PROTECT USER DATA & BE COMPLIANT

MONITOR AND BLOCK DATA LEAKAGE THROUGH THIRD-PARTY SERVICES

TALA

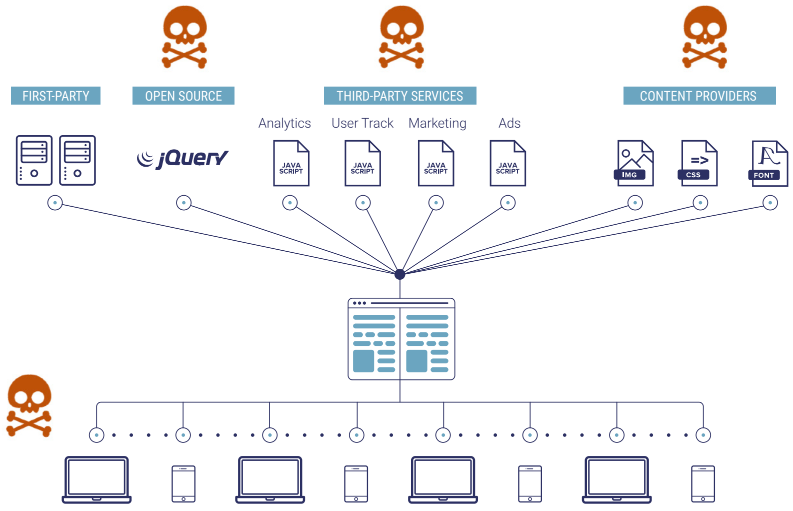
CHALLENGE

Enterprises are increasingly struggling to meet data protection and compliance regulations such as GDPR. Google was recently hit with a €50 million fine - GDPR violations could cost an enterprise up to 4% of its annual turnover in fines. Enterprise websites are one of the key sources of inadvertent user data loss or malicious user data theft, all of which could lead to significant business risk and potential regulatory violations.

What is the problem? Enterprise web sites and apps integrate code and resources from dozens of third-party service providers, all the way from user analytics, marketing tags, CDNs, to third-party JavaScript libraries, and many others (see figure below). In most enterprises, the Infosec organization has little visibility or control over these third-party service integrations.

The lack of adequate risk assessment and monitoring leaves enterprise websites exposed to data leakage. In particular, third- party services can have a direct impact on user data access and GDPR compliance:

- Without adequate monitoring, sensitive application and user PII data can be exposed to unauthorized third-parties. For e.g., third- party services could collect sensitive information such as credentials, passwords, SSNs as the user is typing them into forms. This could lead to a direct violation of data protection compliance rules (e.g., Article 32 of GDPR).
- Third-party services could allow "piggybacking" of other fourth--or fifth- party services that could expose the site to a broader attack surface that may go undetected.
- Without Infosec oversight, compromised or malicious domains could be inadvertently added to an enterprise site, leading to an overall website compromise. Vulnerabilities in third party scripts or open source libraries could be exploited by attackers.



SOLUTION

Tala's enterprise website security platform helps you monitor and protect user data, while staying compliant with GDPR and other regulations.

- **Understand your risks.** Tala's cloud-based app behavior analysis provides a comprehensive risk assessment to help you understand exposure risks related to sensitive user data.
  - Tala automatically enumerates all third-party sources where content, code and iFrames are loaded from on your websites. Tala captures fine-grained behavior of third-party JavaScript.
  - Tala automatically detects parts of the site where users input sensitive data, PII data etc., as well as third-parties that have access to the data.
- **Real2time protection and incident response.** If Tala's protection module is installed on your website, Tala monitors for anomalous data collection activity in the browser and blocks it in real-time.
  - Tala monitors third-party Javascript behaviors while they execute in the browser, ensuring that they are only collecting data that they should have access to.
  - Tala combines the power of threat intelligence, AI and our own fine-grained behavioral model to provide precise attack analytics and incident response capabilities.

FEATURES & BENEFITS

- **Comprehensive risk assessment:** Get comprehensive risk analysis of first-party and third-party (and fourth-party) integrations on the site.
- **Real-time detection and protection:** Monitor your application behavior on client browsers for anomalies and detect and block compromised third-party Javascript.
- **Full visibility into attack surface for incident response:** Tala uses AI to classify attacks and notifies your incident response team if the system has detected a Magecart-style attack.
- **Installs in minutes**: Tala installs in minutes on all major web server technologies without requiring any changes to the application and without requiring any user-agents.
- **No impact to performance:** Tala is not intrusive and adds minimal latency to page loads.