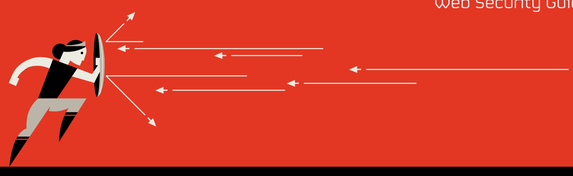


DEFLECT

Get Protected. Stay Connected with Deflect.

Slow-downs and interruptions can only do one thing: **hurt business and readership.**

Today's online world is more connected than ever. Services and content are consumed on demand. **Being knocked offline even just for a couple hours can mean the difference between having a new sign-up or reader, or missing that opportunity forever.**

Small businesses are affected

43% of cyberattacks target small businesses. Why? Because large corporations have had the budget for years to design their own defence systems, while smaller companies remain vulnerable.

What would it take to manage DDOS attack security on your own?

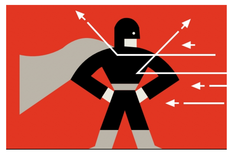
- **Manually handling regular backups**
- **Knowing the exact extent of your hosting provider's web security**
- **Knowing the service and security measures of your domain name provider**
- **Implementing solutions to mitigate attacks in advance**

You would need an IT expert to handle the following:

- Configure caching (either nginx fastcgi or plugins like WordPress super cache).
- Analyze logs and write rules to disable search if an attacker hits the site.
- Ensure server resources - hosting on 1.5 cores with 0 GB of RAM will not be enough
- Block bots using fail2ban tools that create rules for IP tables.
- System resource management - parsing logs and banning/unbanning bots
- Monitoring of site availability (from Google.Metrics before Uptimerobot / Statuscake)
- Read metrics to understand server resource load and total bandwidth
- Install external services such as newrelic/datadog as system support

However, if a sizeable (100 GB or more) attack occurs to your site, it's unlikely you will be able to fight this off using your own infrastructure. Most likely, your server will simply turn off the hosting provider so that other users are not affected by the increased traffic load during the attack.

When you implement a complete cloud service for your website's security, you won't need to set up any additional systems like the ones listed above, saving on system administrator costs and ensuring complete protection.



Connect your site NOW for complete protection from cyberattacks ->

Establishing a proprietary software and hardware system to protect a site or sites makes sense only for very large companies with multi-million dollar budgets. In addition to financial and time costs for the purchase and configuration of equipment and software, you must also staff specialists and constantly update their knowledge and skills.

Even a high-quality defense system will be ineffective if an attack exceeds the capacity of the channel through which the system is connected to the internet. For this reason, the largest companies use several protective systems at the same time, including the channels of protection provided by their service providers.

Any proprietary defensive system that you set up will inevitably become vulnerable. Even if attacks do not happen all the time, your infrastructure will age, and hackers constantly find new ways to infiltrate systems and increase the power of attacks.

Therefore, even the largest businesses now outsource website protection. The use of SaaS (software as a service) security allows you to quickly harness a complete and reliable service without needing to undertake the complex technical integrations listed above. Plus, the cost of upgrading infrastructure and developing new anti-DDoS and other tools is taken over by the security provider.

Learn more at deflect.ca

Added benefits of Deflect

Protection on Deflect's secure cloud server accelerates the delivery of your site's content while blocking malicious traffic before it passes through to the hosting client's servers. This ensures the continuous and responsive operation of any site protected by this system.

DEFLECT

DDoS defence, up to layer 7 protection, malicious bot mitigation enhanced by machine learning, secure hosting and more

Get Protected. Stay Connected with Deflect.