imperva

DATASHEET

Advanced Bot Protection

Protect your business and customers from automated threats and online fraud

The volume of automated threats on the internet is continuously rising, as bad bots account for over thirty percent of all internet traffic. Their sophistication is perpetually increasing too, as bad actors devise novel techniques to evade traditional security tools and even modern detection methods. These bots are not benign nuisances; they are purposely designed and deployed with malicious intent, 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 an 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 Advanced Bot Protection

A three-time leader in the Forrester Wave™: Bot Management, Imperva 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, unauthorized 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.

KEY CAPABILITIES DISCOVERY

Market leading bot mitigation

Superior detection technology

Protects all access points, including deep integration with API Security

Mitigates all OWASP automated threats

Built and maintained by industry experts that founded the bot management category

Delivers vigilant services as your ally in the war against bots

MULTILAYERED DETECTION THAT CATCHES MORE 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

Comprehensive out of the box reporting

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.

Multilayered detection catches more bots

Imperva's multilayered detection approach combines a unique blend of cutting-edge technologies with human intelligence from expert engineers, threat researchers, and bot-focused analysts with more years of experience than anyone else. Beginning with hundreds of reputational models that leverage data from across our global network to an advanced set of proprietary challenges that deeply interrogate the client and user verification through biometrics collection. Dynamically trained machine-learning models are involved throughout every step and help tie everything together. 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

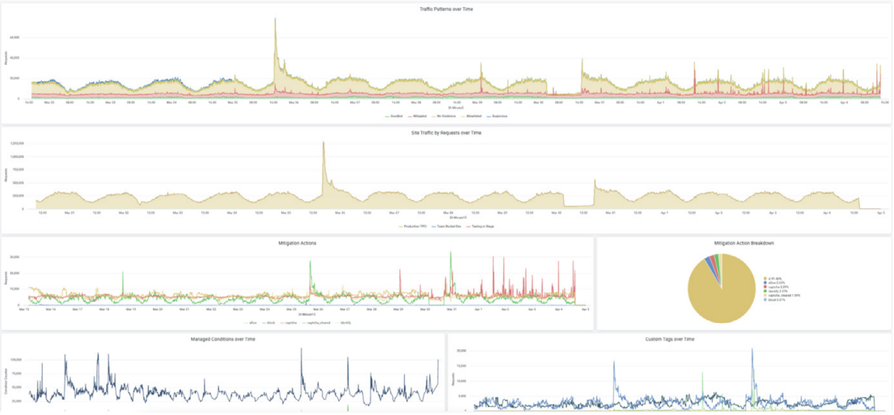
If necessary, more aggressive settings can be activated across critical attack vectors, such as account registration forms and login screens. Smart controls let you manage your protection settings with precision – by path, domain, or entire account. Choose your bot responses including block, allow, CAPTCHA, 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.

Deep integration with Imperva API Security

The Imperva Application Security Platform allows for deep integration of Advanced Bot Protection and API Security. This unified solution classifies APIs based on risk levels and enables seamless onboarding to Advanced Bot Protection. It provides increased security, granular customization, and efficient mitigation of automated threats and fraudulent activities on APIs. By approaching API attacks with an equal focus on bots, Imperva makes securing APIs exponentially more manageable.

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.



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. • Defense-in-depth solution. • Imperva's best-of-breed solutions working together. • Better performance and availability. • 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

IMPERVA APPLICATION SECURITY

Client-side 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

Advanced Bot Protection

Account Tekaover 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 at imperva.com

Imperva is the cybersecurity leader that helps organizations protect critical applications, APIs, and data, anywhere, at scale, and with the highest ROI.