reflectiz
We Mitigate Third-Party Risks

Reflectiz provides advanced website security SaaS solution, allowing organizations stay protected against security breaches such as client-side attacks, data leakage and privacy violations, caused by installed third-parties code on their websites.

The Third-Party Risk Landscape on Websites

Online Business As A Target

Organizations are obliged to do everything in their power to protect their customers against malicious attacks and data breaches. This is by far the number one cyber-security challenge for online businesses today. Installed third-party code on websites allows attackers to easily compromise it, bypass most of the organizational security perimeters and conduct one-to-many attacks for sensitive data theft.

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

The BA data breach by a third-party on their website was executed by Magecart in June 2018 and was not detected for more than two weeks.
In July 2019, BA faced a record fine of $230 million by the UK ICO for GDPR violations.

One in Two Websites Has Already Been Breached

Research indicates that over 50% of online businesses suffered a data leakage involving an integrated third-party website code. These are all the external entities, installed on your website, covering variety of marketing and advertising tools, analytics, and thousands of different JavaScript applications. All are out there, beyond your control, integrated onto your website, directly or indirectly. All can hardly be tracked by common cyber-security tools. Breaches therefore remain undetected for long periods, creating huge damages and financial losses.

WAF Protection. Am I Secured?

The indirect nature of web third-parties attacks occurring on the client's side, remains undetected by website security tools such as WAF. Why? Because it simply works the other way, on the client's side behind the WAF eyes. Even seasonal scans and vendor questionnaire won't expose these type of third-party breaches.

GDPR and CCPA, Privacy Violations

Growing privacy regulation demands over integrated third-party code on websites, have turned into a major concern for organizations. Regulators today consider websites as controllers, posing them to sanctions and huge fines for infringements that also apply to malicious third-party access to their users' data.

Kickstart Your Web Third-Party Security With Reflectiz

Your Safety. Our Mission

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

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

Reflectiz, a zero-effort web third-party security SaaS solution offers remoted ongoing monitoring capabilities. It is especially built to fit your security demands, bringing you the most relevant information and practical value from day one. It requires no prior website installation or production changes. It only needs a URL

info@reflectiz.com | www.reflectiz.com

Visit our social channels: www.linkedin.com/company/reflectiz | Twitter: www.twitter.com/_Reflectiz

We Mitigate Third-Party Risks

With enhanced third-party on-going behavioral analysis for your website, Reflectiz covers even the most undetected vulnerabilities and risks, providing you maximum visibility, with no installation demands.

Web Third-Party Risk Protection From Day One

The Reflectiz Solution Unique Differentiators

- **Ongoing protection -** The Reflectiz platform produces a one touch baseline, followed by a reoccurring monitoring process of the entire third-party inventory on your website. Our continuous analysis allows us to identify risks on your website as they happened, ensuring your organization will not be exposed to supply-chain attacks resulting from compromised installed third-parties on your website.
- **Full inventory visibility** - Reflectiz provides extensive third-party inventory and robust asset management platform, all in one place, presenting extensive data of each third-party application, including its actions, networking, location, relationships and more. All with a friendly user interface and functional management capabilities.
- **Web third-party intelligence** - Reflectiz' ability to analyze thousands of websites nonstop, produces the most up-to-date intelligence platform of web third-party risk detection, covering unfamiliar threats and malicious JS, as well as providing global database of third-parties applications worldwide.
- **Dynamic Analysis -** Reflectiz uses propriety browsing capabilities, offering dynamic third-party client-side behavioral analysis. This unique examination reflects the relationship of each component and the entire third-party supply chain of the website, up to fourth and fifth parties and its in-depth action analysis.
- **Fully automated alert system** - The Reflectiz platform lets you stay in control 24/7, connected to your internal SIEM/SOAR processes, with no effort from your end. Each smart alert and notification provided, is automatically tagged according to the severity of each instance and includes a set of practical security guidelines for your website.

Reflectiz does it all without a single line of code modification or exhausting production implementations

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 hardly detected 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 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. This can lead your organization privacy violations and liability issues unknowingly.

The Magecart Hacking Groups

The term Magecart refers to one of the fastest growing cybercrime activities, leaving multi-million overall damage to organizations globally. The Magecart "syndication" involves 7 to 12 different groups, with a record of over 2 million victim websites, including British Airways, Ticketmaster, Newegg and other big names. Magecart specializes in compromising third-party components and conducting supply chain attack on websites through it.

info@reflectiz.com | www.reflectiz.com

Visit our social channels: www.linkedin.com/company/reflectiz | Twitter: www.twitter.com/ Reflectiz

We Mitigate Third-Party Risks

Reflectiz offers a fully automated and dedicated process that puts your website on spot and seamlessly analyze it. 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 designated proprietary browser.

ANALYZE Big-Data analysis and cyber algorithmics, including global reputation sources.

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

Tailor Made Website Security Bundles

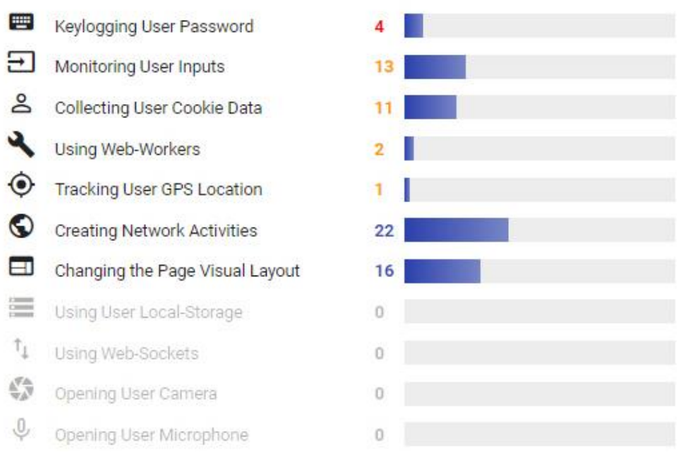
Each website has different functionalities and set of vulnerabilities in accordance.

In order to provide you the most accurate set of security tools, Reflectiz developed different packages, each is designed to address specific client needs, based on different types of website risk analysis.

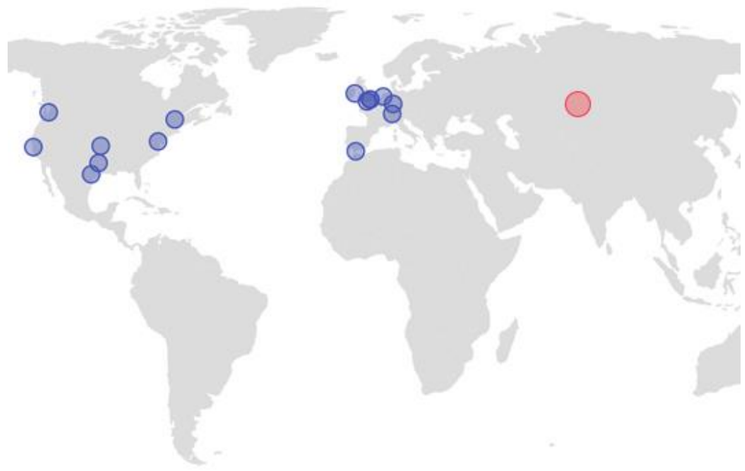
The solution packages are designed to fit websites that only require basic vendor risk assessment, or websites that have a strong need for near real-time third-party risk and supply-chain breach detections.

Matching has never been easier

Our team of dedicated third-party security experts will help you determine the right bundle, according to the risk factor and your exact needs.



Action summary dashboard.
Source: Reflectiz third-party risk scan results for a demo-site.



Third-parties world map
Source: Reflectiz third-party risk scan results for a demo-site.

Reflectiz at a Glance

Our ecosystem is structured from exceptional start-up spirit, longtime security experience and highly active cyber scene. This unique combination allows us to cope new challenges faster, handle risks more effectively, and make sure you will always stay one step ahead when a new threat comes.

Why Reflectiz?

- **We Are Cyber Oriented** - We offer exceptional cyber roots and unique security skills, ranging from ethical hacking to the most complex development challenges. Our solutions were developed and designed by security teams, for security teams.
- **Always Cost-effective** - Our philosophy combines efficiency and fairness. We save you time and money, offer fair price, no setup requirements and full SIM computability. It requires no initial installation or setup and no maintenance beyond it. Simple.
- **Immediate response -** We keep our startup spirit alive. We solve even the most complicated issues at no time, we're always, always(!) up to date, allowing you to stay one step ahead of the next threat.

Want to get a free non-intrusive website third-party risk analysis?

Simply contact us.

info@reflectiz.com | www.reflectiz.com

Visit our social channels: www.linkedin.com/company/reflectiz | Twitter: www.twitter.com/ Reflectiz