YOTTAA

BRAND CTRL for Protecting your Shoppers and their eCommerce Experience

Approximately 20% of shopping sessions have unauthorized ad injections

Traffic and shopper online visits are expensive and getting more costly every day. Retailers' margins are under attack and being impacted by inflation, supply chain issues, the cost of raw materials and unintended shopper discounts. For example, once you get shoppers to your site, they can be redirected to a competing site, given discounts that they didn't need and potentially having their personal data exposed. How? Through browser extensions.

On one hand, some browser extensions, such as Honey or Capital One Shopping aren't intentionally malicious, but they are ultimately stealing traffic off your site and leading shoppers to competitive sites. Brands often lack visibility and control over intended or unintended discounting, which subsequently impacts the bottom line, causing brands to take a big hit on both revenue and margin.

4,800 eCommerce sites have forms compromised per month.

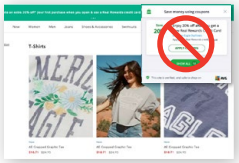
An even scarier circumstance involving browser extensions is that without any security measures in place, hackers can use these extensions as a vehicle to skim forms to lift credit card numbers, passwords, addresses, and other customer data – putting your shoppers and your brand credibility at risk.

Overall, brands need to act now to PROTECT their traffic investments, margin and profits, brand image, and shopper trust. It's difficult for brands to know what percent of traffic is affected by these extensions and it's even more challenging to resolve the problem. Fortunately, YOTTAA has launched BRAND CTRL to address this exact problem, ensuring your shoppers and their eCommerce experience are always protected.

Capabilities

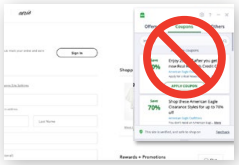
Journey Shield

Protect your brand from unauthorized, competitive and malicious redirection.



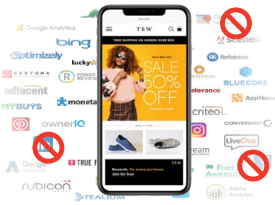
Revenue Protector

Stop unintended promotions and discount codes from being accessed directly on the site and during the checkout process.



Service Blocker

Block malicious 3rd party script attacks from injecting malware, taking over a site, or altering brand experience by allowing only authorized 3rd parties from executing on site.



Shopper Guard

Provides an additional layer of defense for shopper PII data including email, name, credit card numbers and passwords, to ensure they are guarded from Magecart and other skimming attacks.

Threat Diagnostics

Gain visibility and key insights to protect your brand and shoppers with detailed device level diagnostics that help you monitor and track various security related incidents in real-time.

How does BRAND CTRL work?

Quick and Easy Implementation

- BRAND CTRL is an easy-to-install eCommerce experience protection technology that enables online brands to control the execution of all extensions and 3rd parties on their sites.

Extension and 3rd Party Inventory

- Collect data on which extensions and 3rd parties are accessing your brand's site.
- Get deep visibility into your site's inventory of all extensions and 3rd party technologies through YOTTAA's comprehensive dashboards, enhanced with the rich data captured in our 3rd party knowledgebase.
- Learn what percentage of your shoppers are using extensions like Honey, Capital One Shopping, etc.
- Identify malicious activity caused by extensions as well as any new Nth parties and domains.

Control 3rd Parties and Extensions

- Control when and where services are allowed to execute, determine service restrictions, and stop unwanted services and extensions.
- Utilize flexible configuration Rules Engine to easily create and manage security rulesets to flag or block 3rd parties.
- Protect site forms to ensure shopper data being entered at account setup or checkout is not compromised.
- Configure and manage CSP with an easy-to-use interface in the YOTTAA Experience Optimization portal.

Visibility and Diagnostics:

- Monitor page and browser-level diagnostics on various dashboards, powered by YOTTAA's Context Intelligence.
- Obtain detailed data and analytics on what percentage of sessions and pages extensions and 3rd parties are running on, session trends, anomaly alerts, and security violations.
- Monitor and determine which extensions and 3rd parties to allow or block.
- Receive continuous knowledge to manage by exception with YOTTAA's anomaly detection and get service-related alerts based on machine learning and AI.

YOTTAA's Expert Services

- You don't need to tackle these efforts alone. YOTTAA's expert Client Services team will support you every step of the way as you determine what actions will best provide you with peace of mind that your shoppers are having smooth and protected experiences on your site.

What's Next?

Are you ready to take control of your online brand? Start with a Free Site Performance Snapshot Report to get full visibility into what's currently running on your site.

[Visit yottaa.com/performance-snapshot-offer/](yottaa.com/performance-snapshot-offer/)

YOTTAA