## TALA

CASE STUDY

# Tala Security and GESA Credit Union.

With over 255,000 members and more than $4bn in assets to take care of, Gesa Credit Union partnered with Tala to protect its websites and web applications from attack.

## BACKGROUND

With over $4bn in assets and over 255,000 members, Gesa is the second-largest Credit Union in Washington State. Headquartered in Richland, it currently operates 18 branches and 12 student-operated high school branches. Gesa also operates as Inspirus Credit Union, a Division of Gesa Credit Union, headquartered in Tukwila, Washington.

Gesa manages four main websites and over 15 public-facing web properties. Increasing digitization has seen Gesa deploy multiple services and integrations online, and it continues to add and operate more properties. Securing and maintaining full visibility into these mission critical assets is a primary focus for Gesa. They need to do this without any discernible impact on user experience and website performance.

> **"Security has always been 'top of mind' for Gesa and we realized early on the importance of using best in class products for our security needs. We use many other products that protect various layers of security...but to get specifics on each of the scripts that are injected in the browser, we needed a better solution. That is when we looked into Tala."**
>
> Andrew H. Chung, VP of Development & Analytics
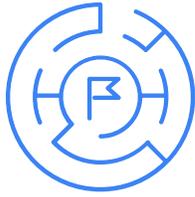
## THE CHALLENGES

- Magecart and other client-side attacks

- Protecting online transactions

- No performance impact

- Protecting PII and sensitive data

- Compliance with NCUA and DFI

## CHOOSING THE RIGHT SOLUTION

When evaluating solutions to secure its websites, web applications and sensitive data, Gesa had key criteria:

- **Keeping customer data safe from Magecart and other client-side attacks:** As a financial institution, securing customers' online transactions is a top priority for Gesa. With the rising incidence of Magecart and Magecart-style attacks, every online transaction on the platform was at risk. In addition, Gesa's CIO wanted to enhance customer security and protect sensitive data from man-in-the-middle attacks, malware deployments, and website cloning.

- **Seamless online experience with no dip in performance:** Gesa's customers valued face-to face interactions and moving them to a similar online experience was a challenge. Gesa wanted new innovations like online video chat to provide a world class customer experience; it was vital that the chosen solution did not disrupt the customer experience or impact website performance.

- **Meeting regulations and guidelines from NCUA and DFI:** Gesa is audited annually by its governing bodies (NCUA, DFI). Data security is always a major requirement for these audits and Gesa wanted to make sure it was compliant in all respects.

## VENDOR EVALUATION PROCESS - SECURITY WITHOUT COMPROMISE

Having evaluated a number of solutions that addressed Magecart, XSS and other threats, Gesa quickly realized that each used different methods and some lacked coverage for a wide range of attacks such as first-party compromise, DOM-based cross site scripting and advanced Magecart attacks. Some of the solutions were unable to operate effectively without significant degradation of website performance and user experience.

> **At Gesa we have always believed in partnering with "best in class" vendors to help us achieve our IT needs. We have experts in-house who know about developer best practices, like making sure we eliminate SQL injection risks, etc. but when it came to addressing the breadth of client-side security, we wanted to strategically partner up and work with experts.**
>
> Andrew H. Chung, VP of Development & Analytics

TALA

While still researching the options,Gesa's CIO came across Tala at the Finovate conference. Following a vigorous evaluation process, Tala's solution perfectly matched Gesa's requirements for both security and zero performance impact. Better still, as the only vendor that adopts a standards based approach to solving client-side security, Tala was able to solve a long-standing issue for the Gesa security team, which had identified the importance of security standards and was seeking industry expertise to learn more and implement this approach.

## BENEFITS AND BUSINESS IMPACT

**Currently, Gesa has deployed Tala across four crucial web properties and realized tremendous benefits in a number of areas:**

### Prevention of Magecart and other client-side threats

Tala's Active Protection mode provided protection against major threats such as XSS, SQL injection, code injection and Magecart. Gesa was able to secure all the scripts running on the client side and obtain valuable insights that helped security teams with threat monitoring and incident response.

### Visibility into indicators of compromise

Tala has helped Gesa increase awareness and insight into the code and applications running on their websites, and conduct periodic reviews with their internal application owners. It has been eye-opening to observe that so many previously unmonitored scripts could be exploited to conduct malicious activities.
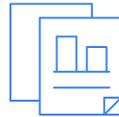
### Partners in compliance

Reports generated by Tala have proved useful in demonstrating compliance to Gesa's governing bodies. Periodic reviews are conducted prior to every audit to make sure Gesa takes a proactive approach and stays compliant.

### Code Reviews

Gesa's developers routinely use Tala prior to key releases to review code and ensure that there are no inherent risks that the web application might be susceptible to.

### Improved user experience

Gesa's customer experience has improved significantly since Tala was deployed. The customer journey is free of disruptions and the web applications have registered almost zero impact to performance.

## RETAIL SECURITY SUCCESS WITH TALA

**"**With Tala, we were able to deploy a strong Content Security Policy on our websites, ensuring our customers enjoy an optimal user experience, free of ad injections or session re-directs. By securing the login, payment and checkout pages with Tala, we have ensured our customers' credentials are safeguarded from malicious actors at all times. In keeping with our commitment to providing a high-quality user experience on our websites, Tala has also ensured that the effect on website performance is near-zero.**"**

**WWW.TALASECURITY.IO | INFO@TALASECURITY.IO**