AKAMAI ソリューション概要

機密コンピューティング：使用中のデータを保護

脅威の範囲と規模、そして巧妙さが増す中で、セキュリティチームは概ね、（特にデータの移動時の暗号化や保存時のアクセス制限を行う際の）課題への対処には成功しています。しかし、データが活発に編集、読み取り、または処理されているとき（一般的に「**使用中のデータ**」と呼ばれる）にもデータを保護する必要があることが、次第に明らかになってきました。

コンピューティングの進化と AI の台頭により、使用中のデータを保護する上でのこのギャップは、ますます重要になっています。ハイブリッドコンピューティングとマルチクラウドコンピューティングの普及により、組織がデータを収集および保存する方法は拡大しています。一方、企業が AI の活用を進める中、膨大なデータセット（多くの場合、最も価値があり、機微な情報）を暗号化されていない状態で使い、それを保護されていない場所に保管しています。

このようなリスクが、機密コンピューティングへの関心を高める要因となっています。機密コンピューティングとは、アプリケーション、プロセス、サービスで使用される機微な情報を暗号化して保護するセキュリティの手法です。

API により高まる複雑さ

API が急増しているのは、企業がリソースを一貫して導入している 2 つの分野（クラウド環境とクラウドサービス、および AI モデル）で重要な機能を提供しているためです。クラウドでは、テクノロジーがデータを通信し共有できるようにするために API が不可欠です。AI により、大規模言語モデル（LLM）は、データへのアクセスと結合に API を使用して、言語理解やテキスト生成などの複雑なタスクを実行します。

残念ながら、セキュリティチームはアプリケーションやインフラと同等の注意を API に向けていません。攻撃者はこのセキュリティギャップを利用しており、過去 12 か月間に 84% の組織が API のセキュリティインシデントを経験しています。[1] クラウドおよび AI 関連の API が扱うすべての機微な情報を保護するため、企業には機密性の高いコンピューティング環境で実行される包括的な API セキュリティ機能が必要です。

3 つのドアすべてをロック

転送中のデータや保存中のデータに鍵をかけても、1 つのドア（すなわち、使用中のデータ）が大きく開いたままであれば、企業はリスクにさらされる可能性があります。

機密コンピューティングでは、そのデータはハードウェアレベルで信頼できると見なされた環境で処理されます。API を使用することで、組織はパブリッククラウドの API サービスを利用するのではなく、API トラフィックを保護することに特化して構築された独自のプライベートな機械学習インスタンスを展開し、アタックサーフェスを大幅に削減できます。機密コンピューティング環境で API セキュリティソリューションを実行すると、追加のセキュリティレイヤーが作成されます。システムの一部が侵害されても、保護された環境内のデータは安全なままです。信頼できる環境でデータに対する API 分析を実行することは、より高いセキュリティを確保し、従来の環境で発生するリスクの排除につながります。

AI、API セキュリティ、そして機密コンピューティングを組み合わせることで、不正なエンティティ（ハイパーバイザー、ホスト・オペレーター・システム・インフラのオーナー、物理的にアクセスできる人物など）が実行中にコードやデータを閲覧または変更するリスクを防ぎ、内的脅威（不正なシステム管理者や信頼できないインフラで実行されているワークロードなど）と外的脅威（脆弱性を悪用する攻撃者など）の両方から保護することができます。

1. Akamai「API セキュリティの影響に関する調査」（2024）

ビジネス上のメリット

データセキュリティの強化
強力な制御で使用中のデータへのアクセスを制限し、アタックサーフェスを縮小し、API を使用する機密性の高いプロセスを不正アクセスから保護します

API の保護
使用中の機微な情報を暗号化したまま、高度な API トラフィック分析を実行し、監視中の情報漏えいのリスクを軽減します

コンプライアンスの強化
進化し続ける厳格なグローバルデータ保護規制に対応し、業界および政府の基準を確実に遵守します

利点

API の脅威が拡大し、使用中のデータが格好の標的となっている中、攻撃者が後れを取ることはないと考えられます。先進的な組織は、次のような理由から、機密コンピューティングを採用し始めています。

- 強力な管理により、使用中のデータに対するアクセスを初めから制限できる
- 増加する API を安全に分析できる
- 機密コンピューティングが提供する制御機能により、世界中の新しい厳格なデータ保護コンプライアンス要件に対応できる

機密コンピューティングは、オンライン取引を保護したい金融サービス企業や、患者データを保護するライフサイエンス企業など、規制の厳しい企業にとって最大のメリットがあります。このアプローチは、独立系ソフトウェアベンダーがエッジからクラウドまで、複数の場所に分散する AI モデルを保護するのにも役立ちます。実際、重要なデータに対してリアルタイムの分析処理を実行する企業の IT 組織は、機密コンピューティングについて考える必要があります。

当社とパートナー企業がサポートできること

効果的な機密コンピューティングには、包括的な制御と保護を提供し、緊密に連携する統合ソリューションセットが必要です。Akamai は、インテルと IBM のパートナー企業とともに、ハードウェアレベルからクラウド、API まで、使用中のデータのセキュリティを提供します。

まず、インテル® トラスト・ドメイン・エクステンション（TDX）は、以下のような信頼できる実行環境を提供します。

- 脅威アクターやアクセスできるべきではない非悪性エンティティによる外部からの侵入を防ぐ
- ネットワーク、サーバー、ストレージなど、クラウドで仮想リソースを作成するために使用するテクノロジーを制御するソフトウェアのセキュリティを向上させる
- これらの分散システムを管理する人の周囲に必要なセキュリティレイヤーを追加することで、うっかりミスやインサイダーによる悪性アクティビティの潜在的な事例のリスクを減らす

さらに、インテル Tiber™ Trust Authority の検証とトークンを使用することで、組織は暗号化されていない使用中のデータへのアクセスを制限し、制御することができます。

Akamai API Security ソリューションは、企業で使用されている API のインベントリを提供し、それらの API がどのように使用されているかを監視および検知します。トラフィックのパターンとふるまいを分析して悪性の API リクエストを自動的に検出して阻止し、手動で介入することなくネットワークエッジで脅威を効果的にブロックします。これにより、データ侵害、不正アクセス、ロジック乱用などの API 攻撃に対するリアルタイムの保護が可能になります。

Akamai のリモート機械学習エンジンを Intel Xeon® プロセッサー搭載の IBM Cloud Virtual Server と組み合わせて、Intel TDX でセキュリティを確保し、Intel Tiber Trust Authority で検証することにより、データ使用時の最終段階で暗号化されていないデータに AI ベースのボット攻撃や人間の攻撃者など、外的脅威によるアクセスを防止するための、拡張性の高いプライベート環境が実現します。

使用中のデータを保護する時代が到来

企業が最も貴重な企業データを安全に保つためには、信頼性の高い環境が必要です。そのような環境には、データの保存やアクセスだけでなく、実際に使用中でも確実に保護できることが求められます。Akamai やパートナーの協力で、包括的なセキュリティソリューションを提供します。これらの信頼できるコンピューティング企業が協力して、データのライフサイクル全体でセキュリティを確実に確保します。

機密コンピューティングのパートナーシップがお客様の機微な情報を安全に守るためにどう役立つかを詳しくご紹介します。
Akamai API Security ソリューションの詳細をご覧ください。