Shieldsquare Bot Detection vs Web Application Firewalls

At least 50% of the Web traffic is comprised of bots.

Bots are automated programs that can be created to execute a variety of tasks, both benign and malicious. In general, search engine bots are benign and bring in traffic and visibility to the website. On the other hand, bots created to execute malicious activities such as content scraping, price scraping, form spam, and so on, impact online businesses and degrade the websites' competitive advantage.

When will you need a bot detection solution?

Bots are a hidden danger, and in most cases, go unnoticed by the webmaster. However, as a CxO, if you notice any or all of the following, you need a bot detection solution:

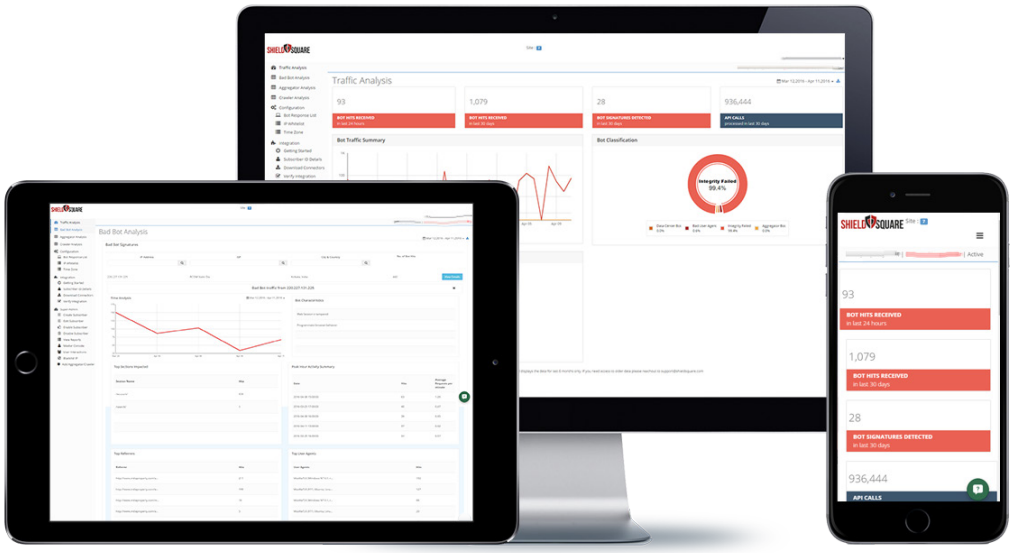
1. Fresh content published on the website appears elsewhere in minutes
2. Original articles are being outranked by other websites that stole your content
3. You block suspect IPs to stop scraping, but still lose content to scrapers from new IPs
4. Your closely guarded dynamic pricing information is being exploited by your competitor
5. Website performance slows down and affects genuine user experience
6. User interaction on forums interrupted with unwanted comments/advertisements
7. Increasing fake leads/registrations via online forms
8. Web analytics data skewed with bot visits, increasing bounce rates

Why a Web Application Firewall (WAF) isn't an effective bot detection tool?

WAFs are primarily created to safeguard websites against threats like SQL Injection, XSS/DDoS and other Web application vulnerabilities. Depending on the predefined firewall rules in the access control list (ACL), the incoming traffic is blocked, thereby stopping a potential security attack. However, if the incoming threat is from bots designed to steal your content, WAFs fall short of stopping such threats. Moreover, when scrapers and hackers that write bot programs use sophisticated techniques to go undetected, WAFs will not be equipped to protect your Web content.

ShieldSquare bot prevention solution protects your website and mobile content from hackers, scrapers and competitors. The table below compares the bot prevention capabilities of ShieldSquare with traditional WAFs.

Anti-Bot Features	ShieldSquare	Traditional WAF
Identify advanced bots	Yes	No
Detect emerging bot patterns	Yes. Bot detection engine constantly updated with new patterns/signatures identified by the data science team.	No
Risk of blocking genuine users (false positives)	Zero	High risk of blocking genuine users.
Collective bot intelligence	Yes. Bot fingerprints identified across multiple customers is made available in the database for faster, smarter bot detection	No
Tweaking bot prevention algorithms to suit business needs	Yes	No
24x7 vigilance for emerging bot threats	Yes. Multi-domain expert knowledge in advanced bot prevention techniques	No
Ability to take action against different categories of bots, based on your business logic	Yes. Implement your custom way of taking action against bots/bot categories	No
Deep insights on bots and custom reports	Yes. Bot categories, intent and the pages targeted are shown in detail. Customer reports available.	No



About Radware

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

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.

Trusted By Businesses Across 70 Countries

FUTURE
Connectors. Creators. Experience Makers.

axel springer

YELLOW PAGES™

zulily

Pearson