reflectiz
Third-Party Application Security

Reflectiz provides an advanced website security solution, allowing organizations to stay protected against breaches like - client-side attacks, data leakages and privacy violations, caused by embedded third-party code on their websites.

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 the number one cyber-security challenge faced by online businesses today. Attackers can compromise installed code on their websites and bypass usual organizational security perimeters, allowing them to conduct one-to-many attacks and steal sensitive data.

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.

One in Two Websites Has Already Been Breached

Research indicates that over 50% of all online businesses have suffered a data leakage emanating from third-party codes integrated on their website. Third-party code is an external entity installed on your websites, allowing you to scale your business and technology. This covers, marketing and advertising tools, analytics and thousands of different JavaScript applications. These integrated components are beyond your control, and could bring in additional unchecked code into your website. Due to the fact that that not all of these codes can 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 breaches.

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, opening them up to sanctions and huge fines for privacy infringements.

Kickstart Your Web Third-Party Security With Reflectiz

Your Safety. Our Mission

Reflectiz is dedicated to providing websites with the best third-party security solutions, allowing your organization to 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, and 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 remote ongoing monitoring capabilities. It is specially 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 LinkedIn page Visit our Twitter page

reflectiz
Third-Party Application Security

With enhanced third-party on-going inventory and 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 happen, 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 an 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 a global database of third-parties applications.
- **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 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 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.

info@reflectiz.com | www.reflectiz.com

Visit our LinkedIn page Visit our Twitter page

reflectiz
Third-Party Application Security

Reflectiz offers a fully automated and dedicated process that protects your website and seamlessly analyzes 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 Reflectiz' designated proprietary browser.

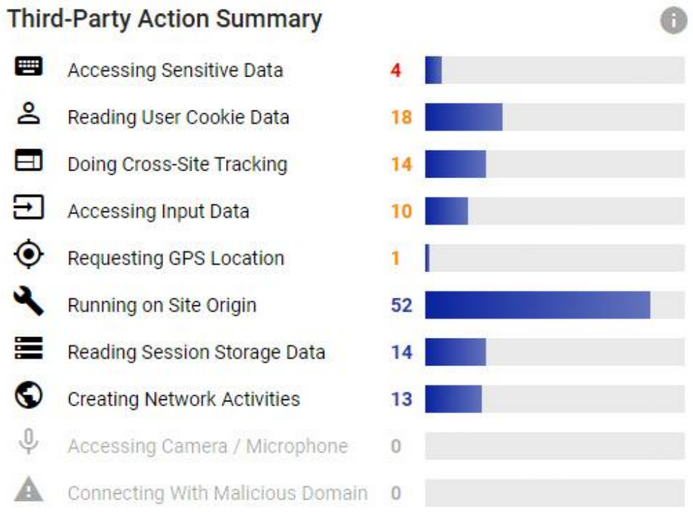
ANALYZE Big-Data analysis, including cyber algorithms procedures, global reputation sources

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

Tailor Made Website Security Bundles

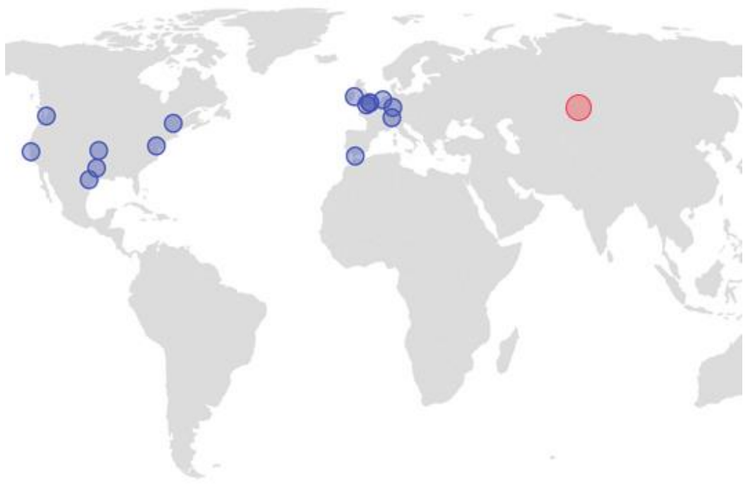
Each website has different functionalities and set of vulnerabilities.

To provide you the most accurate set of security tools, Reflectiz has developed different packages. These packages are designed to address each client's specific needs, based on the data sensitivity as well as various types of website risk analysis and vulnerabilities.



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.

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.

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 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 a fair price, no setup requirements and full SIEM compatibility. It requires no initial installation or setup and no maintenance beyond it. Simple.

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

Contact us

info@reflectiz.com | www.reflectiz.com

Visit our LinkedIn page Visit our Twitter page