Solutions Brief

Protect your applications and websites from bot attacks with Citrix ADC

Automated attacks are on the rise. It is estimated that 38% of all internet traffic is bot traffic - and half of this involves bad bots attacking your vulnerable content and data. Your business is facing multiple bot attacks every day. This will strain your infrastructure, but the outcome can be so much worse.

Bot attacks on your applications cripple your business

Bots and botnets are employed to carry out many malicious activities against websites and applications. The attacks take multiple forms and can have a varying impact on your business. Some common attacks include:

- **Content scraping:** Your valuable content is at risk from bots that can copy it for illegitimate purposes. Pricing data can be stolen by rivals and used to compete against you. Your copy itself could be used to set up fake sites to siphon business away, and possibly harm your business's reputation.
- **L7 DDoS attacks:** More sophisticated than network layer DDoS attacks, bots exploit web applications to issue requests that exhaust your servers' ability to cope. This can prevent your applications from legitimate traffic and even take your applications offline. This of course can have a drastic impact on your business.
- **Account takeovers and fake accounts:** Criminals use bots in an attempt to gain access to accounts in the registered parts of your systems. Once an account is cracked your services can be abused, funds can be transferred and the personal data can be sold for profit. This can affect your business revenue and also leave you with legal exposure if personal data is breached.
- **Ad fraud:** Bots that "click" on your ads generate hits that you pay for but get no return. This can drive up your advertising costs and lower your ROI. It will definitely skew your marketing analytics.

- **Credit card stuffing:** Bots can attack your site and payment processes attempting to make small purchases to validate stolen credit card data. Not only can this put a strain on your resources but also lead to direct financial loss and possibly increased transaction charges from card vendors.
- **Inventory hoarding:** Criminals attack your site at the checkout stage and hoard your inventory in their shopping baskets. This prevents you from selling goods to real customers leading to financial loss. It can also affect your stock planning.

Citrix bot mitigation: A comprehensive, intelligent and integrated solution

Bot mitigation is built into Citrix Application Delivery Controller (ADC) as part of the overall security solution. It helps mitigate the effect of bad bots on your assets by identifying incoming clients as bots and then allowing you to filter them out. There are several mechanisms employed by Citrix ADC to detect bots of varying sophistication.

The simplest methods revolve around the IP address of clients.

- **Blacklist and whitelist:** Set up a blacklist of known bad bots to ensure that they are not allowed into your site. Similarly, you may want to whitelist good bots (e.g. comparison sites, search engine crawlers etc.) as they can be beneficial and promote your business.
- **IP reputation:** Because bots change IP addresses frequently. Citrix ADC has a built-in IP reputation filter that updates dynamically as new bot threats are discovered.
- **Geolocation data:** Use the IP address to determine the location of the client. If you don't have any audience in a particular geography you can block the traffic. More sophisticated bots require more intelligent detection methods that go beyond the IP address. Citrix ADC employs additional techniques to identify bot traffic.
- **Signatures:** Citrix uses request header information (IP address, source domain, user agent) to create a signature database of 3,500+ known bots. Incoming requests are checked against this to identify bot traffic.
- **Fingerprinting:** By identifying 34 different parameters, such as browser plugins, fonts, user agents and screen resolution, Citrix constructs unique fingerprints for client devices. Because human devices and bots have very different identifying criteria the fingerprint is a useful identification technique for more sophisticated bots.
- **Behaviour analysis:** Sophisticated bots emulate humans well. Citrix uses machine learning to establish your applications characteristics then spot behaviour anomalies to detect bots.

  For example:

  - **Client transactions:** Is it a reasonable number for a human?
  - **Data download:** Is the amount of data being downloaded outside normal parameters?
  - **Authentication success and failure rates:** Bots, especially those carrying out credential stuffing, will have a higher than normal authentication failure rate.

Take action on bots

Once bots are detected, Citrix provides a variety of mitigation mechanisms to prevent bots from straining your infrastructure and protect your applications from abuse.

- **Block:** Block the incoming traffic requests from a bot. This simple action stops bot traffic in its stride and will prevent attacks. It will also alleviate strain on your infrastructure and can reduce hosting costs.
- **Redirect:** Divert the requests to an alternate quarantined zone for further analysis and monitoring - e.g. a honeypot server.

- **Rate limit:** Rate limiting the requests from a client can help you control bot traffic and protect back-end resources from becoming overwhelmed.
- **Challenge:** When in doubt about a client's type, you can issue a challenge CAPTCHA to clarify and avoid false positives.

Determining whether traffic is human or a bot enables you to protect your applications from automated attacks. With Citrix bot mitigation you can defend your site against all sorts of different bot attacks. For example:

- Protects you from account takeover attacks by monitoring client authentication success and failure rates.
- Stop bots screen scraping your content by determining the rate at which requests for pages are being made.
- Use the Citrix bot and human ratio data to normalise important business intelligence data skewed by bot traffic for clearer decision making.

Flexible and simple deployment options for multi-cloud

Bot mitigation is available as part of the Citrix ADC offering and is included with the premium edition license. Citrix ADC is available in multiple form factors and in the major public clouds (AWS, Azure, GCP) to suit your deployment requirements. The single code base across the whole Citrix ADC portfolio enables you to maintain operational consistency across your deployments and applications. The single license approach, which includes security features including WAF, bot mitigation and API protection, brings simplicity and reduces TCO.

Keeping it simple lets you keep it secure.

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States