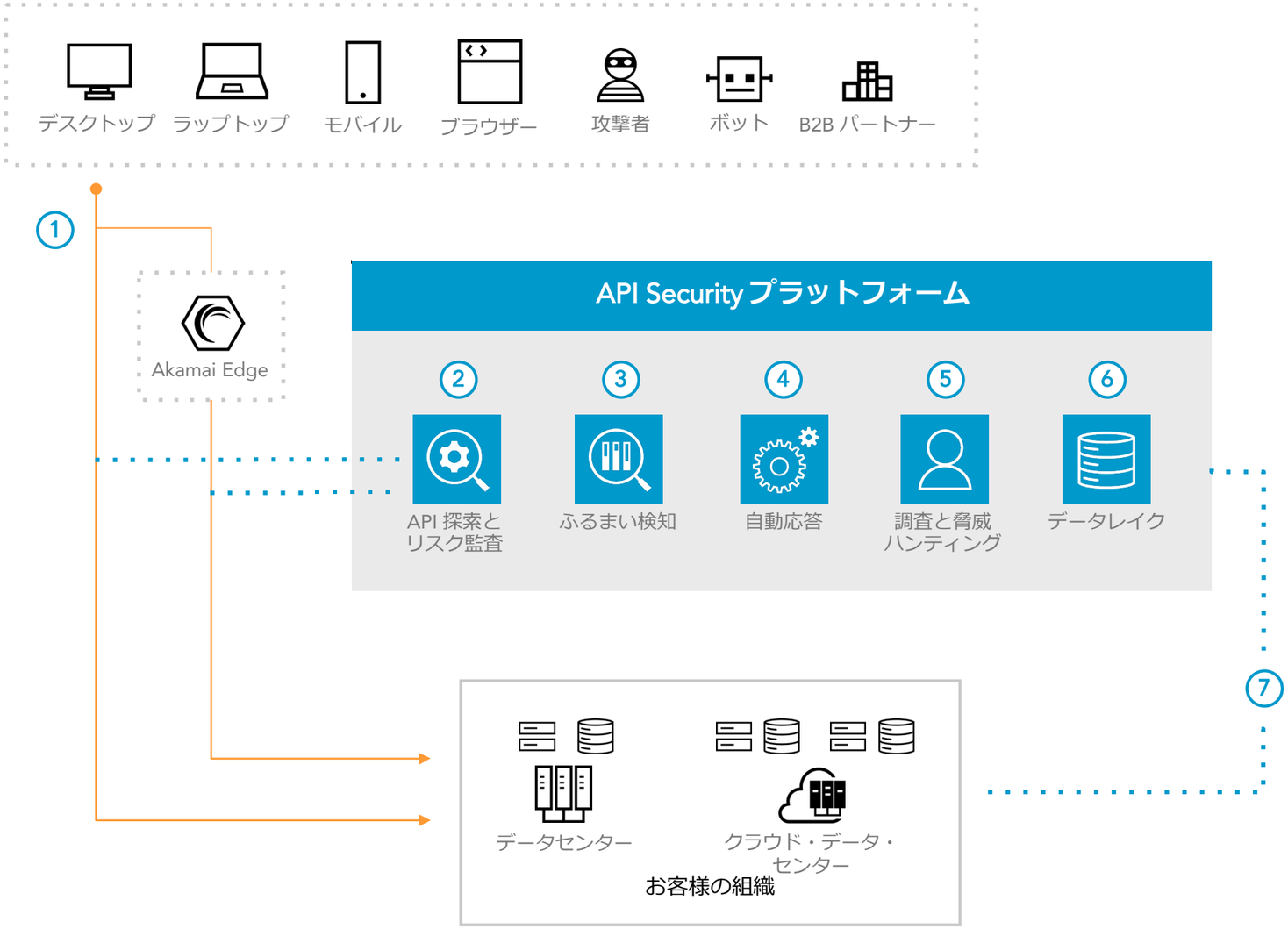
API SECURITY
仕組み



概要

Akamai API Security は、ふるまい分析によってすべての API を探索、監査し、API のアクティビティを監視して、脅威や悪用を検知してそれらに対応します。コンテキストに応じた検知により、シグニチャーベースのソリューションでは検知できないロジックの悪用や API 攻撃を防止します。

1. トラフィックは、お客様の組織から、Akamai Edge プラットフォームを経由して流れます
2. そのトラフィックのコピーが API Security プラットフォームに送られ、そこですべての API が探索されます
3. 異常やロジックの悪用を検知するために、ふるまい検知によって正常なふるまいのパターンを確立します
4. 自動応答により、重要な情報をセキュリティチームに送信したり、Akamai Edge でトラフィックをブロックすることができます
5. セキュリティチームは、ふるまいのコンテキストを使用して API トラフィック内の脅威の調査やハンティングを行ったり、マネージド型脅威ハンティングサービスを使用することができます
6. 過去の API アクティビティはデータレイクに保存され、調査と脅威ハンティングの取り組みに活用されます
7. また、API Security はお客様の組織の API と API アクティビティを完全に可視化します

キープロダクト

API 保護 ► Akamai API Security

マネージド型脅威ハンティング ► Akamai API Security ShadowHunt

詳しくは、akamai.com/products/api-security をご覧ください

公開日：2024 年 4 月