imperva

SOLUTION BRIEF

Prevent Online Fraud

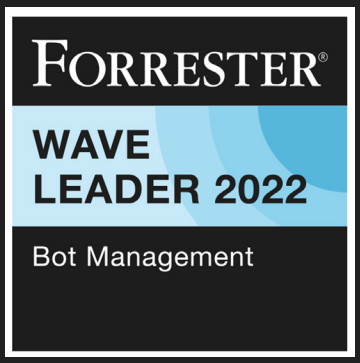
from bot and client-side attacks

The accelerated shift to digital payments has made online fraud more prevalent than ever, as losses from it are expected to exceed $206 billion over the next five years, driven by identity fraud, fake accounts, and payment fraud. Catalyzed by the pandemic, the shift gained substantial traction in 2021 as the popularity of digital payments skyrocketed, growing by 104% compared to 2020. Add to that the fact that the average person has over 100 online accounts and many stored payment methods within them, and this has created the perfect playground for bad actors. Organizations must ensure that they are able to detect and stop fraudulent activity on their applications.

ANALYST RECOGNIZED
A leader in The Forrester Wave™: Bot Management, Q2 2022

SUPERIOR BOT DETECTION TECHNOLOGY
Gain visibility and control over human, good bot, and bad bot traffic without imposing friction on legitimate users

CLIENT SATISFACTION
"Advanced bot protection stands in the way of bad actors"



Online fraud in the era of stealth data exfiltration and evasive automation

With an abundance of online accounts and transactions to attack, the techniques that bad actors devise to commit fraudulent acts online are constantly evolving to maximize profits. From sneaky client-side attacks that steal sensitive data to bots that leverage it for fraudulent acts, online fraud has evolved significantly, rendering traditional security tools ineffective. As financial incentives grow and attack costs decrease, the risk for your business increases.

The digital transformation has created the ideal playground for fraudsters

More consumers to protect

The pandemic has accelerated the shift to digital payments. With more accounts and transactions to protect, the risk of fraud grows.

Fraud has become commoditized

The ease of purchasing leaked credentials and card numbers online, then renting bot infrastructure to test and verify them against websites has increased the lucrativeness for online fraud.

Bots are getting smarter by the day

Bot attack techniques and tools are constantly evolving, allowing them to sneak past traditional bot mitigation measures and commit online fraud.

The fraud assembly line has evolved

Client-side attacks exploit compromised JavaScript to steal sensitive data. That stolen data is then used to feed bots performing automated fraud and account takeovers.

Online fraud prevention must constantly adapt to the ever-shifting threat landscape

Protect while preserving customer experience

Stopping automated fraud requires state-of-the-art detection that ensures legitimate consumers always have availability.

Safeguard your customer accounts

Gain clear visibility into attack attempts, leaked user credentials, compromised user accounts, and successful login attempts.

Ensure consumer data privacy

Prevent compromised third-party JavaScript from stealing your customers' data by simply blocking any unapproved third-party code.

Your ally in the fight against automated fraud

Dedicated support from analysts that are subject matter experts in automated fraud, with years of experience fighting bad bots.

How Imperva helps prevent online fraud

Advanced Bot Protection

Protect websites, mobile apps, and APIs from automated fraud without affecting your legitimate users.

Account Takeover Protection

Proactively block account takeover fraud and inform consumers before they are victimized.

Client-Side Protection

Prevent online fraud from website supply-chain attacks like formjacking, digital skimming, and Magecart.

"Prior to using Imperva Bot Management, we were seeing up to 30 attacks per month. We've only had two instances of attempted brute force attacks since we installed Imperva. In both cases we were able to mitigate the issue within seconds rather than hours."

Shaun Clark,
Head of Infrastructure, Betfred

BENEFITS OF ONLINE FRAUD PREVENTION FROM IMPERVA

Reduce costs

Minimize the direct and indirect costs of fraud – reduce chargebacks and customer support costs, and free your IT team to focus on revenue generating tasks.

Buy-down risk

Reduce the risk of noncompliance with data privacy regulations such as PCI, GDPR, CCPA, and more.

Improve customer experience

Superior bot detection that doesn't compromise on customer experience. Block unwanted traffic without imposing unnecessary friction on your legitimate consumers and improve conversion rates.

Learn more about online fraud prevention at imperva.com