imperva

CAPABILITY BRIEF

Advanced Bot Protection for AWS

Protects your website, mobile app, and APIs from automated threats

Today, the volume of automated threats on the internet is staggering—in fact over 20% of all internet traffic is bad bots. Many consider these bots as only a benign nuisance but in reality they are purposely deployed to achieve specific goals and target businesses around the clock. Fraudsters, hackers, and competitors use bots to commit online fraud, break into customer accounts, and gain an unfair competitive advantage by scraping prices and proprietary content. As the sheer volume, sophistication, and business damage caused by automated threats grows, bots also place a costly strain on IT staff and resources.

Imperva's Advanced Bot Protection

Imperva's Advanced Bot Protection protects mission-critical websites, mobile apps, and APIs from automated threats without affecting the flow of business-critical traffic. It defends customers against web scraping, account takeover, transaction fraud, denial of service, competitive data mining, unauthorized vulnerability scans, spam, click fraud, and web and mobile API abuse. Only 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. With Imperva, there is finally a defense against automated attacks that is as adaptable and vigilant as the threat itself.

KEY CAPABILITIES:

Best-in-class Advanced Bot Protection solution

Protects websites, mobile apps, and APIs from automated attacks

Mitigates all OWASP automated threats including account takeover, web scraping, and online fraud

Superior technology that identifies more bots

Delivers vigilant service as your ally in the war against bots

Industry expertise that understands the bot problem better than anyone else

KEY TECHNOLOGY CAPABILITIES:

Hi-Def fingerprinting analyzes over 200 device attributes

Deeper browser validation catches what other 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

Advanced Bot Protection 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 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.

Catch more bots with superior technology

Imperva's Advanced Bot Protection protects all access points used by bad bots including web, mobile and APIs. Deeper interrogation validates the browser and determines "are they human?" 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.

Smart controls to manage with precision

Smarter controls let you manage your protection settings with precision—by path, domain or entire account. Choose your own bot responses including whitelist, monitor, challenge, unblock form, or hard block. In-depth 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.

Vigilant service from your ally in the war on bots

As your partner in the war against 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 the 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 than competing bot defense products have been in existence.

Flexible deployment

The Imperva Connector architecture enables your enterprise to deploy Imperva's Advanced Bot Protection in any environment in the cloud. Connectors work with almost any technology stack and has proven deployments with leading CDNs, security tools, load balancers, and directly with Amazon Web Services (AWS).

IMPERVA APPLICATION SECURITY

Advanced Bot Protection is a key component of Imperva Application Security, which reduces risk while providing an optimal user experience. Our solutions safeguard applications on-premises and in the cloud with:

Web application firewall (WAF)

Distributed Denial of Service (DDoS) protection

Botnet attack mitigation

Runtime Application Self-Protection (RASP)

Actionable security insights

Security-enabled application delivery

Learn more about Imperva Application Security and our flexible licensing program, FlexProtect, 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.

Advanced Bot Protection
Proxy Layer in AWS

Your Origin
in AWS