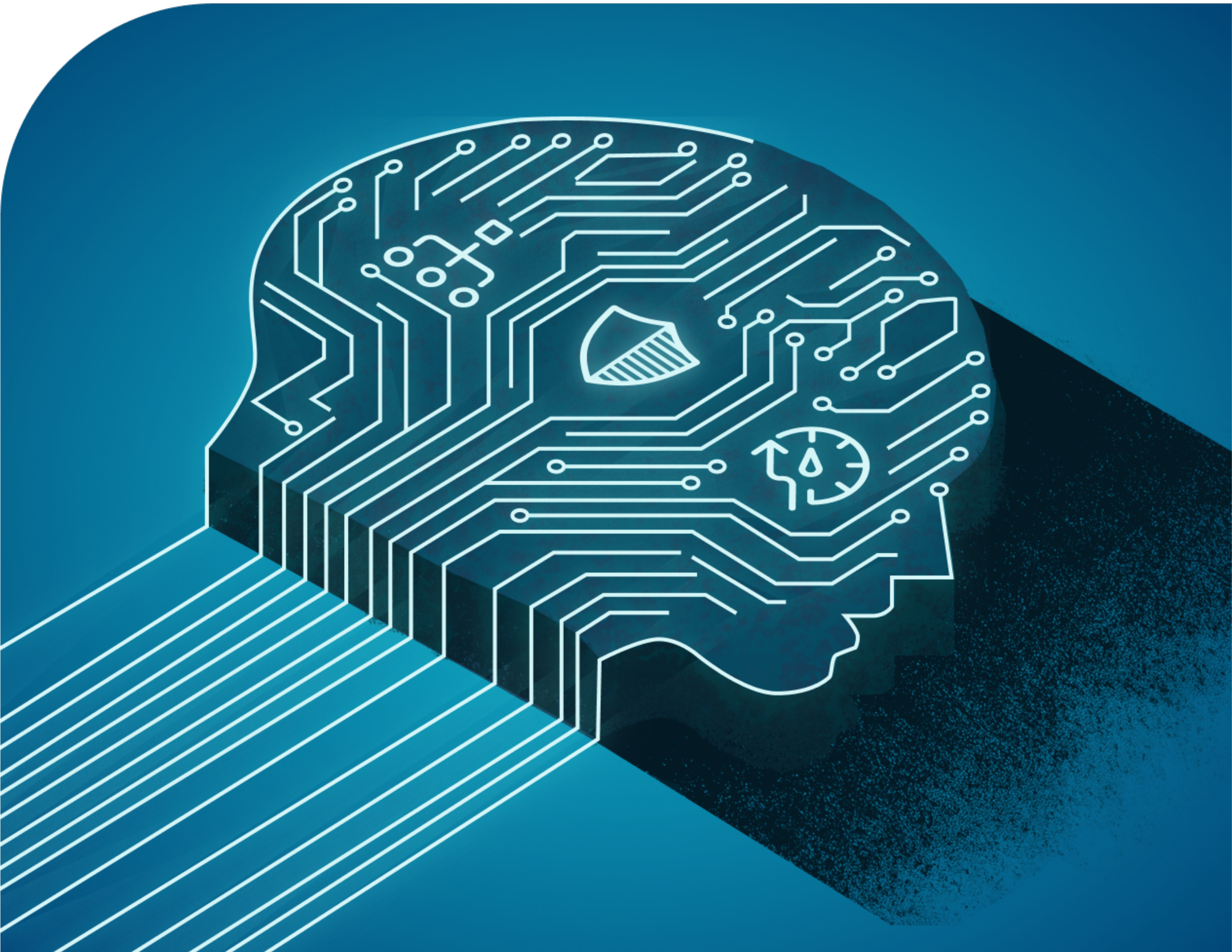
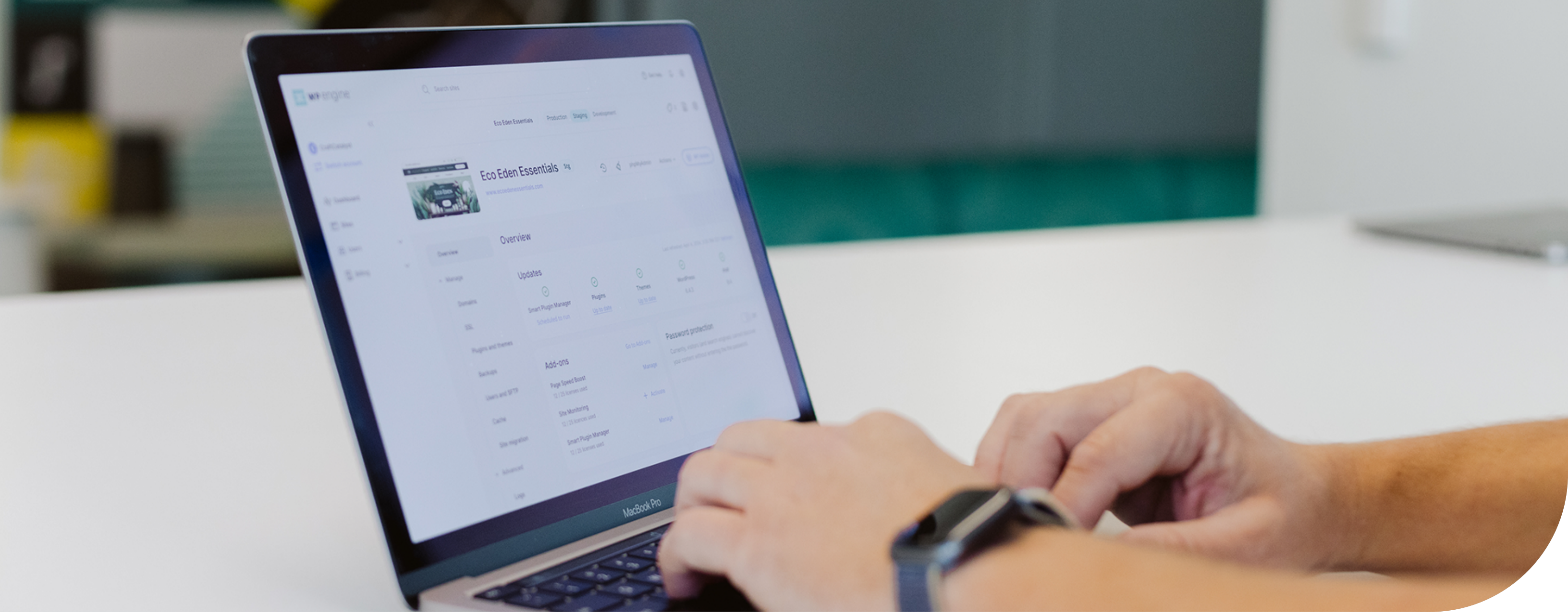
2025 Website Traffic Trends Report

The New Strategic Imperative: Intelligent Traffic Management





Introduction

The landscape of the internet has undergone a rapid and significant transformation. With the advent of Artificial Intelligence (AI), specifically LLMs and Agents, website strategies need **to focus on intelligent traffic management.**

WP Engine's 2025 Website Traffic Trends Report reveals a sobering reality: non-human traffic is rapidly reshaping how the web operates, and as expected, security and performance remain at the top of organizations' concerns and investments. As non-human traffic rises, it's having a growing impact on WordPress®[1] developers', agencies', and marketers' decision-making. This includes choices affecting security, performance, costs, and plugin adoption.

This report analyzes proprietary first-party data and metrics from Google CrUX and Cloudflare Bot Management on how the web is performing and transforming across North America, Europe, the Middle East, and Asia-Pacific.

[1] WP Engine is a proud member and supporter of the community of WordPress® users. The WordPress® trademarks are the intellectual property of the WordPress Foundation. Uses of the WordPress® trademarks in this website are for identification purposes only and do not imply an endorsement by WordPress Foundation. WP Engine is not endorsed or owned by, or affiliated with, the WordPress Foundation."

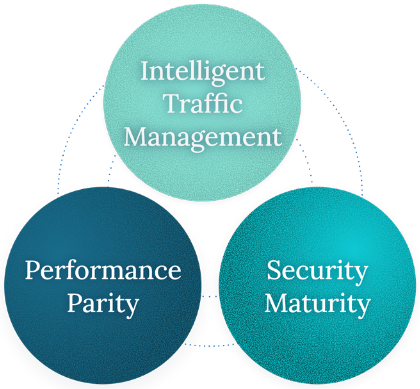
The three pillars of success:

Intelligent traffic management for continued performance and security excellence

- ✓ **Intelligent traffic management:** The AI-driven economy is redefining web traffic. Automated, non-human traffic accounts for a rapidly growing percentage of all web requests. We are seeing that AI-driven bots can consume as much as 70% of total traffic requests, making proactive traffic management a financial and performance necessity.
- ✓ **Security maturity:** We see evidence that intelligent traffic management can also help advance a website's security, and a lack thereof can be detrimental. The adoption of bot mitigation tactics tends to correlate with scale, as does security maturity. Although not strictly interdependent, there is a potential link between the modern bot mitigation and positive security outcomes.
- ✓ **Performance parity:** There is an uneven distribution of site performance between North America and the rest of the world. This is primarily driven by differences in the adoption rate of CDN capabilities.

Additionally, bot traffic is significantly higher in North America, having a more substantial impact on site performance.

Our findings indicate the time to take action to keep pace with AI-driven trends on the web is now. Failure to modernize infrastructure and operational practices in response to the rapid and ongoing shifts in human and AI-driven bot traffic changes is no longer a minor issue; it's a critical risk. To stay competitive, web teams must take urgent action. This report examines data supporting these trends and outlines the essential, immediate steps web professionals must take to secure, optimize, and future-proof their digital experiences.



1. Optimizing traffic at the edge:

How bot mitigation can reduce costs while improving performance and security

The AI-driven economy is redefining traffic

The composition of web traffic has undergone a fundamental change with the rise of automated, unverified bot traffic. The first pillar of a winning web strategy is shifting to **intelligent traffic management.** Simply put, this involves minimizing issues by proactively controlling the traffic that comes to your site.

The biggest shift in human-to-bot traffic distribution has been the rise of AI crawlers and other bot activity. Non-human activity averages about 30% of all traffic worldwide (Cloudflare), but it can vary widely by region and by site. These requests can have a substantial impact on a site's hosting resources and, as a result, impact its performance. This makes monitoring and managing non-human traffic volume and sources a strategic imperative for web teams.

Global human-to-bot traffic distribution is uneven

Cloudflare data indicates that the global average is about **30% bot traffic to 70% human traffic overall** (see Figure 1), with significant variability by region. The United States has far more bot activity than any other country or region; however, the ratio of AI-driven traffic is trending upward worldwide.

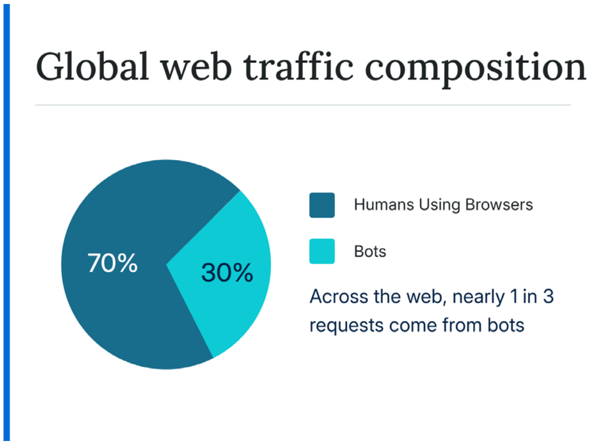


Figure 1. *Global human-to-bot traffic distribution*

Different kinds of non-human traffic can impact security

We also see subcategories of what is classified as bot traffic. Unsurprisingly, many are **AI-based crawlers.** The majority of this type of activity comes from **verified sources.** A verified bot is an automated crawler or software agent that **identifies itself** to the server it contacts.

In other words, when it visits a website, it sends a **user-agent string** or other metadata that clearly states what it is and what it's doing. The top three verified sources are GoogleBot, Meta-ExternalAds, and GPTBot.

A larger and fluctuating percentage of bot traffic now comes from **unverified sources.** An unverified bot is an automated program that hasn't completed a platform's official identity or security check, meaning its developer hasn't met all criteria. This can signify potential security risks, data misuse, or a lack of trustworthiness. Looking at bot traffic across WP Engine's customers' sites, we see a distribution of 24% verified bots to 76% unverified bots (see Figure 2). Unverified bot traffic is growing worldwide, drawing added attention and caution from web teams.

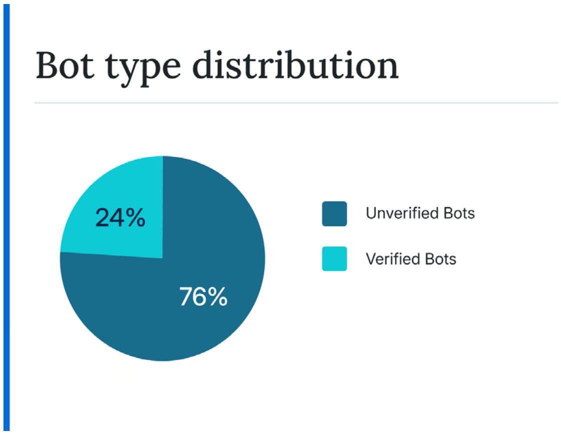


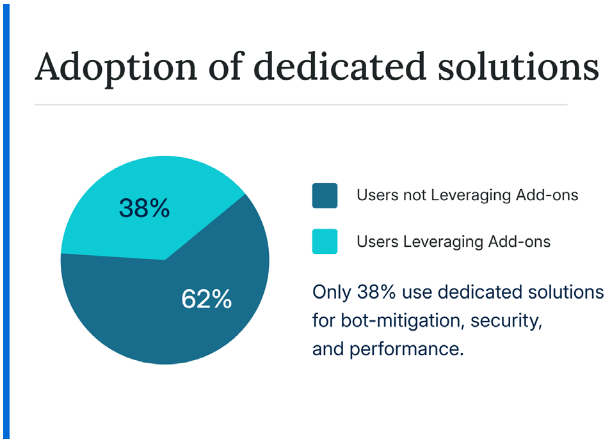
Figure 2. *WP Engine customers' bot type distribution*

Traffic across multiple regions can slow sites down

Sites with multi-region hosting face performance challenges. Traffic across Regional Internet Registry (RIR) boundaries tends to be slower, suggesting edge solutions like Content Delivery Networks (CDN) can improve load times and user experience. A CDN is a system of servers around the world that delivers website content to users from the server closest to them, making sites load faster and more reliably. It should be noted, however, that multi-region traffic may be artificially inflated by bots, highlighting the importance of effective bot management.

Bot traffic management trails security maturity

We analyzed activity across 26 customers and found that only 38% use a dedicated solution for bot mitigation, security, and performance like Global Edge Security (GES) by WP Engine. The remaining customers lacked tools like GES and/or consistent rule-setting, and consequently demonstrated a performance gap (see Figure 3). Bot traffic management appears to still be maturing; however, a clear divide exists between proactive, security-minded customers and those leaving potential performance and security gains on the table, presenting a strong opportunity for differentiation.



Only 38% use dedicated solutions for bot-mitigation, security, and performance.

Figure 3. *Use of tools like GES with bot mitigation*

Proactive strategies for bot mitigation

> **Navigating this new frontier shifts the strategic imperative to proactive intervention."**

The recommended action steps are structural and operational:

- **Factor bot activity into planning.** Hosting providers and web teams must fundamentally adjust bandwidth and resource planning to account for the actual **bot-to-human ratio as well as the verified-to-unverified bot ratio.** The old "traffic = users" equation is obsolete. By monitoring these ratios, teams can adjust hosting environments to scale appropriately in response to human traffic volumes while using mitigation to reduce the financial impact of bot bursts. Furthermore, sites with globally distributed traffic should actively look to reduce traffic from unexpected regions by using bot management technology and choosing a server location near their largest human audience.
- **Leverage edge security tools.** Tools like GES offer built-in, advanced bot mitigation that uses sophisticated techniques like fingerprint-based identification (JA/3 and JA/4). This is essential for accurately distinguishing between known, benign crawlers, malicious attacks, and resource-consuming AI bots. Agencies that regularly launch new projects should consider these comprehensive solutions as a new default security baseline.
- **Implement LLMs.txt.** While LLMs.txt is still in its early stages and hasn't quite hit critical mass among WP Engine-hosted sites, Cloudflare's growing role in mitigating bot infiltration could spur adoption as more enterprises seek better control over how AI crawlers interact with their sites. Following the established practice of robots.txt, a plugin like Website LLMs.txt generates and manages an llms.txt file. This structured, AI-ready index helps large language model (LLM) providers like ChatGPT, Claude, and Perplexity understand your site's most important content and how they should interact with the site. It also allows site owners to legally and technologically opt out of, or limit the use of, their content for training, providing a necessary layer of control over data access.

2. Maintaining security maturity:

How HTTPS and GES helps bring parity regardless of size

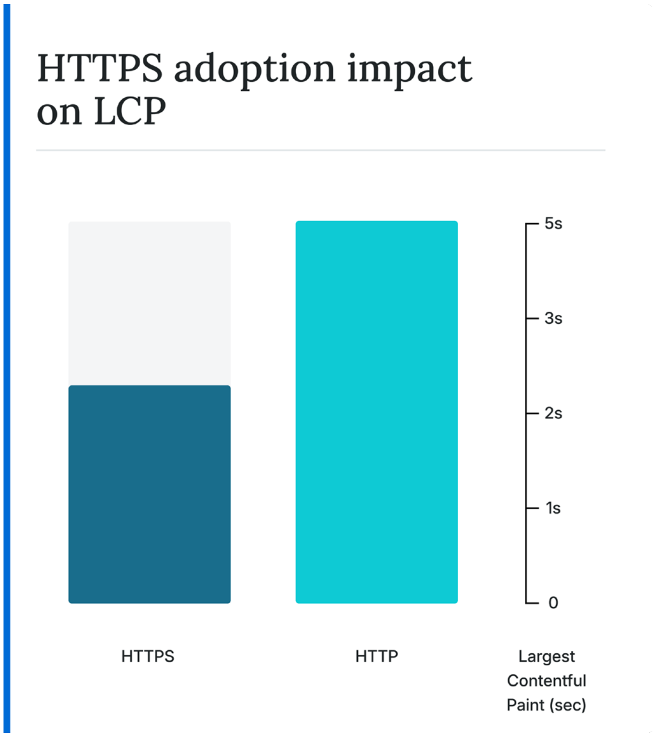
Security and speed are shown to be inseparable star players in a unified performance stack, with robust tools like GES (an enterprise-grade cloud-based security and performance add-on) playing the leading role. We see GES adoption significantly enhances both security and speed for websites built with WordPress. It works by integrating security measures at the network's edge (the server closest to the end user). That's why the most effective strategies for speed in the modern web are inherently security-based. However, our data shows that not all organizations are keeping pace.

The security divide corresponds to scale

Security is always a priority for website owners. However, the data shows us that a security gap is growing, and it's directly correlated with an organization's size. Our data shows that organizations with 10 or more employees, or have a reach of 100 domains or more, all have near-universal two-factor authentication (2FA) and HTTPS adoption is at 90% or greater. In contrast, solo or small site owners lag behind by **25%.** This is often driven by resource constraints, reliance on manual processes, and a misguided perception among smaller entities that they are "too small to be a target."

HTTPS adoption correlates to speed gains

Our data shows that HTTPS, traditionally viewed solely through a security lens, is now also becoming a performance driver. Sites that have not fully adopted HTTPS are experiencing performance losses. WP Engine customers' sites serving traffic exclusively over HTTPS are **1–5 seconds faster** in Largest Contentful Paint (LCP) LCP, demonstrating that encryption can be a performance enabler, not just a security layer. In other words, customers who invest in modern standards not only get HTTPS, but faster sites as well, likely due to improvements in newer HTTP standards and better ability to manage bot traffic.



HTTPS adoption impact on LCP

Figure 4. *WP Engine customers' HTTPS adoption impact on LCP*

Proactive security strategies

Bridging the security gap requires tailoring solutions to the resources and workflows of organizations of different sizes.

For small businesses and solo operators: The solution is not complex, but automation and managed hosting become paramount. For smaller sites where security is often an afterthought or a burden, the most effective way to close the performance gap is to shift the burden of routine security maintenance from the site owner to a managed provider. This is achieved by selecting a managed hosting provider for WordPress that:

- ✓ Enforces 2FA and Multi-Factor Authentication (MFA)
- ✓ Automatically handles core and plug-in updates
- ✓ Integrates vulnerability scanning into its services

For agencies and mid- to larger-sized teams: The focus must be on process enforcement and the elevation of a security culture. Security practices must be fundamentally embedded into DevOps workflows, a process known as DevSecOps. This means:

- ✓ Enforcing MFA across all team members, not just administrators
- ✓ Integrating security scans directly into the Continuous Integration/Continuous Deployment (CI / CD) pipelines
- ✓ Regularly validating backups as part of the security process
- ✓ Developing a proactive security culture that focuses on foundational components of every project and deployment

3. Closing the global speed gap:

How geography, mobile, plugins, and CDNs shape web performance

Every millisecond matters in a world where users expect instant access to content. Report findings indicate that the location of users, the devices they use, and whether sites utilize CDNs and edge caching all significantly impact load times and user experience.

The difference between the fastest and the slowest sites directly impacts user engagement, search rankings, and conversion rates.

Why is this happening? Despite the clear and established benefits of CDNs as a foundational technology for global performance, roughly **50% of the top 10 million sites tracked by Google CrUX are still not leveraging a CDN.** This represents a massive, untapped source of performance and reliability gains. Sites using CDNs see approximately a **20% improvement in LCP**, a key user-centric performance metric. This widespread failure to adopt a basic optimization technology is a surprising and significant contributor to the global speed difference. (See Figure 5)

CDN impact on performance

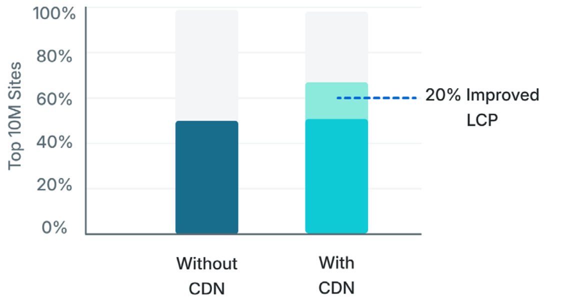


Figure 5. *Sites perform better with CDN adoption*

Mobile speed is a performance differentiator as well. Our data confirms the **persistent mobile lag** continues. Despite mobile being the dominant traffic source globally, mobile performance consistently trails desktop, revealing a costly optimization gap.

Finally, we see regional WordPress plugin patterns reflect different maturity curves and priorities, showing mature markets emphasize technical SEO and structured data, and emerging markets lean toward no-code, design-first tools that enable faster publishing. Globally, SEO tools (Yoast / WordPress SEO) dominate, underscoring the continued centrality of search optimization in enterprise site management.

Regionally, developer-centric tools (ACF PRO, Gravity Forms) are strong in North America, Australia, and Europe, showing a focus on structured content and backend control. The Middle East shows a preference for Genesis Blocks and Elementor, reflecting a visual, no-code approach to site building. (See Figure 6)

Commonly used WordPress® plugins on WP Engine by region

(as of September 2025)

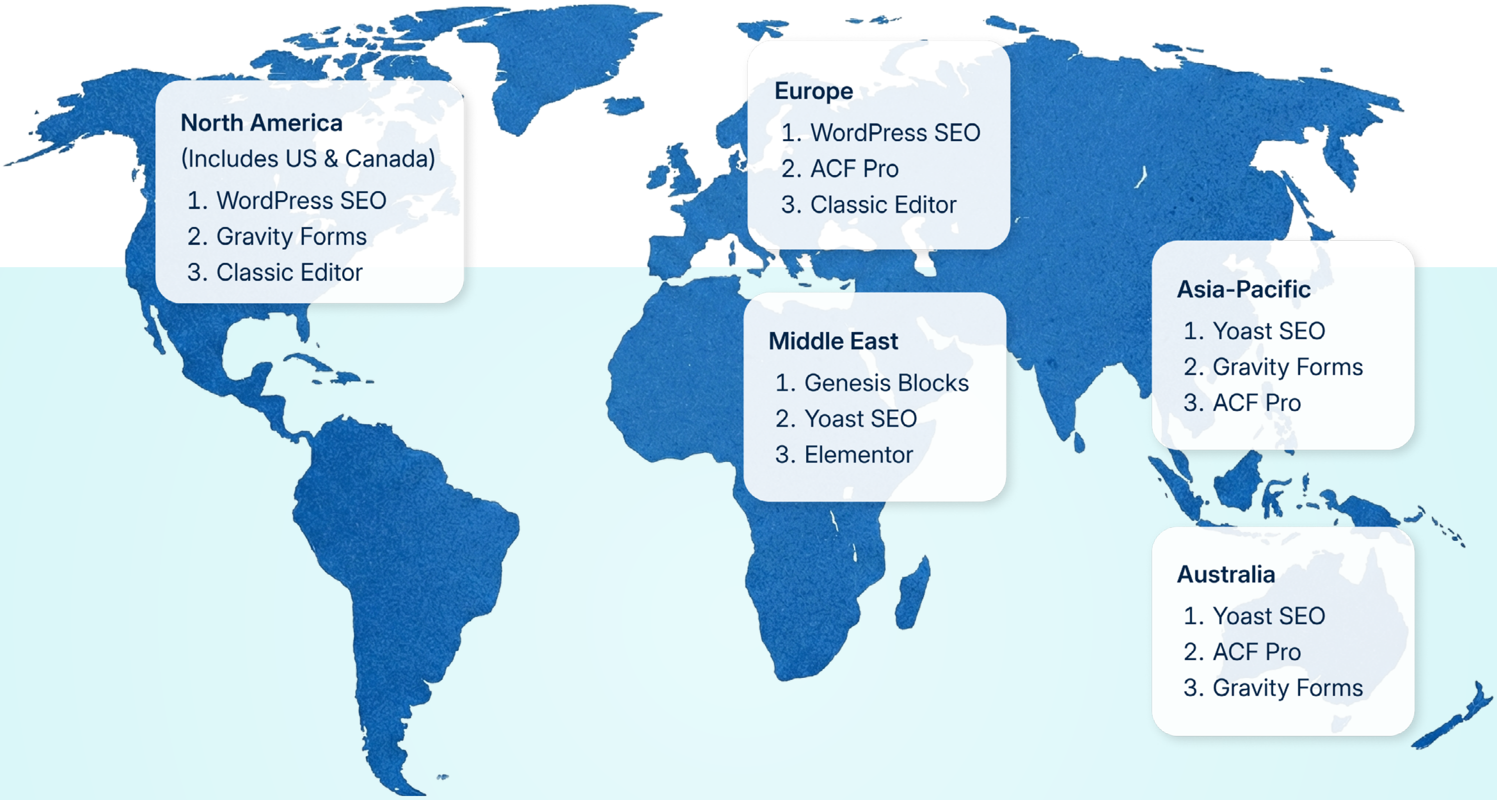


Figure 6. *WP Engine customers' top three plugins by region*

Your action plan

What web professionals must do next

The data in the WP Engine 2025 Website Traffic Trends Report reveals that AI-driven web activity is changing the strategic focus of digital businesses. The impact of non-human traffic on global performance, security, and cost divides is growing, creating a clear separation between web experiences that are competitive and those that are being left behind.

The three strategic pillars of intelligent traffic management, security maturity, and performance parity, **addressed together,** will define success in the competitive, mobile-first, and bot-driven web of 2026 and beyond. Failure to adapt to continuous traffic changes will inevitably lead to higher costs, slower user experiences, and a growing vulnerability gap.

Given these web traffic trends, what should you do next? The data shows those who modernize infrastructure, secure every layer, and proactively manage both human and AI traffic will define the next generation of high-performing digital experiences.

1. Manage AI and bot traffic proactively

□ Publish LLMs.txt or crawler policies to control unwanted crawlers and opt out of training use.

□ Implement bot management tools via Cloudflare or similar edge security providers. Agencies that build new projects regularly should consider using GES, which offers built-in, fingerprint-based bot mitigation.

□ Factor AI bot activity into hosting and bandwidth costs by monitoring the bot-to-human ratio. Hosting providers should consider implementing more robust default configurations in light of the increasing bot traffic.

2. Elevate security culture

□ Embed security practices into DevOps workflows.

□ Use managed hosting or implement DevSecOps pipelines that include vulnerability scanning and backup validation.

□ Implement and enforce Multi-Factor Authentication (MFA) across all users.

3. Make security a performance strategy

□ Adopt HTTPS everywhere.

□ Treat encryption as part of the speed stack, essential for performance and trust.

□ Upgrade to the latest, faster protocols, such as TLS 1.3.

4. Strategize globally

□ Choose a server location near the largest (human) audience.

□ Reduce traffic from unexpected regions using some bot management technology, while choosing a server location near the largest audience.

□ Adopt caching at the edge whenever possible.

□ Select a managed hosting plan that can both scale to human traffic volumes and reduce the impact of bursts of bot traffic.

5. Re-engineer for leaner, faster experiences

□ Audit plugins, scripts, and image weight to minimize static requests.

□ Optimize image delivery using modern formats and lazy loading techniques.

□ Treat page weight (<400KB) and static calls (<5 per page) as key performance KPIs (Key Performance Indicators).

6. Modernize for mobile and global audiences

□ Deploy edge caching and multi-region CDNs.

□ Monitor LCP(Largest Contentful Paint) and TTFB (Time to First Byte) across different geographies and devices to identify and systematically address performance gaps.

□ Localize assets and hosting for key markets to ensure proximity hosting.

At-a-glance: Top 5 priorities for web teams in 2026

Priority	Why It Matters	Action Steps
1. Manage AI and bot traffic	Two-thirds of all traffic is automated; AI bots now drive most costly requests.	• Publish LLM.txt or crawler policies. • Implement bot management via Cloudflare or similar. • Monitor bot-to-human ratios and adjust bandwidth planning.
2. Build security maturity into operations	Larger teams excel with 2FA and automated updates; smaller setups lag 25%.	• Enforce MFA across all users. • Automate plugin and core updates. • Integrate security scans into CI/CD pipelines.
3. Treat HTTPS as a performance enabler	Encryption now directly correlates with speed; HTTPS-only sites load 1–5 seconds faster.	• Enforce HTTPS everywhere. • Upgrade to TLS 1.3 and HSTS. • Combine HTTPS with fingerprint-based bot mitigation.
4. Re-engineer for lean, cached pages	Sites with fewer static requests (<5) and lighter payloads (<400 KB) achieve faster LCP and lower costs.	• Audit plugins, scripts, and image weight. • Use lazy loading and modern formats. • Make static request count a key KPI.
5. Optimize for a mobile-first, global audience	Mobile is now the dominant traffic source, yet global users (especially outside North America) still experience slower performance.	• Enable multi-region CDNs and edge caching. • Monitor LCP/TTFB by region and device. • Localize assets for key markets.

The mandate for modernization

Our research findings are a mandate for modernization. The data demonstrates traditional playbooks are beginning to fail. Global gaps in performance and security are widening. The key takeaways are stark:

- **The cost of inaction:** The rise of AI-driven bot traffic, which consumes up to 70% of the most costly dynamic resources such as hosting, environment, and performance, has transformed traffic management from an optimization task into a critical financial imperative. Ignoring the bot-to-human ratio is accepting inflated operational costs.
- **The security landscape in the context of unverified bot activity:** The 25% lag in security maturity for smaller entities is creating a systemic vulnerability for the entire web ecosystem. Security is no longer optional or reactive; it is a structural necessity that is inseparable from performance.
- **The impact of AI-driven traffic on performance:** Half of the top websites are still not leveraging foundational technology like CDNs, costing them critical seconds in load time and widening the gap between the fastest and slowest sites.

Failure to adapt to this new reality by embracing modern infrastructure and operational practices is no longer a minor issue, but a critical risk that leads to higher costs, slower user experiences, and increased vulnerability.

The strategic priority for 2026 and beyond is clear: commit to modernization. Real success happens where intelligent traffic management unites with performance and security. Organizations that advance all three together will narrow digital divides, secure their competitive advantage, better control costs, and deliver superior experiences on an AI-driven web.

The time for passive monitoring is over. It's time to execute.

Research methodology

The conclusions and recommendations in this report are based on proprietary first-party data from WP Engine with third-party data from Google CrUX Data and Cloudflare Bot Management. The research covers data from Q3 2025 and the period from September 2024 to September 2025 across global regions (North America, Asia-Pacific including Australia, Europe including the UK) and four focus areas: The Global Speed Gap, CMS & Plugin Trends, Security & Resilience, and Traffic Management Best Practices.

WP engine®

WP Engine empowers companies and agencies of all sizes to build, power, manage, and optimize their WordPress websites and applications with confidence.

Serving 1.5 million customers across 150+ countries, the global technology company provides premium, enterprise-grade solutions, tools, and services, including specialized platforms for WordPress, industry-tailored eCommerce and agency solution suites, and developer-centric tools like Local, Advanced Custom Fields, and more. Learn more at wpengine.com.

WP Engine is a proud member and supporter of the community of WordPress® users. The WordPress® trademarks are the intellectual property of the WordPress Foundation, and the Woo® and WooCommerce® trademarks are the intellectual property of WooCommerce, Inc. Uses of the WordPress®, Woo®, and WooCommerce® trademarks in this website are for identification purposes only and do not imply an endorsement by WordPress Foundation or WooCommerce, Inc. WP Engine is not endorsed or owned by, or affiliated with, the WordPress Foundation or WooCommerce, Inc.