radware

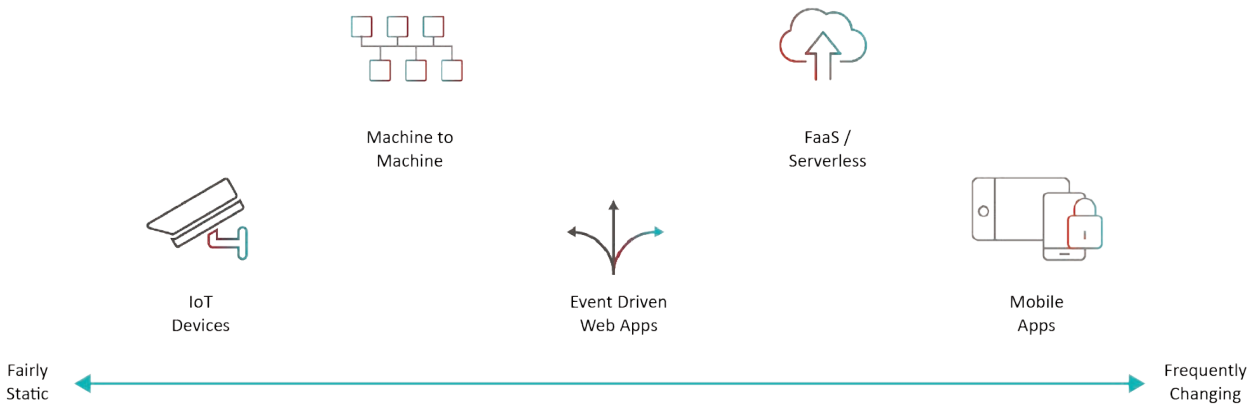
The Technology Behind Radware Bot Manager for APIs

WHITE PAPER

TABLE OF CONTENTS

Introduction: Today's API Security Space and Obstacles

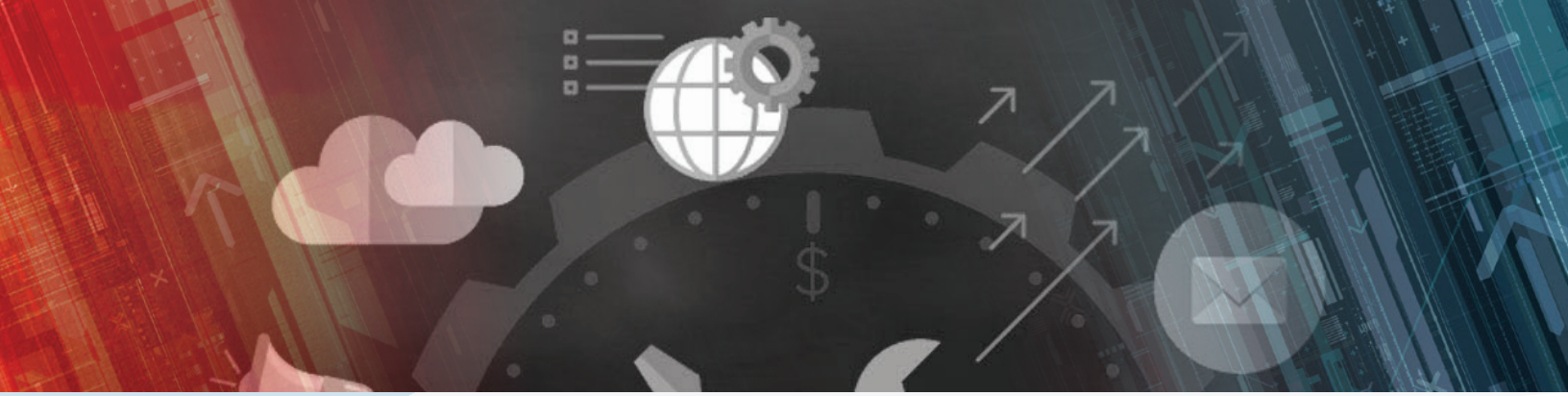
Application programming interfaces (APIs) have emerged as the bridge to facilitate interoperability between different systems, networks, and applications. There are specific communication protocols to APIs, and many ecosystems and architectures – from a smartphone to service mesh to OT (Operational Technology) – are dependent on them. DevOps, cloud architects and IT Operations can't do without them today. With the massive adoption of APIs comes the requirement of securing these APIs against any potential intrusion and exploitation. Unfortunately, despite rapid and widespread deployment, APIs remain poorly protected, and automated threats are mounting. Personally identifiable information (PII), payment card details, and business-critical services are at risk due to bot attacks on APIs.



Automated Threats to APIs and Gap in Security

Bad bot activity in APIs is rapidly increasing with 30% growth in the first half of 2020 compared to 2019. These bots were observed attempting automated attacks targeting APIs, such as account takeover, denial of service, payment data abuse, and denial of inventory. Protecting APIs against automated attacks is different from protecting web and mobile applications, simply because the bot behaviors, navigation flow and indicators are different.

APIs are there to accelerate business processes and since most of the API traffic is legitimate, it is crucial to make a definitive distinction between automated traffic with good and bad intent. In general, bot management solutions build machine learning models based on data collected from browsers and source machines to distinguish between genuine users and bots. Finding a malicious intent in an API call requires a different approach, as there's no human involved directly. While conventional solutions use device fingerprinting to detect bots using rotating IPs or user-agents, this technology cannot be applied to machine-to-machine communication use-cases. This is one of the gaps we are addressing here, with Radware's purpose-built API protection.



Key API Vulnerabilities

1. Authentication Flaws

Many APIs do not check authentication status when the request comes from a genuine user. Attackers exploit such flaws in different ways, such as session hijacking and account aggregation, to imitate legitimate API calls. Attackers also reverse engineer mobile applications to discover how APIs are invoked. If API keys are embedded into the application, an API breach may occur. API keys should not be used for user authentication.

2. Lack of Robust Encryption

Many APIs lack robust encryption between the API client and server. Attackers exploit vulnerabilities through man-in-the-middle attacks. Attackers intercept unencrypted or poorly protected API transactions to steal sensitive information or alter transaction data. Also, the ubiquitous use of mobile devices, cloud systems, and microservice patterns further complicate API security because multiple gateways are now involved in facilitating interoperability among diverse web applications. The encryption of data flowing through all these channels is paramount.

3. Business Logic Vulnerability

APIs are vulnerable to business logic abuse. This is precisely why a dedicated bot management solution is required and why applying detection heuristics that are good for both web and mobile apps can generate many errors – false positives and false negatives.

4. Poor Endpoint Security

Most IoT devices and microservice tools are programmed to communicate with the server via API channels. These devices authenticate themselves on API servers using client certificates. Hackers attempt to gain control over an API from the IoT endpoint, and if they succeed, they can easily re-sequence the API order, thereby resulting in a data breach.

Common Automated Threats to APIs

Account Takeover

Account takeover attacks are of two types: (1) Credential Cracking, (2) Credential Stuffing. During a credential cracking attack, attackers attempt to identify valid credentials by trying different values for usernames and/or passwords. In the event of a credential stuffing attack, attackers attempt mass login to verify stolen credentials. On APIs, cybercriminals attempt direct API access or try to evade device profiling to perform account takeover attacks.

Web Scraping

Today, many online businesses either employ an in-house team or leverage the expertise of professional web scrapers to gain a competitive advantage over their competitors. Scrapers plan attacks in various stages to evade the vulnerabilities of existing systems. On APIs, scrapers deploy bots to perform vulnerability scanning and steal sensitive data from exposed APIs.

Denial of Inventory

Cybercriminals reverse-engineer the API and then use human-like bots to pose as genuine customers to add products into carts. These bots send requests to the API endpoint as if they were instances of the application being used by actual humans. When a massive number of bots simultaneously add items into carts, repeating the process after every timeout has finished, real users cannot make purchases.

Application DDoS

The application layer in an enterprise infrastructure stack directly impacts the user experience. Layer 7 Distributed Denial of Service (DDoS) attacks pose a business continuity threat, strain APIs, and create service performance degradation. Layer 7 attacks also cause downtime in the event of distributed and coordinated DDoS attacks.

Enabling Business Continuity While Securing APIs

It is clear by now that thanks to APIs we can accelerate productivity, automate processes from end to end and design the perfect CI/CD pipeline. The challenge is to find a security solution that will not make any disruptions but rather integrate well into the environment. Unfortunately, most conventional solutions are not designed specifically to address API flows well, and usually leverage historical signatures and fingerprinting techniques to detect automated traffic on APIs. Dynamic user profiling is not enough for API protection. To avert highly sophisticated automated attacks on APIs, bot management solutions with layered detection methods - such as statistical communication analysis, navigation probability, and contextual scoring mechanism - is required. Such approaches assure a minimal rate of false positives, or in other words, no blocking of real users. In addition, as a business enabler – it is imperative that good bots will be let through.

Bot Management tools are first and foremost a business enabler and must not create "*noise*". Thus, to optimize user experience they must be designed for API invocation flows. This way it is environment-agnostic and can integrate into end-to-end automation efforts

Bot Manager for APIs
combines these technologies in its immediate response engine, deterministic engine, and machine learning modules to avert potential attacks. All three engines work together in unison with the Immediate Response Engine being the primary engine to respond to automated attacks. In the following sections, let's examine the role of this multi-layered protection system used to detect and mitigate automated attacks.

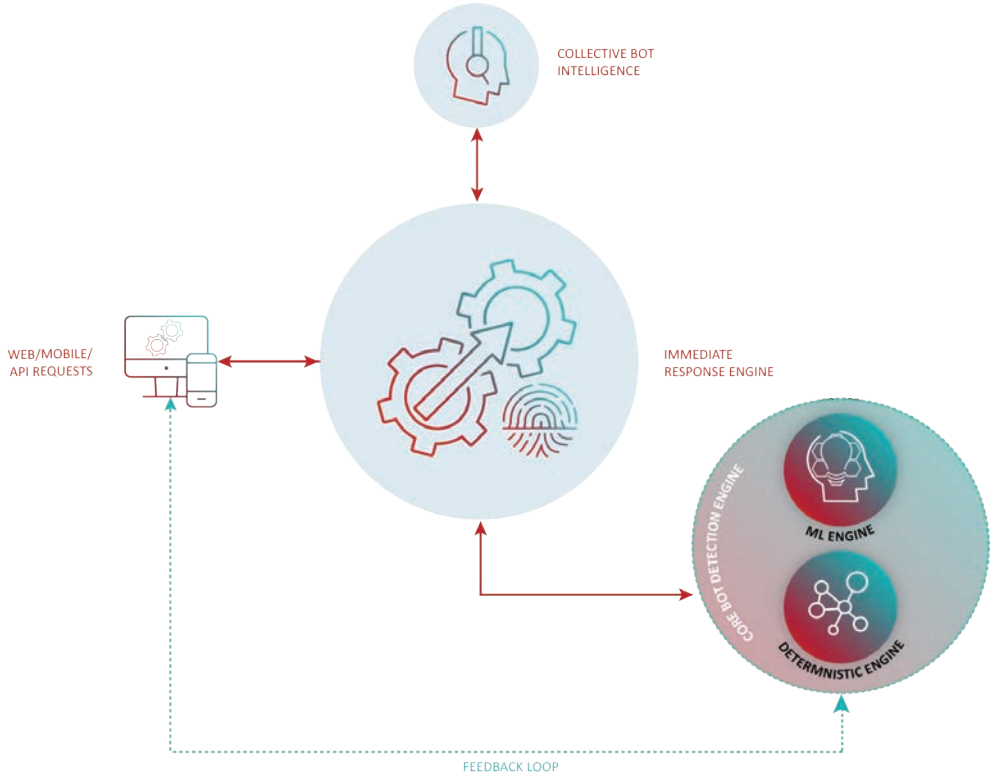


Figure 1: Radware Bot Manager's Core Bot Detection Engine

Immediate Response Engine

The immediate response engine responds to a suspected visitor as soon as it detects non-human activity, mostly on the first hit. Powered by deterministic and ML engine, Immediate Response Engine responds to a suspected visitor as soon as it reaches the web application servers. The module works in collaboration with ML and deterministic engine to respond to potential threats expeditiously. The immediate response engine is aimed at stopping bots on their first hit. As figure 1 suggests, Immediate Response Engine responds to 70% of bad bots on their first hit.

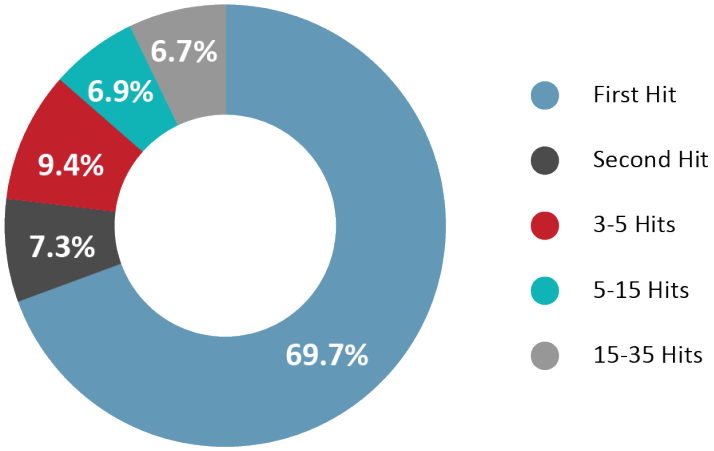


Figure 2: Bots Blocked by Immediate Response Engine — Based on Hits

Machine Learning Models

Machine learning models are crucial components in detecting and averting highly sophisticated automated attacks on APIs. For example, Radware Bot Manager for APIs relies on its proprietary ML models such as API Flow Control module, Invocation Context module, Authentication Flow Analysis, and Intent-based Deep Behavior Analysis. Radware Bot Manager's machine learning engine is built on a positive security model that continuously fine-tunes its system with mutating bot patterns and trends and ensures that subsequent requests are immediately denied access. Let us take a detailed look at how Radware Bot Manager leverages machine learning models to advance its automated attack detection and mitigation capabilities.

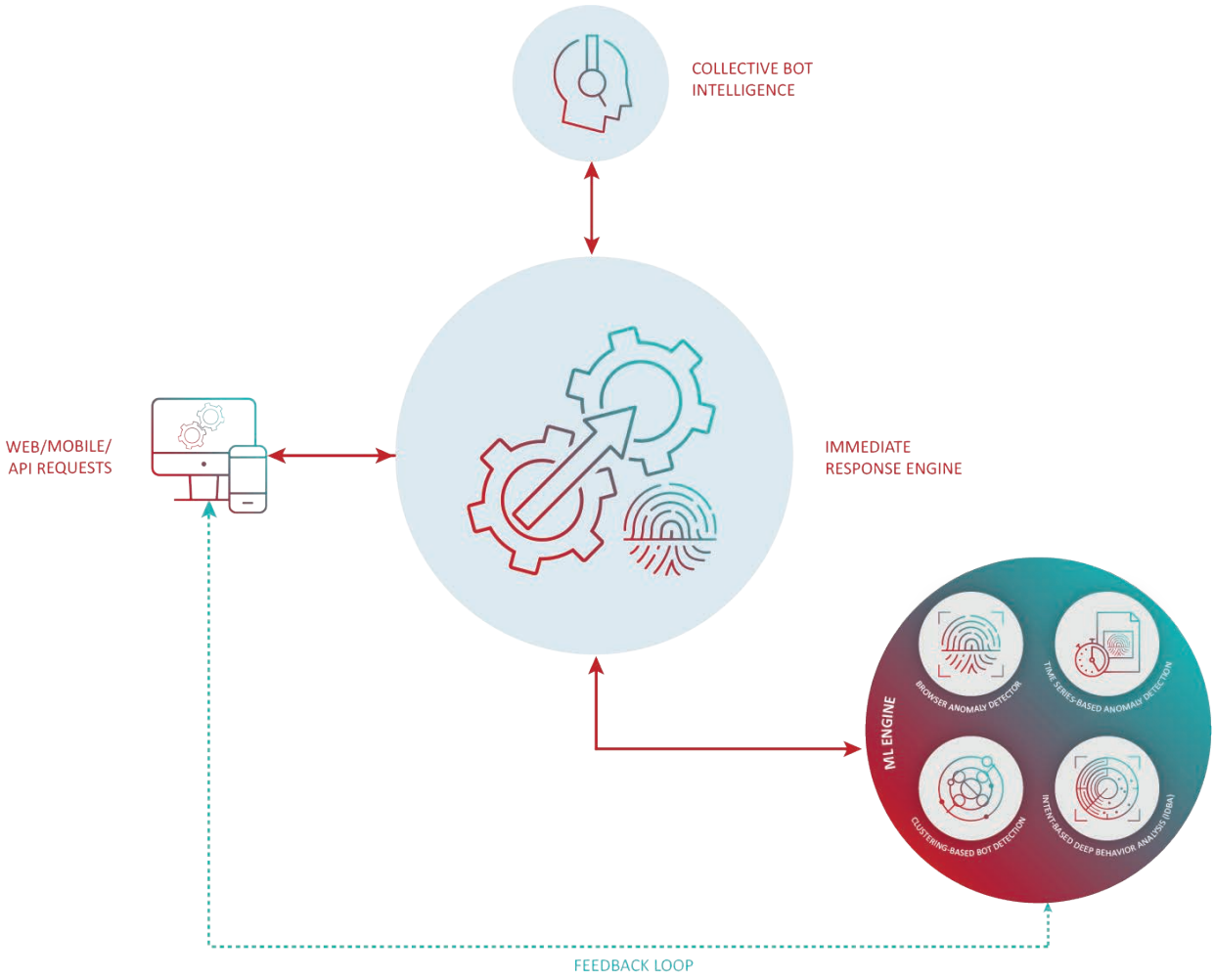


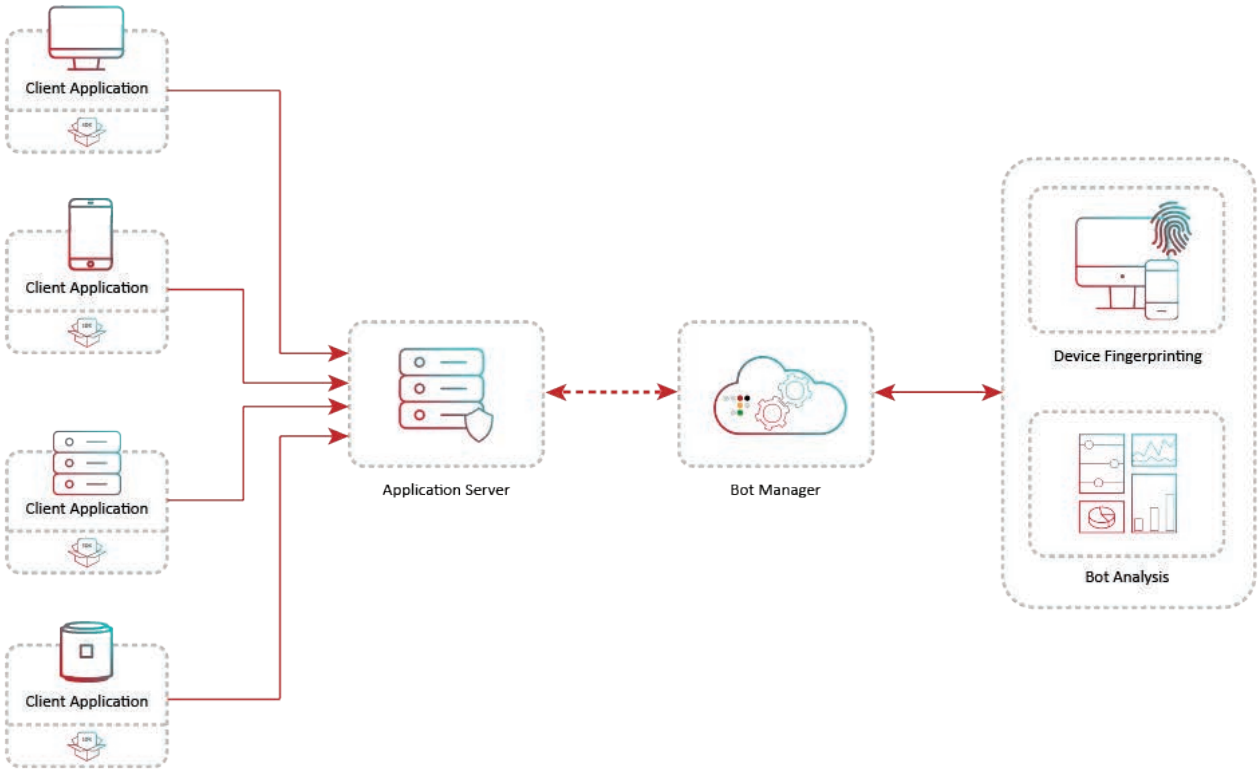
Figure 3: Radware Bot Manager's ML Engine

i. API Flow Control – Protect Machine to Machine & IoT

Detecting malicious behavior on APIs is different than web and mobile applications. On APIs, the distinction is between 'good' API calls and 'bad' API calls. A solution attempting to detect malicious behavior must be fine-tuned to understand machine to machine communication and detect anomalies in behavior. Bot Manager's API Flow Control module is based on a statistical model of API access that is automatically generated by studying the patterns of access during a period. It is based on modelling the API flow between different API endpoints and expected probabilities of transition across different nodes. Once the model is ready, ongoing access patterns are analyzed to check if the sequence is suspicious and blocked. The module provides you with a powerful way to identify malicious API access patterns and strengthen overall API security.

ii. API Client SDK – Protect Machine to Machine APIs

Client SDK for M2M API Protection is another module that works on detecting 'bad' API calls. The module collects various API-specific parameters such as machine architecture, CPU details, etc. to differentiate between genuine and malicious API calls. In this step, each API is a node and the probability of flow navigation from one node to the other represented by the arch weight. Low probability flow is blocked. This module is significantly helpful in detecting malicious bots mimicking genuine API calls on your internet properties.



iii. Invocation Context – Protect Web and Mobile APIs

It is possible to identify malicious bots that target the APIs by looking at the overall invocation context and sequence through which a user is browsing. Many bots try to bypass the steps, such as a regular login, navigating through a set of pages before accessing the APIs to get information in the shortest possible time. Radware analyzes API traffic for the right context and disallows direct access to APIs without a previous web transaction or invocation from a mobile device. The module allows you to filter 'bad' API calls as soon as they initiate any communication.

iv. Authentication Flow Analysis - ATO Protection for APIs

Our Authentication Flow Analysis module allows us to intercept the response to authentication APIs. The module collects the relevant details from the authentication APIs forwards to our core bot detection engine for analysis. The process validates legitimate access to assets, detects unsuccessful login flow, and blocks attack source generating multiple unsuccessful API login attempts. The Authentication Flow Analysis is particularly useful in protecting your authentication APIs against sophisticated account takeover (both credential stuffing and credential cracking) attacks.

v. Intent-based Deep Behavior Analysis (IDBA, A Patented Technology)

Highly sophisticated automated attacks often go undetected by conventional mitigation systems because bots have evolved from basic scripts to large-scale distributed bots with human-like interaction capabilities to evade detection mechanisms. IDBA performs behavioral analysis at a higher level of abstraction of intent, unlike the commonly used, shallow interaction-based behavioral analysis. For example, the account takeover is an example of intent, while "mouse pointer moving in a straight line" is an example of an interaction. The visitor's journey through the web property is captured by analyzing the sequence of URLs traversed, the referrers used, and the time spent at each page. Obtaining intent yields substantially higher levels of accuracy when detecting bots with advanced human-like interaction capabilities. IDBA builds upon our research findings in deep semi-supervised learning.

Additional Protections by Radware Bot Manager

Deterministic Simulation Engine

One of the challenges faced by bot management vendors is a high volume of incoming traffic. Processing all the traffic through an ML engine and then determining their behavior increases overall response time. In an environment when an enterprise is under attack, a swift response is all that matters. Radware Bot Manager for APIs' strategy to use a deterministic simulation engine as the primary module together with Immediate Response Engine is focused on minimizing overall attack response time and detecting most of the bad bots on their first hit. Radware Bot Manager's deterministic simulation engine is a data-driven module. It relies upon deterministic rules based on HTTP headers and JavaScript data collected from the end user's device to detect sophisticated malicious behavior.

Integrity Checks

Due to the flexibility of APIs, it is common to expose some of them to third-party applications outside the organization. Cybercriminals exploit exposed APIs to steal PII and other business-critical data. For organizations maintaining personal and financial data, any form of data exposure can lead to loss of revenue and reputation. Radware performs advanced integrity checks to identify bots and emulators and attempts to reverse engineer the mobile SDKs or access exposed APIs. It also provides rate limiting based on multiple parameters to prevent token cycling and token distribution.

Collective Bot Intelligence

Collective bot intelligence combines threat intelligence gathered from our vast client base (spread across geographies and verticals) to build a unique database of bots and human fingerprints to strengthen the bot detection system. Our core bot detection engine leverages Collective Bot Intelligence to identify bots, flag them, and utilize the intelligence to proactively protect APIs.

Benefits

Dedicated Machine Learning

Flexible Deployment

Complete Protection

Granular Visibility

Conclusion

In today's automated threat landscape, adversaries are adept at evading security defenses. They have advanced tools, exploit kits, and deception techniques to program their bots to masquerade as humans and undermine information security solutions. They are constantly updating their attack methods to keep their bots effective. As API deployments increase, so do bot attacks using an arsenal of advanced threats, taking advantage of unmonitored traffic flows and ungated access to sensitive data. As the attack surface expands, organizations will struggle to rise above the chaos. To win the war with bot herders and the sheer volume of bots they face, defenders need to go beyond a one-size-fits-all solution and need to deploy a dedicated solution such as Radware Bot Manager for APIs that combines problem-specific machine learning models to deal with ever-increasing sophisticated bot attacks on APIs.

About Radware

Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, acquired ShieldSquare in March 2019. ShieldSquare is now Radware Bot Manager.

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

radware

www.radware.com | www.shieldsquare.com