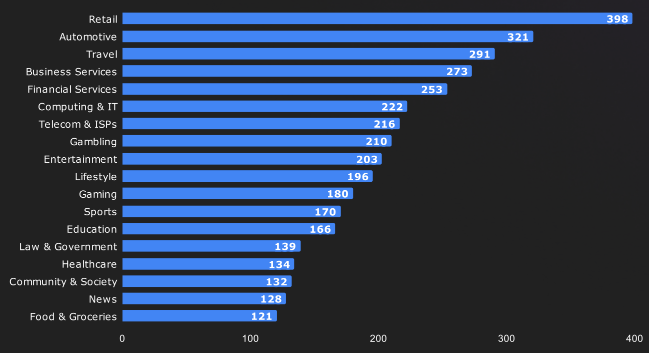
imperva

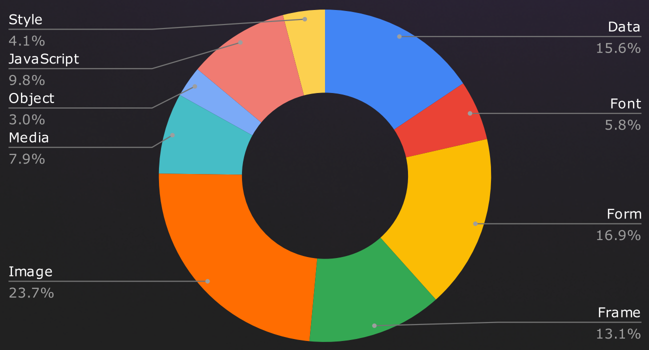
The Client-Side Threat Landscape

Modern web applications are richer and more interactive than ever, thanks to a blend of resources loaded on the client-side. On average, web applications load 209 client-side resources, including anything from JavaScript and images to frames, forms, and fonts.

Average Number of Client-Side Resources by Industry



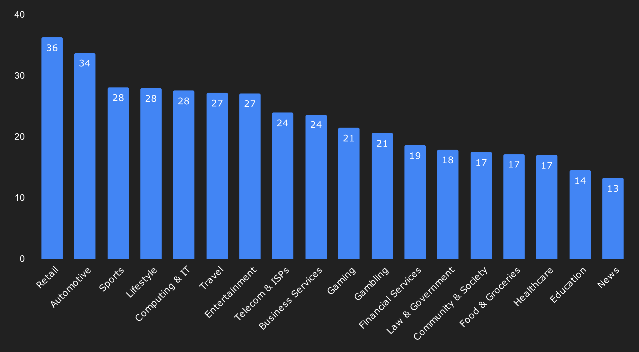
Average Makeup up of the Client-Side



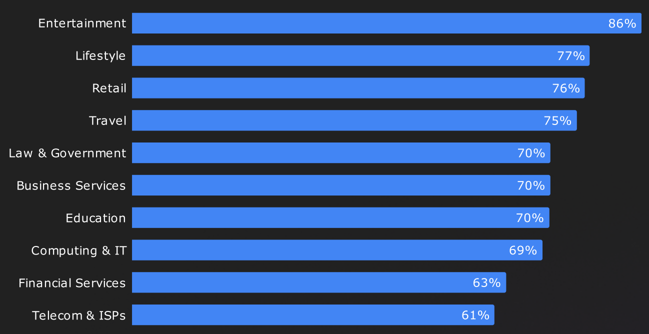
But while these resources provide an interactive user experience, they also create potential security vulnerabilities: Attackers can exploit them to inject and execute scripts from unauthorized domains, leading to data breaches through attacks commonly referred to as Magecart.

JavaScript, in particular, is a favorite vector for abuse. Even a single line of malicious code, such as a JavaScript sniffer, can wreak havoc. On average, modern web applications load 23 JavaScript resources on end users' browsers. Of those, an average of 66% are third-party scripts, increasing the risk of attackers exploiting compromises in the website supply chain.

Average Number of Client-Side JavaScript Resources by Industry



Highest Ratio of Third-Party JavaScript Resources by Industry



However, attackers can also exploit other client-side resources, making it imperative to have a holistic view of the client-side. For example, attackers can use a fake resource to inject inline JavaScript or to exfiltrate sensitive user data.

Imperva Client-Side Protection prevents data theft from client-side attacks like formjacking, Magecart, and other digital skimming techniques that exploit client-side resources and vulnerabilities in the website supply chain. It empowers security teams to effortlessly determine the nature of each client-side resource and block any unapproved ones with just a single click. Providing continuous monitoring, actionable insights, and easy controls ensures the security of your client-side while allowing you to maintain compliance with data privacy regulations, such as GDPR, CCPA, and PCI DSS 4.0.