Ongoing Risk Mitigation for Websites

reflectiz
Third-Party Application Security

Reflectiz security solution protects websites from next generation third-party application threats, such as client side attacks, web skimming, data breaches and privacy violations.

Third-Party Risk Landscape on Websites

Emerging Threats for Online Businesses

Third-party apps on websites has turned into one of the toughest cyber-security challenges of defending websites.
No, these are not your apps, but still, they run on your website. Now guess what? Your organization is accountable for it all! Losing customer's confidence, financial loses and regulations, are only a fraction of it. Your website uses dozens of third-parties. All are running on the client-side, allowing attackers easily bypass organizational application security perimeters.

The British Airways Breach:
A Magecart attack, 500K victims in 15 days, $230 million record fine

The BA data breach through a third-party code on their website was executed by Magecart in June 2018 and was not detected for more than two weeks. In July 2019, UK Watchdog, ICO slapped BA with a $230 million record fine for violating GDPR regulations.

The Escalating Risks of Third-party Applications

Research indicates that over 50% of all online businesses have suffered data leakage emanating from third-party codes integrated on their website. Third-party apps are external entities installed on your website, allowing you to scale your business and technology. This covers, marketing and advertising tools, analytics and thousands of different JavaScript applications.

These integrated apps are beyond your control and could bring in additional untested code into your website. Due to the fact that most of these apps can't be tracked by traditional cyber-security controls, breaches can, and do, remain undetected for long periods of time, leading to massive damages and financial losses.

WAF Protection. Am I Secured?

The indirect nature of web third-party attacks occurring on the client's side remains undetected by website security tools such as WAF.

Why? WAF simply works the other way around, protecting the web application, not the client. Even seasonal scans and vendor questionnaires won't expose third-party issues.

GDPR and CCPA, Privacy Violations

Growing privacy regulation demands, relating to integrated third-party code on websites, have turned into a major concern for organizations.

Regulators today consider websites as controllers, that are require to govern their processors. Opening them up to sanctions and huge fines for privacy infringements.

Quick and easy solution, without a single a line of code

Your Safety. Our Mission

Reflectiz provides the best application security third-party solution, allowing your organization to stay one step ahead of the next emerging threat. Our advanced technology is designed to protect your website against client-side attacks and Magecart threat actors, form-jacking, GDPR/CCPA violations, and data breaches. It is also designed to detect vendor errors that can affect your website's security posture.

Let's Start. We Only Need Your Website's URL

Our solution is designed to fit your security demands and easily integrate with your business processes. We are committed to bring you the most relevant information and practical value from day one, all with no prior installation or production changes.

info@reflectiz.com | www.reflectiz.com

reflectiz
Third-Party Application Security

Reflectiz on-going third-party behavioral analysis, covers even the most challenging security blind-spots, bringing application security to the third-party risk landscape for the first time.

Web Third-Party Risk Protection From Day One

Reflectiz Unique Differentiators

- **Ongoing protection -** The Reflectiz platform produces a one-touch baseline, followed by a reoccurring monitoring process. Our continuous analysis allows us to identify risks on your website as they happen. This smart gap-analysis, ensures your organization will not be exposed to supply-chain attacks resulting from compromised third-parties.

- **Full inventory visibility -** Reflectiz provides an extensive third-party inventory and robust asset management platform. Thanks to our proprietary WWW methodology, we know exactly WHO the third-parties are, WHAT risks they create and WHERE the data goes. This essential overview is the most comprehensive third-party risk mapping technology for any application running on your website.

- **Nothing changes -** Unlike standard solutions, Reflectiz is the only third-party security tool that actually eliminates on-premise installation requirements. Our fully automated remote-browser technology is the perfect plug & play that works without a single line of code or production changes.

- **Website Sandbox -** Reflectiz uses propriety browsing capabilities, offering dynamic behavioral analysis, *creating the first website sandbox*. This provides root cause analysis for the entire third-party web supply chain, up to fourth and the Nth chains.

- **Third-party intelligence -** Reflectiz' ability to analyze thousands of websites nonstop, produces the most up-to-date intelligence platform for web third-party risk detection, covering unfamiliar threats and applications anomalies, as well as providing a global database of third-parties applications.

How web third-party risks threat your organization?

Supply Chain and Magecart Attacks - A third-party code running on your website is controlled remotely. Once attackers compromise your vendors, they can inject their malicious code and run it on your website, exposing your visitors to an invisible and undetected data breach.

Brand Reputation Vendor Side Effects - An installed third-party code is an integral part of your website, even if it isn't yours. Each error it makes, even simple hosting mistakes or an unvalidated certificate, can directly affect your website, your brand reputation and damage your user's trust.

Privacy, GDPR / CCPA violations - A third-party that runs on your website has access to your most sensitive user data and can easily extract it. According to the latest rulings and privacy regulations, organizations are considered as controllers when the third-party code is running on their websites. In such cases your organization can be liable and accountable unknowingly.

The Magecart Hacking Groups

The term Magecart refers to one of the fastest-growing cybercrime activities, leaving multi-million-dollar damages to organizations globally.

The Magecart "syndication" involves 7 to 12 different groups, with a record of over 2 million victimized websites, including British Airways, Ticketmaster, Newegg, Macy's to name a few. Magecart specializes in compromising third-party components and through it conduct supply chain attacks on websites.

reflectiz
Third-Party Application Security

Reflectiz offers a fully automated and dedicated platform that analyzes and protects your website. The monitoring process is completely transparent and has no effect on your website performance.

How the Reflectiz Platform Works?

The Reflectiz Analysis Process

SCAN Automated remote scan for the website, allowing discovery of the important website's pages and assets.

INSPECT In-depth page behavioral analysis performed by Reflectiz' designated proprietary browser.

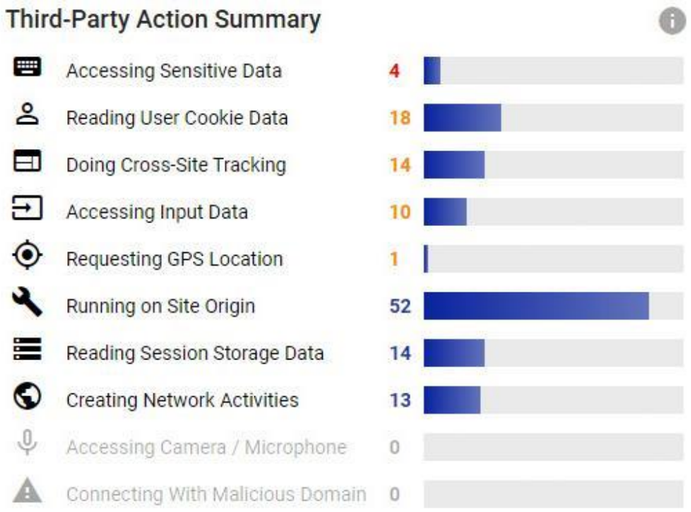
ANALYZE Big-Data analysis, including cyber algorithms procedures, global reputation sources.

SIMPLIFY Producing filtered results and actionable items for your internal SIEM/SOAR processes.

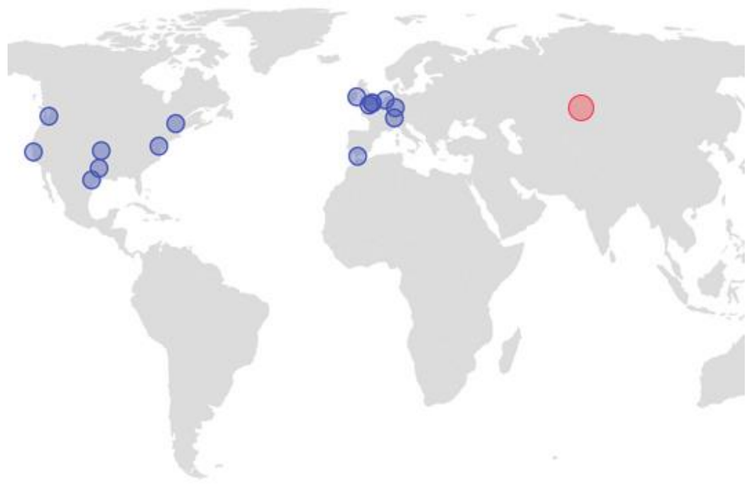
Alerts & Recommendations

All notifications and action items are provided on immediate basis to mitigate risks before they happen.

Each smart alert is tagged by severity level and includes a set of practical security guidelines for your website that address the business owner.



Action summary dashboard
Source: Reflectiz third-party risk scan results



Third-parties world map
Source: Reflectiz third-party risk scan results

Tailor Made Website Security Bundles

Each website has different functionalities and sets of challenges and risks.

To provide you the most accurate security package, Reflectiz created different bundles that are designed to address each client's specific needs, based on the data sensitivity, organization risk level, and online exposure.

Reflectiz at a Glance

Reflectiz brings an exceptional start-up spirit coupled with longtime security experience. This unique combination allows us to adapt to any new challenge, handle risks more effectively, and make sure that you will always stay one step ahead of any new threat.

Why Reflectiz?

- **We Know Cyber-Security from the Inside -** Year of experience of white-hat hacking, taught us to pinpoint exactly where the threats are.
- **We Keep it Simple** - Reflectiz has no setup requirements, no installation demands and no maintenance. Even our full SIEM compatibility is effortless, and yes - we do it all for you.
- **We are Cost-Effective -** Our cloud based solution is designed to save you time and money. We offer easy onboarding, instant results and immediate outputs. No extra or hidden costs, no production requirements and no maintenance at any stage.

Want to get a free non-intrusive website third-party security analysis?
Contact us

info@reflectiz.com | www.reflectiz.com