HUMAN | E-book

The Client-side Blind Side:

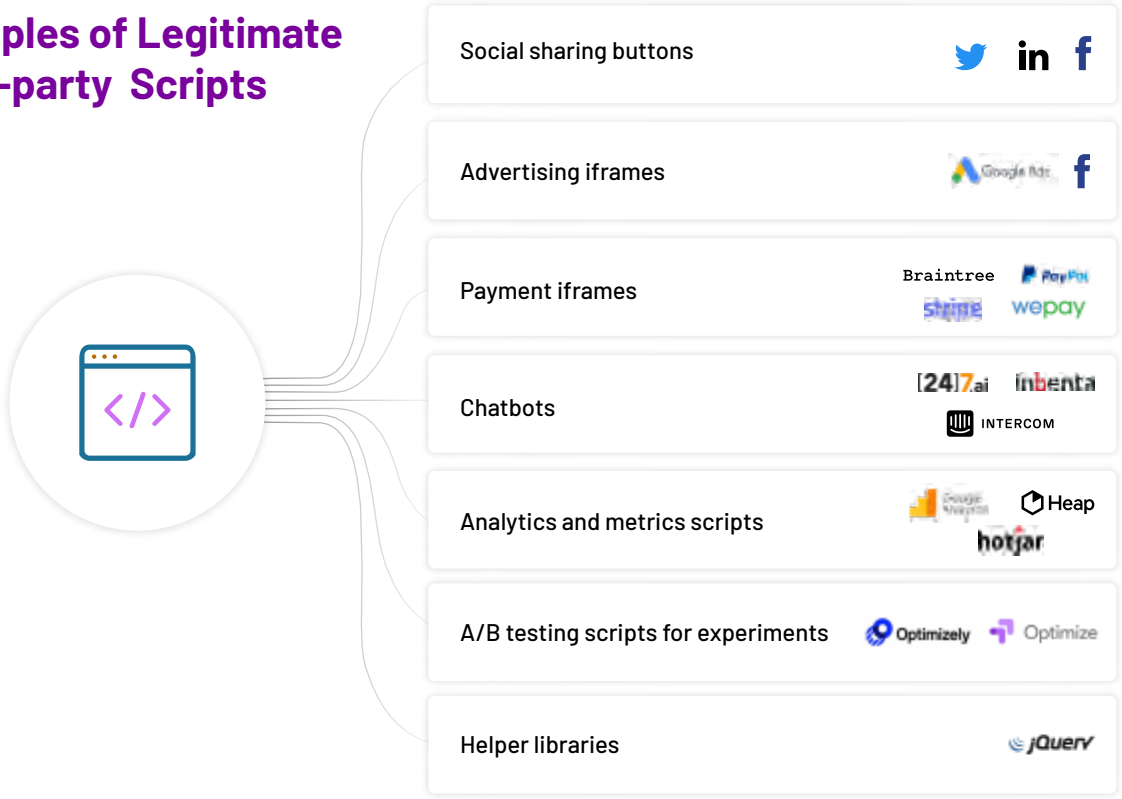
Gain Visibility Into Your Website Supply Chain

Shift to the Client Side

As consumer behavior changes and typical daily interactions are increasingly moving online, businesses are enhancing website functionalities to deliver a better experience for the user. To achieve this, modern web and mobile applications shift application logic to the client side — i.e., users' browsers. Instead of residing in a central website server, client-side code runs on users' browsers when they visit a site. This improves performance and enriches the user's digital experience.

> **"We've seen two years' worth of digital transformation in two months."**
>
> — Satya Nadella, CEO, Microsoft

Examples of Legitimate Third-party Scripts



The Digital Supply Chain

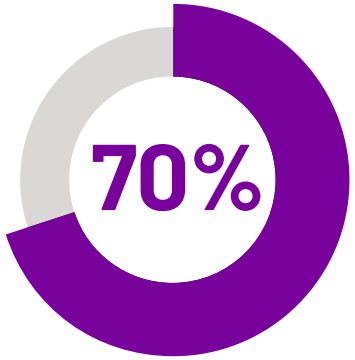
A significant portion of client-side code is JavaScript, which is sourced from open source libraries and third-party vendors. Front-end JavaScript code has grown over 256% for desktop apps and over 479% for mobile apps in the last decade[1] — and it keeps growing.

Today, it is estimated that up to 70% of the scripts on the average website come from a third party[2]. Nearly 55% of website developers use six or more different supply chain vendors to source the code on their site. These third-party scripts, in turn, call other scripts, which creates a digital supply chain of fourth-, fifth- and Nth-party scripts powering your website.

Client-side JavaScript code has increased

700% ↑
for mobile applications

411% ↑
for desktop

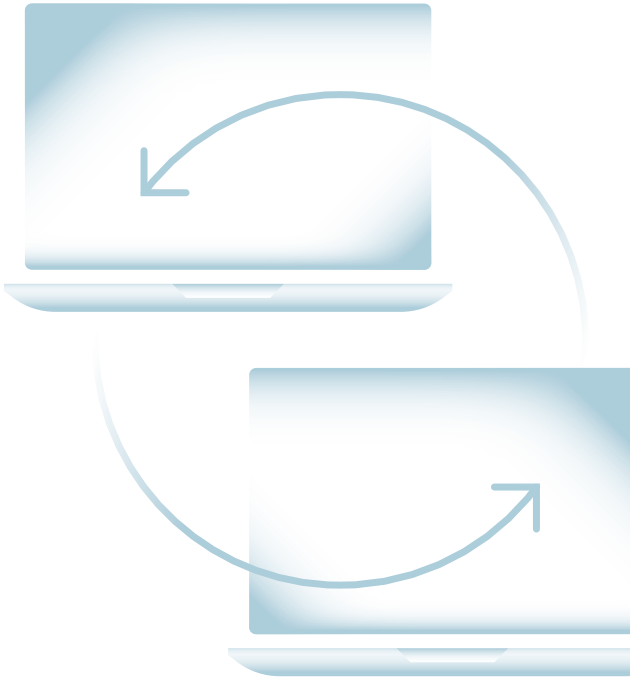


of the scripts running on a typical website are third-party

Client-side Supply Chain Attacks

Cybercriminals exploit vulnerabilities in the first-, third- and Nth-party JavaScript running on your site to inject malicious code. This leads to JavaScript behavioral changes on the page, which can affect network protocols and destinations, Document Object Model (DOM) elements, and storage properties and associated keys, including cookies and local or session storage.

Bad actors can take advantage of misconfiguration errors, typos, and outdated scripts to modify JavaScript and inject malicious code. They can also leverage code obfuscation techniques to hide the script's true intent.



By modifying client-side JavaScript, attackers can:

Change the behavior

of existing payment forms

Create fake payment forms

on the real site

Hide skimmers in images

that load on payment pages in users' browsers, the technique that was used in the 2022 attack on Segway[3]

Point to fake sites

with similar URLs to the site they intended to visit, leading the buyer to unknowingly submit a form on a fraudulent site

Malicious JavaScript In Action

The malicious client-side JavaScript loads into users' web browsers and collects the information typed into form fields when users submit a form. More sophisticated malicious code can capture what users type without them even hitting submit. A copy of the data is sent to a server controlled by the cybercriminal, even as the information continues to flow to your systems. This allows attacks to steal payment card industry (PCI) data and personally identifiable information (PII) from your users.

Here are some common types of attacks:

Digital Skimming and Magecart

These attacks steal payment information card data from visitors to your online store.

PII Harvesting attacks

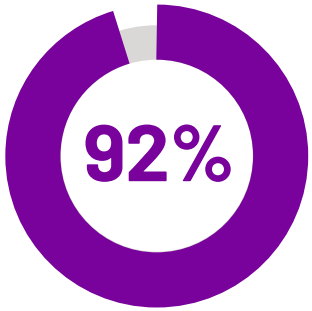
These attacks steal sensitive personal information, including login credentials, names addresses and social security numbers.

HUMAN researchers have identified multiple toolkits in the wild that make it easy for even inexperienced hackers to launch client-side supply chain attacks. Some of these toolkits are offered as Skimming as-a-Service, with "revenue" sharing between the hackers and the toolkit creators.

Why It's Difficult to Detect Risky Client-side Code

Lack of visibility at run-time

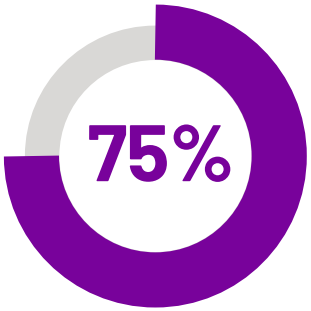
Because JavaScript code runs on users' browsers, it can be difficult to detect the behavior of scripts that load dynamically at runtime.



of website decision makers do not have complete visibility into the third-party code running on their site.

Insufficient security reviews

Developers may introduce code to an application without going through the appropriate security reviews to avoid delays in deployment.



of businesses do not run a security review for every third-party script modification.

Frequent code changes

Even if a script is reviewed when it is first added to a site, it does mean that subsequent modifications are secure.

of website owners state that the third-party scripts running on their web properties change four or more times every year.

Long supply chain

Third-party code may call on other fourth-, fifth- or Nth-party code, lengthening your software supply chain and increasing business risk.

of websites use 6 or more supply chain vendors, many of which may call on code from other Nth-party vendors.

Business Impact of Client-side Supply Chain Attacks

59%

of consumers won't buy from a company who has experienced a data breach in the past year[4]

Brand reputation damage

People may lose trust in your brand following a data breach, both current customers whose data was compromised and potential ones who saw bad press.

Regulatory fines

Many countries and states have enacted data privacy legislation that imposes hefty fines on businesses that fail to protect consumer data.

Lawsuits

Consumers may file lawsuits against businesses who expose their personal data, even if the breach arose from a third-party vendor.

Impaired website functionality

Supply chain attacks can affect a company's ability to deliver products and services, which affects business continuity and creates data inaccuracies.

Lower stock value

If you are a public company, your stock price may plummet following a supply chain attack, and investors may sell your stock to circumvent losses.

Costs to Your Business

Digital skimming attacks steal your users' personal data from your website. The resulting client-side data breaches expose your business to significant regulatory and civil penalties.

Cost of Client-side Data Breaches

Monthly uniques visitors to your website	10,000,000
Estimated records exposed	200,000
CCPA fines	$60,000,000
Statutory damages	$18,000,000
Administratvie costs	$3,600,000
Your estimated exposure from client-side data breaches	**$81,600,000**

LARGEST GDPR FINE

The largest fine ever to be levied under GDPR was for a client-side data breach. In 2019, British Airways was fined **$240 million** by the UK ICO for a data breach resulting from a Magecart attack on their travel booking website. This was later reduced to around $24 million.

Fines and Exposure

California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

- Up to $2,500 for each unintentional data breach, and up to $7,500 for each intentional disclosure
- California victims can seek significant statutory penalties, ranging from $100 to $750 per violation

General Data Protection Regulation (GDPR)

- Up to $22 million or 4% of the violating company's annual total revenue from the previous fiscal year — whichever is greater.

Reduce Your Client-side Code Risk

Information security teams can follow a few best practices to regain control of client-side code without becoming blockers.

1. Set up an agile notification and approval process for any third-party scripts or libraries used in your applications. This will ensure basic visibility and responsiveness, and facilitate a smoother feedback loop between developers and information security teams.

2. Use code analysis and verification tools to detect vulnerabilities before deployment. Static Application Security Testing (SAST) tools can find vulnerabilities in first-party scripts while Software Composition Analysis (SCA) solutions take inventory and analyze open source libraries in your own applications. Note that these cannot catch malicious scripts that load dynamically at runtime.

3. Enforce allowlists with Content Security Policy (CSP) to prevent unauthorized scripts from being loaded and stop malicious scripts from exfiltrating data. A few caveats are that CSP is complex to manage, can be bypassed and does not protect against a first-party compromise or insider threats where the attacker has access to resources on the allowlist. And CSP is all or nothing; you can either turn off a script entirely or leave it on as is.

4. Enable granular JavaScript blocking. This allows you to block client-side JavaScript from accessing sensitive form fields without disabling the entire script.

5. Invest in client-side application security solutions that provide continuous real-time visibility and control over all scripts running on your website. These solutions can detect if a new unfamiliar script gets loaded on the client side or if an existing script starts exhibiting suspicious behavior indicating a potential compromise. Such solutions can also automate CSP management and granular JavaScript blocking, and facilitate a trust-but-verify model for security.

Safeguard Your Digital Business

With a few best practices, your business can take advantage of third-party software and open source libraries without sacrificing security. An automated client-side application security solution provides continuous visibility and control over your client side supply chain, mitigating risk without adding manual work.

HUMAN Code Defender uses behavioral analysis and advanced machine learning to identify vulnerabilities and anomalous behavior. The solution proactively mitigates risk with a combination of granular JavaScript blocking and Content Security Policy (CSP).

GET A FREE CUSTOMIZED RISK ASSESSMENT

Understand your exposure to Shadow Code and reduce your risk of data breaches.

Protect Your Customer Data

Comply with Data Privacy Regulations

Preserve Brand Reputation

[1] httparchive.org
[2] Osterman Research: Shadow Code: The Hidden Risk to Your Website, https://www.perimeterx.com/resources/whitepapers/shadow-code-the-hidden-risk-to-your-website-2021/
[3] ThreatPost: Segway Hit By Magecart Attack Hiding in a Favicon, https://threatpost.com/segway-magecart-attack-favicon/177971/
[4] Security Intelligence: How the Rise in Cyberattacks Is Changing Consumer Behavior,https://securityintelligence.com/articles/rise-cyberattacks-changing-consumer-behavior/

HUMAN

About HUMAN

HUMAN is a cybersecurity company that safeguards 500+ customers from sophisticated bot attacks, fraud and account abuse. We leverage modern defense—internet visibility, network effect, and disruptions—to enable our customers to increase ROI and trust while decreasing end-user friction, data contamination, and cybersecurity exposure. Today we verify the humanity of more than 15 trillion interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN. **To Know Who's Real, visit www.humansecurity.com.**