TALA

SOLUTION BRIEF

# WARD: Tala's Detection Platform

## Every piece of code, from every vendor in your website supply chain, can potentially be modified to steal sensitive data or degrade user experience. Detecting it is the first step to securing it.

Hidden or unmonitored JavaScript vulnerabilities on thousands of websites are targeted every month by attackers to steal sensitive data, financial information and more.

**Today's dynamic web makes dealing with this threat a significant challenge for enterprises, due to:**

- Limited awareness and visibility into the risk profile of their web applications
- Difficulty with continuously monitoring web application changes to enable timely action that could prevent data breaches
- Ensuring compliance with evolving data privacy regulatory frameworks

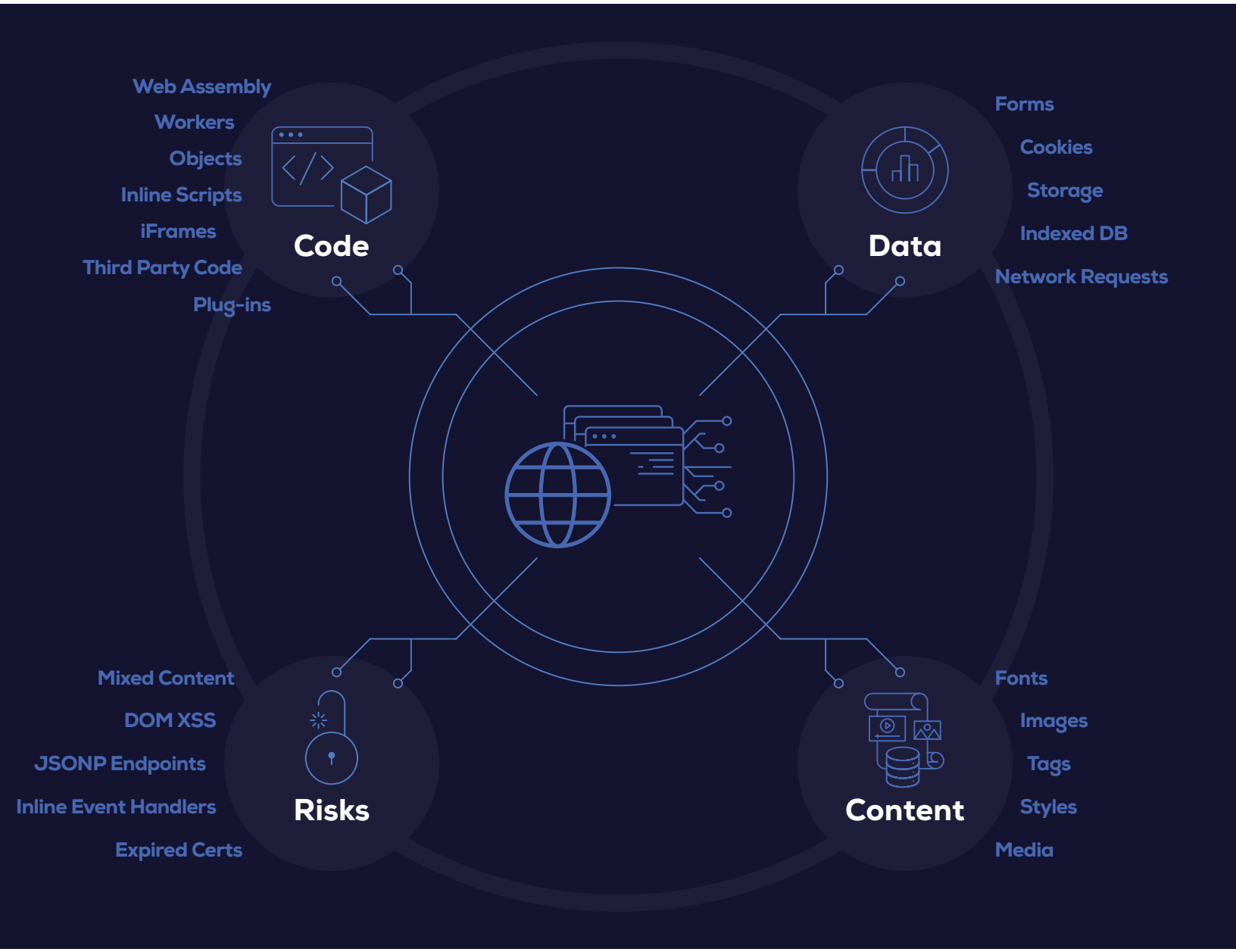
Tala's Web Application Runtime Detection (WARD) platform provides fine-grained data discovery, mapping, governance and alerting for enterprise websites. With no need for integration into the customer environment, WARD scans and continuously monitors complex workflows within web applications to detect malicious behaviors, code vulnerabilities and sensitive data exposure.

### INVENTORY AND BEHAVIOR ANALYSIS

Tala's patented scanning engine uses offline dynamic crawling and static analysis to automatically analyze enterprise web applications to extract and evaluate 150+ fine-grained, security-relevant behaviors on each page. Tala identifies sources of code and content on each page as well as sensitive data exchange between vendors present on the site:

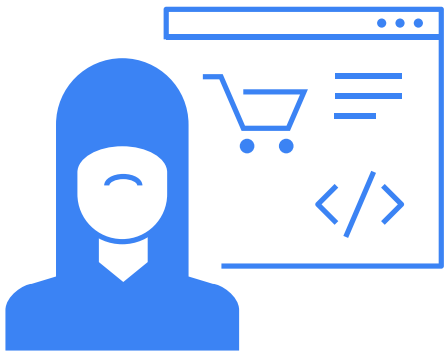
- Scan authenticated parts of the application and complex workflows to discover all third-party data and code sources, including fonts, styles, connections, and forms
- Domain reputation analysis and threat intelligence for all third-party integrations
- Model the website supply chain, uncovering all script sources and loading sequence, providing visibility into piggybacking scripts or tags
- Detection of iframe behaviors
- Discovery of sensitive data in forms, first party/ third party cookies and storage

Copyright © Tala Security Inc, All Rights Reserved




## RISK PROFILING

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.



TALA

Copyright © Tala Security Inc, All Rights Reserved

## SENSITIVE DATA EXPOSURE AND LEAKAGE

Protecting web applications from data theft requires sensitive data discovery, mapping and continuous monitoring. Even legitimate third-party integrations provide unintentional access to sensitive data, often without the site owner's knowledge. Tala identifies all sensitive data access in forms, network requests, cookies, storage etc and maps exposure and leakage to unintended vendors. Regulations such as GDPR and CCPA require an enterprise to be aware of where this data is flowing, as well as the purpose of these data flows. Our highly sophisticated continuous monitoring tool provides fine-grained data discovery, data mapping, data compliance/ audits and violation alerting for enterprises websites:

- **Sensitive data exposure:** Which vendor has access to what sensitive data?
- **Sensitive data readers:** Which vendor actually reads sensitive data?
- **Sensitive data exfiltration:** Which vendor actually sends the sensitive data out?

## SCRIPT MONITORING AND MAGECART DETECTION

Cross-site scripting and JavaScript insertion attacks exploit vulnerabilities in your code that allow the injection of malicious JavaScript or integration with malicious domains. Tala continuously monitors hashes for scripts running in your environment to alert you of any suspicious behavior.

- **Periodic computation** of hash value deltas for JS files on sensitive pages
- **Periodic monitoring** of unauthorized structural changes to AST hashes to discover indicators of compromise
- **Comprehensive threat intelligence** from internal and external threat feeds on suspicious domains and javascript files

## REPORTING, ALERTING AND ANALYTICS

Tala provides insightful reports, useful to AppSec, App Development, Data Protection, Risk & Compliance, Marketing teams.

- **Comprehensive page-by-page resource inventory** of the web application including presence of code vulnerabilities and sensitive data
- **Mapping of data flows to third-party vendors** in terms of exposure, access and leakage
- **Alerting based on intelligence from hundreds of threat feeds** and Tala's internal heuristics for malicious activity observed from both domains and scripts

Copyright © Tala Security Inc, All Rights Reserved

TALA

SOLUTION BRIEF | **WARD**

## THE TALA TECHNOLOGY PLATFORM

Tala is the leading Security and Privacy platform for the modern web. We offer two core products, one focused around security, the other around privacy.

**Web Application Runtime Protection (WARP)** stops advanced attacks such as Magecart, cross-site scripting (XSS), formjacking and more. It hardens websites against browser attacks that threaten data security by automating security standards such as CRP and SRI, without impacting user experience, DevOps or other resources. WARP includes Web Application Runtime Detection (WARD) to map, identify and stop data leakage.

**Web Application Runtime Detection (WARD)** is a highly sophisticated, continuous monitoring tool that provides fine-grained data discovery, data mapping, data governance and violation alerting for enterprise websites. Tala's WARD is available as a standalone solution or as part of our comprehensive WARP platform.

Extend data security and protection to the browser, with no performance impact or user interaction. **Book your demo today.**

## The Tala Technology Platform

### Automated, In-Depth Scans


- ✓ Fully dynamic scan (not just statically loaded JS)
- ✓ Captures complex workflows that are hard-to-reach which normal scans
- ✓ Support for multiple authentication options
- ✓ API support for CI/CD integration

### Data Tracking

- ✓ Identifies sensitive data and PII in forms, cookies, and local storage
- ✓ Data tracked across 3 dimensions – exposure, capture and leakage
- ✓ Data exposure – which vendors can read the data?
- ✓ Data capture – which vendors are actually reading the data?
- ✓ Data Exfiltration and Leakage – which vendors are actually collecting the data?

### In-Depth Behavioral & Risk Analysis

- ✓ 100+ behaviors recorded per page
- ✓ JavaScript (dynamic, static, first-party, third-party, inline), iFrames, images, CSS, XHR, event handlers, plug-ins, loading sequence graphs, etc.
- ✓ JavaScript coding risks, exposure to DOM injections etc.

### Threat & Anomaly Detection

- ✓ Continuous monitoring of website and third-party services
- ✓ Record and analyze Domain, script changes
- ✓ Identify of potentially malicious script changes
- ✓ Integration with third-party threat intelligence

### Real-Time Protection, Recommendations & Analytics

- ✓ Instrumented via CDN, web server, load balancer, app middleware
- ✓ Automated policies for protection: CSP, SRI, HSTS, iFrame sandbox, ...
- ✓ Recommendations to reduce coding risks
- ✓ Improve cyber-risk rating scores



Copyright © Tala Security Inc, All Rights Reserved