TALA

Securing Web Operations for a Fortune 500 Financial Institution

Deploying a Comprehensive Set of Client-Side Web Application Security Controls Across a Complex Global Environment

Background

A leading global financial services provider was looking to secure their mission-critical web applications against client-side attacks such as cross-site scripting (XSS), clickjacking, Magecart and other client-side malware. They also needed to control and secure their expansive JavaScript-based web-application supply chain. Existing security products such as application security validation testing like DAST and RASP, along with server-side security approaches like Web Application Firewall (WAF) can't deliver dynamic security to resolve client-side vulnerability.

Prior to working with Tala, the global application security (AppSec) team had taken a manual approach to hardening web applications, implementing client-side web security controls such as Content Security Policy (CSP). The AppSec team relied on a global set of security policies created by the core development team and, in order to accommodate the work of the various application development teams, had to manually approve all changes to the global CSP. This created a necessary but burdensome process that diminished the overall effectiveness and delivery of application development and enhancement. The AppSec team also lacked an effective way to analyze the massive volume of alerts generated by these security controls.

Faced with a rapid acceleration of attacks like Magecart, the customer recognized the need to secure their web applications quickly and effectively against theft of sensitive customer data. A CISO-sponsored mandate from AppSec required the deployment of standards-based, best-practice controls such as CSP, Subresource Integrity (SRI) and others across all applications in the global site architecture, encompassing both internal and external applications. The customer was looking for an effective, reliable solution to meet their global infrastructure needs.

PROBLEMS

- Manual web application hardening
- CSP approval bottlenecks
- Massive volume of alerts generated

URGENCY

- Rapid escalation of attacks like Magecart
- CISO-sponsored mandate to implement CSP, SRI etc

The Challenge

To Deploy Effective Security Reliably, Efficiently And At Scale

1. COMPLEXITY

Web application(s) complexity and customization meant that a universal policy configuration could not be deployed. Also, the applications themselves are very dynamic and require constant change, meaning a global policy would require continuous review and adaptation.

2. ADMINISTRATION

Defining and deploying policies across all of these applications was extremely complex and placed a significant burden on application development teams that lacked security expertise. Additionally, recent experience with policy deployment generated millions of administrative alerts that burdened IR and SOC teams.

3. MAXIMUM COVERAGE OF THE ATTACK SURFACE

As a global financial institution, the company was an attractive target for cybercriminals. Protection against a broad range of threats including, but not limited to, Magecart, cross-site scripting, trojans, credential theft and credit card skimming attacks was required.

4. RESOURCES AND STAFFING

Implementing standards-based security controls required a significant investment in additional security expertise to enhance application development, analytics and alert management capability.

5. CHANGE MANAGEMENT

Transforming the organization to accommodate the application of client-side security would require significant changes to existing workflows, adaptations of delivery timelines and additional validation checkpoints. Given these challenges, seamless integration into the CI/CD pipeline presented a daunting obstacle.

Vendor Evaluation Process

Recognizing the need for an external solution, the organization began evaluating vendors capable of implementing client-side security controls quickly, across their complex global architecture.

Tala's customer ran a comprehensive POC process to evaluate our preventative security model against various client-side attacks. A wide range of attack-types were simulated to measure security efficacy, deployment efficiency, performance impacts and adaptation to their complex and dynamic internal and external site architectures.

Vendors were gauged against the following selection criteria:

1. APPLICATION AVAILABILITY

The security solution could **not break legitimate application functionality** in a changing environment (such as the addition of new pages). This was a fundamental requirement.

2. DETECTION VS PROTECTION

The solution had to be capable of **blocking and preventing client-side attacks and breaches**. Detection-based approaches identified problems but did not solve them.

3. MAXIMUM COVERAGE OF THE ATTACK SURFACE

Protection against a broad range of client-side vulnerability, including 1st party, 3rd party, open-source, content, trojans, malware, MITB and browser extension attacks were measured.

4. PERFORMANCE IMPACT

The impact on website performance, measured by latency and page load times at scale, had to be **<2 ms**. Any delay in load times would interfere with user experience, ultimately resulting in poor customer experience and lost revenue. After preliminary POCs, the evaluation team dismissed competing solutions that relied on injecting proprietary JavaScript due to the significant performance impacts these solutions produced.

5. CENTRALIZED REPORTING

A centralized reporting process was required for efficient operations and management.

Vendor Evaluation Process

6. DATA HANDLING

Data Privacy, as defined by regulatory requirements, including **confidentiality, integrity and prevention of unauthorized access** had to be demonstrated.

7. FUTURE-PROOF ARCHITECTURE

The customer wanted a flexible solution capable of **fighting zero-day vulnerabilities** and rolling out **new and emerging standards-based security controls**.

8. FLEXIBILITY OF INTEGRATION OPTIONS

Due to the heterogenous technology stack across new and legacy web applications, it was important for the solution to **have multiple integration options**. With applications hosted on Apache, NGINX and other different web servers, the solution needed to integrate seamlessly with the organization's existing architecture. Additionally, for some applications, the company also sought integration with middleware.

9. RELIABILITY AND DATA PROTECTION

The organization required a **highly scalable, reliable solution with fault tolerance** at multiple levels. The solution had to deploy critical components in a redundant way to ensure availability of discovery services, critical caches and databases. Incremental database backup on a nightly basis, along with flexibility to deliver an on-premise component (to further ensure smooth functionality in the event of a loss of network connectivity), was also considered important.

10. MINIMIZE OPERATIONAL IMPACTS

The solution had to **minimize requests to network teams for firewall changes**, and also **minimize software updates** to code running on web servers, reverse web proxies and middleware components.

Tala Deployment

Following the POC assessment, Tala's solution was deployed across multiple critical applications serving 75+ countries. Tala was seamlessly integrated into the CI/CD pipeline and the team quickly built out a process around testing and deployment of all future changes. Tala integrated with the applications through multiple methods, including web server (Apache, NGINX, IIS) and middleware (NodeJS, JBoss).

Multiple critical applications

75+ Countries

Seamless CI/CD Pipeline integration

Integration through Webserver, middleware

Solution Benefits And Business Impact

The benefit of Tala's implementation was felt across all teams, including Application Security, Web Operations, Fraud and Risk Management, Incident Response and SOC. With Tala, these teams were able to **save 5-7 man-days per month** that were previously spent optimizing security policies and responding to threats.

Time Savings through Security Automation

Automation of CSP and other security controls led to a significant reduction in the workload of development teams. Tala's solution was initially deployed in reporting mode, ensuring that security policies could be deployed and tuned before moving to block mode. The policy deployed by Tala can dynamically adapt to changes in the application environment and architecture, requiring little oversight from development teams.

Saved 5-7 man-days per month

Protection against attacks

When operating in Active Protection Mode, Tala prevented attacks across a broad range of observable simulated attacks. Additionally, Tala was able to provide important information to incident response and risk teams for streamlining the threat management process. Tala exceeded the security requirements initially scoped for evaluation. In fact, after the impressive results in first round testing, a second round of tests included a newly discovered trojan that was successfully attacking applications. Tala was able to block this attack. Choosing a standards-based solution ensures that both today's and tomorrow's threat vectors are accommodated in the security model.

Protection against new trojan

Near-Zero Impact on Performance

Through post-deployment optimizations, Tala was measured to achieve a sub-millisecond latency representing a <1% overhead impact for most web applications.

<1% Overhead impact

Solution Benefits And Business Impact

Dramatic reduction in alert volume

Due to Tala's advanced analytics and interaction with dynamic architectures and threat intelligence, alert volumes were reduced exponentially. After initially operating in reporting mode to gain analytics insights, the move to block mode saw a reduction from 8 million alerts daily to less than 5 real attack alerts per day requiring review.

8 M daily alerts to < 5 alerts per day

Administration

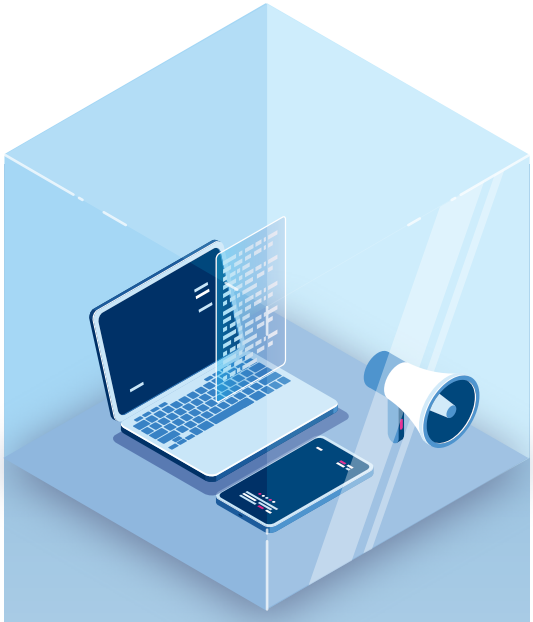
Tala's Deployment Manager (TDM) minimized requests to network teams for firewall changes. Additionally, Tala's data/spec-driven engines ensured that code changes could be rolled out as config changes, minimizing the requirement for updates to code running on web servers, reverse web proxies and middleware components.

Minimized firewall changes

Reporting and Analytics

Tala introduced a reporting process leveraging key metrics provided by our analytics engine. This helped teams to build a repository of web assets and track security controls for each of

- With Tala, the internal teams were able to gain insights into the security posture of multiple web applications. Tala's APIs and integration with reporting tools like Splunk helped with the reporting of the state of client-side security across these applications.
- Tala's inventorying of the web application supply chain helped the AppSec and risk management teams gain visibility on the vendors currently integrated with the enterprise for threat monitoring purposes.
- Tala's javascript analysis helped the company with their code monitoring processes, highlighting vulnerabilities that need action, such as the use of unsafe-inline, unsafe-eval, etc.



Tala's excellent performance as a security vendor led to mandated adoption across the organization

As validation of the efficacy of the Tala solution, the AppSec team mandated that Tala be deployed across all applications across the organization. This not only served as a vote of confidence in Tala's capabilities but also reinforced the organization's outstanding commitment to web application security and ensuring a safe website experience for visitors and customers.

Thank You!

Get in touch today

www.talasecurity.io

info@talasecurity.com