Data Exchange Layer

複数のアプリを簡単に連携し、迅速な通信を実現

リアルタイムのアプリケーション フレームワークにより、データを簡単に共有し、アプリケーション間でセキュリティ タスクの調整が可能になりました。新しいオープンなソフトウェア開発キット（SDK）を使用することで、統合作業の手間を省き、サイバーセキュリティの効率を阻害する遅延や弱点を排除できます。

統合は簡単に実現されないようです。セキュリティ チームやベンダーがアプリケーションを統合する場合、最もよく行われる手法は、1対1の統合、手動スクリプト、スケジュール プロセスの3つです。これらは、サイバーセキュリティ チームが最高のパフォーマンスを実現するために必要な効率性、正確性、速度を阻害する要因となっています。このため、脅威インテリジェンスの共有、インシデントの調査、レスポンスの調整が限定的なものになっています。

では、何が問題なっているのでしょうか。データをリアルタイムに安全かつ簡単に共有する方法はまだ確立されていません。

- セキュリティ インフラやITインフラの多くは、複数の技術、ベンダー、社内アプリケーションを利用して、時間をかけて構築されてきました。
- APIを使用して製品を統合するのでは、構築までに時間がかかり、製品のアップグレードやデータ フォーマットの変更に簡単に対応できません。
- 2つのセキュリティ製品を統合する場合、2つのベンダー間で打ち合わせを行い、プロセスを承認し、実装しなければなりません。
- 従来のポーリングとスケジュールによるデータ公開モデルでは、処理に時間がかかります。

オープンな標準とエコシステム

Open Data Exchange Layer（OpenDXL）イニシアチブでオープンな業界標準を確立する動きが進んでいます。OpenDXLイニシアチブは、開発者が柔軟な方法で簡単に統合を行い、組織のセキュリティ オペレーションを強化することを目標としています。OpenDXLイニシアチブでは、新しい開発者や参加者でもMcAfee Data Exchange Layer（DXL）を簡単に使用できるようにSDKを提供しています。これにより、DXLの統合または配備の価値が大幅に増大します。

DXLでセキュリティが変わる

- **脅威対策ライフサイクルのワークフローを短縮**
  情報をすぐに共有し、タスクを調整することで、新たに識別した脅威の検出から隔離、修復までの時間を短縮できます。
- **セキュリティ製品やベンダー間の統合を促進**
  オープンなプラットフォームを採用しているので、異なるベンダーのセキュリティ製品を自社のアプリケーションやツールに簡単に接続できます。ベンダーとの交渉結果を待つ必要はありません。
- **配備したアプリケーションの価値を高める**
  アプリケーション間で有益な脅威データを共有できるので、アクションをすぐに実行できます。

このSDKを使用してアプリケーションを作成することで、DXL通信ファブリック経由で異なるベンダーのアプリケーションや社内のアプリケーションに接続し、データをリアルタイムで安全に共有したり、アクションを調整することができます。1対1の統合を繰り返す必要はありません。

アプリケーションは、メッセージトピックの公開と取得を行うか、RESTful APIと類似したリクエスト/レスポンスの形式でDXLサービスを呼び出します。ファブリックはメッセージの配信と呼び出しを迅速に行うので、セキュリティ、IT、その他の社内ソリューションが1つのシステムのように機能します。OpenDXLには、OpenDXL ClientとOpenDXL Brokerというオープンソースの DXLクライアントとブローカーが含まれています。これにより、ツールと情報源の間にオープンソースの通信モデルを構築できます。

2014年にDXLが登場して以来、30を超えるベンダーのアプリケーションがDXLエコシステムに参加し、100以上の統合が行われています。多くの企業、サービスプロバイダー、政府機関がすでにこのシステムを採用し、意思決定からアクション実行までの時間を短縮しています。これにより、運用コストを削減し、セキュリティの管理と脅威対応の負担を軽減できます。貴重なセキュリティ　チームのリソースを手間のかかる作業から解放し、より戦略的な仕事に振り分けることができます。

1つの統合プロセスですべてに対応

標準的な統合形態と異なり、各アプリケーションは共通のDXL通信ファブリックに接続します。統合プロセスは1つだけです。OpenDXLは、様々な言語に対応しているので、開発者は慣れている開発環境で統合を行うことができます。1つのアプリがメッセージを公開するか、サービスを呼び出すと、複数のアプリがそのメッセージを取得したり、サービス要求に対応します。標準化を目的としているため、統合技術の基礎となる専用アーキテクチャへの依存度は低くなっています。ベンダー固有のAPIや要件から解放されるため、統合作業は非常に簡単になります。

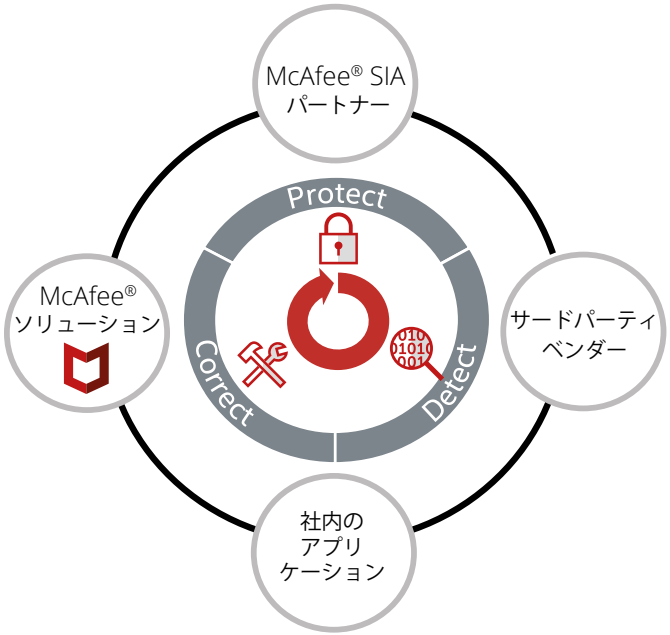

図1. DXLが迅速な統合モデルとリアルタイムの通信ファブリックを実現

DXLで統合するだけでなく、対話するサービスや市販の製品のAPIをラッピングして、データをDXLに公開することもできます。他のサービスは、DXLメッセージや呼び出しを待機し、最新のデータで機能を強化したり、適切なアクションを実行します。より洗練されたアプリでは、調整結果を反映し、一連のアクションをスクリプトで実行します。

ホストに小規模なDXLクライアントをインストールし、メッセージの交換を管理するDXLブローカーを用意することで、既存のネットワークに標準化された統合環境と通信レイヤーを配備できます。すべてのDXLトラフィックは会社のネットワーク内で送受信されるので、プライバシーが保護され、オペレーションを制御できます。ファイアウォール対応モデルでは、DXL経由で最新の情報に常にアクセスできるように、クライアントとサーバー間の通信が維持されます。アプリケーション自身の変更が公開または受信されると、DXLの抽象レイヤーが配備環境の残りの部分を隔離してリスクを回避するので、保守コストを削減できます。

より良いサイバーセキュリティ エンジン

以前は利用できなかった最新のデータにアクセスできるようになったことで、セキュリティは大きく変わります。分析、インシデント対応、運用の担当者は、できるだけ最新のデータを取得して分析を行い、アクションを実行したいと考えています。ベンダーや開発者もこのニーズに応えようとしていますが、技術的な問題やパートナー企業との関係で統合が進まないことが少なくありません。

このような障害はすでにありません。ベンダーや開発者の対応を待つ必要はありません。

セキュリティ オペレーションで次のようなデータをすぐに入手することができます。

- 偽の脅威イベント
- ファイルとアプリケーションのレピュテーションの変更
- 検出されたモバイル デバイスと資産
- ネットワークとユーザーの動作の変更
- 正確なアラート
- 脆弱性と侵害兆候（IoC）のデータ

DXLは、セキュリティとITの活動を促進し、ソフトウェアや顧客の環境で新しい機能を実現するフレームワークとなります。新しいデータが利用できることで、より複雑な分析が可能になります。これにより、エスカレーション、封じ込め、修復または対応を迅速に行うことができます。データをリアルタイムで共有することでプロセスをスムーズに統合できます。

さらに詳しく

詳細については、**www.mcafee.com/jp/solutions/data-exchange-layer.aspx**をご覧ください。

〒150-0043
東京都渋谷区道玄坂1-12-1
渋谷マークシティウエスト20F
Tel. 03-5428-1100（代表）
www.mcafee.com/jp

2018年10月