TALA

WHITE PAPER

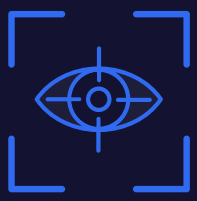
Tala Detect

Tala *Detect* is a highly sophisticated, continuous monitoring tool that provides fine-grained information flow analysis including data discovery, mapping, and violation alerting for enterprise sites.

Tala *Detect* also continuously monitors application behaviors and detects changes that equip administrators with insights and information to investigate and stop unauthorized content injection and JavaScript threats.

With **no need for integration** into the customer environment, Tala *Detect* continuously monitors web applications to detect malicious behaviors, code vulnerabilities and sensitive data exposure.

The Tala *Detect* Technology Platform

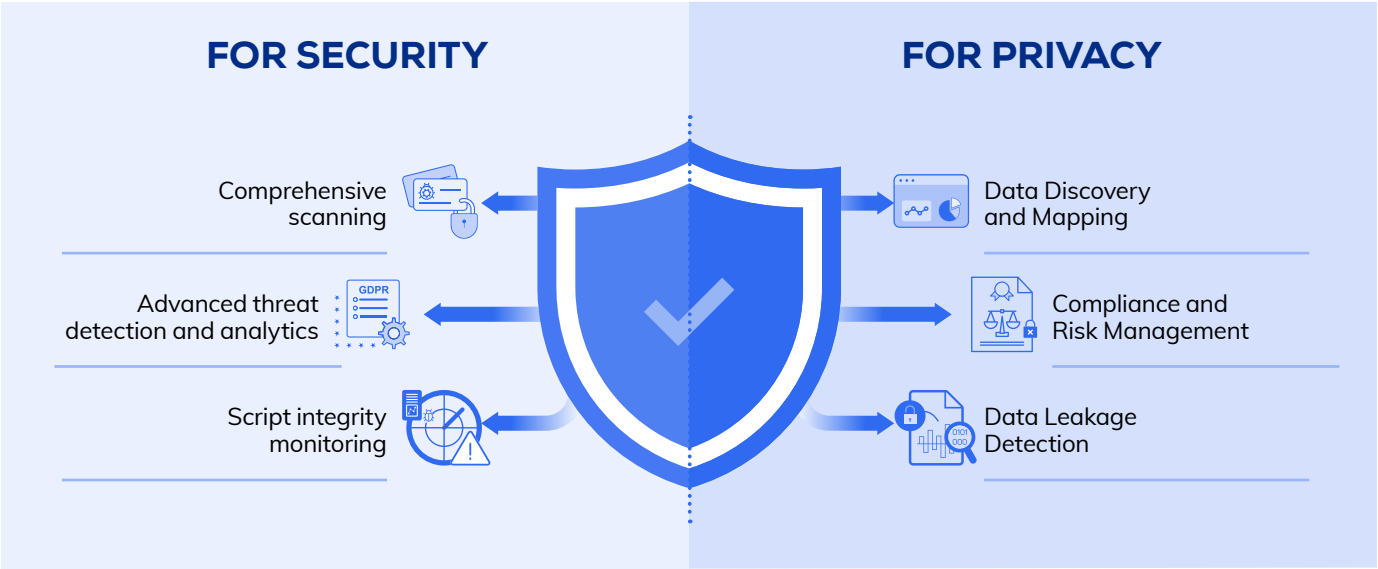


In-Depth Scanning

Data Discovery and Mapping

In-Depth Behavioural & Risk Analysis

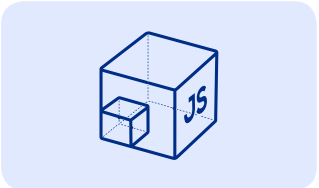
Threat Detection and Monitoring



1 In-depth and Comprehensive Scanning

Tala builds an Application Information Model (AIM) by automatically analyzing enterprise web applications to extract 150+ fine-grained, security-relevant behaviors on each page.

- **Analyze your website supply chain in minutes:** Identify all sources of content and code on your website, including static and dynamically loaded scripts and third-party integrations.
- **Gain comprehensive insight into sensitive data exposure and risk:** Tala analyzes all forms, cookies and storage on websites, including hard to reach pages.
- **Gain visibility into risky JavaScript constructs in your code:** Tala uncovers problematic constructs such as DOM XSS sinks, JavaScript URLs and other unsafe APIs.



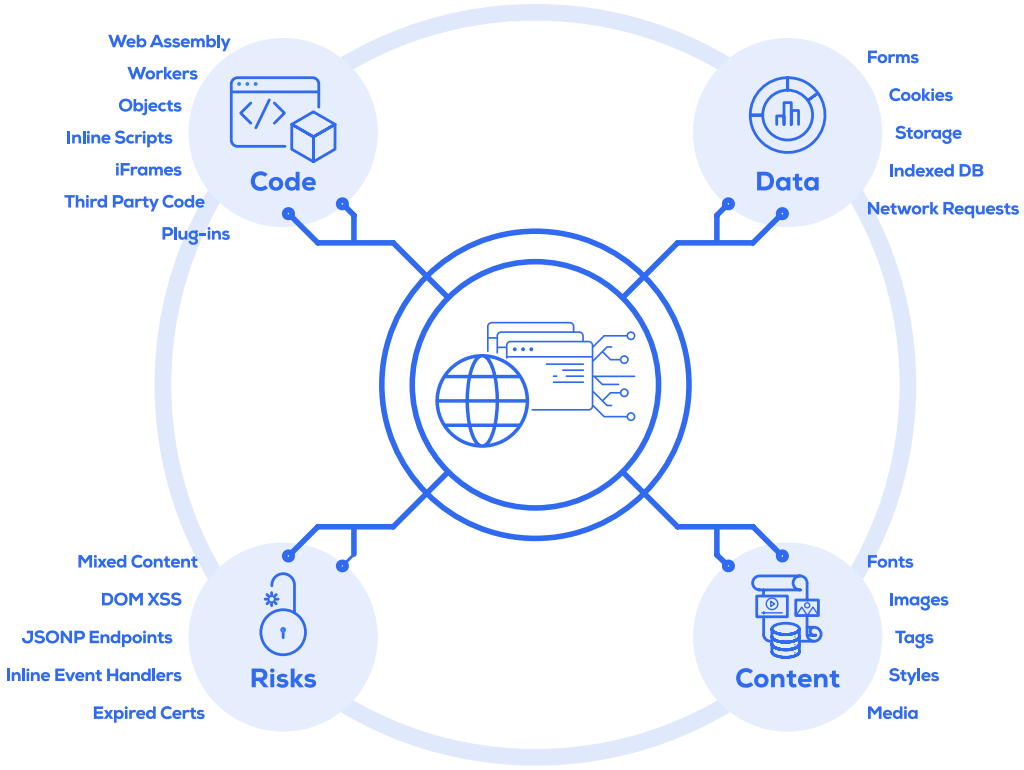
Fully dynamic scan (not just statically loaded JS)

Support for multiple authentication options

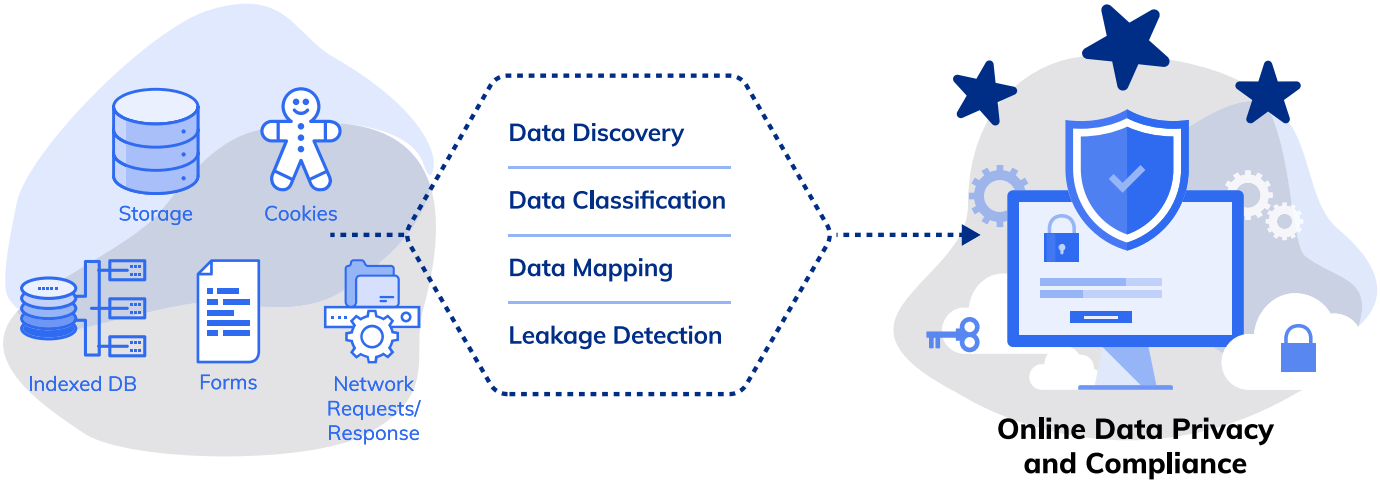
Captures complex workflows using synthetic transactions

API support for CI/CD integration

TALA



2 Sensitive Data Discovery and Mapping



Data Discovery

Network requests, indexed DBs, forms, cookies and storage are comprehensively and dynamically scanned to discover all sensitive data behind complex workflows using synthetic transactions and non inline JS virtualization techniques.

Data Classification

Tala classifies and captures sensitive data based on internal DLP dictionary as well as user defined sensitive fields to comprehensively discover data such as payment details, logins , contact details, passport numbers, and SSNs, etc.

Data Mapping

Tala uses non inline JS virtualization techniques to track data exposure, access and exfiltration and map the flow to third party, fourth party vendors and beyond.

Leakage Detection

Leakage initiation chain analysis is performed for every sensitive data flow, providing detailed insights into the data path for investigation and remediation, providing important contextual information for audits and compliance.

TALA

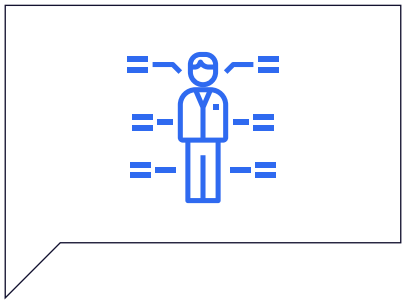
Tala identifies sensitive data in forms, cookies, storage, network requests, etc. and tracks it across three dimensions: exposure, capture and exfiltration/leakage

Tala's non-inline **synthetic JS virtualization technique** facilitates the detection of data leakage and inadvertent exposure without requiring inline deployment, insertion of external JS or impact to web application performance.

Access

Third-parties that have **access** to sensitive data

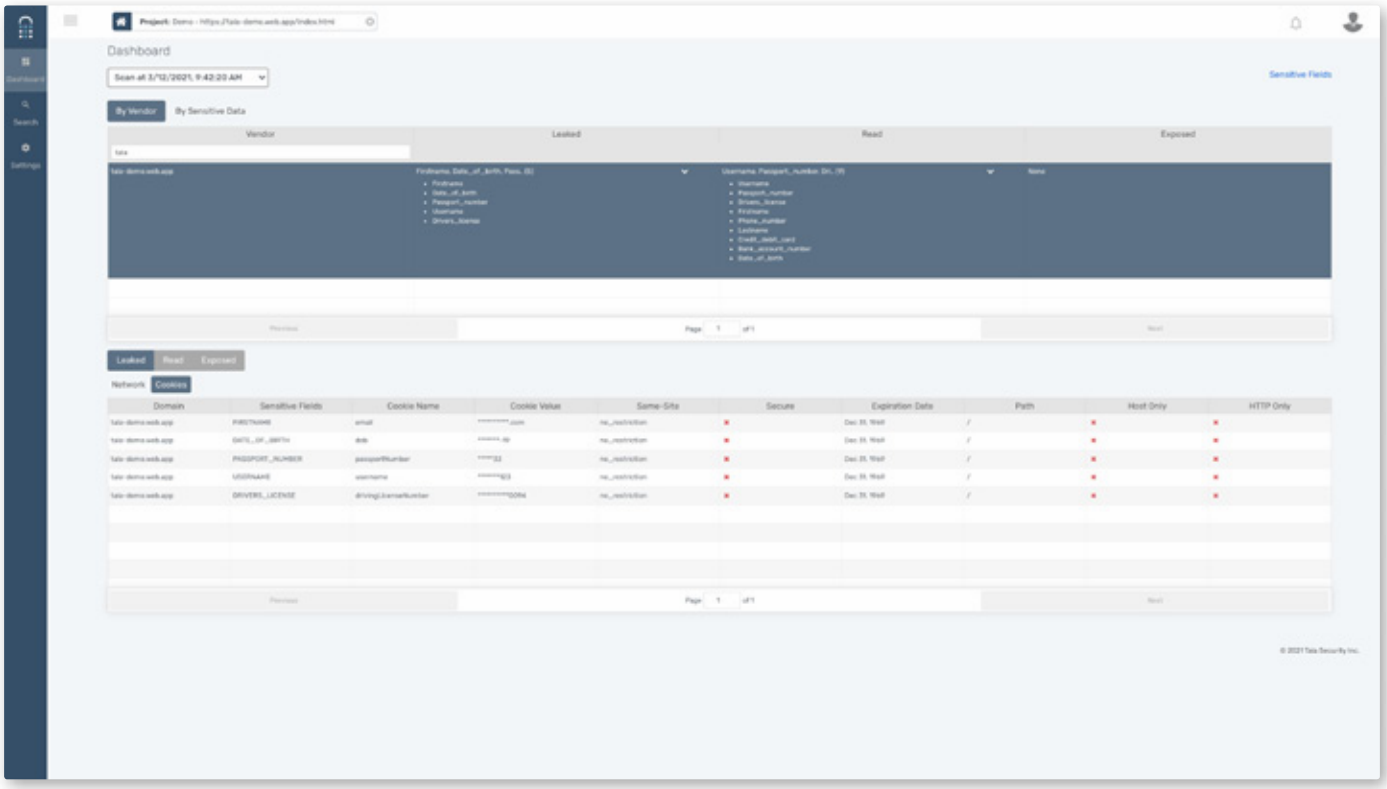
Read



Third-parties that are **reading** sensitive data from the browser

Steal/Collect

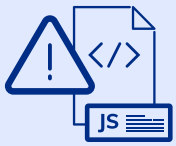
Third-parties that are actively **collecting** sensitive-data and sending it through the network



TALA

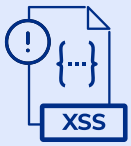
3 Behavioral and Risk Analysis

Tala's analysis builds a comprehensive behavioral model of the web application, forming a baseline risk assessment of whether the application is vulnerable to advanced attacks, third-party compromises, customer data loss or disruptions in customer experience. Tala also detects the presence of code vulnerabilities, expired certificates, use of insecure protocols and risky sink functions. Comprehensive risk modelling captures all third-party risks, Magecart, and sensitive data, programming, privacy and compliance risks.



Script Vulnerabilities

Tala analyzes scripts running in the application and leverages internal and external vulnerability databases to identify indicators of compromise and common vulnerabilities.



Programming Risks

Tala's comprehensive scanning identifies the use of risky sink functions such as 'eval' and 'document.write' that could expose DOM XSS risks. Tala also identifies the use of insecure protocols or expired certificates.

Third Party Risks

Tala analyzes all third party integrations and leverages external and internal threat feeds to alert on malicious third party domains or javascript files.

Privacy Risks

Tala's advanced data leakage detection capability identifies malicious and inadvertent data leakage to third party vendors through network requests, forms, cookies, storage, etc.

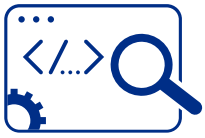
TALA

4 Threat Detection and Monitoring

Vulnerabilities in your code enable cross-site scripting (XSS) and JavaScript insertion attacks like Magecart to inject malicious scripts or integrate with malicious domains. Tala's advanced threat detection solves this by dynamically scanning and continuously monitoring web application behavior for threats and anomalous behavior.

Advanced Threat Detection

Tala's advanced threat detection scans applications to generate an initial behavioral model of all scripts as they are executed on the client side. Tala then continuously monitors the application to detect anomalies by leveraging both internal heuristics, databases and external vulnerability databases.



Continuous Monitoring

Tala continuously monitors hashes for scripts running in your environment, alerting you to any suspicious behavior. This is done through periodic computation of hash value deltas for JavaScript files on sensitive pages, and monitoring of unauthorized structural changes to AST hashes to discover indicators of compromise

Alerting and Threat Intelligence

Tala combines internal heuristics, external threat intelligence together with insights extracted from Tala's application information modeling and script monitoring to alert on malicious behaviors or compromises observed for third party domains and javascript files. Tala's continuous detection capability diagnoses javascript threats and provides actionable intelligence to help with remediation.

Find, Fix, Finish...

Tala's patented scanning engine provides continuous monitoring of complex workflows within web applications to detect malicious behaviors, code vulnerabilities, sensitive data exposure and data leakage. The results are leveraged for risk modelling, privacy & compliance risks as well as unintended, malicious and accidental data leakage.

See how easy it is to secure your site with Tala! **Book your demo today.**