WEBSCALE

DATASHEET

Webscale CloudEDGE Bot Manager

50% of Your Storefront's Traffic Could be Bots

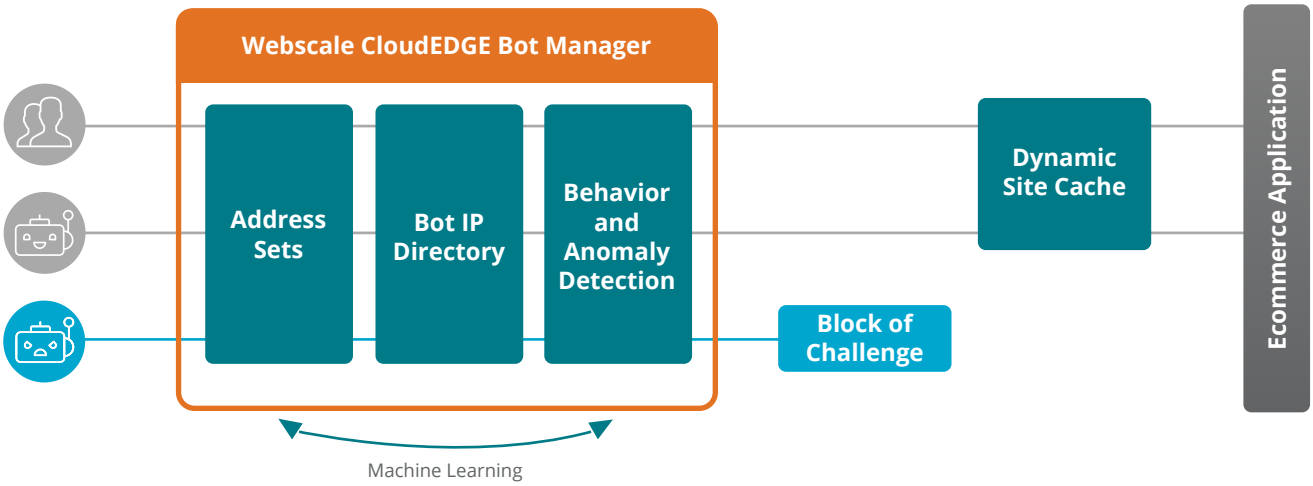
Bots comprise a significant portion of traffic to a web application. While some of these bots are good and help with the searchability of your site, many have malicious motives and can hijack your site (perhaps hold it to ransom), take over customer accounts, steal sensitive information like credit card details, cause DDoS attacks, or scrape valuable content (pricing, inventory, images and more) for the competition. All of this can significantly damage your brand reputation, customer loyalty, and competitive advantage, ultimately leading to a loss of revenue. Conversion rates and other business metrics, such as traffic volumes, can also be skewed by accounting for bad bot traffic, leading to misaligned investments, budgets, and website design choices.

While good bots should be allowed, bad bots need to managed or blocked. Hackers are becoming more sophisticated, designing their bots to bypass standard detection solutions, which means that bad bots will often masquerade as real humans, or other good bots, making them harder to identify. A comprehensive strategy and solution is required to manage bots, for better security and efficiency of infrastructure usage.

Webscale CloudEDGE Bot Manager

Webscale CloudEDGE Bot Manager offers 360-degree protection against the threat of malicious bots. A cloud-native security solution, CloudEDGE Bot Manager monitors the behavior of bots accessing any web-based application, identifies anomalous activity, and takes the appropriate action. The identification of good and bad bots is automated and occurs in real-time.

CloudEDGE Bot Manager is complemented by a 24x7 SecOps team that monitors security feeds and traffic, and rapidly distributes security learnings across its SaaS customer base of thousands of stores worldwide. This ensures Webscale customers are always up-to-date with the latest security protocols, even if their own site has not seen issues.



Product Benefits

Instant Attack Detection

Webscale CloudEDGE Bot Manager uses a combination of techniques to detect malicious bot attacks. These techniques include IP reputation-based filtering, user agent based identification, behavioral analysis based on machine learning (by tracking suspicious activity and behavior over time and across multiple accounts), anomaly patterns, browser tests (using JavaScript execution), and classification. Suspect behavior is dynamically added to the relevant Address Set to determine the appropriate action.

Real-time Bot Mitigation

All bots should not receive the same response in the form of a block. Once identified, bad bots can either be blocked proactively or, in the case of search crawlers, managed appropriately after they access the application. CloudEDGE Bot Manager challenges suspect bots to prove they are human, and administrators can then drop requests, delay responses, avoid scripts or limit suspicious sessions (Rate Limiting) to use the right amount of capacity. Scrapers can also be sent to an alternate backend or a site with inaccurate information or pricing.

Bot IP Directory

Webscale leverages a Bot IP directory, a dynamic database of approximately 10 million dangerous IPs updated every five minutes, powered by the Webroot BrightCloud® IP Reputation Service. CloudEDGE Bot Manager matches incoming web request IPs against this directory to identify and if desired, manage or block threats before they reach the application origin.

Intelligent Caching

Webscale's Dynamic Site Cache is automatically deployed close to the application backend, and enables caching of the entire website or a subset of it. When trusted good bots are requesting pages, these can be delivered from the cache without accessing the backend, improving performance by ensuring available capacity at the application backend for real human visitors.

Real-time Monitoring, Reporting and Management

Webscale's portal provides full visibility into bot traffic and offers proactive controls to prevent damage to the application or brand. A centralized management interface deeply integrated with website infrastructure enables users, of all skill levels, to analyze traffic and combat attacks. Reports can be generated to troubleshoot bot activity and understand the effect of bots on performance and infrastructure usage.

Key Features

Detect and Classify Bots by Behavior

Sophisticated bots often mimic real humans or good bots. CloudEDGE Bot Manager applies machine learning techniques to analyze traffic behavior, enabling the identification of suspect/bad bots.

Mitigate Bad Bots in Real-time

Malicious bot attacks can result in significant loss of brand, revenue, and customer loyalty. Secure your business from account takeovers, payment and credit card fraud, checkout abuse, inventory buyout, DDoS attacks, content and price scraping, and digital ad fraud.

Minimize False Positives

Validating human behavior, by issuing challenges, reveals bots with suspect intentions. Constantly refining these challenges allows for more consistently accurate identification of malicious bots, minimizing disruption to real users.

Improve Performance for all

Validating that bots identifying as good bots, such as Google bots, are real allows you to cache traffic so they can be served faster and outside the infrastructure. This filtering of bot traffic opens up capacity to improve performance for real humans accessing the application.

Multi-cloud capable and Cloud- and CDN- Agnostic

Webscale CloudEDGE Bot Manager integrates with all CDNs and Cloud Providers. While alternative Bot Management solutions are either expensive or require the use of premium CDNs, or both, Webscale CloudEDGE Bot Manager is CDN-agnostic and has a much lower total cost of ownership.

Improve Business Metrics

Bots make up a sizeable portion of overall user traffic. Business metrics, such as conversion rates, and traffic volumes, can be skewed by accounting for bot traffic, leading to misaligned investments, budgets, and website design choices. By filtering out bots from real human visitors, merchants can gather truly accurate data on clean traffic and genuine users, boosting conversion rates, while also improving SEO through caching of desirable responses for good bots.

Reduce Infrastructure Spend and Improve User Engagement

Bot traffic consumes unnecessary computational power and causes scaling of infrastructure. CloudEDGE Bot Manager improves the efficiency of the application infrastructure by offloading bot traffic. This leads to more efficient infrastructure usage, lower spend, and a better user experience, including faster page load times for real visitors.

Simple, Easy-to-use and Deploys in Seconds

CloudEDGE Bot Manager is programmable through Web Controls with customizable actions, all available in an easy, user-friendly DIY format through the Webscale portal. A single DNS change is all it takes to deploy the solution. CloudEDGE Bot Manager can also be deployed within a customer's cloud infrastructure in the form of a dedicated data plane to satisfy performance, security and manageability needs in enterprise use cases.