Hoe Imunify360 met Captcha werkt

Wat is Imunify360 Beveiliging?

Imunify360 is beveiligingssoftware die geïnstalleerd is op al onze Shared Hosting servers bij PixelHosting. Het is ontworpen en ontwikkeld door het geweldige team van Cloudlinux. Imunify360 maakt gebruik van kudde-immuniteit en de zes-lagen aanpak om onze hosting klanten te voorzien van het hoogste niveau van beveiliging tegen alle soorten van kwaadaardige aanvallen. Dit omvat DDOS-aanvallen, Mod Security-bescherming, malware scanning, website reputatiebeheer en een geavanceerde firewall. Imunify360 is ontworpen om abnormaal gebruikersgedrag te detecteren, waaronder brute-force aanvallen die steeds vaker voorkomen bij WordPress sites.

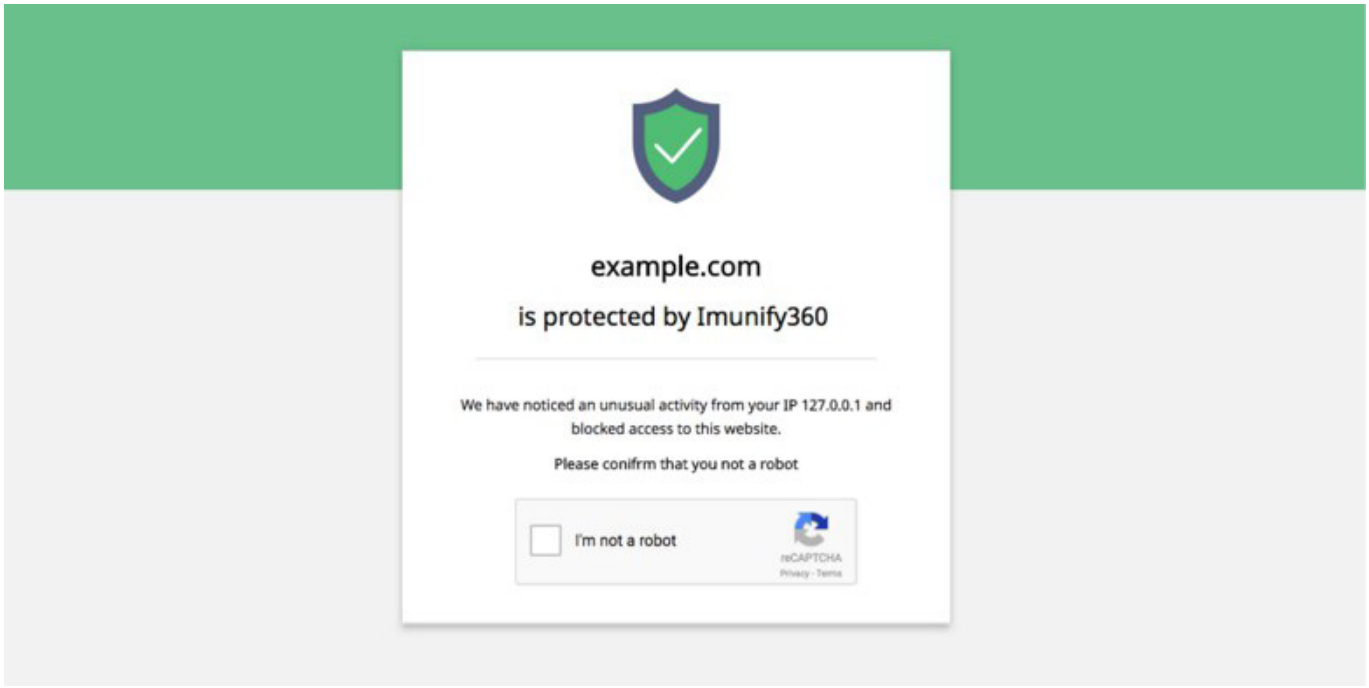
WordPress is een groot doelwit voor hackers en het aantal aanvallen dat een op WordPress gebaseerde website dagelijks op ons netwerk ontvangt loopt in de duizenden. De meeste gebruikers zijn zich daar niet van bewust en dat komt omdat Imunify360 er is om hun websites te helpen beschermen. De zes-lagen aanpak omvat:

- In real time scannen op malware
- Geavanceerde firewall met greylisting
- Inbraakdetectie
- Kernelpatching voor server
- Website reputatiebeheer
- Web Toepassingen Sandboxing

Hoe Imunify360 Captcha werkt

Imunify360 inbraakdetectie is gebaseerd op Mod Security regels. Zonder al te veel in detail te treden, Mod Security is een applicatie firewall op de server-side. Imunify360 heeft mod security ‘rules’ geïntegreerd die dagelijks worden geüpdatet. Deze regels beschermen de websites van onze klanten tegen allerlei soorten aanvallen. Bijvoorbeeld, als je een bepaald aantal mislukte login pogingen hebt op WordPress, cPanel, Email of FTP binnen een bepaalde tijdspanne zal je IP adres geblokkeerd worden door de firewall. Dit is een tijdelijke blokkering op basis van tijd.

De inbraakdetectie scant serverlogs op verdachte gebeurtenissen, zoals mislukte inlogpogingen, en blokkeert IP-adressen die dergelijke gebeurtenissen triggeren. Als u de website probeert te bezoeken en u krijgt een ‘**Protected by Imunify360**‘ Captcha-scherm te zien zoals in de onderstaande afbeelding.



of een spinner krijgt zoals deze in de onderstaande afbeelding.

Je krijgt dan een Captcha uitdaging te zien wanneer je je website bezoekt, het voltooien van de Captcha zal je IP adres deblokkeren en het op een tijdelijke witte lijst zetten. Het systeem is

ontworpen om geautomatiseerde bots te verhinderen zich een weg te banen naar je account en tegelijkertijd het ongemak voor mensen te minimaliseren. Dus als u per ongeluk de verkeerde inloggegevens invoert op uw website, kunt u nu de blokkering opheffen zonder contact op te nemen met de supportafdeling. Bij herhaalde overtredingen wordt uw IP-adres automatisch weer toegevoegd aan de Grijze Lijst en moet het proces herhaald worden.

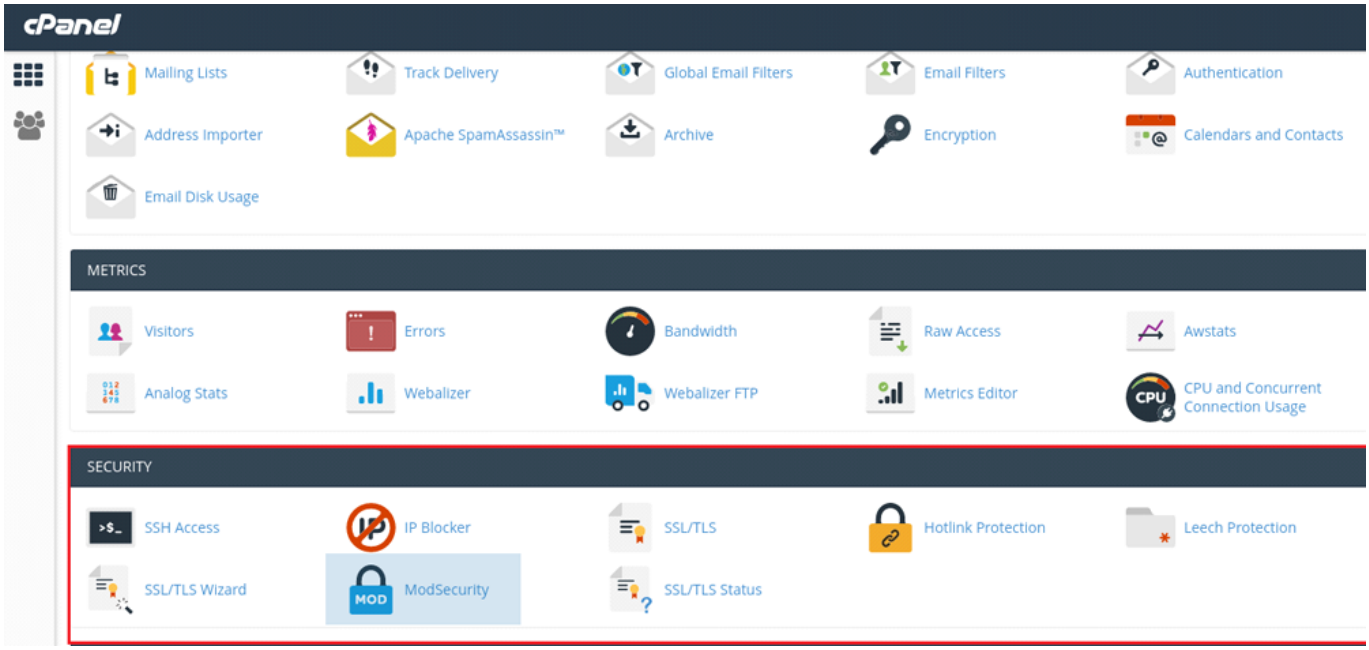
Sinds maart 2018 hebben we de **Invisible reCaptcha geïmplementeerd in Imunify360**. Dit heeft het Captcha-scherm voor legitieme gebruikers sterk verminderd en wordt voortdurend verbeterd.

> In een notendop, de Invisible reCAPTCHA gebruikt Google's Advanced Risk Analysis technologie en Artificial Intelligence om te bepalen ***of het een mens is of niet***. Als een echte persoon bijvoorbeeld meerdere keren heeft geprobeerd zijn wachtwoord in te voeren, dan wordt de gebruiker automatisch doorgestuurd naar de bestemmingspagina, met slechts een paar seconden vertraging, zonder een vervelend validatiescherm.
>
> Natuurlijk is veiligheid nog steeds belangrijk, en wanneer de Invisible reCAPTCHA bot-gerelateerde verzoeken detecteert, zal het nog steeds de CAPTCHA-uitdaging activeren. Dit zal de geautomatiseerde software blokkeren om de website of een pagina te bereiken. – bron CloudLinux Blog

Hoe zet ik Imunify360 uit?

Hoewel het misschien onhandig lijkt om door het Captcha scherm te gaan, is het er om je te beschermen tegen de duizenden aanvallen die dagelijks op je website worden uitgevoerd. Denk eraan dat je de Captcha alleen te zien krijgt als je login mislukt is of als je een veiligheidsregel van Mod Security geactiveerd hebt. Een gewone gebruiker zal de Captcha nooit zien, tenzij hij zich herhaaldelijk niet kan aanmelden op een deel van je website of iets ongewoons doet.

Dat gezegd zijnde, Imunify360 zelf kan niet uitgeschakeld worden. Het is een server-side software en beschermt elke klant op de server. Hoewel Imunify360 niet kan worden uitgeschakeld, **kunt u Mod Security** wel uitschakelen in uw cPanel.



Stappen om Mod Security uit te schakelen in cPanel

1. Log in op uw cPanel controlepaneel
2. Klik op het Mod Security icoontje onder de Security sectie in cPanel
3. Naast uw domeinnaam kunt u het op de UIT positie zetten

Dat is het! Mod Security zal worden uitgeschakeld voor de opgegeven domeinnaam. We raden ***nooit*** aan om het permanent uit te schakelen. Mod Security speelt een belangrijke rol in de veiligheid van je website, dus als je merkt dat je geblokkeerd wordt bij het uitvoeren van een specifieke taak op je website, kun je het uitschakelen en weer inschakelen als je klaar bent.

Redenen waarom u geblokkeerd kan worden door Immunify360

De meest voorkomende reden dat Immunify360 een IP adres zal blokkeren is mislukte logins. Dit kan zijn mislukte logins op cPanel, E-mail accounts of FTP. Als je WordPress gebruikt en meerdere mislukte logins hebt zal dit ook een blokkade veroorzaken. Zoals eerder vermeld, een andere reden waarom u geblokkeerd kunt zijn is als u een van onze Mod Security regels heeft geactiveerd. Het is niet ongewoon om een regel te activeren als u WordPress gebruikt, aangezien veel thema’s en plugins niet altijd de beste coderingspraktijken gebruiken, wat er op zijn beurt voor kan zorgen dat u geblokkeerd wordt.

Als je geblokkeerd bent kun je contact opnemen met ons PixelHosting Support Team via een support ticket. Wij kunnen je dan vertellen waarom je geblokkeerd bent en de blokkade ook verwijderen.

Real-time malware scanner

Imunify360 heeft een ingebouwde scanning engine die bestanden die geüpload worden naar uw hosting account in real-time scant. Als er malware wordt gevonden, wordt het bestand onmiddellijk in quarantaine geplaatst om te voorkomen dat er schade wordt toegebracht aan uw website.

PixelHosting + Imunify 360

Bij PixelHosting doen we er alles aan om ervoor te zorgen dat onze klanten de nieuwste technologie achter zich hebben. Met de integratie van Imunify360 zijn we in staat geweest om een gelaagde benadering van server-side security te bieden met behoud van optimale prestaties en eindgebruikerservaring. Wij werken nauw samen met onze partners om ervoor te zorgen dat ons hostingplatform sneller en veiliger is.

Imunify360 beveiligde servers bij PixelHosting bieden een hands-off automatisering die voortdurend leert van real-time bedreigingen op het web. Wij willen ervoor zorgen dat onze klanten de beste webhosting ervaring hebben met de gemoedsrust van de wetenschap dat hun hosting account is beveiligd tegen kwetsbaarheden en aanvallen. Wij zijn ervan overtuigd dat alles wat we kunnen doen om de veiligheid van ons platform te verbeteren, een investering is die de moeite waard is.

Unieke FAQ ID: #1002
Auteur: Maik Polman
Laatst bijgewerkt:2023-03-10 21:00