Guide

Bot Manager vs. WAF: Why You Need Both

Over 50% of web traffic is comprised of bots, and 89% of organizations have suffered attacks against web applications, according to Radware research. Websites and mobile apps are two of the biggest revenue drivers for businesses and help solidify a company's reputation with tech-savvy consumers. However, these digital engagement tools are coming under increasing threats from an array of sophisticated cyberattacks, including malicious bots.

While some bots are used to automate business processes and tasks, others are designed for mischievous purposes, including account takeover, content scraping, payment fraud and denial-of-service attacks. Often, these attacks are carried out by competitors looking to undermine a company's competitive advantage, steal information or increase your online marketing costs.

When Will You Need a Bot Detection Solution?

Sophisticated, next-generation bots can evade traditional security controls and go undetected by application owners. However, their impact can be noticed, and there are several indicators that can alert a company of malicious bot activity:

Sophisticated, next-generation bots can evade traditional security controls and go undetected by application owners. However, their impact can be noticed, and there are several indicators that can alert a company of malicious bot activity:

Fresh content is published on your website or app (prices, ads, account credentials, articles, etc.)

Website performance slows down and affects the genuine user experience

Original articles are being outranked by other websites that stole your content

User interaction on forums are interrupted with unwanted comments/ advertisements

You block suspect IPs to stop the scraping but still lose content to scrapers from new IPs

Increasing fake leads/ registrations occur via online forms

Your closely guarded dynamic pricing information is being exploited by your competitor

Web analytics data is skewed with bot visits and increasing bounce rates

Why WAFs + Bot Management Is A Critical Combination

Web application firewalls (WAF) are a cornerstone for safeguarding websites against application vulnerability exploitations like SQL injections, cross-site scripting (XSS), cross-site request forgery, server-side request forgery, session hijacking and other web assaults. When to it comes to bot management, WAFs typically come equipped with basic bot mitigation capabilities and can block bots based on IP addresses or device fingerprinting.

However, when facing more advanced, generation 3 and generation 4 bots, these aforementioned capabilities fall short. Next-generation bots use sophisticated techniques to remain undetected, such as mimicking human behavior, abusing open-source tools or generating multiple violations in different sessions.

Against these sophisticated bot-based threats, organizations require a more comprehensive solution.

The Benefits of Synergy

As the sophistication and array of both bot- and application-based cyberattacks increases, cybersecurity systems must work in concert to mitigate these threats by providing comprehensive protection. In the case of application security, a combination of behavioral analytics to detect malicious bot activity and a WAF to protect against vulnerability exploitations and guard sensitive data is critical.

Security Capabilities	Bot Manager	Traditional WAFs	Having Both
Protection from simple bots	Yes	Yes	Yes
Fingerprinting of malicious devices	Yes	Yes	Yes
Mitigation of dynamic IP and headless browser attacks	Yes	Limited	Yes
Detection of sophisticated bot attacks	Yes	No	Yes
Risk of blocking genuine users (False Positives)	Very Low	High	None
Collective Bot Intelligence (Ips, fingerprints and behavioral patterns)	Yes	No	Yes
Customized actions against suspicious bot types	Yes	No	Yes
Protection from OWASP Top 10 vulnerabilities	No	Yes	Yes
Protection from OWASP Top 21 Automated Threats to Web Apps	Yes	Limited	Yes
Protection from API vulnerabilities	Partial	Yes	Yes
Protection against Layer 7 denial of service (DoS)	Partial	Yes	Yes
HTTP traffic inspection	No	Yes	Yes
Masking of sensitive data	No	Yes	Yes
Compliance with HIPAA, PCI, & GDPR	Yes	Yes	Yes
Integration with DevOps	No	Yes	Yes
Blocking of malicious sources at the network level—access control list (ACL)	Yes	Yes	Yes

Why Having A WAF And Bot Management Solution From The Same Vendor Is Critical

1. Having bot management and WAF from the same vendor provides a unified and convenient overview for security teams
2. Superior integration of security tools that were designed for maximum efficacy when used together
3. Optimal compliance with HIPAA/ PCI/ GDPR is provided by integration of bot manager and WAF

Comprehensive, 360-Degree Protection

Web application and API protection (WAAP) is now the standard when it comes to protecting apps and APIs, according to Gartner's *Critical Capabilities for Cloud Web Application and API Protection* report. It is the preferred choice because it combines both broad scope and comprehensive security with ease of deployment at scale.

When evaluating application/API security solutions, organizations should have the four key capabilities of WAAP top of mind: web application firewall (WAF), bot management, API protection and application-layer DDoS protection.

Doing so means building a security strategy that provides comprehensive protection in multi-threat environments. It also helps ensure that your organization is moving beyond best-of-breed, point solutions that might be good at identifying and categorizing attacks, but provide limited mitigation functionality.

Learn More About Why Comprehensive Application Protection For Any Environment Is Critically Important

About Radware

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.