Schnelleinstieg Sucuri

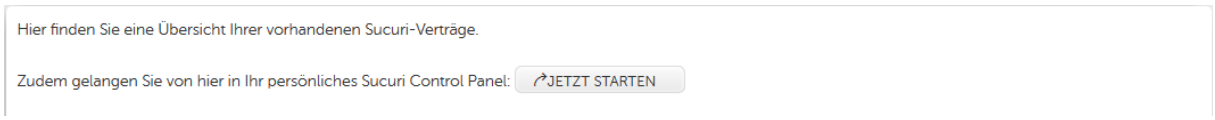
INHALT

Was ist Sucuri?

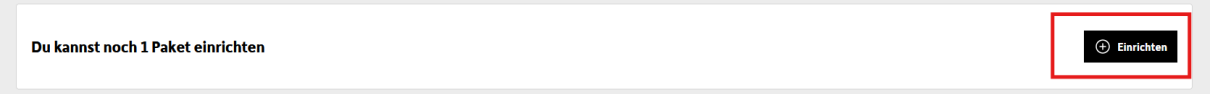
Sucuri ist ein cloudbasiertes Website Security-System, mit dem Ihre Website vor Online-Bedrohungen geschützt wird. Es ist eine besonders einfache und wirkungsvolle Möglichkeit, Ihre Website vor Hackern, Malware, DDoS und weiteren Angriffsformen zu schützen.

Wie richte ich Sucuri ein?

Im KIS wählen Sie den Produktbereich Sucuri und anschließend wählen Sie „Jetzt Starten“:



Es öffnet sich nun ein neues Fenster und Sie können Ihr Sucuri Paket einrichten:



Nun werden Sie aufgefordert, anzugeben, ob Ihre Domain bei Host Europe/GoDaddy registriert ist oder bei einem anderen Anbieter:

Auf der nächsten Seite können Sie Ihre Domain eingeben:

Nachdem Sie die Domain erfolgreich eingerichtet haben, können Sie das Paket verwalten.
In der ersten Übersicht der Verwaltung sehen Sie zuerst die Meldung:

„Website gerade hinzugefügt, niemals geprüft

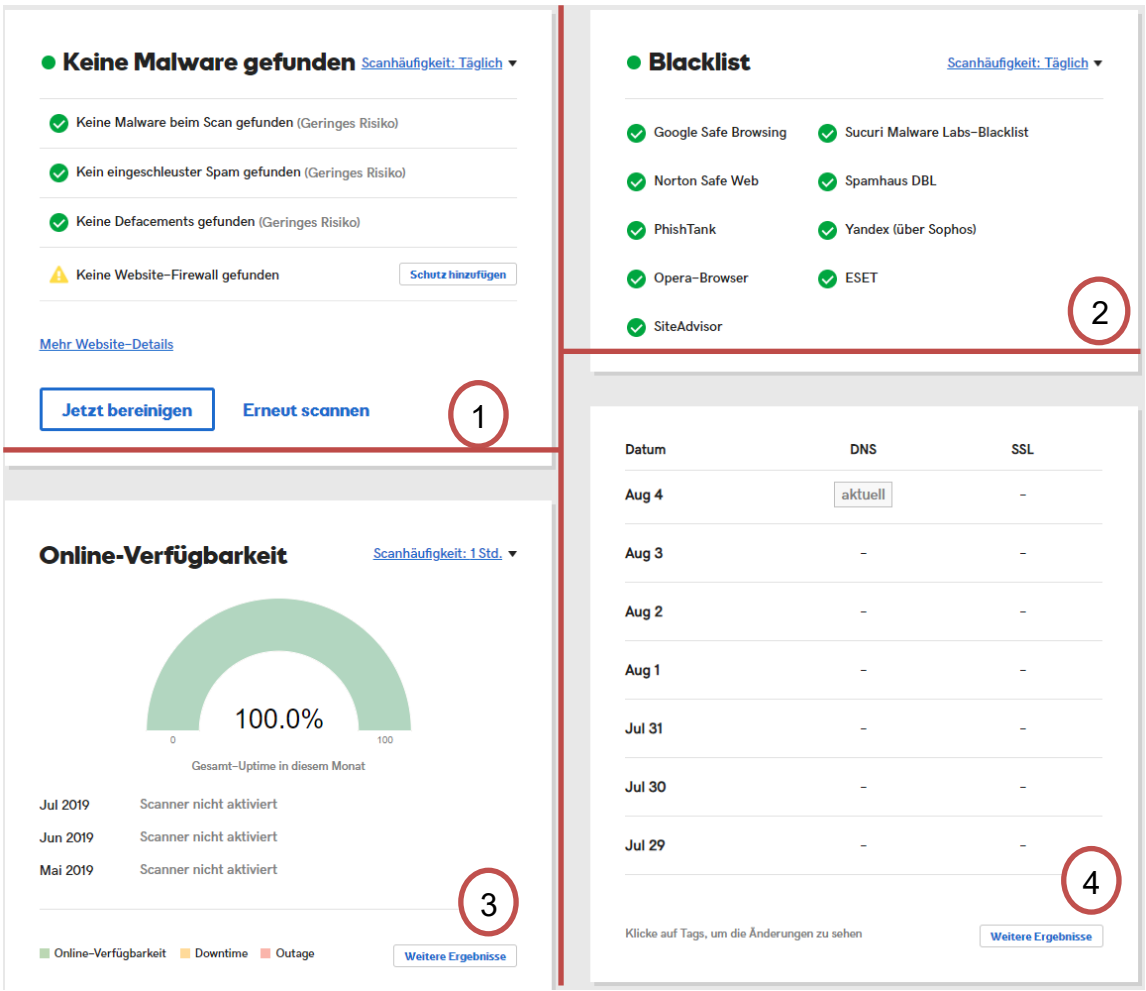
Die Malware Prüfung erfolgt automatisch und ist nach einigen Stunden abgeschlossen.
Sobald die erste Prüfung erfolgt ist, können Sie unter „Einstellungen - Monitoring-Arten“ weitere Prüfungen wie Online-Verfügbarkeit/DNS/SSL aktivieren.

Wenn die Malware Prüfung Auffälligkeiten auf ihrer Webseite feststellt, werden Sie per E-Mail benachrichtigt. Anschließend sollten Sie eine Anfrage zur Bereinigung unter dem Punkt „Aufräumen“ einreichen. Weitere Informationen dazu finden Sie auf Seite 12.

Erklärung der Menüpunkte

Monitoring: Überblick

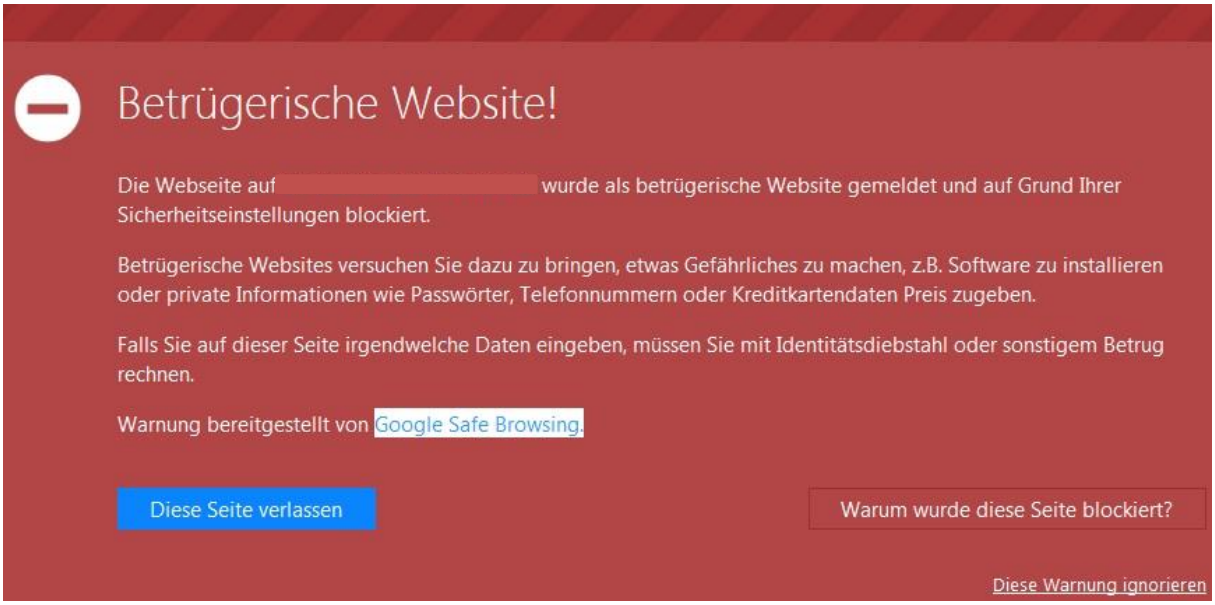
Wenn Sie alle Prüfungen aktiviert haben (siehe Monitoring: Einstellungen) sehen Sie folgende Übersicht:



1. Hier erhalten Sie eine Auflistung über den Status der letzten Überprüfungen(Scans).
   - Malware (eingeschleustes Schadprogramm/Schadcode)
   - eingeschleuster SEO Spam (Schlagwörter und eingeschleuste Verlinkungen)
   - Defacements („Verunstaltung“ unberechtigtes Verändern einer Website)
   - Website-Firewall (Schützt die Webseite vor Angriffen wie z.B. DDoS)

   Mit „Jetzt bereinigen“, können Sie eine manuelle Anfrage zur Malware Bereinigung einreichen. Mit „Erneut scannen“, wird ein Auftrag in die Warteschlange gelegt, der Scan erfolgt so bald wie möglich.

2. Bei der Auflistung der Blacklists erkennen Sie, ob Ihre Seite bereits als Verdächtig eingestuft worden ist. Sollte Ihre Seite z.B. bei „Google Safe Browsing“ gelistet sein, wird beim Aufruf Ihrer Seite in den gängigsten Browsern eine Warnmeldung angezeigt.

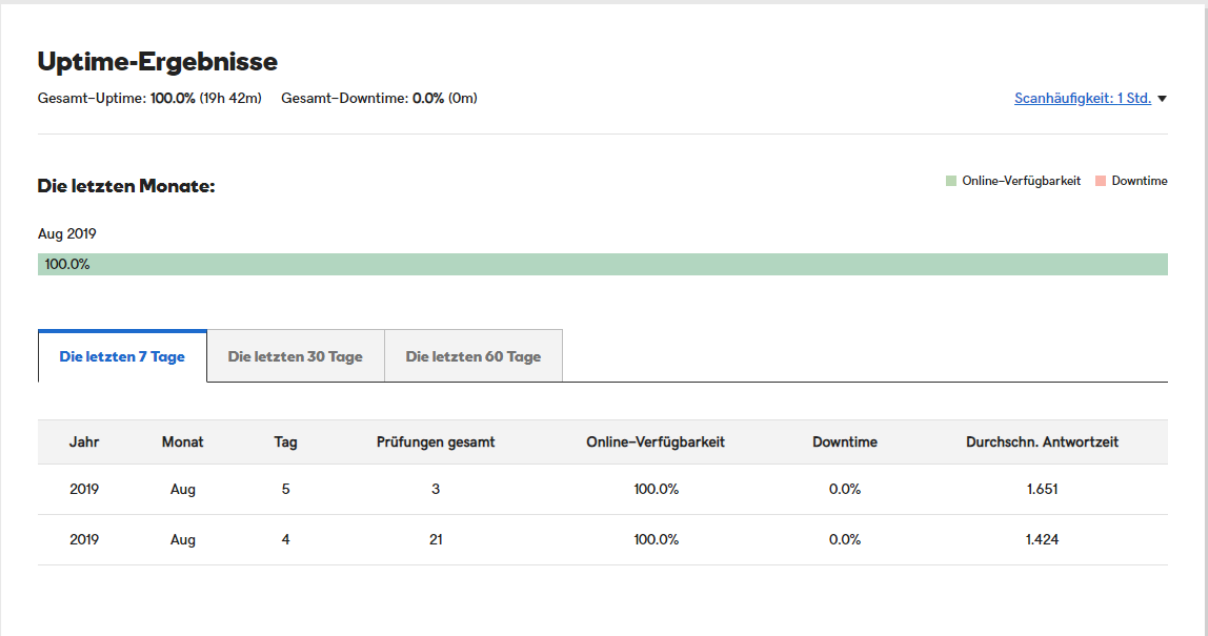


3. Die Online-Verfügbarkeit prüft im eingestellten Intervall, ob die Seite über „http/s“ erreichbar ist und informiert Sie per Mail, sobald eine Nichterreichbarkeit festgestellt wird

4. In dieser Übersicht finden Sie den Status zu DNS- und SSL-Änderungen.
   Beim DNS werden Sie z.B. informiert, sobald sich die IP Ihrer Domain ändert.
   Für SSL-Zertifikate, werden Änderungen an den Zertifikatsdaten wie z.B. der Signatur selbst beobachtet.

Monitoring: Online-Verfügbarkeit

Die Online-Verfügbarkeit zeigt Prozentual an, wie lange die Webseite erreichbar und nicht erreichbar war.



Uptime-Ergebnisse

Gesamt-Uptime: **100.0%** (19h 42m) Gesamt-Downtime: **0.0%** (0m) Scanhäufigkeit: 1 Std.

Die letzten Monate: Online-Verfügbarkeit Downtime

Aug 2019

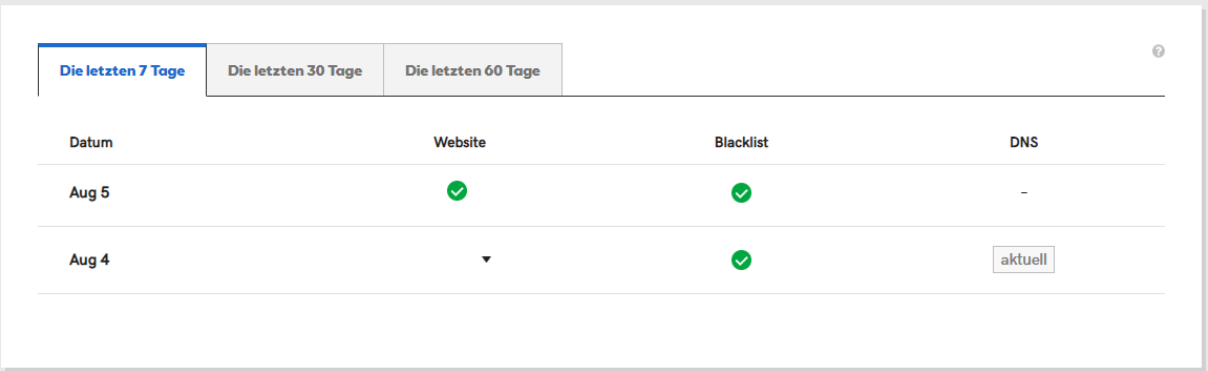
100.0%

Die letzten 7 Tage | Die letzten 30 Tage | Die letzten 60 Tage

Jahr	Monat	Tag	Prüfungen gesamt	Online-Verfügbarkeit	Downtime	Durchschn. Antwortzeit
2019	Aug	5	3	100.0%	0.0%	1.651
2019	Aug	4	21	100.0%	0.0%	1.424

Monitoring: Verlauf

Im Verlauf sehen Sie, wann Ihre Seite z.B. mit Malware infiziert oder auf einer Blacklist war.

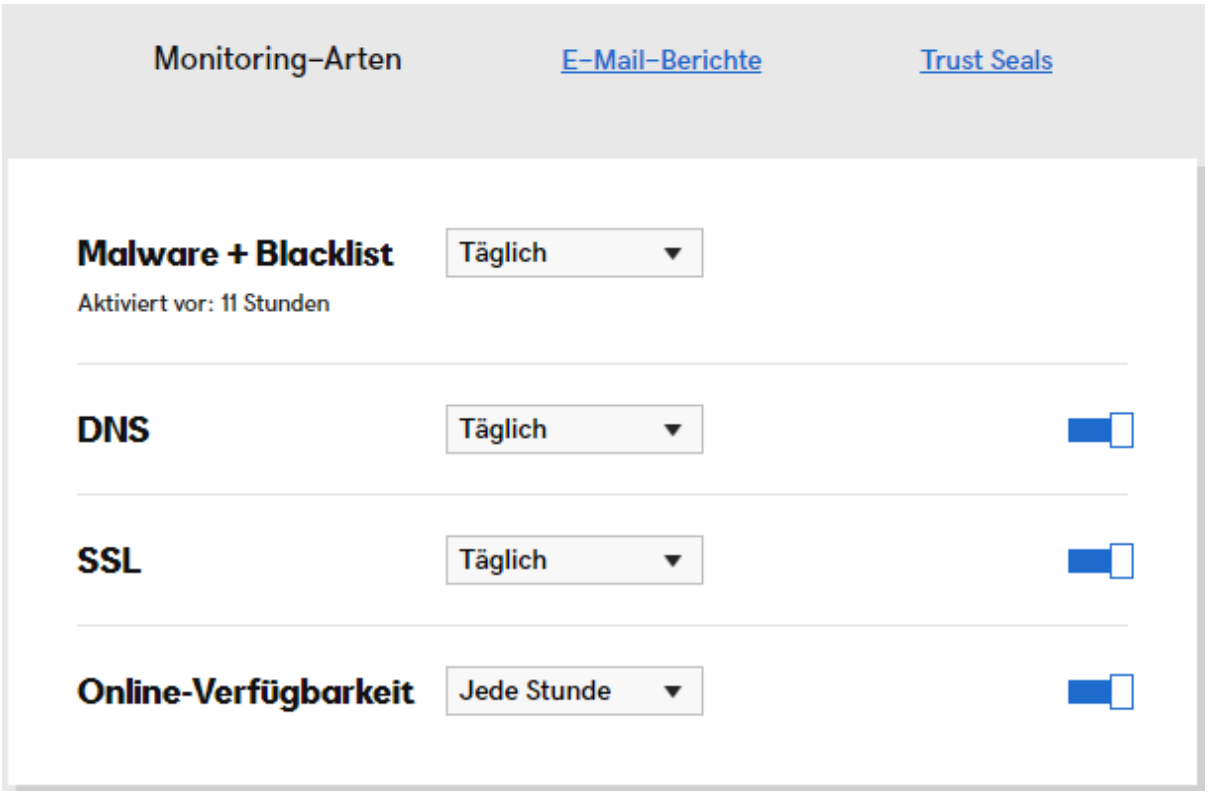


Die letzten 7 Tage | Die letzten 30 Tage | Die letzten 60 Tage

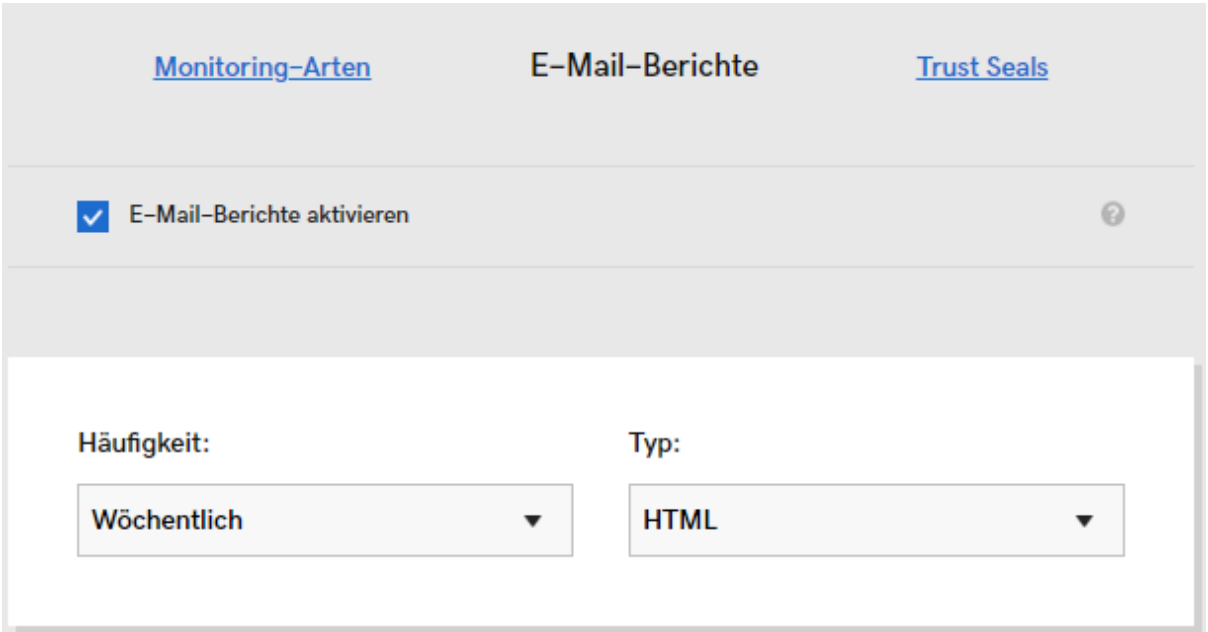
Datum	Website	Blacklist	DNS
Aug 5	✓	✓	-
Aug 4	▾	✓	aktuell

Monitoring: Einstellungen

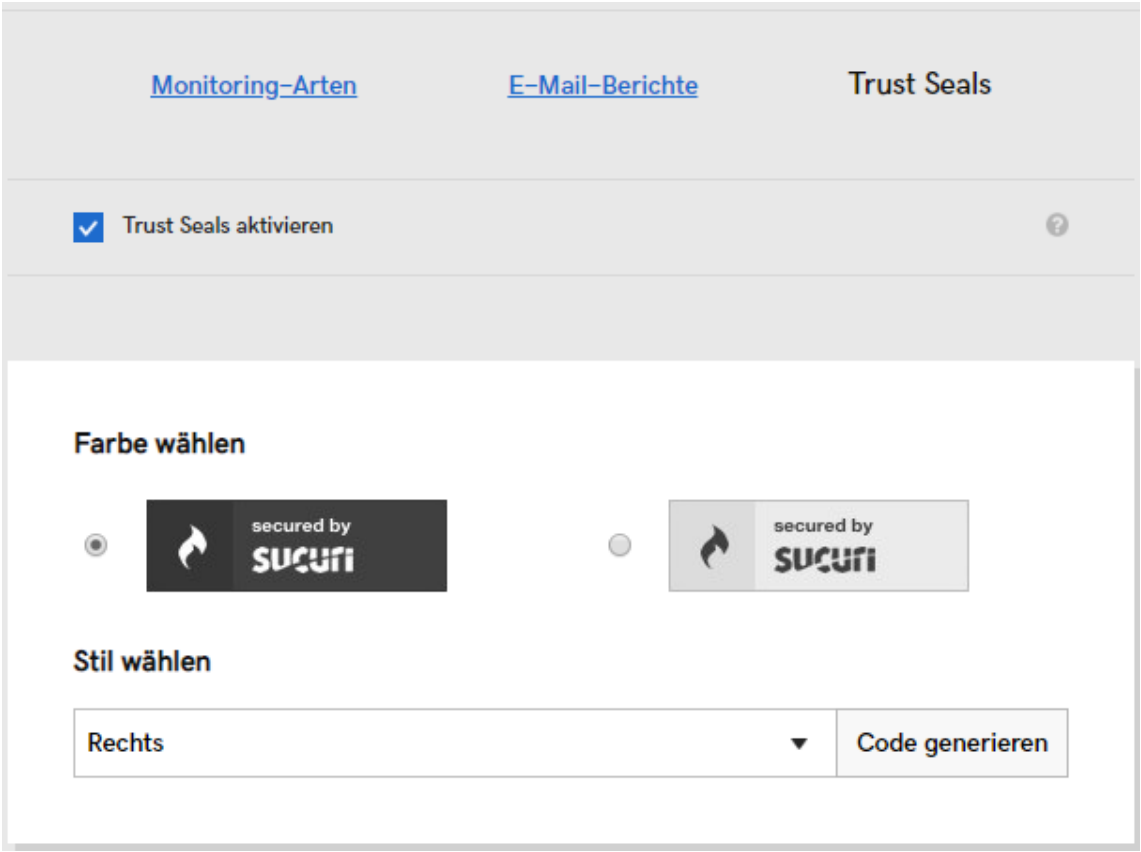
Bei den Monitoring-Arten können Sie bestimmen, welche Scans aktiv sein sollen.
Außerdem können Sie hier die Häufigkeit der Scans konfigurieren.



Sie können einen E-Mail-Bericht aktivieren und diesen z.B. so einstellen, dass Sie wöchentlich eine Übersicht aller Überprüfungen erhalten.

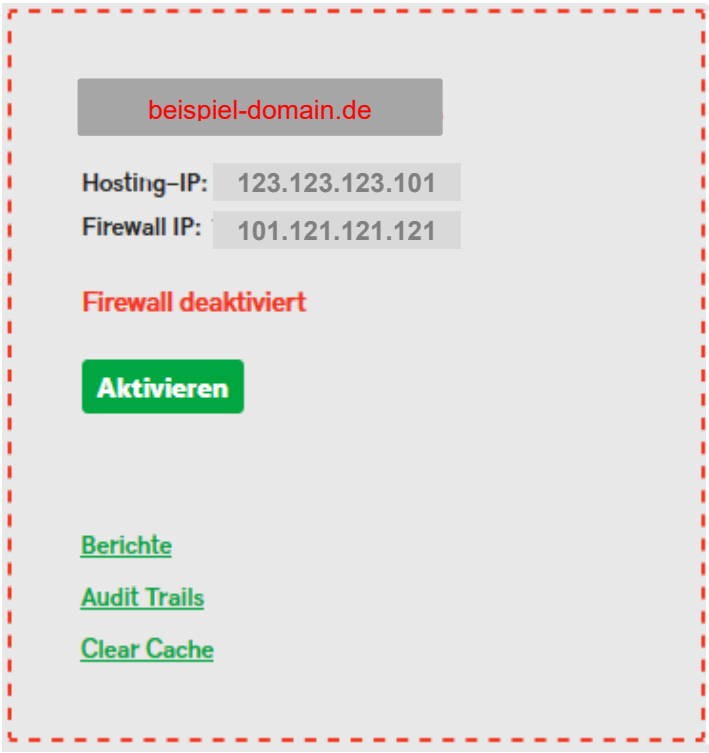


Mit dem Trust-Seal können Sie ein Siegel auf Ihrer Webseite einbinden und damit dem Besucher zeigen, dass Ihre Webseite Sucuri verwendet bzw. verifiziert und gesichert ist.

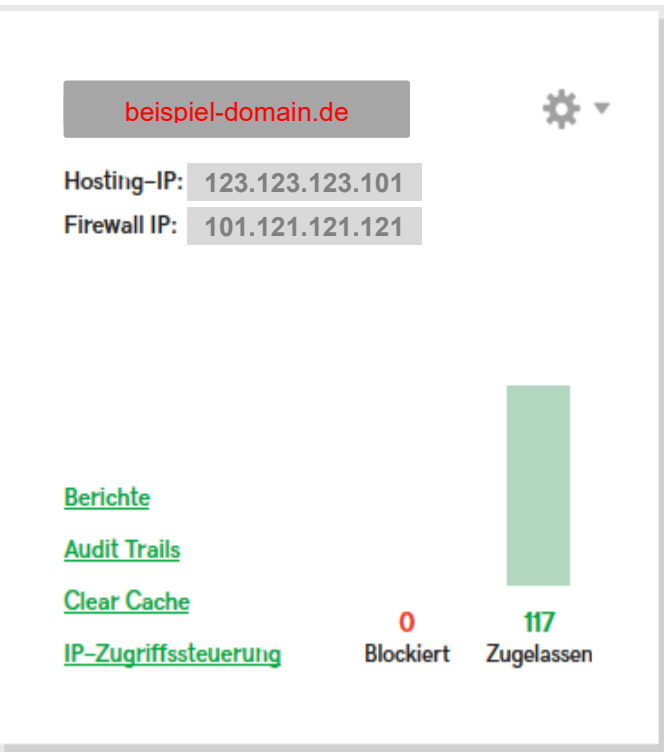


Firewall: Aktivierung

Für die Aktivierung der Firewall müssen Sie die Firewall-IP für Ihre Domain in Ihren DNS-Einstellungen hinterlegen. Anschließend dauert es bis zu 24 Stunden, bis die neue IP-Adresse von Sucuri erkannt wird und die Firewall aktiviert werden kann.



Firewall deaktiviert



Firewall aktiviert

Firewall: Berichte

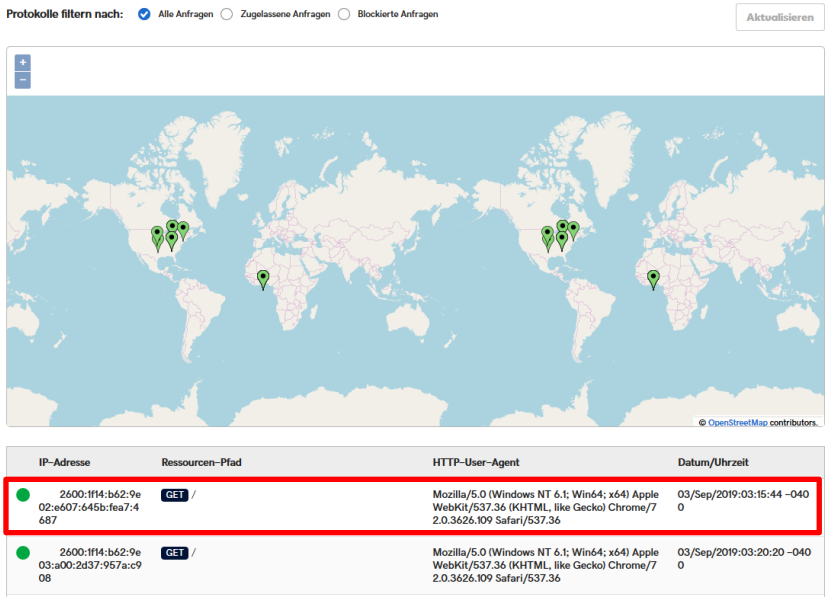
Im Bericht finden Sie eine Analyse der Zugriffe wie z.B. Anfragen nach Land sortiert oder die Zugriffe pro Stunde. Diesen Bericht können Sie sich auch per E-Mail zusenden lassen, damit haben Sie eine bessere Übersicht über die Anfragen auf Ihrer Webseite.

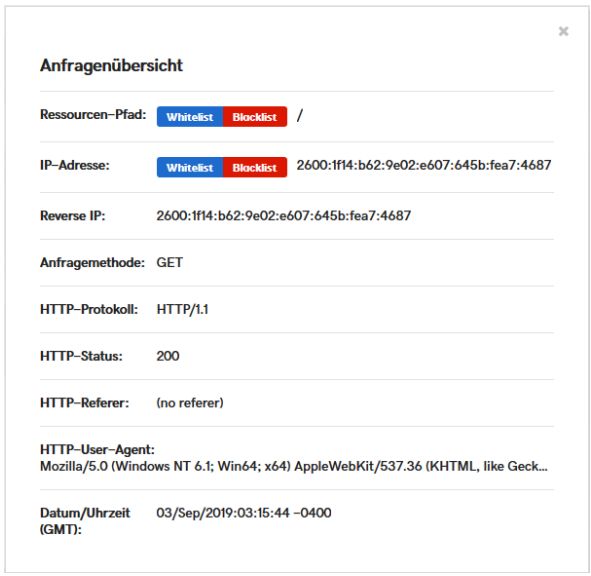
Firewall: Audit Trails

Die Audit Trails bieten Ihnen Details zu den blockierten Anfragen.
Hier sehen Sie ob die Anfrage z.B. als Bot erkannt wurde und welcher Pfad aufgerufen wurde.

Firewall: Echtzeit

In der Echtzeit Übersicht sehen Sie alle aktuell eingehenden Anfragen auf Ihre Webseite.
Bei Auswahl einer einzelnen Anfrage erhalten Sie weitere Details.
Anschließend können Sie die IP-Adresse oder den aufgerufenen Pfad auf die Whitelist (immer zulassen) oder auf die Blacklist (immer blockieren) setzten.

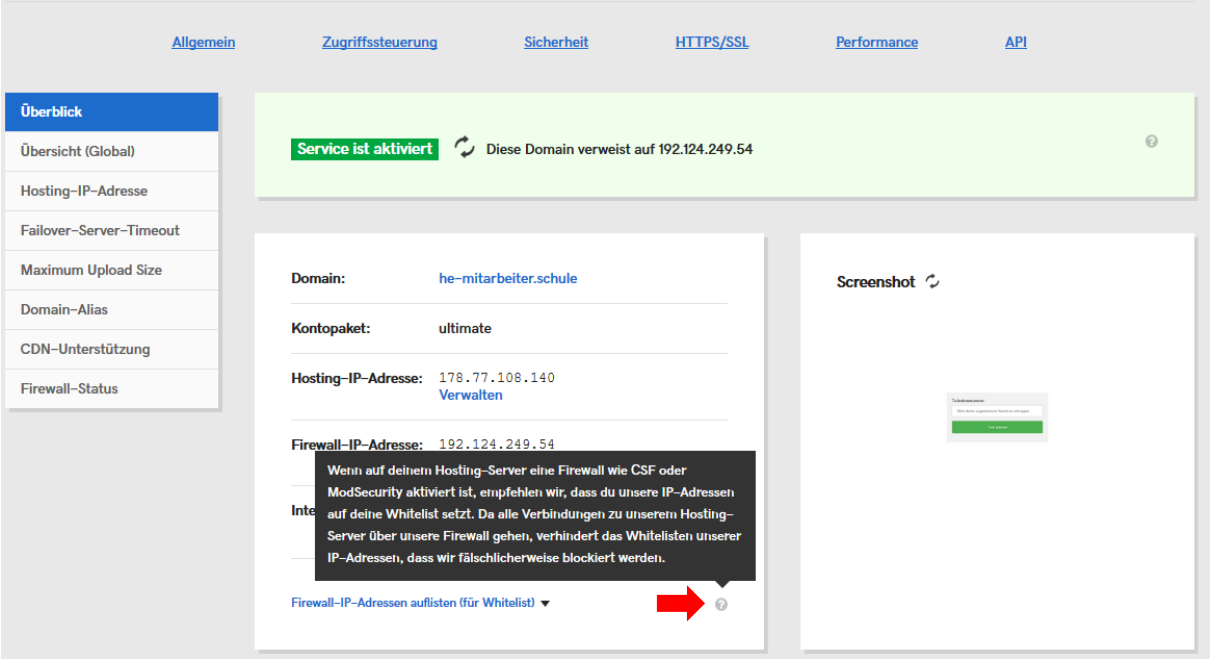




Firewall: Einstellungen

In den Einstellungen finden Sie sehr viele Informationen und Konfigurationsmöglichkeiten.
Die meisten Punkte sind hier bereits ausführlich erklärt, bei einigen finden Sie auch das „?“ Symbol für weitere Informationen. Daher werden die einzelnen Punkte hier nicht im Detail beschrieben.

Im Allgemeinen Bereich sehen Sie z.B. eine Übersicht der aktuellen Firewall Konfiguration oder können weitere Server als Backupserver hinzufügen.



Über die Zugriffsteuerung können Sie IPs/URLs oder User-Agents blockieren oder auf die Whitelist setzen.
Außerdem können Sie hier ganze Länder aussperren (Geo-Blockierung).

Im Bereich Sicherheit haben Sie erweiterte Optionen zum Schutz Ihrer Webseite.
Hier können Sie die Sicherheitsstufe erhöhen oder zusätzliche Sicherheitsheader aktivieren.

Unter HTTPS/SSL verwalten Sie die Umleitung auf HTTPS und das SSL-Zertifikat.
Im Bereich Performance können Sie das Verhalten des Cache konfigurieren.
Sie können hier auch einzelne IP-Adresse vom Caching ausschließen, wenn Sie z.B. Änderungen an der Seite vornehmen und diese sofort überprüfen möchten.

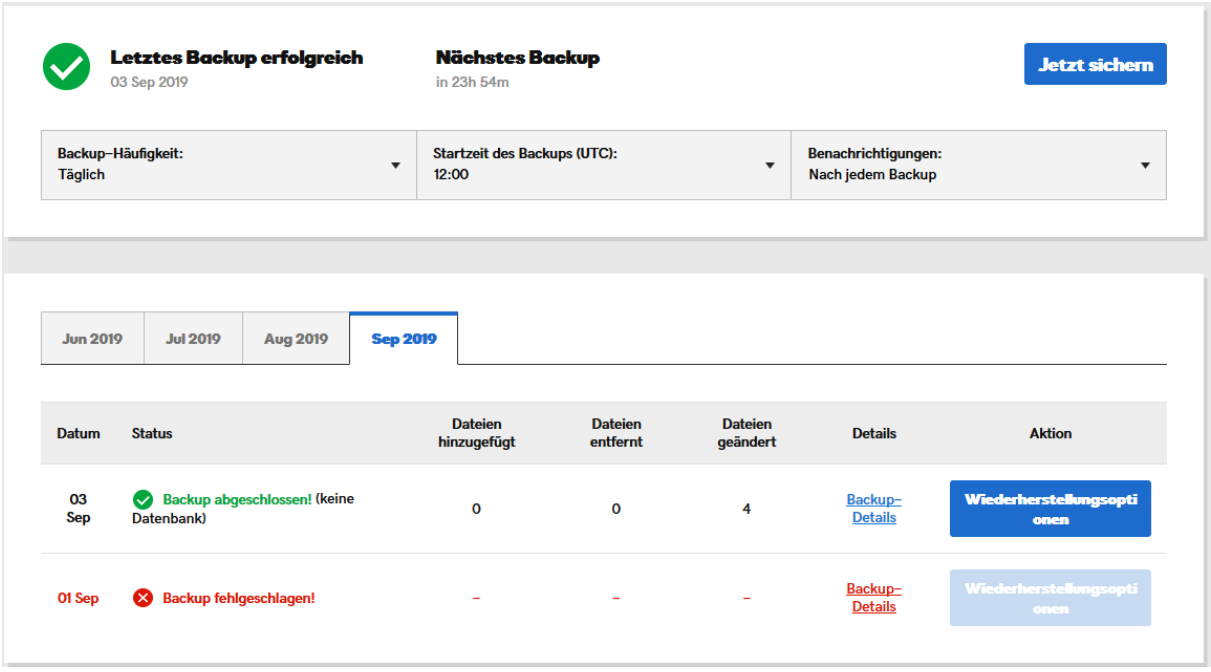
Die API bietet die Möglichkeit über ein Skript die Konfiguration der Firewall zu steuern und z.B. ohne Login in das Dashboard den Cache zu leeren. Dies ist z.B. für Entwickler und fortgeschrittene Nutzer interessant.

Backups

Die Backup-Funktion sichert Ihre Webseite über einen FTP/SFTP Zugang. Die Datenbank wird über einen direkten Zugriff oder PHP-Skript gesichert, welches lokal auf dem Server abgelegt wird. Für die Datenbank und den FTP Zugriff müssen Sie die entsprechenden Zugangsdaten manuell hinterlegen.

In der Übersicht sehen Sie den Status der letzten Backups.
Außerdem können Sie ein Backup sofort anstoßen und den Zeitpunkt der automatischen Backups definieren.
Für eine Wiederherstellung wählen Sie beim gewünschte Datum den Punkt „Wiederherstellungsoptionen“. Hier können Sie die Dateien/Datenbank automatisch wiederherstellen lassen oder als ZIP herunterladen. Bei der automaischen Wiederherstellung werden die bestehenden Daten ersetzt. Es werden jedoch keine neuen Daten gelöscht die im Backup noch nicht vorhanden sind.

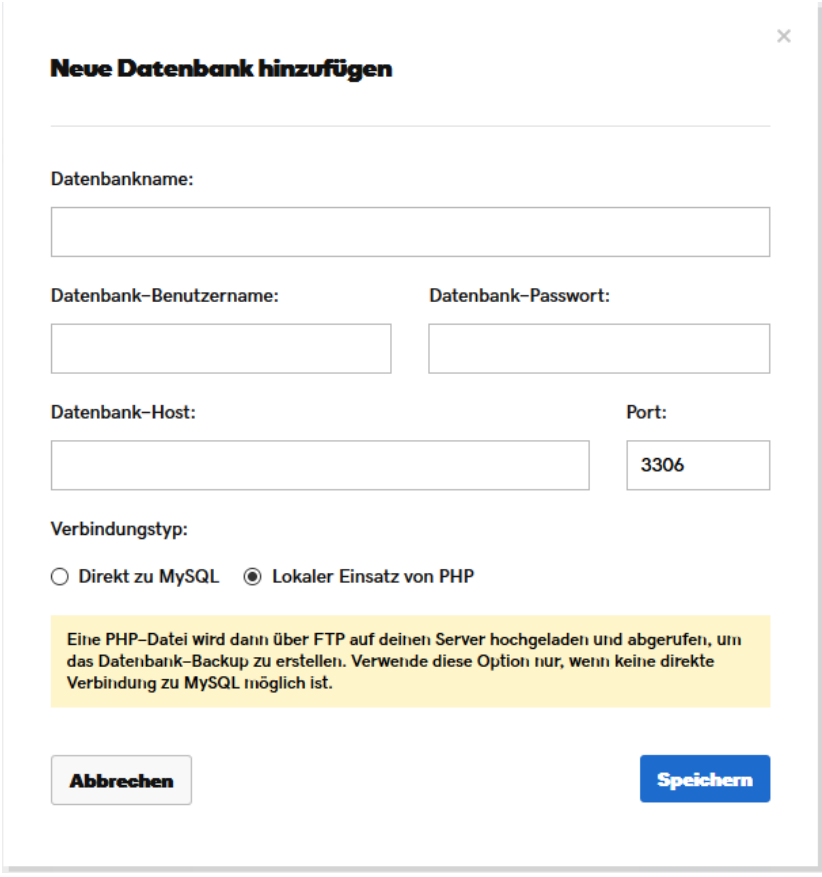
Sollte ein Backup fehlschlagen, können Sie sich in den Backup-Details den genauen Fehler anzeigen lassen.



Backups: Einstellungen

In den Website-Details können Sie die Zugangsdaten für den S/FTP-Zugang hinterlegen und anpassen. Die SFTP-Methode benötigt einen SSH Zugang.

Bei den Datenbankoptionen ist es wichtig die manuelle Konfiguration auszuwählen, da sonst keine Verbindung zur Datenbank möglich ist.
Anschließend fügen Sie die gewünschte Datenbank hinzu:



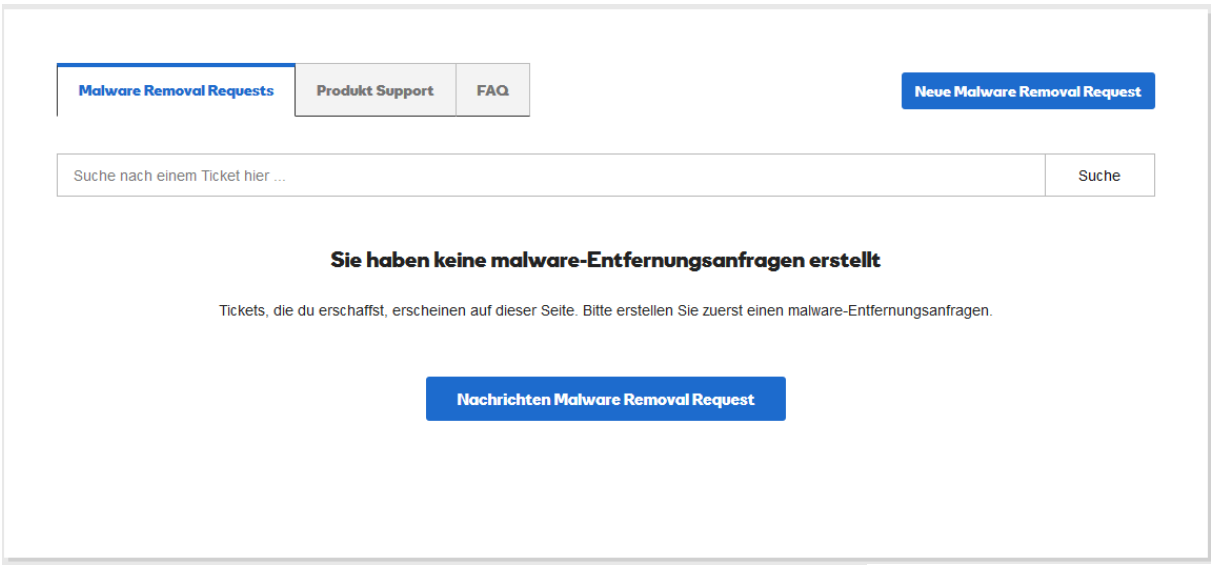
Bei dem Verbindungstyp wählen Sie „Lokaler Einsatz von PHP“ damit der Zugriff auf die Datenbank lokal auf dem Server erfolgt.

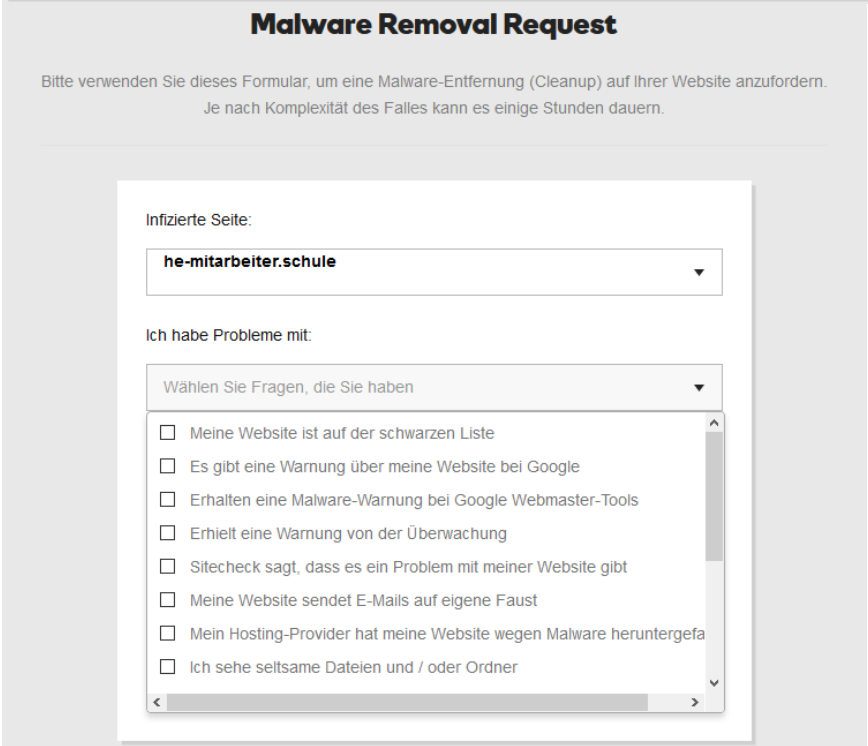
Alternativ können Sie den externen Zugriff für die Datenbank erlauben, dann funktioniert die automatische Erkennung bei bekannten CMS wie Wordpress und es werden keine weiteren Daten benötigt.

Unter Weitere-Optionen können Sie das Backup Intervall konfigurieren.
Außerdem können Sie hier Verzeichnisse hinzufügen die von Backup ausgeschlossen werden sollen. Dies können z.B. Verzeichnisse sein wo Daten nur temporär abgelegt werden, wie z.B. ein Cache-Verzeichnis

Säubern: Malware Removal Requests

Sie sehen hier eine Übersicht aller Anfragen bzw. offener Tickets und deren Status.
Außerdem können Sie hier einen neuen Vorgang zur Entfernung von Malware und anderen unerwünschten Inhalten eröffnen. Dafür gehen Sie auf „Neue Malware Removal Request“ und wählen anschließend die betroffene Domain und die zutreffenden Punkte aus.





Säubern: Produkt Support

Wenn Sie eine Frage zu Sucuri haben, können Sie ein Ticket unter „Produkt Support“ öffnen.
Hier können Sie z.B. allgemeine Fragen zur Firewall stellen oder Probleme bei der Einrichtung klären.