G.E.S.

GLOBAL EDGE SECURITY

okidoki

‘Säker Drift’ Security

At Okidoki, we prioritize the security of our clients’ websites with utmost seriousness. This commitment involves ensuring our clients benefit from access to some of the most sophisticated security solutions available today.

Our service, “Säker Drift,” is equipped with an array of advanced security features right out of the box, designed to safeguard your digital presence effectively. Such as **Site Monitoring**, **Smart Plugin Manager**, **SSL**, standard **DDoS Mitigation** and **Cloudflare**. Cloudflare provides a suite of services aimed at improving the performance, security, and reliability of websites and web applications. These features help safeguard your website from some of the most common security threats and ensure encrypted connections.

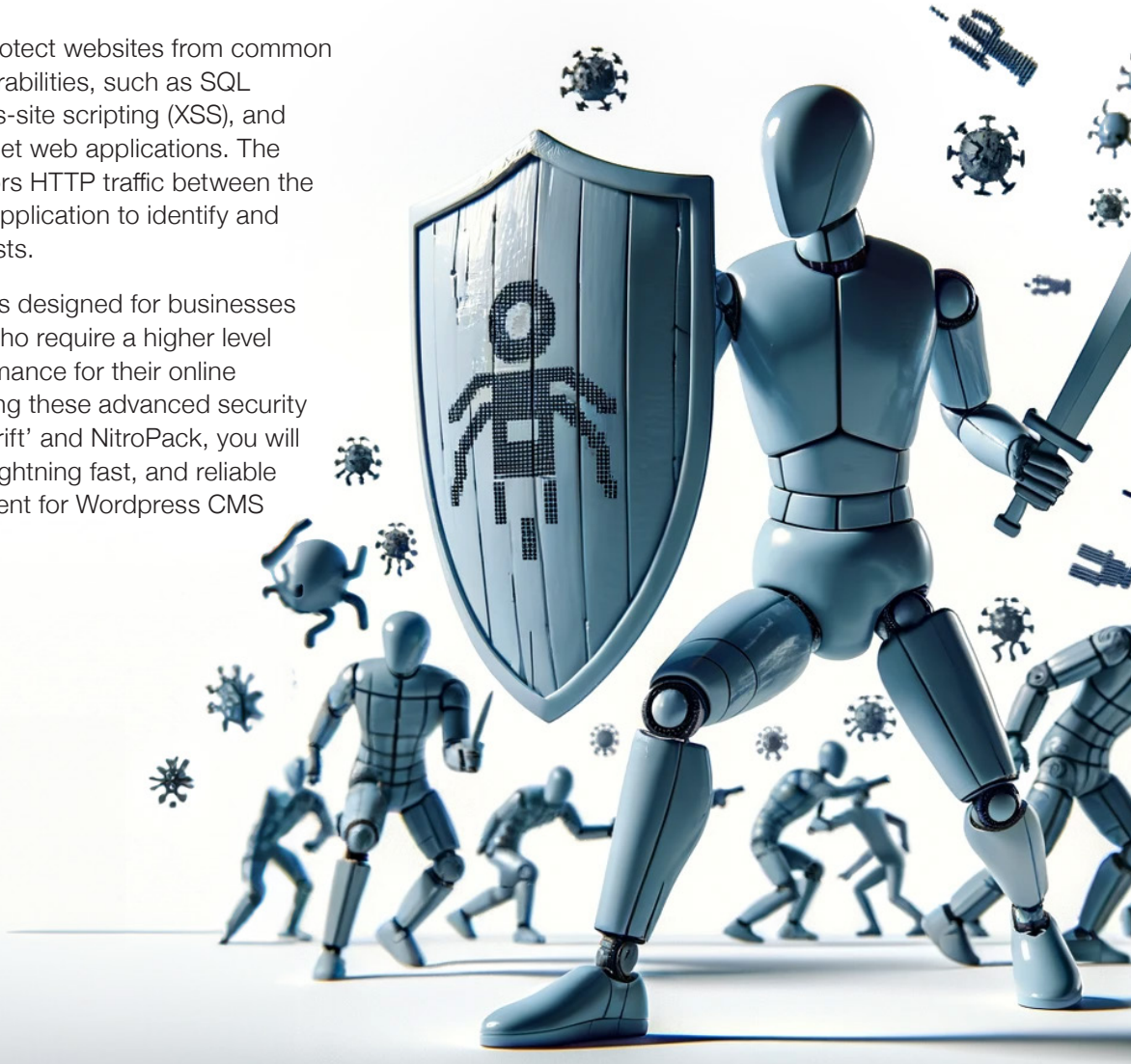
However, there are instances when a standard solution doesn’t quite meet all the needs. In such cases, the **Global Edge Security, or GES,** steps in to provide an additional layer of sophisticated protection.

What is Global Edge Security?

Global Edge Security (GES) is a comprehensive security solution designed to enhance the security, performance, and reliability of websites hosted on our cloud platform. This solution leverages advanced technologies and partnerships, including Cloudflare’s global network, to provide a robust suite of security features.

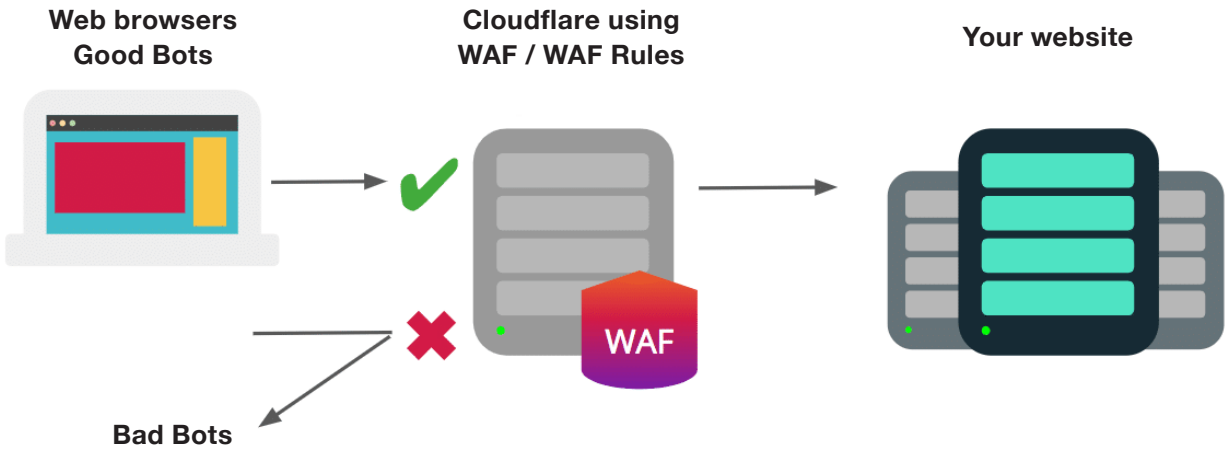
GES uses a WAF to protect websites from common web threats and vulnerabilities, such as SQL injection attacks, cross-site scripting (XSS), and other exploits that target web applications. The WAF filters and monitors HTTP traffic between the internet and the web application to identify and block malicious requests.

Global Edge Security is designed for businesses and website owners who require a higher level of security and performance for their online presence. By combining these advanced security features with ‘Säker Drift’ and NitroPack, you will get the most secure, lightning fast, and reliable web hosting environment for Wordpress CMS available today.



Managed Web Application Firewall (WAF)

The Managed WAF provides a robust security layer designed to identify and block sophisticated attacks against your web applications. It uses a set of predefined, constantly updated security rules to protect against vulnerabilities:



Cross-Site Scripting (XSS)

These types of attacks happen an attacker injects malicious code into a legitimate (but vulnerable) application. Attackers can manipulate JavaScript and HTML to trigger the malicious code or scripts. In this way, the vulnerable application or website is used as the "vehicle" to execute the script on the end user.

SQL Injection

SQL injection attacks happen when an attacker attempts to input meta characters into a vulnerable web-based form with malicious intent, and these attacks affect database-driven sites (which include WordPress).

Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery involves taking over or impersonating a user's browser session by hijacking the session cookie. CSRF attacks can trick users into executing malicious actions the attacker wants, or into taking unauthorized actions on the website. In this example, the session cookie is the "vehicle" an attacker uses to impersonate a legitimate user.

Cloudflare's edge servers also use the OWASP ModSecurity rule set at the edge, protecting your website from the OWASP top-10 vulnerabilities at all times. And, the automated Browser Integrity Check will evaluate request headers to determine whether a request is coming from a real web browser or not.

In addition to the security vectors outlined above, the WAF powered by Cloudflare takes advantage of a unique set of security rules defined by Cloudflare through years of experience identifying and mitigating attacks.

Implementing the Managed WAF comes with an additional cost over the basic Cloudflare services included in 'Säker Drift'. However, the investment is justified by the enhanced security and potential cost savings from preventing security breaches.

The choice to use Cloudflare with Managed WAF should be guided by your specific security needs, compliance requirements, cost and the sensitivity of the data and applications you are protecting.

‘Säker Drift’ Comparison overview

PRE-INSTALLED SECURITY

- ☑ **Site Monitoring**
- ☑ **Managed SSL Certificates**
- ☑ **Third-party SSL option**
- ☑ **Standard DDoS Mitigation**
  Standard and Cloudflare
- ☑ **Automatic Wordpress Version update**
- ☑ **Smart Plugin Manager**
  Every sunday during off hours
- ☑ **Content Activity Log**
- ☑ **WP 2FA (Optional activation)**
- ☑ **ReCaptcha (Optional activation)**

GLOBAL EDGE SECURITY UPGRADE

- ☑ **Advanced DDoS Mitigation**
  Standard, Cloudflare, and WAF rules
- ☑ **Managed Web Application Firewall (WAF)**
- ☑ **Optimized Network Routing using Cloudflare Argo**
- ☑ **Tiered Caching using Cloudflare Argo**
- ☑ **Additional monthly cost $250**

PRE-INSTALLED SPEED OPTIMISATION

- ☑ **CDN using Cloudflare**
- ☑ **Dynamic Content**
  Cached at origin
- ☑ **Static Content**
  Cached by CDN
- ☑ **Automatic Image Optimization**
  Cloudflare Polish
- ☑ **Automatic WebP Conversion**
  Cloudflare Polish
- ☑ **HTTP/3**

NITROPACK ‘LUDICROUS’ UPGRADE

- ☑ **World-class proprietary speed algorithm**
- ☑ **Built-in global CDN**
- ☑ **Smart cache invalidation**
- ☑ **Preloading data & Automatic cache warmup**
- ☑ **Device and cookie-aware caching**
- ☑ **Browser and session-aware caching**
- ☑ **Lossy and lossless image compression**
- ☑ **Advanced Lazy loading (including background images defined in the CSS)**
- ☑ **Preemptive image sizing**
- ☑ **Automatic WebP Conversion**
  Using NitroPack
- ☑ **Adaptive Image Sizing**
- ☑ **HTML, CSS and JS minification & compression**
- ☑ **Critical CSS, DNS prefetching, preloading ... and more**
- ☑ **Additional monthly cost $35**

okidoki

Contact us for additional information via
E-mail info@okidoki.se or by
Phone 013 - 31 22 17