imperva

DATASHEET

Advanced Bot Protection

Protect your business and customers from automated threats and online fraud

The volume of automated threats on the internet today is continuously rising. In fact, over a quarter of all internet traffic is bad bots. Their sophistication level is also increasing, allowing them to evade traditional security tools and even sophisticated detection methods. These are not benign nuisances, they are purposely deployed with malicious intent to achieve specific goals, targeting businesses and their customers around the clock. Fraudsters, hackers, and competitors use bots to commit online fraud, break into customer accounts, gain an unfair competitive advantage by scraping prices and proprietary content and gain advantage over legitimate users. As the sheer volume and sophistication of bot attacks grow, so are the damages to businesses and their customers. These bots also place a costly strain on IT staff and resources.

Imperva's Advanced Bot Protection

A leader in the Forrester Wave™: Bot Management, Q2 2022, Imperva's Advanced Bot Protection safeguards mission-critical websites, mobile apps, and APIs from automated threats and online fraud without affecting the flow of business-critical traffic. By continuously monitoring online traffic, it protects every aspect of your web applications against any attempt at fraudulent activity. It defends customers against web scraping, account takeover, scalping, transaction fraud, gift card fraud, denial of service, competitive data mining, unauthorised vulnerability scans, spam, click fraud, and web and mobile API abuse. Imperva's unique, more holistic approach provides the vigilant service, superior technology, and industry expertise needed for full visibility and control over human, good bot, and bad bot traffic. As their ally in the war against bots, we provide customers with vigilant and dedicated support so that when they're under attack, there is a team of experts ready to help.

Figure 1: Advanced Bot Protection dynamic reporting provides visibility and control over abusive traffic

KEY CAPABILITIES:

Superior Online Fraud Prevention

Best-in-class bot mitigation

Protects websites, mobile apps, and APIs

Mitigates all OWASP automated threats

Delivers vigilant service as your ally in the war against bots

Industry expertise that understands the bot problem better than anyone else

SUPERIOR TECHNOLOGY THAT CATCHES MOR BOTS

Hi-Def fingerprinting analyzes over 200 device attributes

Deeper browser validation catches what others miss

Biometric validation leveraging both global and local machine learning models

Real time updates leverage data from our global network

Easily manage specific protection settings for each path

Set custom response options by threat or path

Bot management as adaptable and vigilant as the threat itself

Solves real business problems caused by bad bots

Bad bots are deployed by bot operators resulting in genuine business problems. Because Advanced Bot Protection identifies all the OWASP automated threats it provides genuine ROI to your business. From preventing fraud after credential stuffing and carding attacks, to reducing competitive scraping of prices the business benefits financially – and by removing unwanted bad bot traffic IT departments also spend less on infrastructure and time managing the bot problem, freeing them to focus on revenue generating business tasks.

Catch more bots with superior technology

Protects all access points exploited by bad bots by combining a multilayered detection process with community intelligence. Deep interrogation validates the browser and determines "are they human?". Next, machine learning algorithms learn your legitimate traffic patterns to pinpoint dangerous anomalies. As each device roams your website, Imperva collects and analyzes data about its behavior, then pinpoints anomalies specific to your site's unique traffic patterns. Ensemble machine learning models identify bad bot behavior across all Imperva protected sites, so that all customers can benefit from real-time threat intelligence.

Smart controls and custom reporting

If necessary, more aggressive settings can be activated across critical attack vectors, such as account registration forms and login screens. Smart controls let you manage your protection settings with precision – by path, domain or entire account. Choose your own bot responses including block, allow, CAPTCHA, force-identify, monitor, challenge, rate-limit, delay, tarpit and more. In-depth, custom reporting provides granular log-level analysis of over 100 data dimensions to reveal real-time answers to questions posed by bad bots within your web traffic. Schedule timely reports to be sent out automatically to all relevant stakeholders.

Your ally in the war on bots

Imperva provides you with vigilant and dedicated support. We understand that any attack, at any time, is a threat to your business livelihood. The reason we are a recognized industry leader is because of our expertise. We understand the bot problem better than anyone else. Our analysts have more years of experience fighting bad bots and automated fraud than competing bot defense products have been in existence.

IMPERVA WEB APPLICATION & API PROTECTION (WAAP)

Advanced Bot Protection is a key component of Imperva's Web Application & API Protection (WAAP), which reduces risk while providing an optimal user experience. Our solutions safeguard applications on-premises and in the cloud with:

- Web application firewall (WAF)
- API Security
- Distributed Denial of Service (DDoS) protection
- Account Takeover Protection
- Client-Side Protection
- Runtime Application Self Protection (RASP)
- Actionable security insights
- Security-enabled application Delivery

Learn more about Imperva Application Security at +1.866.926.4678 or online at imperva.com

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.

Flexible deployment

DEPLOYMENT MODEL	Integrated within Imperva's Application Security (Cloud or on-premise)	Connectors
ADVANTAGES	Ideal for companies seeking a single stack security solution offering CDN, WAF, DDoS and Advanced Bot Protection. • Defence-in-depth solution. • Imperva's best of breed solutions working together. • Best performance and availibility. • Fast deployment.	Ideal for Companies that want Advanced Bot Protection to quickly integrate with already deployed popular technologies. **Available Connectors:** AWS, Cloudflare, F5, NGINX, Fastly