WP engine | CLOUDFLARE

Security as a competitive advantage.

Protect your website from DDoS threats with Global Edge Security powered by WP Engine and Cloudflare.

WHITE PAPER

Table of Contents.

Introduction.

Enterprise-grade security isn't just a requirement for the enterprise anymore. Today, the growing availability of tools used for cyber attacks has significantly lowered the barrier of entry for would-be attackers, making businesses of all sizes potential targets. Taking proactive measures against threats like Distributed Denial of Service (DDoS) attacks has become a crucial step every organization needs to take, especially as these attacks become more sophisticated, and target more businesses across a wider set of verticals than ever before.

An evolving threat, a growing target list.

Imagine filling a water balloon with so much water it bursts. A DDoS attack does a similar thing to a website; a nefarious actor sends a flood of bogus traffic to a website, application, or server in an attempt to knock it offline. DDoS attacks have been around for a long time—about as long as the Internet has seen widespread use—so why are they still an issue? Because they've evolved. As defenses against DDoS attacks have gotten bigger and better, so too have the attacks themselves. While this arms race of sorts has played out, it's created a changing set of dynamics.

Rise of the botnets.

The main ingredient of a DDoS attack is capacity—the network resources an attacker uses to overwhelm their victim. Capacity can be built up using a number of tools, although botnets are one of the most popular. A botnet is a network of infected computers that flood an IP address with traffic in an attempt to knock a server or network offline. Because each bot is a legitimate Internet device, separating attack traffic from normal traffic can be a challenge.

A growing scale.

The capacity of a DDoS attack is generally measured by the amount of data an attack is sending every second. Early DDoS attacks, for example, were clocked at less than 100 gigabits per second (gpbs), and those lower-level attacks can still cause damage, but today, attacks measuring in the hundreds of gpbs have become commonplace. As defenses against DDoS attacks harden, the size of these attacks has increased. In 2018, for example, Github was hit with one of the largest DDoS attacks ever recorded, at 1.35 terabits per second. A few days later, a 1.7 tbps attack was recorded against another target.

As hackers create more powerful DDoS attacks to try and outmaneuver growing security measures, they're finding new ways to amplify their efforts. Memcached servers, which use an object caching system that speeds up web applications by reducing database load, have become a new, favorite tool of attackers. These types of DDoS attacks are some of the largest ever recorded, including the Github attack mentioned above.

New motivations.

Early DDoS attacks were often attributed to lone hackers testing the limits of their technical prowess, but today's attackers run the gamut from skilled, individual criminals to groups of well-trained nation-state actors. Their motives are different—they span everything from silencing political opposition to financial gain—but the sheer power of these attacks, combined with the widespread availability of the tools needed to conduct them, has made DDoS the weapon of choice for a growing number of bad actors with a laundry list of grudges.

Carrying out a DDoS attack used to require a distinct set of skills and capabilities. Today, there's even a growing market for DDoS attack services, which are bought and sold using cryptocurrencies on the dark web. This has effectively democratized the DDoS attack, making it available to anyone who wishes to harm an organization (or an individual) for any number of reasons. DDoS attacks are now deployed for things like revenge or ransom, against smaller targets that appear vulnerable to these types of attacks.

DDoS as a vehicle for ransom.

Because they can tap into new, powerful attack methods with relative ease, a growing number of criminals are using DDoS attacks as a way to victimize smaller businesses that don't have strong cyber defenses in place and hold them hostage. Today, hackers will initiate a DDoS attack, or simply threaten to do so, until their victim pays up. Unfortunately, without any DDoS mitigation in place, businesses or website owners have little recourse in this situation, and today, hackers will target anyone they believe is able to pay the ransom, including "low profile" small or medium-sized businesses.

Today, all businesses need protection.

Going offline, even for a few seconds, can be extremely damaging to a business. This is particularly true for ecommerce companies, which can measure lost revenue by the second, but it can affect any business long-term when it comes to their brand and reputation. Being associated with any type of security breach can have a devastating effect and years of carefully building a brand can be destroyed in seconds by even the smallest cyber attack.

Trust is key.

As younger generations increasingly prefer more authentic, personalized digital experiences, safeguarding their trust is paramount to capturing the data needed to tailor those experiences for them. Put simply, you need your customers to trust you if they're going to share data with you, and if your website goes down due to a security breach of any kind, you will lose that trust. This is one of the main reasons security has become a competitive advantage today—it enables trust, and allows you to continue building loyalty among a widening customer base.

WordPress-specific expertise.

While every website needs security, the solutions needed will differ depending on the site. WordPress, for example, has specific security considerations that need to be taken into account to prevent bad actors from successfully attacking the platform. To make sure these considerations are top of mind, WP Engine leans on an army of in-house WordPress experts to help you keep your WordPress environments up-to-date and free of faulty plugins.

Security as a competitive advantage.

For protection against today's DDoS attacks, which helps protect your revenue stream and builds consumer trust, WP Engine offers customers advanced security solutions such as Global Edge Security. Offered in partnership with Cloudflare, Global Edge Security is enterprise-grade security intelligence built on dynamic learnings from more than 12 million websites. It prevents and mitigates risks through DDoS protection with a globally distributed edge network and a managed WAF with customized rulesets. This advanced security offering also includes access to Cloudflare's global CDN with a staggering 150+ PoPs, and it brings your SSL encryption to the edge to ensure a performant experience for your end clients. Combined with the security built into WP Engine's Digital Experience Platform, Global Edge Security is the highest level of security available to our customers.

About WP Engine.

WP Engine is the world's leading WordPress digital experience platform that gives companies of all sizes the agility, performance, intelligence, and integrations they need to drive their business forward faster. WP Engine's combination of tech innovation and an award-winning team of WordPress experts are trusted by over 70,000 companies across 130 countries to provide counsel and support, helping brands create world-class digital experiences. Founded in 2010, WP Engine is headquartered in Austin, Texas, and has offices in San Francisco, California; San Antonio, Texas; London, England; Limerick, Ireland; and Brisbane, Australia.

www.wpengine.com

CLOUDFLARE®

About Cloudflare

Cloudflare is the leading cloud-based Internet performance and security company that provides content delivery network services, DDoS mitigation, Internet security, and scalability features such as CDN and page caching. Cloudflare's services sit between site visitors and the Cloudflare user's hosting provider, acting as a reverse proxy for websites. Founded in 2009, the company's headquarters are located in San Francisco, California, with additional offices in Singapore; London, England; Champaign, Illinois; Austin, Texas; Boston, Massachusetts; and Washington, D.C.

WP engine®

CLOUDFLARE®

wpengine.com

cloudflare.com