YOTTAA

Service Blocker

Yottaa's Service Blocker capability enables Content Security Policy (CSP), Page Security Rules, and form field protection. Each of our content security features is designed to increase detection and mitigation of certain types of security attacks, including Cross-Site Scripting (XSS), data injection, and other Magecart-style attacks. With Service Blocker you can limit which data sources are allowed by your storefront. Service Blocker provides configurable directives that are published directly into the HTTP response header of your website. Once a directive is published, Service Blocker flags and can block potential exploits through Yottaa's real user monitoring.

A Content Security Policy (CSP) allows developers to control the resources which a particular web page can fetch or execute, reducing the potential harm from malicious injection attempts. Content Security Policy, a Candidate Recommendation of the W3C, is a security standard introduced to prevent cross-site scripting (XSS), and other code injection attacks with wide support by modern web browsers.

Rule Types

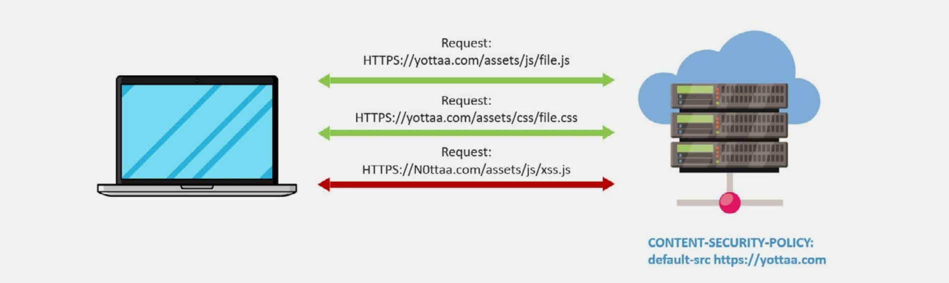
Service Blocker protects your site and users from malicious third-party activity by enabling three types of security rules to be configured on your website: Content Security Policies (CSP). Page Security Rules, and Form Protection.

- **Content Security Policy (CSP)** rules define which domains are allowed to inject code onto your site. As an example, you may want to enable Cloudflare CDN to have access to your Shopping Cart page and deny any other domain.
- **Page Security Rules** define access to certain page content like cookie and storage data which may contain user PII
- **Form Protection** will lock down forms or form fields, such as on a login or checkout page, to prevent third parties from data scraping.

Rules can be configured into two types of modes; "report only" or "enforce".

- Rules configured in report only mode will monitor services accessing defined content, but still allow open access to the site, site pages, and forms. Report only rules will display "flagged" violation in the Service Blocker dashboard.
- Rules configured in enforce mode will monitor services attempting to access defined content, and will prevent access to the site, site pages, and forms. Enforce mode rules report "blocked" violations in the Service Blocker dashboard.

Each of these rule types can be created and immediately published to your site.


Request:
HTTPS://yottaa.com/assets/js/file.js
Request:
HTTPS://yottaa.com/assets/css/file.css
Request:
HTTPS://N0ttaa.com/assets/js/xss.js
CONTENT-SECURITY-POLICY:
default-src https://yottaa.com

Example security rule for website assets: Requests from approved domains are allowed access, while requests from undefined domains are denied access.

Dashboards & Reporting

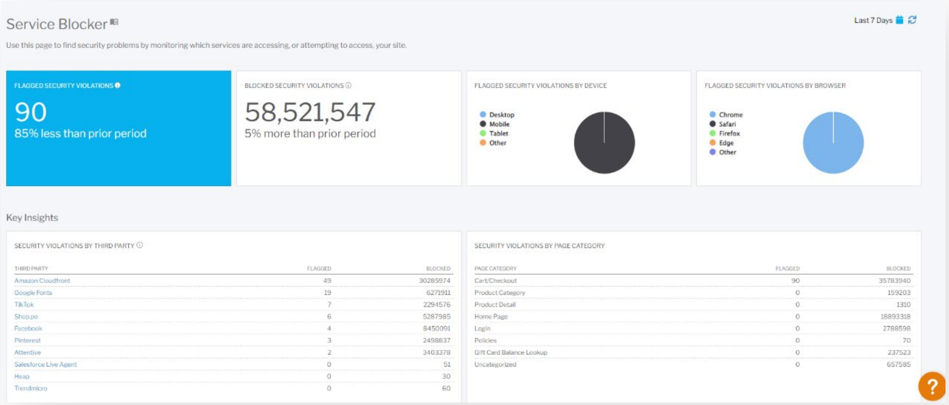
After any security rule is published to your site, Yottaa will monitor, enforce, and report on all services attempting to access secured site content, pages, or form fields. The dashboard allows you to quickly identify which resources violated which rules reducing the time it takes to tune your rules. Dashboards include insights on:

- **Total Flagged and Blocked Violations** – The number of requests attempting to access content, pages, or forms defined in a Service Blocker rule for a selected period of time. If you choose to configure a rule as a report only rule, Service Blocker will display it as a "flagged" event.
  - **Flagged security violation** – An event resulting in report only rule mode. Any service attempting to access defined content will be reported as a flagged security violation.
  - **Blocked security violations** – An event resulting from any rule set to enforce mode. Any service attempting to access your site, but is blocked by an enforced CSP, page security, or form protection rule will be reported as a blocked security violation.
- **Device type violations** – Reports on violations by user device types (e.g. mobile, desktop, tablet, or other) involved in a flagged service request.
- **Browser level violations** – Reports on violations by user browser types (e.g. Chrome, Safari, Firefox, etc.) involved in a flagged service request.
- **Third parties blocked or flagged** – Shows the third parties causing the most security violations and how many times they occur. Data shows both flagged violations in report only mode and blocked violations in enforce mode.
- **Blocked or flagged count by site page** – Shows the most viewed pages with at least one flagged or blocked security violation. Data shows both flagged violations in report only mode and blocked violations in enforce mode.
- **Daily and Hourly trend data** – A data graph showing data in one-minute increments. By default, the graph shows the past hour.
- **Deeper diagnostics** – Tables with information about each type of violation by:
  - Most viewed pages
  - Top directives
  - Top resources
  - Top domains
  - Top third parties
  - Most recent violations

In addition to rule performance diagnostics, Service Blocker provides you with insight into third-party services detected by a security rule.

Anomaly AI

Service Blocker monitors rule violations over a rolling two-week period to identify periods where the number of violations fall outside of a benchmark average. Any significant events falling outside of trend thresholds are reported in the Yottaa Anomalies dashboard. From the Anomalies dashboard you can view time periods when blocking events or logged security events fall outside of the two-week benchmark



Service Blocker

Use this page to find security problems by monitoring which services are accessing, or attempting to access, your site.

Last 7 Days

FLAGGED SECURITY VIOLATIONS

90

85% less than prior period

BLOCKED SECURITY VIOLATIONS

58,521,547

5% more than prior period

FLAGGED SECURITY VIOLATIONS BY DEVICE

FLAGGED SECURITY VIOLATIONS BY BROWSER

Key Insights

SECURITY VIOLATIONS BY THIRD PARTY

THIRD PARTY	FLAGGED	BLOCKED
Amazon Cloudfront	49	30285974
Google Fonts	19	6271911
TikTok	7	2294576
Shop.pe	6	5287985
Facebook	4	8450091
Pinterest	3	2498837
Attentive	2	3403378
Salesforce Live Agent	0	51
Heap	0	30
Trendmicro	0	60

SECURITY VIOLATIONS BY PAGE CATEGORY

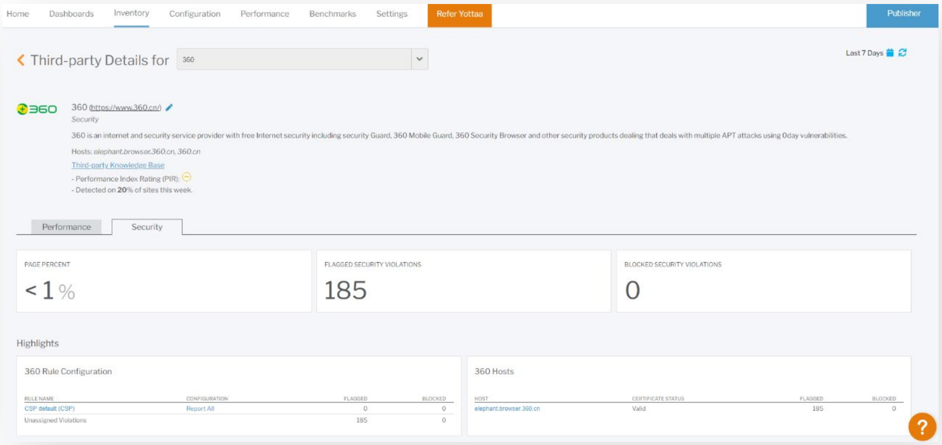
PAGE CATEGORY	FLAGGED	BLOCKED
Cart/Checkout	90	35783940
Product Category	0	159203
Product Detail	0	1310
Home Page	0	18893318
Login	0	2788598
Policies	0	70
Gift Card Balance Lookup	0	237523
Uncategorized	0	657585

Example Service Blocker dashboard showing security rule events, third parties impacted by a rule, and pages where flagged or blocked events occurred.

Security Activity Inventory

An inventory of all third-party services that are flagged against any published security rule is provided in a dashboard. It allows you to view each of the third parties by domain. It also allows you to view uncategorized domains, which are detected services not yet in our Third-party Knowledge Base. Included data:

- **Third Parties** - Displays all the services running on your site that are categorized in Yottaa's Third-party Knowledge Base
- **Domains** - Displays all the services running on your site by domain. Shows a separate entry for each domain, even if they are part of the same third party.
- **Uncategorized Domains** - Displays all the services running on your site that are not categorized in our Third-party Knowledge Base. You can use the domain name to investigate what the service is. Unidentified fully qualified domain names can be new third parties, second party resources, or bad actors attempting to access your site.
- **Flagged Security Violations** - The number of times a flagged service accessed your site over the last seven days or the selected period. Flagged violations result from events occurring from rules set as a report only mode rule.
- **Blocked Security Violations** - The number of times a blocked service attempted to access your site over the last seven days or the selected period. Blocked violations result from events occurring from rules set as an enforce mode rule.



Third-party Details for 360

Last 7 Days

360 (https://www.360.cn/)

Security

360 is an internet and security service provider with free Internet security including security Guard, 360 Mobile Guard, 360 Security Browser and other security products dealing that deals with multiple APT attacks using 0day vulnerabilities.

Hosts: *elephant.browser.360.cn, 360.cn*

Third-party Knowledge Base

- Performance Index Rating (PIR):

- Detected on **20**% of sites this week.

PAGE PERCENT

< 1 %

FLAGGED SECURITY VIOLATIONS

185

BLOCKED SECURITY VIOLATIONS

0

Highlights

360 Rule Configuration

RULE NAME	CONFIGURATION	FLAGGED	BLOCKED
CSP default (CSP)	Report All	0	0
Unassigned Violations		185	0

360 Hosts

HOST	CERTIFICATE STATUS	FLAGGED	BLOCKED
elephant.browser.360.cn	Valid	185	0

Example third-party detail view showing flagged or blocked events resulting from a content security rule.

Yottaa's Service Blocker goes beyond creation of CSPs. With Service Blocker capabilities you can set policies for your entire site, individual pages, content on pages, all forms or individual form fields. Service Blocker protects your site and your users from malicious events like Cross-Site Scripting (XSS) and Magecart attacks. Along with robust security rule setup, you'll find diagnostics and maintenance tools to manage your site security policies. Setting up a rule can be done by internal teams or by contacting a Yottaa support representative.

The Next Step

Don't just assume that your eCommerce site is performing as fast as it needs to – be sure with a free, no obligation YOTTAA trial. Start the process today with a FREE Performance Snapshot. **Click HERE for more information. You can't afford not to.**