
- ドメイン・フロンティング検出およびクラシフィケーションの手法による回避型トラフィック (Ultrasurf、Viber、Hotspotshield など) の可視化
- DPI エンジンを「だます」ためのトラフィック・スプーフィング・アプリケーション (HTTP Injector、Eproxy など) のクラシフィケーションで高い成功率
- ICMP／DNS トンネリング・トラフィックで高い検出率
- 一般によく利用されている暗号資産の検出とマイニング・プール・トラフィック (クリプトジャッキング) の検出

ディープ・ファイル・インスペクション

ファイル・タイプの検出、MIME タイプとファイル拡張間の整合性チェック、ファイル・ハッシュの計算、メタデータの抽出

- ファイルのハッシュ値：MD5、SHA-1、CTPH
- 280 を超えるファイル・タイプ：アプリケーション、動画、音声、テキスト…

データ・アグリゲーション

- クロス・フローのレコード (IP 別、アプリケーション別、ホスト名別などの統計) の送信機能により、1 秒当たりイベント数を削減

カスタム・シグネチャー・モジュール (CSM)

独自のクラシフィケーション・シグネチャを作成し、Qosmos Probe にリアルタイムでロードすることが可能

サイバーセキュリティ・オペレーションの解析サンプル

- キー：flow_id、application、ip_srv、port_srv、ip_clt、http.server、http.uri_path、http.code…
- メトリクス：stc_packet-count、stc_volume、dfi.mimetype*、dfi.ctph*、http.mime_type…

*dfi = ディープ・ファイル・インスペクション (ファイルコンテンツのインスペクション)

統計は、CSV、IPFIX、または JSON 形式でエクスポート可能 (ELK および InfluxDB データベースと互換性あり)

コンフィギュレーションとマネージメント

- NETCONF API
- 設定およびステータス情報 (設定、カウンタ、エラー、ログ・メッセージなど) 用のマルチテナント・セントラル・マネジメント・コンソール

物理アプライアンスとの統合

- コモディティ・ハードウェア上で実行 (x86_64 アーキテクチャ)
- CentOS または RHEL 7
- DPDK パケット・キャプチャー・フレームワーク

仮想システムとの統合

- SD-WAN ルーティング、セキュリティ、モニタリングの各種機能をアプリケーション・レベルで可視化
- 「クラウド・レディ」(クラウド対応済み) であり、テナントごとの DPI 利用をサポート

提供形式

- Qosmos Probe は、完全にカスタマイズ可能な Linux アプリケーション (VM、コンテナ、RPM など) 形式で提供されます。

NTA での DPI の使用の詳細については、Enea の MSSP のケース・スタディをご参照ください。
https://www.qosmos.com/mssp-uses-qosmos-probe-in-nta-solution-to-improve-service-levels/

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

Find out more!

ENEA

www.enea.com www.enea.co.jp

Enea は、テレコムおよびサイバーセキュリティ向けの革新的なソフトウェア・コンポーネントの世界的なリーディング・サプライヤです。モバイル・コア、ネットワーク仮想化、トラフィック・インテリジェンス向けのクラウド・ネイティブな 5G 対応製品を主力としています。Enea のテクノロジーは、世界中の 30 億以上の人々に日々利用されています。Enea の DPI ベースの IP トラフィック・クラシフィケーションおよびネットワーク・インテリジェンス・ソフトウェアは、業界の最先端を行くソリューションとして幅広いベンダーおよびインテグレータに採用され、テレコム企業、クラウド・サービス・プロバイダ、大手企業向け製品に組み込まれています。Enea の Qosmos Probe や Qosmos DPI テクノロジーについては、www.qosmos.com をご覧ください。