Product Newsletter

January 2019 Edition

It is a new year and no better time to get back to good habit of providing monthly updates.

Over the past few months huge strides were made both from WAS as well as AppTrana perspective including the announcement of CDN for all our SaaS sites at no additional cost. Apart from that, some long standing customer asks were met and many niggles found in the usage of the portal which was reported by our users were fixed. Here are the summary of changes that went out

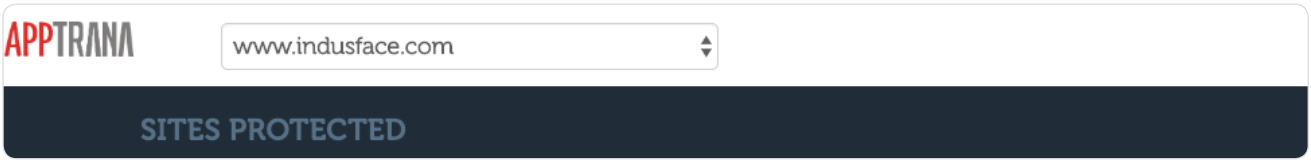
APPTRANA

PORTAL ENHANCEMENTS

Significant changes had been made to make AppTrana more usable & right information are presented to the user.

NAVIGATION ENHANCEMENT

Website dropdown has been added in Apptrana. Users with multiple sites can now change website from any page using the website filter dropdown instead of flipping to the dashboard page every time.



USABILITY

1 Requesting POC or Custom rule for already requested vulnerabilities will show message *'POC already requested'* and *'Custom Rule already requested'* respectively. Vulnerabilities found through Penetration testing comes with POC and users wont be able to request POC again.

2 If POC is already available, user will see message *'POC already available'* for selected URL.

3 Similarly if an url is already protected then during requesting custom rule, user will see message *'Selected URL is already protected'*.

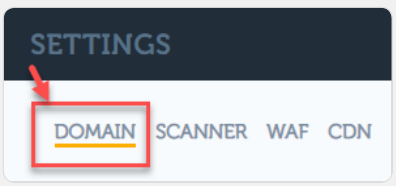
4 Messaging is improved to show if vulnerability is protected by AR (Advance Rule), PR (Premium Rule) or CR (Custom Rule).

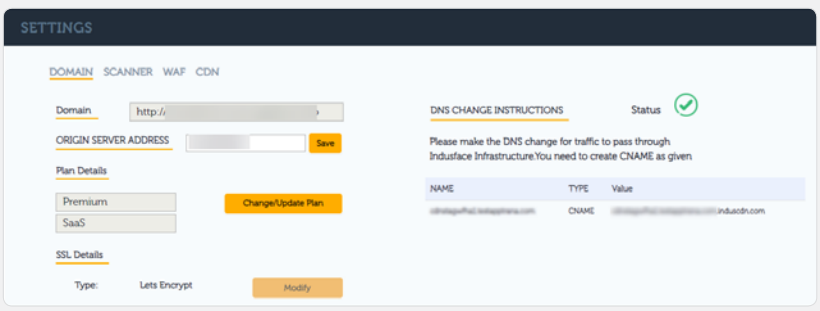
5 If a vulnerability cannot be protected at WAF level then that information is also provided and custom rule cannot be requested for such vulnerabilities.

SETTINGS PAGE

Settings page layout has been changed to support additional features and better flow. Now settings page has 4 tabs which allows user to find and change settings conveniently.

DOMAIN TAB

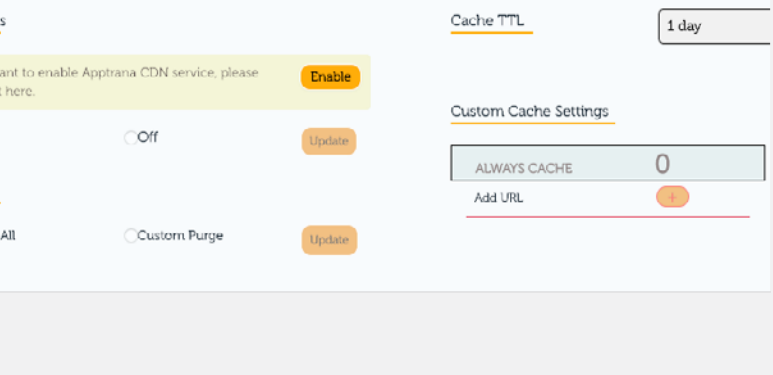




Domain tab, contains all the information of the site configured under protection and customer can make necessary changes here including uploading their SSL certificates directly. Please note, SSL certificates uploaded are stored using envelope encryption and only the WAF machines have access to them. No one manually has access to these certificates.

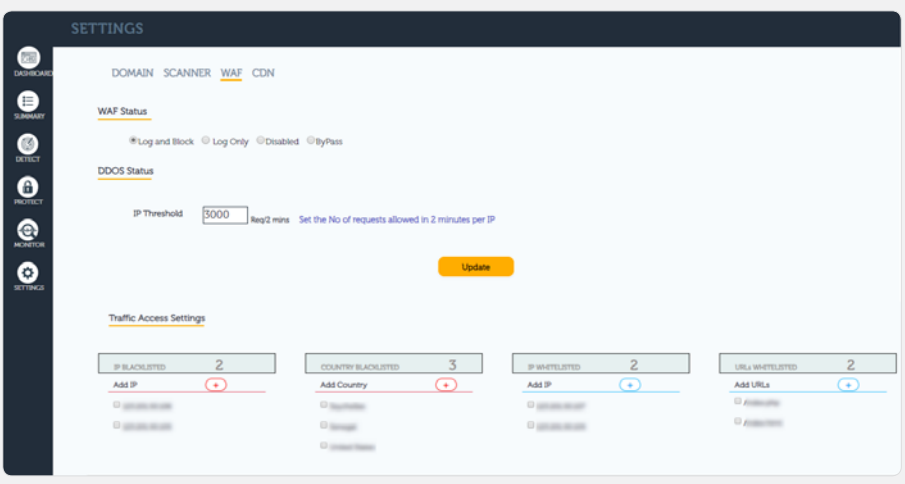
SCANNER TAB

Scanner tab has all configurations needed to scan. One can change the FQDN that needs to be scanned and also provide details around the dummy credentials required to do authentication scan if required.



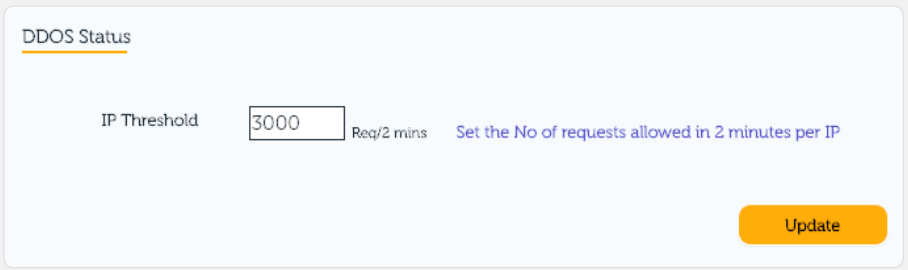
WAF TAB

WAF Tab contains configurations that governs how protection should behave.



All these information were previously available at different places in the portal which is now consolidated. Now customer can whitelist/blacklist IP/ countries from this tab.

Additional setting that is available is the DDOS Settings which allows you set the rate limiting threshold. This is a rate limiting rule, which will limit the number of requests an IP can make to a website in 2 minutes. This is available only for SaaS sites at this movement.



By default the limit is 3000 req every 2 minutes per IP.

This means, if from a same IP the website receives more than 3000 req in 2 mins then the IP will be marked malicious and any further traffic from the IP will be blocked. Once the IP is marked malicious, AppTrana would require 3 mins of cool down period before it allows the request from the same IP. i.e.) For a period of 3 minutes, AppTrana should not receive any further request from the malicious IP. If it continuous to receive requests from the IP, then it will continue to block until there is a cool down of 3 mins where no request is received from the IP.

CDN TAB

As you are aware we have recently launched CDN that can be enabled by all our CDN customers. All our existing SaaS customers can enable CDN for their site at no additional cost.

To enable CDN, go to the CDN tab and click on Enable

Once user click on enable it would take few hours to set the necessary configurations. Once that is done customer needs to set the Cache Status to ON for traffic to start being served from CDN. When CDN is enabled by default static contents are cached, for additional settings and more information talk to our support team or check out our docs portal.

SIEM API'S BETA ACCESS (BETA ACCESS)

One of the long standing ask of our customers has been the ability to integrate WAF configs with their SIEM tools for their SOC team. We are now happy to announce that SIEM API's is now available in Beta mode. Customer who want it, can contact our support team to get it enabled. We will go GA in some time after sorting out any niggles we see in production, when it will be readily available for all our customers.

ADVANCE DDOS (BETA ACCESS)

This is advance rate limiting rule ,which will limit the number of requests an user can make to a website in 2 minutes. This is done using advance machine fingerprinting to uniquely identify a user.

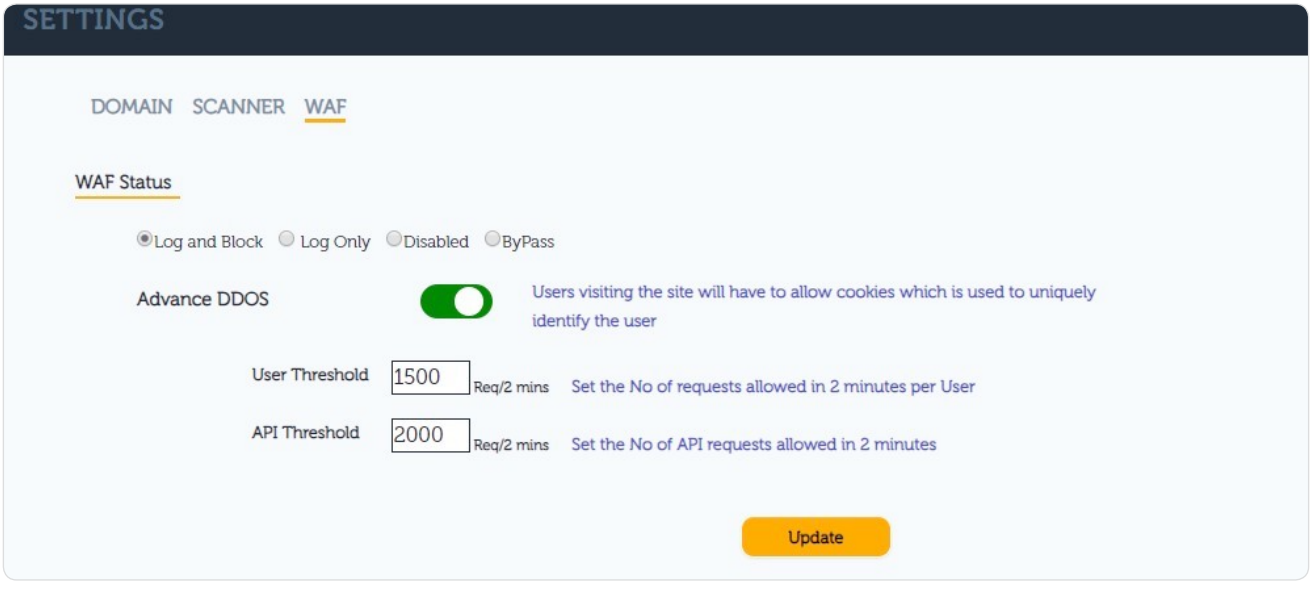
When Advance DDOS is enabled, users will be tracked with help of a cookie that would be injected when the user tries to connect to the website first time. This cookie is non-intrusive and no personal information are tracked using this cookie. This cookie creates a fingerprint to identify the user separately.

When Advance DDOS is enabled, 2 thresholds will be in play.

User Threshold – This governs the number of request a user is allowed to be made in 2 mins. Default value is 1500/2 min

API Threshold – API's won't be able to serve cookie it is for this reason API traffics are isolated and they are tracked by IP. This thresholds number of requests the API server can make in 2 minute.

Default value is 3000/ 2 min.



Customer can choose to enable Advance DDOS based on their need from Portal*. Please do it with caution and do it at off-hours to monitor the behaviour of your site when cookies are enabled. Please contact Support for any help.

*This feature is released incrementally and all customer will see this feature in the portal by Feb 15th.

WEB APPLICATION SCANNING

As you would be aware we had been working on new age scanner for last few quarters and now we are happy to announce all our customer sites are being scanned using the new scanner. This will not only provide us capabilities to scan new age single page sites but also the modular architecture of our new scanner lends itself to rapid development and tighter integrations between WAF and Scanner module, fruits of which will be seen in coming quarters.

Some of the major advances made on WAS side are as follows:

SIGNATURE UPDATE

Pluggins were created to find the following checks, this will go live in next couple of weeks.

1 Asp.Net Tracing Enabled

Trace should not be enabled, If trace is enabled then sensitive information such as Session ID values and physical path to the requested file might be exposed to malicious users.

2 Asp.Net Version Checker

Signatures are added to see if version is accessible, If a malicious user got to know the version of framework used, it might be used to create more attacks on the application.

3 Sensitive Information Gets Stored In Cache

Check is added to see if sensitive information are stored in Cachec. If page contains possible sensitive information (e.g. a password parameter) and are cached then even in secure SSL channels sensitive data could be stored by intermediary proxies which can lead to exposure of sensitive information. To prevent this, a Cache-Control header should be specified.

4 HTML Form Susceptible To Spam

A HTML form in a page looks susceptible to spam attacks if the form has a hidden input form with an email address as value. This is usually an indication that the recipient of an email sending form is hardcoded in a hidden input form. If that's the case this allows malicious users to send email messages using your server without authorization by changing the input value. A malicious spammer could use this tactic to send large numbers of messages anonymously.

5 Internet Explorer XSS Protection Disabled On This Page

Internet Explorer includes a feature that makes "Type-1" Cross-Site Scripting (XSS) vulnerabilities much more difficult to exploit from within Internet Explorer for this Internet explorer XSS protection is needed to be enabled.

6 Slow Response Time

Checks are added to report pages that have slow response time as these pages can be targeted for denial of service attacks.

7 Microsoft IIS Version Disclosure

If malicious user got to know the version of the framework then it might be used to make more attacks towards the application.

8 Suspicious Comment

If page contains one or more comments that may disclose sensitive information then those will be reported as it can used by attackers.

9 Documentation File Found

Presence of documentation file (e.g. readme.txt, changelog.txt, ...) will be reported. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

10 User Controllable Tag Parameter

An attacker can control one or more parameter values of a sensitive HTML tag (e.g. link href). In some conditions this can cause security issues such as XSS (cross-site scripting).

11 User-Controlled Form Action

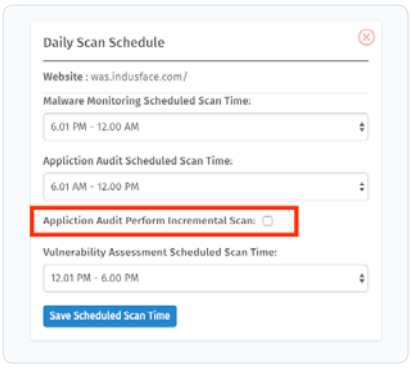
If the Action URL parameter for one HTML form in a page is directly controlled by user input then that will be reported. The Action parameter specifies the website where the user-submitted information is being sent. An attacker can provide a website controlled by him for the form action parameter and send this malicious link to your users. Any user who will click that link and submit the vulnerable form will send his information to the attacker.

INCREMENTAL SCANS (BETA ACCESS)

We are happy to announce the launch of Incremental scans. This will help all our customers who have large sites configured for scan. Before this, customers who wanted to get a complete scan report for their site had to let scan run for hours together which was not feasible for all. Now customer enable incremental scan for their site. This means, scan will happen incrementally each day in the permitted time window until the entire site is scanned.

Customer can enable incremental scans for their site by going to *Settings > Website Settings > Daily Scan Schedule*

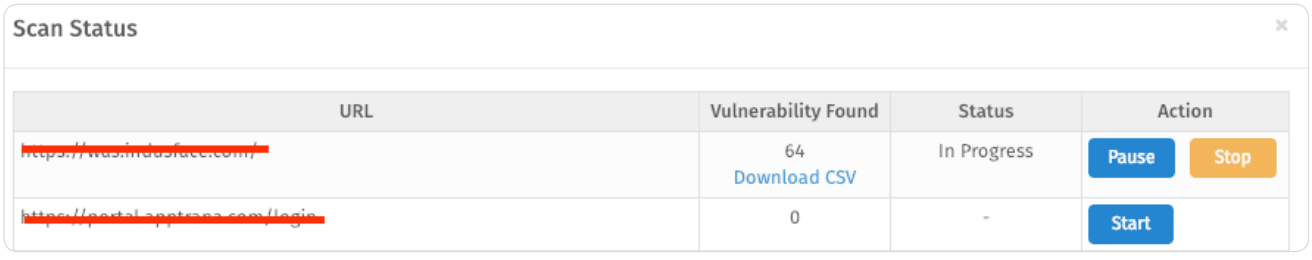
This is enabled as a beta version and would be made available to all our customers in an incremental manner over the coming weeks.



PAUSE & RESUME

Also users can pause any running scan at any point and resume it any time directly from the portal. If user do not resume it then it will automatically resume during next scan schedule.

To Pause running scans, please go to Dashboard and click on Scan Status. You will see all the scans configured under application audit scan like below



Click on the pause button to pause any scan running at this point. You will also be able to see vulnerabilities found till scan paused by clicking on "Download CSV", here. If you want to start any scans configured you can do the same from here.