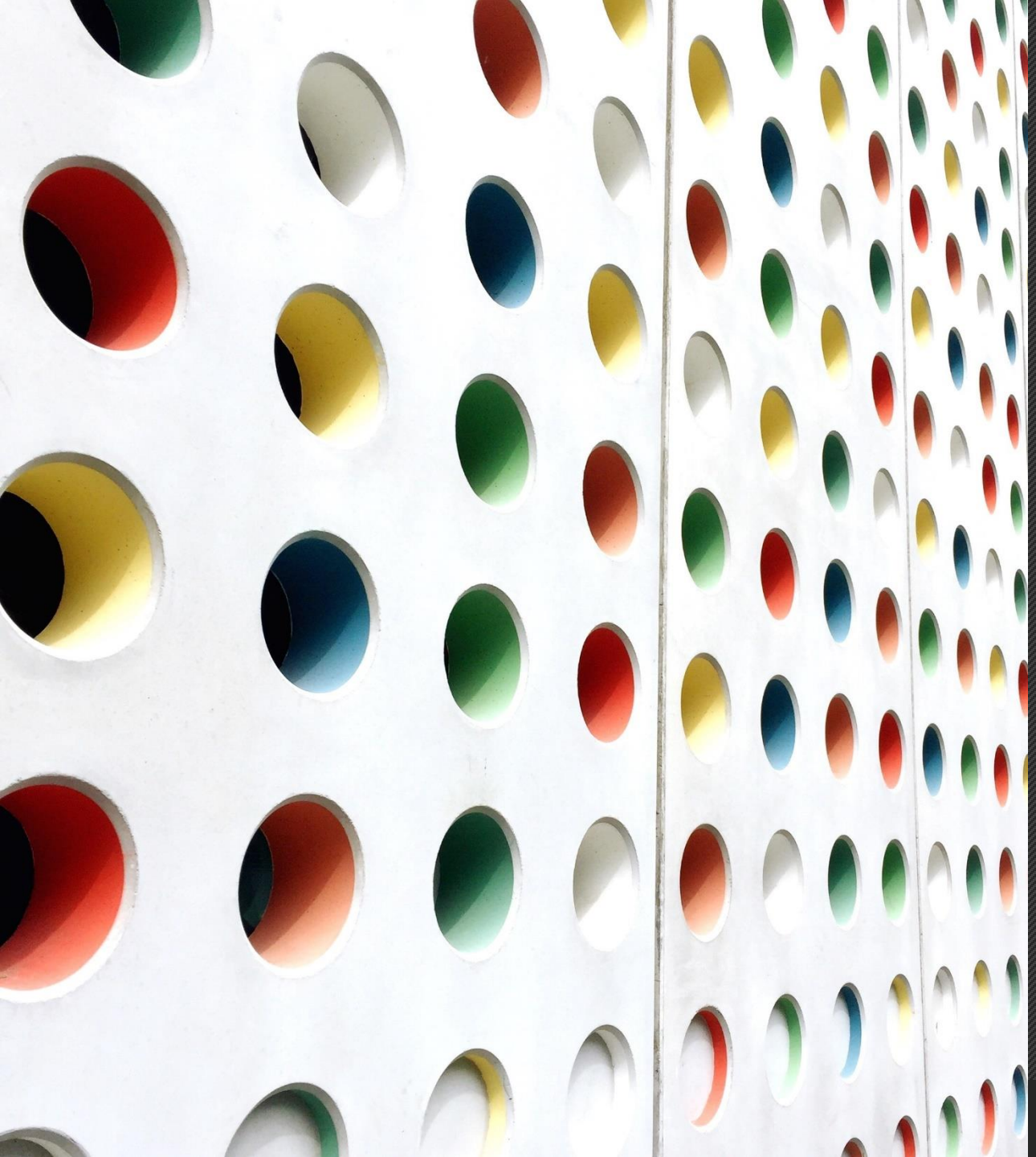


Third-Party Scripts

THE ELEPHANT ON YOUR WEBSITE

Most websites are getting bogged down by the bulk of the third-party scripts on them. Techniques to improve speed and security while dazzling your customers with a feature rich website.

N7 NITROGEN

www.n7.io

Third-Party Scripts

Third-Party Scripts are the external code fragments that can be embedded into a site directly from a third-party vendor.

These scripts are designed to augment the existing functionality on the site, especially where it is better to buy or rent the functionality rather than build on your own. Mostly, Third-Party Scripts are used for social sharing buttons, advert, analytics, tracking, personalized content, product reviews, live chat etc.

Before we dive further on how these almost obscure entities impact the user experience and thus the bottom-line, let us quickly review how we got here…

The Progressive march of JavaScript and the Third-Party Scripts…

Late Nineties to early Noughties

Network and caching were the mantra for performance. CDNs gained popularity by caching static assets, let's call them images as back then, JS and CSS were more or less non existent.

Fewer network hops and improving cache hits strategies worked well in this era because the network latencies used to be high - most people were still on dial-up internet and broadband was starting to emerge in the mainstream.

Rest of the Noughties

The second wave of web commercialization, Web 2.0, was a push to make it look pretty with hefty images and powerful styles. Alongside, Java Script was gaining momentum towards driving interactive functional aspects on the browser itself, threating the server-side's control.

Need for speed got people focusing on image optimizations as that was the bulkiest thing on the page.

Twen-teens

By now, JavaScript had proved it is here to stay and rule the browser world for the foreseeable future. This led to an explosion of JavaScript-based frameworks that in turn enabled thicker web front-ends.

Personalization became the mantra for success and with JavaScript becoming powerful and standardized across browsers, the division of control between front-end and server-side functionality is now blurring.

Performance optimizations now focused on how to optimize the JavaScript code files.

Later part of the decade saw H2 gaining support and the techniques to optimize JavaScript code in the new H2 world changed a bit. *Though many sites are still using the methods from the earlier part of the decade, which are counterproductive.*

Nevertheless, the prevalence of JavaScript support led many innovations to happen and allowed companies to provide browser-based integrations of their services directly in the browser.

2020 and beyond…

Digital Commerce and Content landscape is changing. Third-Party Scripts have proliferated all sorts of use cases from analytics to personalization to live-chat to product reviews and the list goes on. So much so that before, if 90% of the programming was 1st party now, its almost becoming the opposite.

It is an age of services. The world is adopting Microservices. Such loose coupling across multiple systems gets consolidated on the front-end using Third-Party Scripts. In some architectures, the original platform has decoupled its internal functional elements as if they are Third-Parties. A single page can have more than 100 third party requests and it would not be an outlier.

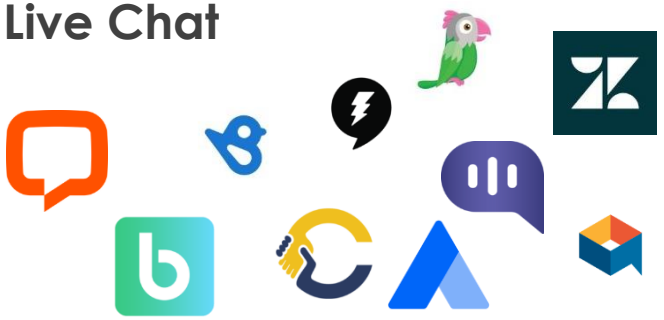
1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

N7 NITROGEN

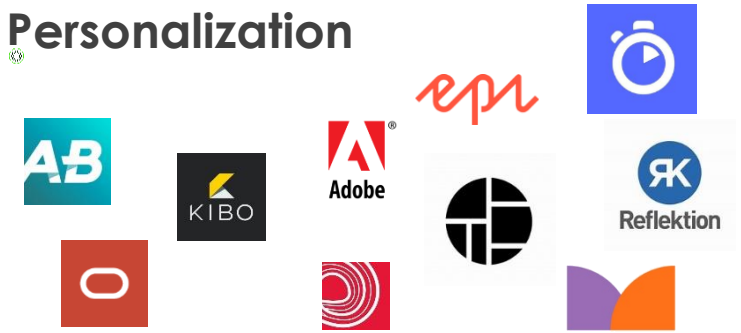
Value of Third-Party Scripts in 2020

Third-Party Scripts have proliferated all sorts of use cases .

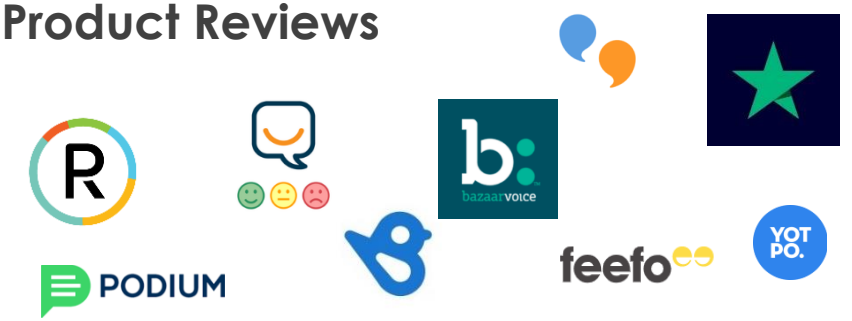
Live Chat



Personalization

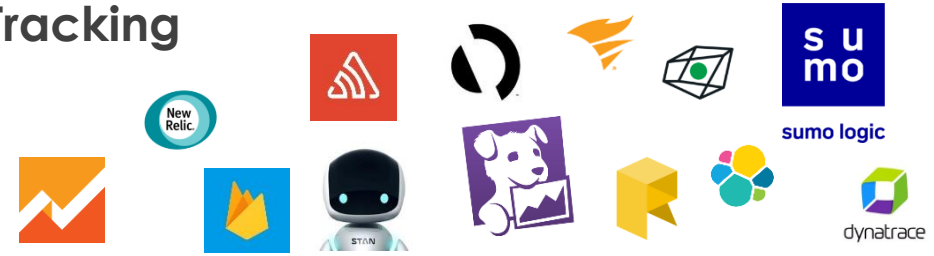


Product Reviews

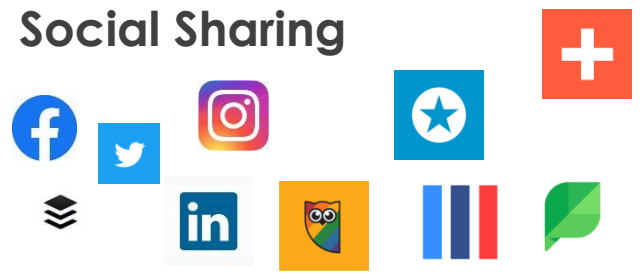


Analytics

Tracking



Social Sharing



N7 NITROGEN

What's the Problem?

POOR **SPEED** + POOR **SECURITY** = POOR **UX** → LOST **$£€₹**

Third-Party Scripts are the primary cause of poor page speed. They leak information off the page to the third-party vendors while opening up vulnerabilities for Cross-Site-Scripting attacks.
Poor User-Experience undoubtedly reduces the bottom-line of any digital property.
Third-Party Scripts add functional value to the site, however, they need to be managed effectively to yield gains.

POOR SPEED + POOR SECURITY = POOR UX → LOST $€₹

Third-Party Scripts are the primary cause of poor page speed.

Often, issues on a web sites slowing pages down are due to third-party scripts. Embedding Third-Party Scripts means we often rely on them to be fast.

Situation becomes even further bleak when most sites do not have effective measurement metrics that monitors impact of Third-Party Scripts on their users' experience.

Performance issues then are not noticed by the site owners yet bite the end users.

Sites which have such measurement tools in place, mostly brush the issue under the carpet as something beyond their control.

Technical team washes their hands that this is not their code and hence beyond the control.

Poor Speed undoubtedly reduces the bottom-line of any digital property, hence Third-Party Scripts should be given careful attention such that they do not negatively impact the speed.

POOR SPEED + POOR **SECURITY** = POOR UX → LOST $£€₹

Third-Party Scripts are the intentional inclusion of JavaScript code that is downloaded and communicate with extremal servers.
XSS (Cross-Site Scripting) vulnerability is where attackers are attempting to inject external JavaScript code into your web site pages.
A keen eye would realize that these two are not much different.

Any time external scripts are included on a page, there is an inherent security risk because that script has full access to the content, cookies and user interactions on that page. It may be sharing a lot more data with the third parties than expected.

Challenge in a traditional digital security approach is that it tries to build security fences and governance processes around vectors that are originating from with-in the system. Security professional mostly fails to realize that Third-Party Scripts, which are not originating from any internal system and not pushing data to any internal systems can be a cause of data leaks.

N7 NITROGEN

What's the Solution?

Impact on user experience due to allowing an external source to control content and function on the page is the elephant in the room that many sites are failing to see.

Exciting challenges in speed and security are emerging. New focus and effort are required to improve the user experience in this age of microservices.

In three steps, Third-Party Scripts can start to realize the promise of enhanced user experience.

Catalogue Third-Party Scripts


Contents

Introduction 4

Unit 1: Parts of Speech
Nouns 5
Proper Nouns 7
Names and Titles of People and Animals 8
Names of Special Places 9
Days of the Week, Months, and Holidays 10
Singular and Plural Nouns 11
Plural Nouns 12
More Plural Nouns 13
Irregular Plural Nouns 14
Pronouns 15
Using I or Me 16
Action Verbs 17
Singular Verbs 18
Helping Verbs 19
Verbs That Do Not Show Action 20
Present-Tense Verbs 21
Past-Tense Verbs 22
Irregular Verbs 23
Adding ed or ing to Verbs 24
Using Is or Are 25
Using Was or Were 26
Using See, Saw, or Seen 27
Using Ran, Runs, or Run 28
Using Give, Given, or Gave 29
Using Do or Does 30
Using Has, Have, or Had 31
Adjectives 32
Adjectives That Compare 34
Using A or An 35

Unit 2: Sentences
Sentences 36
Sentence Parts 38
Naming Part of Sentences 39
Action Part of Sentences 40
Word Order in Sentences 41
Telling Sentences and Asking Sentences 42
Kinds of Sentences 43
Joining Sentences 45
Adding Describing Words to Sentences 47
Beginning Sentences in Different Ways 48
Writing Clear Sentences 49

Unit 3: Mechanics
Writing Names of People 50
Writing Initials 51
Writing Titles of Respect 52
Writing Names of Places 53
Writing Names of Days and Months 54
Writing Names of Holidays 55

The biggest hurdle in implementing any sort of Third-Party Script solution is proper definition of the issue. Most site owners do not realize how many Third-Parties Scripts are being used on their site.

Further, the collective ownership of the digital property across the technology, operations and marketing teams is leading to dissolved responsibility of the site. Third-Party Scripts get introduced by different teams and lack of governance around this process is at the core of this issue becoming unmanageable.

#1 task should be to catalogue all the Third-Party Scripts that are being used on the site. Each such entry must be thus vetted for its value to the business objectives and evaluated for potential risks.

Classification of the Third-Party Scripts under their use-cases like personalization, analytics etc. will not only help towards standardization and removing of overlapping use cases, it would also identify different optimization and security protocols for them.

N7 NITROGEN

2 Speed up Third-Party Scripts

One way to reduce the impact of slow Third-Party Scripts is avoid using them. However, given the prolific use-cases and the enormity of options available that avoidance is not recommended. Rather, the industry is moving towards even further increase in using loosely coupled applications. A prudent approach is needed that entails careful management of Third-Party Scripts where their slowness has minimal impact on the user experience.

There are a few techniques at our disposal that can reduce the impact of slow Third-Party Scripts.

Circuit Breaker

If a particular script is slow beyond a limit or not working, it needs to be taken out of the call sequence to stop degrading the user experience of the page.

Caching

Leveraging faster CDN caches, ideally the same caching layer that the origin pages are using would result in better and more consistent performance.

Delayed Async Execution

Downloading of the script and its execution on the client browser can be independently managed. Furthermore, different functional use case may yield better results if the Third-Party Script can be marked for delayed execution, for example, we can execute Product Reviews to be embedded in the page if user has started interaction with the page however, in contrast analytics tracking scripts need to be included at the onset.

3 Secure Third-Party Scripts

For the sake of business information leak and customer privacy, there must be a governance process in place that ensures only the approved Third-Party scripts are injected in the specific pages. For example, one may not want to have a Third-Party Script that provides Product reviews to be included on pages that have personal or credit card information.

Zero Trust Goveranance

Another perspective on security is to be risk averse and adopt a Zero Trust approach for Third-Party Scripts along side the rest of the organization's internal assets.

Having a periodic review of the state and security audit of the Third-Party vendors should be conducted to ensure information is being handled appropriately.

Catalog Audit

Building a catalogue of all Third-Party Scripts and conduct a security audit to quantify the risk. Following this, a balanced decision can be made based on the risk factor and the business value of the use-case.

Security at the Browser

Multiple techniques are available to assist in this process. Content Security Policy is a set of browser instructions that help in securing access to content on the page. Tools like Nitrogen provide much granular control over inclusion of Third-Party Scripts across different pages.

N7 NITROGEN

How Nitrogen helps…?

The Nitrogen Platform provides easy to implement cloud based software-as-a-service that enhance user experience and protects the bottom line.

Our JS Manager module understands an ever growing catalog of Third-Party Scripts. This catalog is categorized based on the use case.

Platform also is capable of circuit breaking and providing delayed async execution to enhance user experience.

In conjunction with the Nitrogen accelerated delivery platform, the third party scripts can be served from the super fast content delivery network.