Bot Management

Why It’s Important and Why Akamai Is a Leader.
The Forrester New Wave™: Bot Management Q1 2020 Names Akamai a Leader

The Challenge of Bot Management

Up to 75% of a website’s traffic can be automated.¹ A lot of this traffic – search engines, virtual assistants, and chatbots – have legitimate purposes and provide valuable benefits to your business.

However, more than half of the bots on the Internet are what we call “bad bots.”²

Some scrape unprotected, sensitive information or scan for vulnerabilities. Others attack your applications and APIs.

Working alone or in coordinated botnets, bad bots can take over accounts, steal and exploit customer data, commit fraud, and disrupt your business. The most sophisticated of these bad bots mimic human behaviors, evade bot challenges, and even take over browsers and tokens.

According to Forrester Research, “evolving bad bot attacks require sophisticated solutions.”³

Findings from The Forrester New Wave™: Bot Management, Q1 2020

A new report, The Forrester New Wave™: Bot Management, Q1 2020, evaluates 13 emerging bot management providers on 10 criteria – seven based on product functionality and three on strategy.

In naming Akamai a Leader, the report informs security professionals and other readers that Akamai:

Leads the pack with robust attack response and reporting capabilities. Akamai offers a wide range of predefined and configurable attack responses, including tarpit, honeypots, and custom deny. Their Bot Intelligence Console provides information on individual bots, and benchmarks bots according to industry and against the entire Akamai customer base. Akamai maintains a directory of about 1,500 legitimate bots and business services.
Akamai received a “differentiated” rating – the highest possible – in the Attack Detection, Attack Response, Management UI, Reporting and Analysis, Feedback Loops, Performance Metrics, Roadmap, and Market Approach criteria.

That’s eight of the 10 criteria that Forrester evaluated.

**More Data to Detect and Protect Against More Bots**

Data is a key to the success of any bot management tool. If you have more data, you can detect more bots. You can be more accurate in your detections. You can accelerate the identification of new bots and new bot behaviors. And you can alert your customers and adapt defenses faster.

Akamai has more data than anyone else.

On a typical day, the Akamai Intelligent Edge Platform interacts with 1.3 billion devices. This traffic generates an unmatched data feed to the advanced machine learning algorithms built into our bot management solutions. At the same time, we tune these bot detections to drive a level of accuracy only Akamai can deliver.

The result is a cloud-based bot management solution designed to readily adapt its protections to changing threats.

**Unparalleled Scale to Stop the Largest Attacks and Minimize Performance Impact**

Because Bot Manager runs on the Akamai Intelligent Edge Platform, there’s more computing power, memory, and bandwidth to inspect traffic for threats without degrading user experience.

On average, Akamai detects more than 480 million bot requests per hour and 280 million bot logins – credential stuffing attacks – per day.

The platform architecture also lets bot manager readily scale to deflect extremely large bot attacks. Even multi-vector, multi-type attacks.

Akamai once defended a transactional bot attack that peaked at around 11,000 requests per second. This took place during a high-profile sales event. The attackers attempted to overwhelm the bot management solution in order to get through to the site and buy limited-edition goods for gray market sale.

Akamai also once defended a DDoS attack that peaked at 1.35 Tbps, 4 sending packets at a rate of 126.9 million per second.
How Akamai’s Bot Management Solution Works

Akamai’s lead bot management product, Bot Manager Premier, combines the visibility and scale of the globally distributed Akamai Intelligent Edge Platform with bot-specific capabilities to identify, categorize, manage, and report on bot traffic.

Using a combination of Akamai’s visibility into worldwide bot activity, custom bot signatures, and the real-time detection of unknown bots, Bot Manager identifies bots as they connect to websites through the closest Akamai edge server.

Bot Manager also gives organizations the flexibility to manage identified bots individually or to create categories of bots. You can then assign different management policies based on the desired interaction with each bot or bot category.

To help you with this tuning, the Security Center dashboard and built-in Bot Activity and Bot Analysis reports help you build a better understanding of bot traffic and its impact on your business.

Key Bot Manager Capabilities

- Leverages bot intelligence from a continuously updated directory of more than 1,500 known bots in 17 categories that commonly interact with Akamai customers
- Manages bots by reputation, based on past activity across all Akamai customers, including many of the world’s most heavily trafficked and attacked websites
- Detects unknown bots through behavior analysis, browser fingerprinting, automated browser detection, HTTP anomaly detection, high request rate, and more
- Automatically updates, through machine learning, the characteristics and behaviors used to identify bots based on observations across the entire Akamai platform
- Tunes to your bot traffic, using custom bot signatures and categories to identify and assign actions to bots that regularly interact with your website
- Enables business-oriented policies that apply different management policies to different categories of bots, in order to achieve business and IT outcomes
- Manages bots with a wide range of actions that can be applied to different types of bots, including alert, block, delay, serve alternate content, and more
- Fine-tunes management by assigning different actions based on the URL or time of day, or by percentage of traffic
Additionally, Bot Manager Premier offers optional:

- Security information and event management (SIEM) integration, to enhance visibility into all web traffic by integrating event logs with your SIEM tool
- Protection for mobile apps and APIs against automated bots, by integrating Bot Manager’s bot detections into your native mobile app
- Site Shield to hide your application origin from the public Internet, to help prevent bots from bypassing the cloud-based protections and directly accessing the origin
- Readiness and Response Service, to bring dedicated Akamai experts to regularly analyze bot traffic and update Bot Manager configurations as needed, and provide emergency support for discovered security events

Access the full report, courtesy of Akamai

The Forrester New Wave™: Bot Management, Q1 2020 report methodology includes inviting vendors to participate in an RFP-style demonstration and interviewing customer references. It’s an invaluable resource for security and technology leaders looking to protect their enterprises.

Read Now

Sources

2) For more information, see the Forrester report New Tech: Bot Management, Q4 2019.
3) The Forrester New Wave™: Bot Management, Q1 2020
4) https://www.wired.com/story/github-ddos-memcached/

Akamai secures and delivers digital experiences for the world’s largest companies. Akamai’s intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai’s portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world’s top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 3/20.