What is CloudFlare?
CloudFlare is a performance and security service that we provide to our customers. On average, a website on CloudFlare loads twice as fast, uses 60% less bandwidth, has 65% fewer requests and is way more secure.

What is the association between HostArmor and CloudFlare?
CloudFlare is a third-party vendor that is offering CloudFlare to HostArmor customers through a partnership. This partnership is in beta.

We are continually striving to make the service the most effective, so let us know what you think. You can contact either HostArmor or the CloudFlare Team at support@cloudflare.com.

How does CloudFlare's technology work?
CloudFlare works as a reverse proxy. What this means is that once your website is part of the CloudFlare community, your web traffic is routed through CloudFlare's global network.

CloudFlare's network stores copy of your static files closer to your visitors, which means they are delivered more quickly than before. We cache resources such as CSS, JavaScript and images. You do not have to make any changes on your end, CloudFlare's technology automatically decides which resources to cache based on file extension names. We do not cache dynamic content. CloudFlare also does compression for every request.

CloudFlare's network also blocks threats and limits abusive bots before they hit your server, which means less wasted bandwidth and server resources for you.

Where are CloudFlare's data centers located?
CloudFlare's network currently has 12 locations. San Jose (US), Los Angeles (US), Chicago (US), Washington, DC (US), New Jersey (US), Dallas, Amsterdam, Paris, Frankfurt, Hong Kong, Singapore and Tokyo. At each of these nodes, CloudFlare does caching and bot filtering. We will be adding additional data centers in London and Miami in July 2011.

What types of websites can use CloudFlare?
Almost all websites can use CloudFlare. CloudFlare works for both static and dynamic websites.

CloudFlare is not suitable for websites that stream video or audio directly from their origin server. If you use YouTube or Vimeo for the videos embedded on your website, then that is compatible with CloudFlare.

My website has SSL. What do I do?
If you have SSL, your website can use CloudFlare, however there is an extra step. If your SSL is on its own sub-domain (i.e. SSL), then ensure that this sub-domain is marked with a gray cloud. If your SSL is on your root domain or www, then you have to upgrade to the paid, Pro service and follow the directions outlined here.

Will CloudFlare accelerate and protect my root domain?
CloudFlare can only accelerate and protect CNAMES. Since your root domain is an A record, we recommend that you forward your traffic to 'www' through your .htaccess file. If you do not forward the traffic, then any traffic to www.mydomain.com will be accelerated and protected by CloudFlare (and shown in the statistics) and any traffic to mydomain.com will not be served by CloudFlare.

Are there sub-domains I shouldn't enable with CloudFlare?
Sub-domains on CloudFlare are marked with an orange cloud. Sub-domains not on CloudFlare are marked with a gray cloud.

The CloudFlare network can only proxy web traffic over port 80 and 443. The following sub-domains should be marked with a ***gray cloud*** to prevent performance issues:

cpanel
direct
ftp
ghs.google.com
mail and webmail
mysql
nameservers (NS1, NS2)
secure* (unless you enable CloudFlare SSL)

View the full list of sub-domains here:

http://www.cloudflare.com/wiki/What_subdomains_are_appropriate_for_orange_/_gray_clouds

Can I enable CloudFlare on a wildcard (*) sub-domain?
No, for security reasons, CloudFlare does not proxy traffic to a wildcard sub-domain. You have to explicitly list the sub-domain as a CNAME in your DNS records to be able to activate CloudFlare.

Can I enable CloudFlare on my root domain (i.e. mywebsite.com) that is an A record?
If you activate CloudFlare through HostArmor, CloudFlare can only accelerate and protect CNAMEs, not A records, which often includes the root domain. If you have traffic that goes to your root domain and you want to accelerate and protect the traffic using CloudFlare, you can add a redirect to 'www' in your .htaccess file. You should work with HostArmor, but as a general outline, a redirect looks as follow:

```
RewriteEngine On
# Rewrite added for CloudflareInstall - mysite.com
# Wednesday 25th of August 2010 04:59:42 AM
RewriteCond %{HTTP_HOST} ^mysite.com$ [NC]
RewriteCond %{SERVER_PORT} ^80$
RewriteRule ^(.*)$ http://www.mysite.com/$1 [R=301,L]
```

I activated CloudFlare from my HostArmor account. Do I also get an account on CloudFlare.com? What is the difference?

Once you activate CloudFlare on HostArmor you also get an account at www.cloudflare.com. The basic statistics and settings are shown in your HostArmor control panel. To see more statistics, your Threat Control panel and all the CloudFlare settings, you have to log in to your www.cloudflare.com account.

(Hint: To access your account the first time, enter the email address associated with your HostArmor account and use the "I forgot my password" feature).

I tried CloudFlare and have an issue. What should I do?
When you enable CloudFlare, there should be no noticeable difference to your website. If your site is loading slowing after enabling CloudFlare, there is most likely a problem. First, disable CloudFlare by

clicking the orange cloud so it becomes gray. Second, report the issue to HostArmor. The HostArmor team will work with CloudFlare to resolve the issue.