TALA

WHITE PAPER | *PROTECT*

Web Application Runtime Protection

Web Application Runtime Protection is the underlying technology that powers Tala *Protect* and Tala *Detect* to provide comprehensive data security and privacy for the modern web.

Tala *Protect* is designed to address multiple data security and privacy challenges faced by enterprises, without impacting performance or taxing DevOps resources:

- Ensures data security by preventing advanced website attacks.
- Hardens web applications against browser-based attacks by automating standards.
- Provides fine-grained data discovery, mapping, governance, risk modeling monitoring and alerting for enterprise websites and applications

> **“Tala uniquely provides comprehensive information flow analysis and the means to control it.”**

The Tala Technology Platform

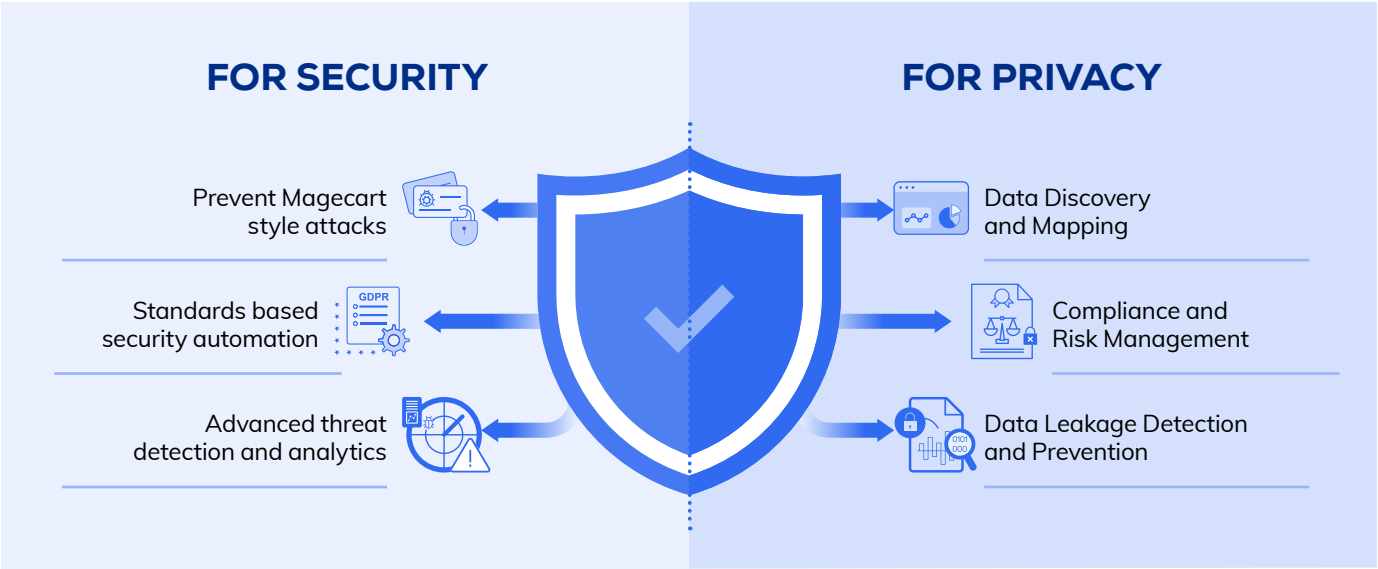
Real-Time Protection Recommendations & Analytics

Threat and Anomaly Detection

Automated In-Depth Scans

In-Depth Behavioral & Risk Analysis

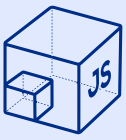
Data Tracking



1 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.

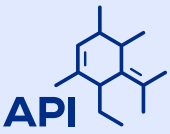
- **Analyze your website supply chain in minutes:** Identify all sources of content and code on your website, including static and dynamically loaded scripts and third-party integrations.
- **Gain comprehensive insight into sensitive data exposure and risk:** Tala analyzes all forms, cookies and storage 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 statistically loaded JS)

Support for multiple authentication options

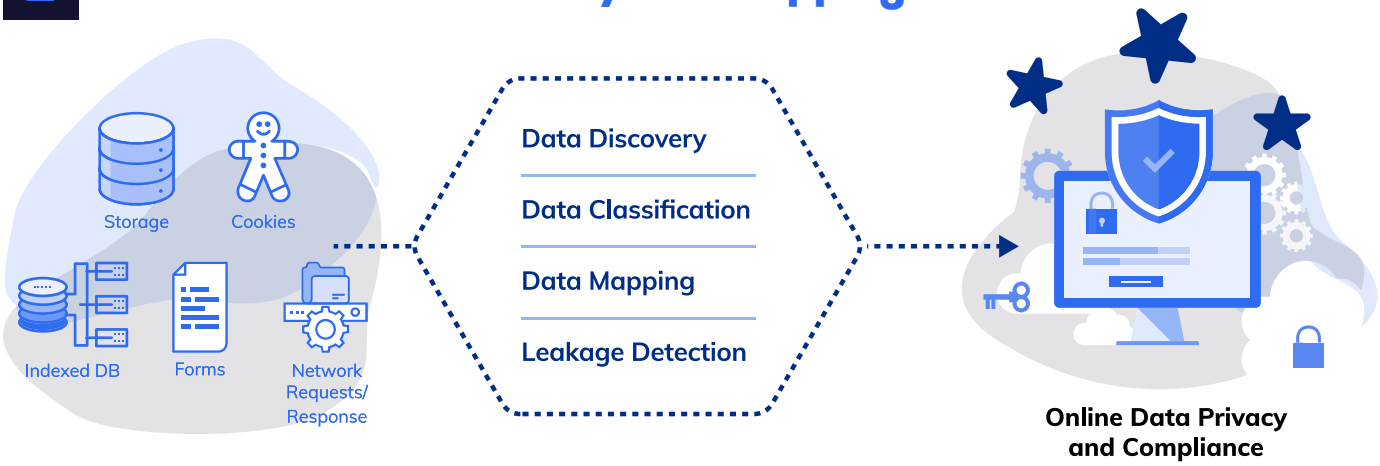
Captures complex workflows using synthetic transactions



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, remediation and providing important contextual information for audits and compliance.

3 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.

Find, Fix, Finish...

Tala's continuous monitoring engine automatically detects malicious and anomalous behaviors during web application runtime in even the most complex workflows, providing the actionable insights needed to immediately address data leakage and vulnerability.

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 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.

TALA

4 Protection-in-Depth and Threat Analytics

One of the most important elements of Tala's approach to protecting web apps is the use of broadly adopted, powerful web security standards. Tala eliminates the technical expertise and operational overhead required for implementing these policies to give you all the benefits without the hassles.

Endorsed by experts

Vetted and monitored by organisations like W3C and leading figures in the web security community

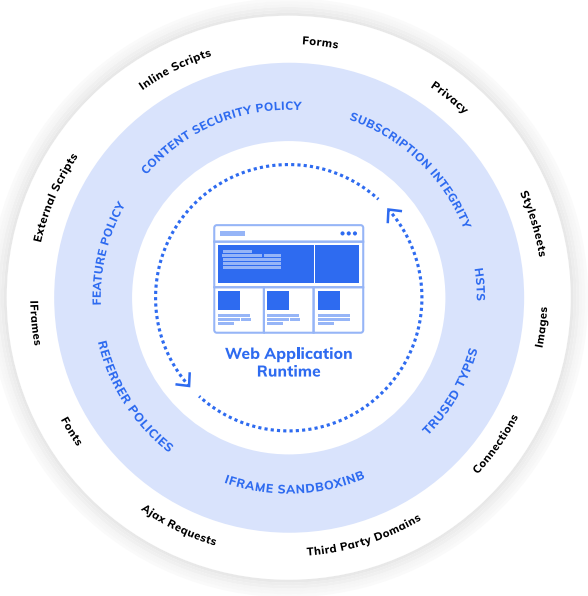
Recommended and endorsed by leading organisations like the PCI Council and RH-ISAC

Broadest Coverage

Applying a comprehensive set of standards that complement each other plugs the gaps to deliver a far wider breadth of protection against the broader range of attacks beyond just Magecart

No Performance Impact

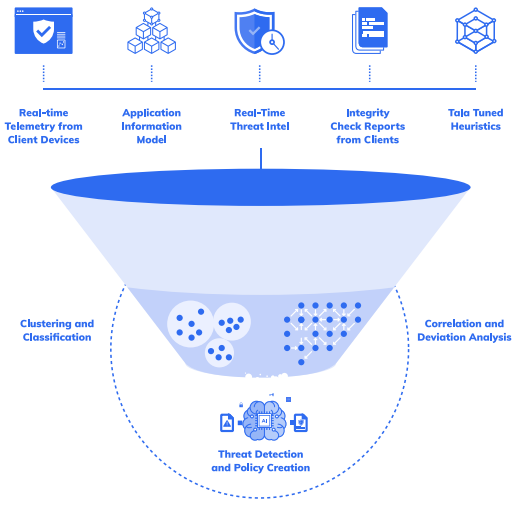
Browser-based standards and controls offer significant performance advantages over all other client-side security approaches. Because standards-based security is built into all modern browsers, it loads at application runtime, meaning there's no perceptible impact on user experience or page load times.



Tala protects sensitive data and code by automating security standards, including CSP, SRI, HSTS and more. No other solution on the market provides the same breadth of coverage and resilience , with absolutely no impact to website performance.

Tala's continuous monitoring engine monitors all client-side activity and dynamically adjusts security policies to block anomalous behavior and data exfiltration.

Once Tala policies are deployed, each user device (mobile or PC) that connects to the website, receives all the Tala protection policies. Tala policies monitor the behaviour of first and third-party content and code as they are executed on the client device. Tala applies advanced analytics, machine learning and heuristics on the telemetry received from client devices. Combined with threat intelligence, the application information model and integrity checks from client devices, this provides visibility into the app layer attack surface and identifies remediation mechanisms.



- ☑ Monitor content injection activity and cross-site scripting attempts in real-time.
- ☑ Monitor percentage of users being redirected through links
- ☑ Identify hot-spots of attack activity within the application
- ☑ Identify Trojans and other dangerous malware activities at the client side
- ☑ Continuously monitor scripts and trusted third-party domains for malicious activity or
- ☑ Track the security through our in-built scoring system

TALA

FEATURES

Comprehensive
Tala automates the application of standards like CSP, SRL, HSTS, referrer policy, iFrame sandboxing and more. Tala determines, develops and automates all CSP capabilities and directives, including reporting and analytics.

Zero maintenance overhead
Tala integrates with CL/CD pipelines via APIs and continuously monitors your websites for changes. Policies are dynamically updated on changing application behaviour.

Incident response and analytics
Comprehensive analytics and incident response support to pinpoint where and how your mission-critical web assets are being attacked.

Near-Zero performance impact
Tala leverages on-board overhead by activating browser-native capabilities that do not result in additional latency.

Automated
Tala policies are generated automatically and precisely with minimal manual intervention.

Real-time protection
Protection against XSS, clickjacking, redirection, ad injection, code injection and many other attacks.

PLATFORM AGNOSTIC DEPLOYMENT

Tala's future-proof and data driven integration platform automatically supports any future updates to security standards and features. Tala's platform supports all major web servers, load balancers, application middleware and CDN technologies, ensuring the installation of policies in minutes with no changes to application code.

SECURITY STANDARDS

Content Security Policy + Nonces
Enables the whitelisting of sources from which scripts and other content are loaded into the browser. Provides valuable insights into your website's behavior through violation reports.

Protects From
- Magecart-style attacks
- Cross-site scripting
- Formjacking
- Content Injection

HTTPS Strict-Transport-Security
Instructs the browser that the website or web asset is only to be accessed via a secure protocol (HTTPS)

Protects From
- Protocol downgrade
- Packet sniffing
- SSL stripping

Subresource Integrity
Ensures that resources fetched by the browser are delivered without unexpected manipulation through the implementation of script specific hashes.

Protects From
- Code tampering
- Cryptojacking

HTML5 iFrame Sandboxing
Enables fine-grained control over the behavior of individual iFrames by restricting associated capabilities like opening popups, executing scripts, etc.

Protects From
- Malvertising
- Clickjacking
- Cross-site scripting

Referrer Policy
Controls header content to help mitigate privacy and security concerns around information contained in the referrer header.

Protects From
- Inadvertent leakage of sensitive information via referrer header

Feature-Policy
Enables the whitelisting of domains that can access 25+ features on the website such as camera, microphone, geolocation, etc.

Protects From
- Unauthorized access to features and APIs