

SERVICE CTRL

BY YOTTA

Enabling eCommerce brands to control the execution of all browser services running on their sites which provides a layer of defense and enhances brand security posture to protect shopper data.



Browser Services Endanger Shopper Data

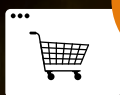
eCommerce sites are a major target for cyber attacks due to the transactional nature of the data they collect. These sites are essentially an open platform, and every host, JavaScript tag, and line of code is an opportunity for security issues. Malicious code can be injected via tag managers, source code, 3rd, 4th, and 5th parties, and browser plugins. Once external code is injected onto your site, it has full access to everything.

Discovering code injections, unwanted services, or anything else suspicious can be difficult, as code never stops changing. Even just one second after reviewing everything on your site, you'd need to check again to ensure nothing new has been added. And there are so many opportunities for services to access sensitive customer data. The [2020 3rd Party Technology Index](#) industry research identified an average of 25+ 3rd parties executing with full data access on checkout pages. If any of those services are malicious, or hacked without the service provider knowing, a basic form-scraping technique would easily capture that transactional data and put it in the hands of bad actors.



89%

89% of surveyed consumers reported being concerned that 3rd party tech could steal their personal information.



27

Mobile eCommerce sites averaged 27 3rd parties on checkout — WAY too many.

2020 3RD PARTY
TECHNOLOGY
INDEX

Because many eCommerce brands don't have the technology in place to monitor, analyze, and control browser services across their sites, many end up making unwanted headlines (i.e., Macy's, Claire's), losing shoppers and revenue, facing non-compliance fines with privacy laws, or attracting lawsuits.

SERVICE CTRL

Yottaa's SERVICE CTRL is an easy-to-install governance solution purpose-built to control browser services on eCommerce sites, protect and mitigate attacks (such as Magecart, code injections, and form-jacking), while providing in-depth, real-time analytics and AI-based service alerts. SERVICE CTRL's high-level capabilities enable the protection of eCommerce sites from online threats.

Functionality

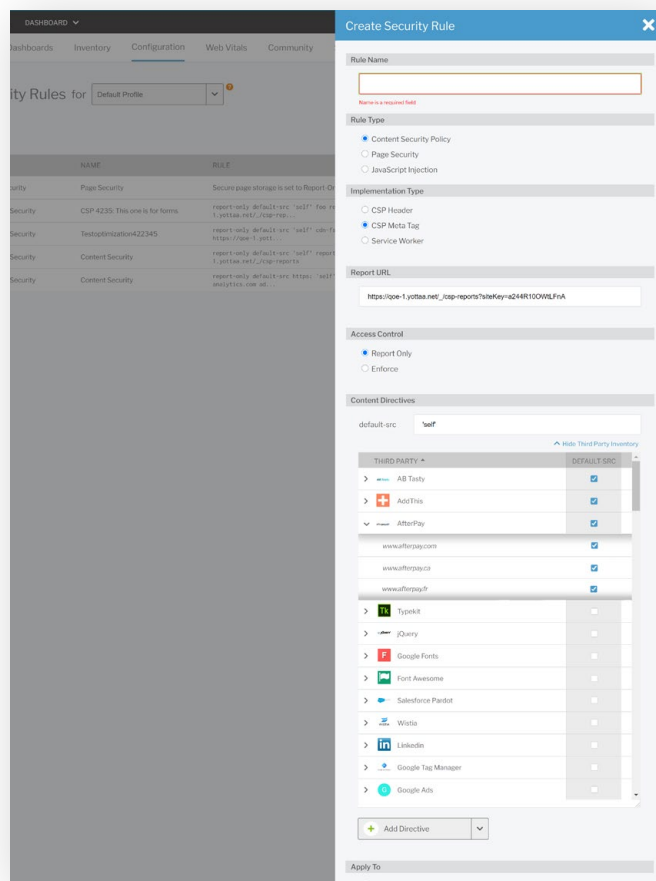
SERVICE CTRL protects eCommerce sites from online security vulnerabilities by providing brands with the capabilities you need to implement and manage your security policies simply and effectively. SERVICE CTRL users leverage the following powerful functionalities:

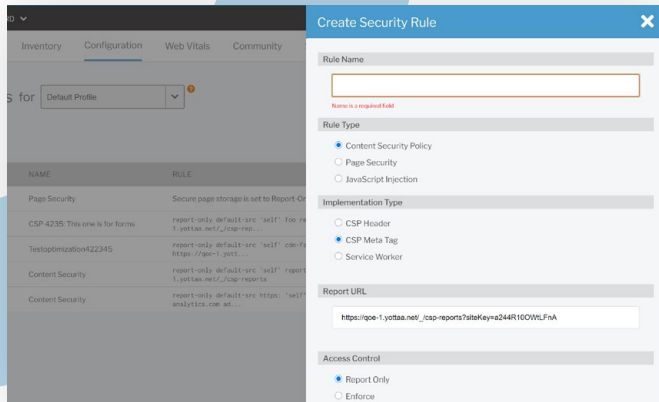
Build and Manage your Content Security Policy

eCommerce services and 3rd party tech can be vulnerable to code injections, malware, and cross side-scripting. To help mitigate the risk, sites leverage Content Security Policies (CSPs), which control what services can and can't load on your site's pages.

We understand brands stress about building and managing CSPs because they are complex when a manual approach is taken. Also, deploying CSPs incorrectly can negatively impact shopper experience and weaken defenses. There is inevitably more work when trying to manage CSP manually without a toolset.

Brands can protect themselves from these different types of attacks if the right CSP policy is implemented correctly. SERVICE CTRL provides easy and flexible options to set up CSP policies at the root and sub-domain level of your site. Also, brands don't need security experts to manage their CSP. SERVICE CTRL simplifies the process to create and manage CSPs without custom code.





Allow, and then Block, Services with CSP Rules

You won't need to worry about blocking the technology and services you want on your site. With SERVICE CTRL, CSPs can be created in report-only mode to gather data about how best to implement your CSP. In order to capture all the potential traffic on your site, the CSP will run in report-only mode for a period of time. This will give you time to ensure that you allow all the 3rd parties that are necessary for proper functioning of your site. You can monitor this data on the SERVICE CTRL Dashboard.

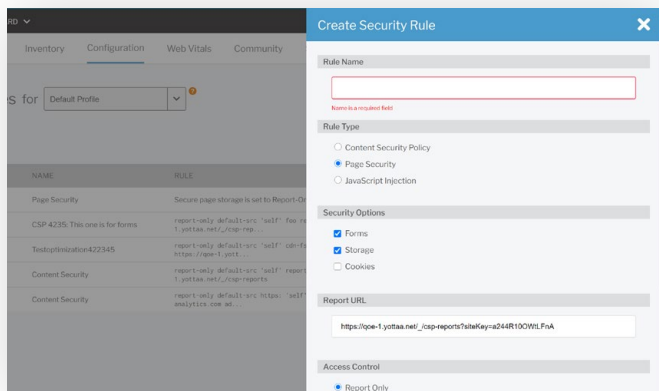
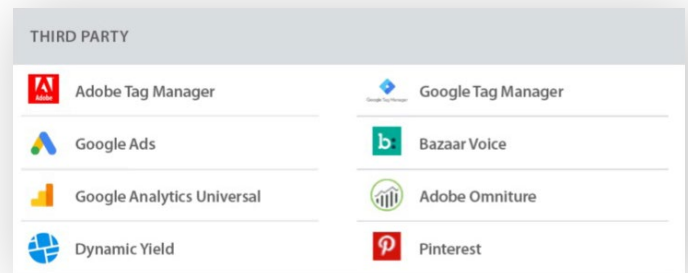
Once in place, your security rules will include:

- A Content Security Policy for all your browse pages (home page, categories, product details, etc.)
- A Content Security Policy for just your checkout pages
- Several Page Security rules controlling access to form fields on your checkout pages

Utilize Services Library

YOTTA's easy-to-implement and powerful SERVICE CTRL library:

- Monitors your site and maps complex web of requests to recognizable 3rd parties.
- Identifies all uncategorized services and validates security certificates on the fly.
- Leverages YOTTA's 3rd Party Knowledgebase which contains dynamic benchmarking data on over 1,000 3rd party technologies that gather with every page load across YOTTA's 1,500 eCommerce sites.



Secure Pages

eCommerce is an extremely targeted industry for malicious hacker threats, like content tampering and Magecart attacks.

SERVICE CTRL can help protect user data by limiting the services or 3rd parties that run on site pages, which in turn helps brands to ensure privacy law compliance. Robust rule configuration allows for unique blocking and allowing rule sets for each page type, specific domains, sub-domains, page categories, browser, or device. Page security policies provide the ability to manage rules at forms, storage, and cookie levels. Individual HTML and CSS selectors can be blocked with page security policies.

For example, we recommend creating a stricter form protection policy for your checkout pages than for your browse pages (such as product descriptions, categories, and home page), since checkout pages include sensitive user information. As a general best practice, checkout pages should only allow about six 3rd parties access. According to the [2020 3rd Party Technology Index](#), **eCommerce sites averaged around 27**. SERVICE CTRL can then create several Page Security rules that protect your customers' information by controlling access to form fields on your checkout pages.

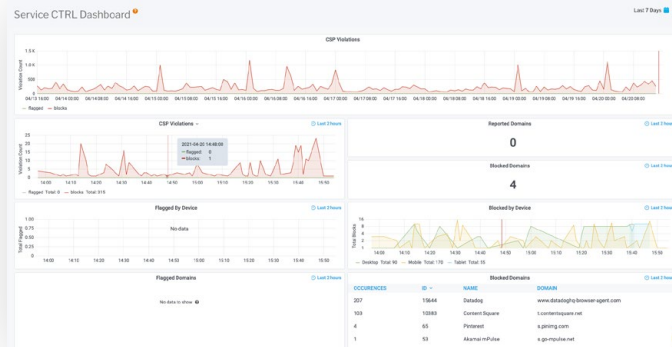
Gain Full Visibility

To enable total control of services running on your eCommerce site, full visibility is a necessity. Brands must be able to detect unknown domains, identify secure sites, and validate sites' certificates on the fly.

SERVICE CTRL provides at-a-glance visibility into service data by presenting categorized and uncategorized services and grouping services by root domain.

Unidentified Root Domain Names

ROOT DOMAIN NAME	
u1	cdnwidget.com
u2	cdnbasket.net
u3	sitelabweb.com
u5	datadoghq.com
u4	480app.com
5 of 12 Unidentified Third Parties View All	



Leverage Robust Analytics

Having visibility and understanding of the violations caused by services on your site helps brands prepare for anything. Focus on capturing real-time security violations and analytics on blocked domains, as well as analytics on individual service level security violations.

SERVICE CTRL measures and provides detailed analytics on reported and blocked violations and domains, CSP violations details, and a breakdown by device and browser.

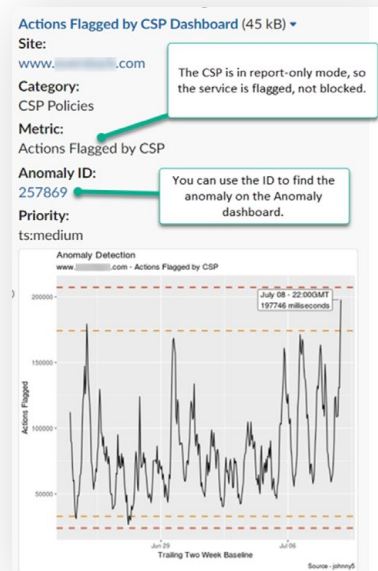
Detect & Alert on Anomalies

An anomaly, when referring to eCommerce sites, is an occurrence or measurement that's outside normal expected variation. Anomalies can be an indication of a change in performance or traffic, but can also indicate something more sinister, like an attack on customer data.

SERVICE CTRL leverages an AI-based alerting system to monitor unidentified services and integrates with email and Slack. Anomaly AI instantly notices when your site's trends change and enables even tighter security as the system learns more.

When you receive an anomaly alert:

1. Investigate the alert to find out which service triggered it.
2. If the service is necessary to proper functioning of your site, use the Services Inventory page to allow it.



Use Case: Leading Apparel Brand

After seeing numerous articles about online security breaches at other retail brands, a leading apparel and footwear brand chose not to sit and wait for a problem. The retailer wanted to deploy technology to gain full visibility into its online security initiatives, prevent page skimming and other attacks, and implement a content security policy (CSP). Key requirements included the ability to demonstrate its site is protected in real-time, gain greater site security visibility through robust analytics, and easily block specific 3rd party technologies.

In its trial of Yottaa's SERVICE CTRL, the retailer found a solution that addressed all its requirements — and more. In order to test YOTTAA's effectiveness, the brand's security team created multiple synthetic attacks, including the deployment of a malicious code to attempt to scrape form fields on the retailer's site. YOTTAA instantly identified all attacks, and the brand could have immediately mitigated them through YOTTAA if they had been real. The retailer ran similar synthetic attacks with other vendors and those attacks were not identified by competing solutions.

In addition, YOTTAA was able to provide a full inventory of all 3rd party technologies of the brand's site and easily identify 3rd parties

that presented potential security risks. This inventory also enabled the retailer to easily build a CSP to create multiple layers of proactive defense. The other solutions evaluated did not provide this type of inventory making it practically impossible to build a CSP, much less manage it easily moving forward. YOTTAA's extensive site analytics also provided the brand's security team granular data and deep insight into the security governance of their site.

Finally, through YOTTAA the retailer was able to proactively block one (or many) specific 3rd parties on any page with a simple, granular, and rules-driven approach. Other solutions were only able to block a 3rd party across the entire site and having the page type or specific page control was critical to the effectiveness of the solution. And using YOTTAA's Anomaly AI, the brand was able to quickly detect site anomalies, such as 3rd party performance issues, and easily mitigate them. Having the confidence to manage by exception has put the leadership and eCommerce teams at ease knowing their brand won't be in the news.














Content Security Policy

lwehtrekjrdt

Last 24 Hours

Select the third parties and services that are allowed access to this security policy.

38 Identified Third Parties

THIRD PARTY *	CATEGORY	RESOURCES	ALLOW ACCESS
 Amazon S3	CDN	s3.amazonaws.com	<input checked="" type="checkbox"/>
 Bazaar Voice	Customer Reviews	bazaarvoice.com	<input checked="" type="checkbox"/>
 Bing	Social Media	bing.com	<input checked="" type="checkbox"/>
 Bold Chat	Chat	boldchat.com	<input type="checkbox"/>
 Bounce Exchange	Marketing Tech	bounceexchange.com	<input type="checkbox"/>
 Bounce-X	Marketing Tech	bouncex.net	<input type="checkbox"/>
 Certona	Personalization	certona.net, certona.com, res-x.com	<input type="checkbox"/>
 Cloudfront CDN	CDN	cloudfront.net	<input type="checkbox"/>
 Criteo	Ad Tech		<input type="checkbox"/>
 Curalate	Marketing Tech	curalate.com	<input type="checkbox"/>
 Extol	Marketing Tech	extole.io, extole.com	<input type="checkbox"/>
 Facebook	Social Media		<input type="checkbox"/>
 FanPlayer	Marketing Tech	fanplay.com	<input type="checkbox"/>

Conclusion

Online traffic is skyrocketing for eCommerce brands. While this will result in more shoppers and more revenue, it also increases the risk of security vulnerabilities. Brands must ensure that their eCommerce environments are fully secure so that they do not end up as a headline in a news article about another major eCommerce security breach involving customer data.

Yottaa's SERVICE CTRL provides eCommerce brands with a critical layer of visibility and control over their online security posture and enables them to protect their site against multiple security threats. By helping to create and manage a Content Security Policy (CSP) to provide page level security across individual browser elements, brands can granularly block unwanted or potentially dangerous services and

3rd party technologies from key pages across its sites. SERVICE CTRL also helps identify and mitigate site anomalies, and most importantly, protect sensitive shopper data.

Would you like to find out if you have any services running on your site that pose a security risk? [Click here to receive a free eCommerce Site Security Snapshot](#). The Snapshot will identify all 3rd parties on your checkout page and let you know which ones should be there and which ones might put your shoppers' data at risk. All you need to do is provide the URL you would like evaluated and a YOTTAA Security Engineer will examine your checkout page and email you a PDF report. It's that simple!

[Click here for your Free eCommerce Site Security Snapshot!](#)



YOTTAA