

DeNA：運用コスト削減と同時にネットワークの一元的な可視化を実現



株式会社ディー・エヌ・エー
(DeNA)

本社:〒150-8510

東京都渋谷区渋谷2-21-1
渋谷ヒカリエ

課題

従来の WAF では、特にトラフィックスパイクが発生した際の運用コストが高く、レスポンス時間が長いことが DeNA にとって大きな課題でした。

DeNA はゲームやライブストリーミングなどのエンターテインメント事業、eコマースなどを主に手掛ける企業です。

同社がサービスを拡大し、顧客に質の高いデジタルエクスペリエンスを提供し続けるには、それに見合った Web セキュリティ対策が必要であることが明らかでした。しかし、従来のハードウェア型 WAF にはさまざまな問題点があり、効率的な運用が困難でした。

DeNA が利用していた従来の WAF では、トラフィックスパイク時に管理ポータルの読み込みが遅く、問題に迅速に対処することができませんでした。さらに、WAF が正常に機能していない場合、ユーザーのリクエストを再ルーティングすることが不可能でした。

従来の WAF の効率の低いパフォーマンスに加え、ハードウェアの拡張にかかる高額なコストを考慮すると、高負荷のプレッシャーにも耐えられる新しいソリューションが必要であることが明らかでした。



「Signal Sciences により、よりコスト効率に優れたスケールアップが可能になりました」

茂岩 祐樹 氏

システム本部 セキュリティ部 部長

ソリューション

Signal Sciences は、従来のハードウェア型 WAF では実現できなかった拡張性の高いパフォーマンスやネットワークの一元的な可視性をもたらしました。

DeNA は Signal Sciences を 5つのプロパティにデプロイした結果、簡単なインストールの後に、パフォーマンスの改善が見られました。

運用および資本的コストの削減

Signal Sciences を導入することで、DeNA は運用コストの削減を実現することができました。まず、従来の WAF には欠かせなかったルールやポリシーのチューニングなど、専門のエンジニアによるコストのかさむ業務が必要なくなりました。さらに Signal Sciences の活用により、従来のハードウェア型 WAF よりもコスト効率に優れたスケールアップが可能になりました。

Web リクエストのリッチコンテキスト情報に基づいた攻撃検出機能

DeNA が使用していた従来の WAF は、静的な正規表現のパターンマッチングのルールに基づいていたため、リッチコンテキストを使用できず、偵察攻撃などの攻撃を見逃してしまうことがありました。Signal Sciences はより優れた、画期的なアプローチを用いることで潜在的な攻撃を検出してブロックすることができます。独自の SmartParse テクノロジーに加え、既知の不適切な IP アドレスのリストを活用することで迅速にインライン決定を実行し、悪質な Web リクエストをブロックします。また、Signal Sciences の Network Learning Exchange により、Web リクエストのソース IP アドレスの信頼性を見極め、さらに優れた決断を下すことができます。

組織のネットワーク全体の一元的な可視化

Signal Sciences の導入により、DeNA は組織的な攻撃に対してより優れた可視性が得られるようになりました。ダッシュボードで信頼できる情報を一元管理し、企業内のチームや関係者と共有することができます。さらに、Tor ネットワークからのトラフィックなど、今まで検出できなかったネットワークアクティビティも可視化できるようになりました。



「Signal Sciences はより優れた画期的なアプローチで潜在的な攻撃を検出し、ブロックしてくれます」
安永 貴之 氏
システム本部 セキュリティ部 セキュリティ技術グループ