Client-Side Protection

https://campus.barracuda.com/doc/97517860/

Client-Side Protection protects against attacks on a web application's supply chain. These attacks target potential weak points, such as commonly used code libraries, third party software and other resources and the systems that store and deliver them. Client-Side Protection includes Content Security Policy and Subresource Integrity practices.

Content Security Policy (CSP)

CSP is a HTTP Response header that contains directives for various file types and references used by an application to prevent cross-site scripting (XSS), clickjacking, and other code injection attacks. A report-uri directive is also provided and can be used by browsers to report violations of the policy.

Subresource Integrity (SRI)

SRI was created in response to a number of attacks where content delivery network or other third party housed content was injected with malicious code and delivered to thousands of websites using it. SRI directs the creation of a cryptographic hash of the resource that modern browsers then compare against a locally generated hash. Matching hashes verify that the resource has not been compromised. If they do not match, the resource is discarded.

Enabling Client-Side Protection

Set **Enable Client-Side Protection** to **On** to enact this protection for your application.

> You must be on datapath 12.0 or higher to use this component.

Enabling Client-Side Protection provides a default policy that is report only. If you wish to configure the CSP or SRI policies to take greater action you will need to use Support-Assist.

The dashboard provides the following for the selected time period:

- **Violations** – Number of CSP and SRI violations.
- **Clients** – Number of clients affected.

- **Pages Impacted** – Number of application pages impacted by the policy violations.
- **Violation Directives** – The directives that were violated.
- **Client Browsers** – Client web browsers used during the violation.
- **Sources** – The sources that provided the violated resource.