Report URI

RESEARCH REPORT

10 Years of Web Security

2026 Edition

Snapshot taken 13 June 2026

Prepared by Scott Helme, Founder
Report-URI Ltd

> *The top 1 million websites, crawled every day since 2016. The figures in this report are the snapshot taken on 13 June 2026, when 819,002 sites responded.*

The decade in ten numbers

Our founder, Scott Helme, has crawled the top 1 million websites every day since 2016. This is the sixth time a decade of that data — HTTPS, CSP, header, and DNS — has been pulled apart in one place, across the 819,002 sites that answered on the day of this snapshot. Here is the whole thing compressed into ten numbers, and every section below unpacks one of them in more depth.

HTTPS adoption grew from 62,043 sites in 2015 to 658,038 today — 80.3% of everything that responded

252,846 sites now send HSTS

CSP adoption grew more than 12,000% over ten years, to 170,057 sites — and 114% since the 2022 crawl alone

Despite that growth, 46.8% of CSP policies still contain unsafe-inline, and only 0.2% use require-trusted-types-for, the strongest available defence against DOM-based XSS

Only 21% of sites sending HSTS qualify for the browser preload list once all three required directives are checked together

Of 314,878 sites that set cookies, 802 use the __Host- prefix and 1,913 use __Secure- — the strongest cookie hardening available, and free to implement

289,021 sites send Report-To, and 279,362 of those point at a single Cloudflare endpoint — around 97%

358,115 responding sites — 44% — now negotiate post-quantum key exchange, again driven by default changes at Cloudflare and Google

440,832 sites — nearly 54% — still score an F on basic security header grading

DMARC is published by 398,597 sites, and 204,769 of those — 51.4% — never left monitor-only mode

> **The pattern across all ten years: security controls that infrastructure providers can enable by default have improved steadily. Controls that require ongoing, active configuration have consistently lagged — even when adoption numbers look strong.**

The encouraging part first

Ten years ago, HTTPS was still a minority protocol. Today it is the default.

HTTPS — 62,043 sites in 2015, 658,038 today

A tenfold increase, and 80.3% of everything that answered the crawl.

HSTS — 252,846 sites, still climbing

No sign of plateauing.

CSP — roughly 1,400 sites in 2016, 170,057 today

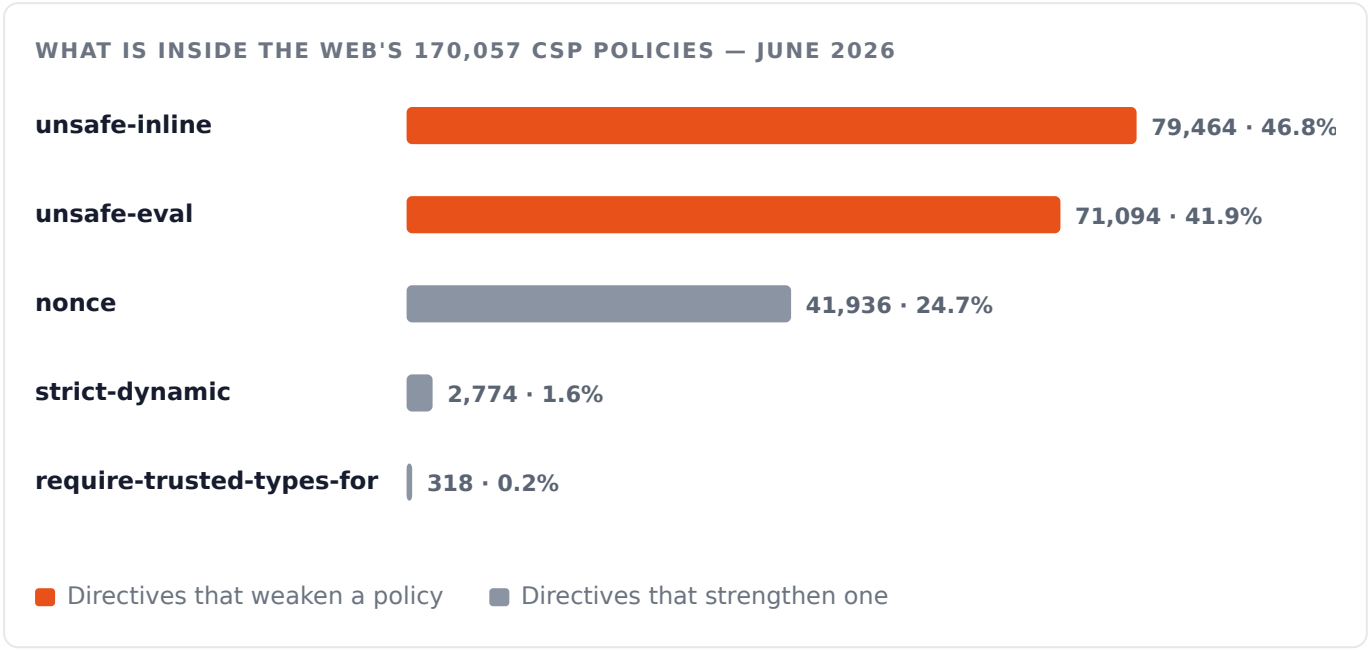
An increase of more than 12,000%, and the single biggest riser of the decade.

The foundational stuff is working. Browsers, CDNs, and hosting platforms have spent a decade pushing these numbers up, and it shows.

Adoption isn't the same as protection

CSP adoption more than doubled since the last crawl in 2022 — a 114% rise. That is the headline. It is also not the whole story.

Scott looked inside all 170,057 CSP policies from this year's crawl. This is what is actually in them:



`unsafe-inline` and `unsafe-eval` weaken the specific protection CSP exists to provide. A site with one of them set can accurately say “we have a Content Security Policy” while remaining exposed to the class of attack that policy was written to stop.

That is not carelessness, and it is worth being precise about why so many policies look like this. `unsafe-inline` is where nearly every policy starts, because removing it means knowing every inline script and style your pages actually run — across every template, every third party, and every tag someone added last quarter. Guess wrong and you break the site, usually on the page you could least afford to break. Faced with that, keeping the directive is the rational choice.

The way out is not willpower, it is data. Deploy in report-only mode, where nothing is blocked, and let real browsers tell you what is actually executing. Once the list is in front of you, moving to nonces or hashes is a known quantity rather than a gamble, and the directive can come out with the evidence to back it. That is exactly what these numbers say most sites have not done yet — not because CSP does not work, but because almost nobody has had the visibility to finish the job safely.

> **The 170,057 sites in this data are the ones that got the hard part right. They shipped a policy. What most of them are missing is the feedback loop that turns a first draft into a strong one.**

This is the clearest single example in ten years of data of a pattern that shows up everywhere else in this research: presence is easy to measure and easy to improve. Strength takes a feedback loop. See how CSP reporting provides one →

This isn't just a CSP problem

Once you see the presence-versus-strength gap in CSP, it is easier to spot elsewhere in the data.

HSTS — adoption up, configuration behind

252,846 sites send the header. But only 49.8% include `includeSubDomains`, 69.2% set a `max-age` of at least a year, and 29.2% send `preload`. Require all three — the actual bar for the HSTS preload list — and only 21% qualify.

Cookies — the basics land, the hardening doesn't

Of 314,878 sites setting cookies, most get `Secure` and `HttpOnly` right. But the `__Host-` prefix appears on just 802 sites, and `__Secure-` on 1,913. The strongest cookie protections available are free, and almost nobody uses them.

DMARC — half-measures at scale

398,597 sites publish a DMARC record. 204,769 of them — 51.4% — are still in monitor-only mode. The record exists, but enforcement was never turned on.

What all four have in common: none of them require new infrastructure. They require someone to go back and finish the configuration after the header, policy, or record was first switched on.

Improved by default	Stalled without active ownership
HTTPS — 658,038 of 819,002 sites (80.3%)	CSP strength — 46.8% still allow unsafe-inline
Reporting API — Cloudflare default	HSTS preload-readiness — only 21% qualify
Post-quantum key exchange — Cloudflare and Google default	Cookie hardening — 2,715 sites use __Host- or __Secure-
TLS 1.3 and 90-day certificates — CDN and CA driven	DMARC enforcement — 51.4% still monitor-only

The clearest gains came from one company flipping a switch

Some of this decade's biggest jumps did not come from thousands of individual security teams making thousands of individual decisions. They came from infrastructure providers changing what is on by default.

Reporting API — 289,021 sites, up from around 12,000 in 2020

Almost entirely because Cloudflare turned on Network Error Logging by default. Of those sites, 279,362 point at a Cloudflare endpoint — roughly 97% of the total.

Post-quantum key exchange — 358,115 sites, 44% of the responding web

From research curiosity to nearly half the web, because Cloudflare and Google enabled it by default.

Certificates — 77.4% now last 90 days or less

Driven by Let's Encrypt and Google Trust Services automating renewal. Over the same period ECDSA overtook RSA, 340,498 sites to 306,042, because certificate authorities changed what they issue by default.

The counter-example proves the rule. Extended Validation certificates — the one control here that required somebody to actively choose, buy and renew it — fell 51% to just 4,186 sites. Every control that got easier grew. The one that stayed manual died.

Infrastructure defaults are genuinely good for the web. They are also the reason the easy wins have concentrated at the top while the controls that need active, ongoing attention — the ones no CDN can flip for you — have lagged behind for a decade. One default flip, and an entire security posture changes overnight, for hundreds of thousands of sites at once.

Knowing you have a control isn't the same as knowing it's working

Across ten years and 819,002 sites, the pattern holds: the things that can be turned on for you tend to improve. The things that require someone to keep watching — what is actually

executing, whether a policy is still doing its job, whether a script changed since last week — tend to stall, even when adoption numbers look encouraging.

None of that is an argument against these controls. CSP is the single most effective thing you can put in front of a client-side attack, and the sites in this data were right to deploy it. The gap is not the policy — it is that most teams have never had sight of what their policy is doing once it is live, so a first draft stays a first draft. That is the gap Report URI closes, and each of the three pitfalls in this data has a specific way out.

Stuck on unsafe-inline

Run report-only and every inline script and style on your pages reports itself, from real browsers. Replace the directive with nonces once you can see the whole list, instead of guessing at it.

No idea whether the policy still holds

Policy Watch watches the header you actually serve and tells you when it changes, so a policy weakened during a release does not stay that way until someone happens to look.

New scripts arriving unannounced

Script Watch keeps a continuous inventory of what executes on your pages and flags anything new or changed — which is also what PCI DSS 6.4.3 and 11.6.1 ask you to evidence.

> **The next decade's challenge is not getting more sites to turn these protections on. Adoption climbs on its own. The unfinished work is getting the sites that already flipped the switch to finish configuring it properly — the difference between having a CSP and having one worth having.**

The same data, five different questions

Everything above is one dataset. What it obliges you to do next depends on what you are accountable for.

If you're a CISO

You can likely report “we have CSP” today. Can you report what is actually in it? The gap between deployed and enforced is exactly the kind of unquantified risk that turns into an uncomfortable answer at the next board question or audit.

If you're a Compliance or GRC lead

PCI DSS 6.4.3 and 11.6.1 require continuous script authorisation and change detection — not a policy on paper. A CSP header alone does not produce audit-ready evidence.

If you're a Security Engineer

If you have suspected your team's CSP looks better on paper than it performs, this data is confirmation rather than surprise. Every number here is a specific, countable directive, and that precision is what makes a finding actionable instead of another alert to tune out.

If you're an AppSec lead or Security Architect

“Most CSP deployments are weaker than they look” is not an opinion — it is 170,057 policies' worth of evidence, and the directive breakdown above is built to go straight into an internal deck.

If you're a developer or technical owner

None of this needs new infrastructure. Every gap here — removing `unsafe-inline`, adopting nonces, adding `__Host-` cookie prefixes — is a configuration change rather than a deployment. The barrier was never technical difficulty. It was that nobody circled back after the initial setup.

Frequently asked questions

How many websites use Content Security Policy (CSP)?

170,057 of the 819,002 sites crawled in June 2026 have a CSP — up from around 1,400 sites in 2016, an increase of more than 12,000%.

Is having a CSP enough to prevent XSS attacks?

Not on its own. Of all CSP policies crawled, 46.8% still contain unsafe-inline and 41.9% contain unsafe-eval — directives that undermine the exact protection CSP is designed to provide.

What percentage of websites use HTTPS?

658,038 of 819,002 responding sites, or 80.3%, now redirect to HTTPS.

Why did Reporting API adoption grow so quickly?

Almost entirely due to one company: Cloudflare enabled Network Error Logging by default for sites behind its network. Of the 289,021 sites sending Report-To, 279,362 point at a Cloudflare endpoint — around 97%.

What is the strongest CSP directive for preventing DOM-based XSS?

require-trusted-types-for. It is also the least used, present on just 318 of the 170,057 policies crawled — 0.2%.

How this was measured

The top 1 million sites, from the Tranco list, are crawled every day and have been since 2016. The figures here are the snapshot taken on 13 June 2026, when 819,002 sites responded; the ten-year comparisons come from the same daily series rather than from separate one-off crawls. Full methodology, per-metric data files, and the raw dataset are published at Crawler.Ninja, updated daily.

The findings here cover headers, cookies, CSP, and email and DNS hygiene. For the cryptography deep-dive — TLS versions, certificate lifetimes, and the arrival of post-quantum

key exchange at scale — read the full two-part analysis:

Part one: ten years of web security →
Part two: the state of crypto →