AKAMAI PRODUCT BRIEF

Bot Manager

Who do you trust? Just as important: Who trusts you? You need to trust that the consumers, partners, and bots on the other side of online transactions are who they say they are. Unfortunately, many bots — which can account for up to 70% of site traffic — try to impersonate legitimate users, steal your intellectual property, and harm your operations. Akamai Bot Manager gives you visibility and control over bots to help you guard your business and, in turn, protect the trust in your online relationships.

Companies increasingly implement good bots for efficiency online — automating interactions with consumers, partners, suppliers, and third parties. You must manage the impact of those bots on site performance and customer experience.

Scammers and criminals are also automating more. They're scaling botnets to:

- Grab inventory before customers can buy it
- Launch credential stuffing attacks
- Steal loyalty points and gift cards
- Exploit business logic vulnerabilities
- Attack the business to slow sites and increase costs

With bot operators working so hard to harm you and your customers, how do you now you can trust your online interactions? And how do you demonstrate trustworthiness to others?

Bot Manager's unmatched detections and mitigation capabilities allow you to run automated operations more effectively and safely, increasing trust for you and your entire ecosystem.

Trust starts with Akamai for bot management

You can trust Akamai because of our global strength, both technologically and as a corporation. We serve more than 50% of Global 500 organizations, have over 4,167 points of presence in more than 131 countries, and an annual revenue of more than US$3.6 billion. We bring all this strength to Bot Manager, continuously innovating to make sure it doesn't degrade over time and stays ahead of bot trends and evasion techniques.

BENEFITS FOR YOUR BUSINESS

Enhance trust: Yours and theirs
Know which interactions are legitimate, reduce friction for users, and protect them from fraudulent activity to fuel trust among consumers, partners, and you

Lessen the burden of remediation
Reduce the financial and resource drains of checking for compromised accounts, replacing stolen accounts, addressing user complaints, and other bot-attack fallout

Improve operational control
Enhance your efficiency, reduce business and financial risks, control IT spend, and strategically manage partner bots

Make better, data-driven decisions
Detailed analytics and reporting help you to make creative and effective choices about customer journeys, security posture, risk tolerance, and IT operations

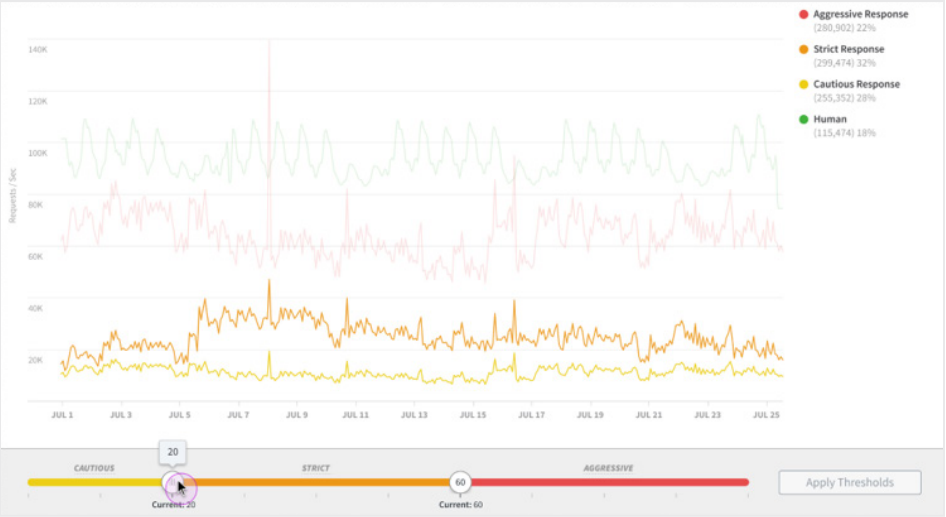
Akamai

Bot Manager uses patented technologies to detect and mitigate bots where they make initial contact instead of allowing them to reach your site first. And we constantly work to update your protection as threats evolve. We automatically incorporate insights from our threat intelligence researchers into Bot Manager's detections and analytics; you don't need to ask for any special upgrades or enhancements.

Bot Manager protects your company wherever others interact with you, including endpoints via web, native mobile apps, and APIs. We even protect you as a request crosses from one domain to another. If you have multiple brands or businesses, Bot Manager follows the initial request throughout the interaction so you don't have protection gaps.

Bot Manager AI framework

Bot Manager starts with an artificial intelligence (AI) framework that works inline on Akamai Connected Cloud. This allows Bot Manager to see the traffic at the edge, where a user first connects to an application — providing clean data on traffic patterns, traffic types, and traffic volume. Across the network, Akamai sees an average of 37 billion bot requests per day.



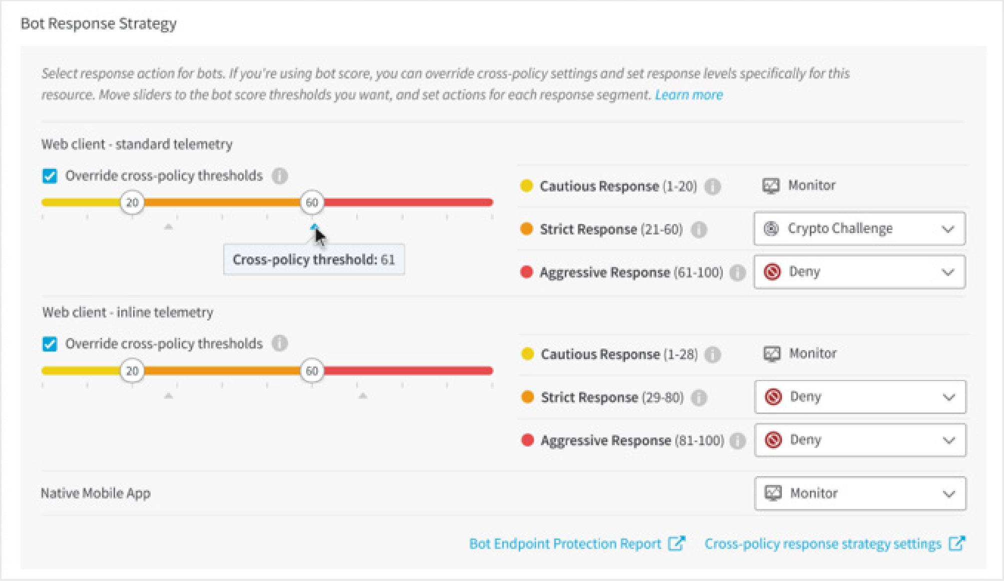
AI, machine learning, and threat intelligence

Collecting "clean traffic" data across a wide distribution of data types and in large volume trains our machine learning (ML) algorithms to make them more accurate. Across the Akamai network, we see traffic from 1.3 billion unique devices daily, with record traffic of 164 Tbps. This data visibility allows our algorithms to learn more and learn faster. And Akamai's team of more than 400 threat researchers constantly tracks trends in attack patterns, technology innovation, and new evasions in order to improve our detections. Akamai threat researchers analyze 662 TB of new attack data every day — up from 290 TB in 2021.

In addition to Akamai's robust AI and ML techniques, we're now providing the capability for customer-specific models. These deep learning models study the most sophisticated attacks that we see on highly targeted, big-brand websites. The model then casts the learning into advanced algorithms to implement mitigations against novel attacks in minutes rather than the days and weeks it takes other methods.

Bot Score — Evaluate every bot with every detection

Bot Score holistically combines all the detection triggers to identify sophisticated bots and give you a more accurate assessment of each request, optimizing the overall detection efficacy of the system — all without adding latency. And it gives you the ability to define a response strategy based on score ranges.



Bot Response Strategy

Select response action for bots. If you're using bot score, you can override cross-policy settings and set response levels specifically for this resource. Move sliders to the bot score thresholds you want, and set actions for each response segment. Learn more

Web client - standard telemetry

☑ Override cross-policy thresholds

Cross-policy threshold: 61

● Cautious Response (1-20)	Monitor
● Strict Response (21-60)	Crypto Challenge
● Aggressive Response (61-100)	Deny

Web client - inline telemetry

☑ Override cross-policy thresholds

● Cautious Response (1-28)	Monitor
● Strict Response (29-80)	Deny
● Aggressive Response (81-100)	Deny

Native Mobile App: Monitor

Bot Endpoint Protection Report

Cross-policy response strategy settings

Innovative challenges

Combining Bot Manager's Bot Score capability with cutting-edge challenges gives you the comfort to automatically take action using predefined thresholds and response actions. Move the burden of proof from legitimate human users to bots using our invisible-to-humans challenges. The crypto challenge forces bots to spend CPU cycles on minimum-time-to-solve cryptographic puzzles, slowing sophisticated bot attacks to a crawl and driving costs up for the attackers. The interstitial challenge requires clients to prove they support storing cookies and executing JavaScript. If not, Bot Manager enforces a time penalty plus whatever response action you choose as a mitigation.

Network-effect attack protection

We protect some of the largest and highest-profile companies in the world, which are often the targets of the most advanced bot operators. If a new bot is detected at one customer, the data about the bot is added to both the known-bot library and our unique "catapult algorithm" for all customers within minutes. This network effect doesn't just allow customers to manage bots effectively, it also allows us to preemptively stop some bots from attacking others at all.

Rapid, simplified deployment

Bot Manager's inline architecture allows you to deploy it quickly and seamlessly. And it's accurate from the moment it's turned on, detecting bots in real time with no latency or impact on site or network performance. Bot Manager also scales with you, using the Akamai network's massive capacity. What's the capacity of our network? Traffic on our network peaks above 100 Tbps every day, with an all-time peak of 261.21 Tbps on December 14, 2022.

Key capabilities

Known-bot directories — Bot Manager automatically responds appropriately to known bots, and we continuously update our current directory of 1,750 known bots.

Sophisticated, dynamic bot detections — Bot Manager accurately detects unknown bots from the first interaction using a variety of AI and ML models and techniques. They include user behavior analysis, browser fingerprinting, automated browser detection, HTTP anomaly detection, high request rate, and more. Bot Manager's dynamic obfuscation of code and telemetry protects against reverse engineering, keeping Bot Manager's effectiveness high over time.

Scoring model — The Bot Score model evaluates every request with every Bot Manager Premier detection. It then calculates the likelihood that the request is coming from a bot and issues a score from 0 (definitely a human) to 100 (definitely a bot).

Browser impersonation detection — Bot operators often try to impersonate certain browsers to evade detection. We've created our browser impersonation detection to be highly accurate without requiring regular tuning, so customers see fewer false negatives than with other detection methods.

Custom setting per endpoint — The Bot Score capability gives you the ability to set your strategic responses differently for each endpoint. For example, you can choose to apply the Cautious (watch/monitor) response to bots with scores of 35 or less on your search page but lower the threshold to 20 for requests on your login page.

Response tuning simulator — You can tune your strategic responses based on endpoint and on your organization's risk tolerance. Bot Score allows you to simulate your tuning before you put it into action — visualizing the impact of changing thresholds based on your past traffic.

Autotuning — Reduce the need for human intervention in tuning, even as bots evolve. Bot Manager learns the normal traffic patterns of your site(s) and automatically tunes detections based on your unique patterns to avoid potentially misclassified requests.

Nuanced response actions — Enhance your bot mitigation with actions that go beyond block and allow, such as serve alternate content, serve challenge, slow, and more.

Granular reporting and analysis — Make decisions based on trusted data with Bot Manager's real-time and historical reporting. Get visibility into big-picture trends and detailed analyses of individual bots or other segments of your bot traffic. You can also compare your bot traffic with others in your industry and across all Akamai customers.

Managed Security Service (optional) — Optimize Bot Manager without burdening your internal team. Dedicated Akamai experts monitor and provide proactive response recommendations, as well as deliver emergency support for discovered security events.

Risk-aware bot management

- Support corporate objectives by aligning your bot response to your firm's risk tolerance
- Modify score thresholds to match long-term goals and for individual events like flash sales
- Match strategic responses based on endpoint — for example, applying aggressive actions at lower risk scores for high-value endpoints

Contact your Akamai representative or visit Akamai.com to learn more.