Ready for a WAF Alternative? Your Peers Are Too

BLOG IN **APPLICATION SECURITY**

BY **BRET SETTLE**

Sep 14, 2021

Holy crap it's a pain to use. Maybe I just didn't absorb enough of the training, but dang, I hate trying to configure stuff in it.

Web application firewalls do not offer enough context to investigate incidents.

Too much manual configuration!! Too hands on!!

Thousands upon thousands of false-positive detections per day due to the WAF not identifying SQL injection keywords from true SQL injection.

implementation/management." That was closely followed by "lack of visibility" and "false positives."

We hear you Black Hat attendees, we agree, and that's why our WAAP solution is better. ThreatX was founded to deliver an alternative to the cumbersome and error-prone solutions of the past. From the beginning, the guiding principles were as follows:

- Designed from the ground up for the cloud
- Simple to deploy with fast time to value
- Eliminate false positives and constant tuning
- Provide actionable threat intelligence and security insights

Here's a deeper dive into the results, the comments, and how we can help.

Difficult implementation/management

This was the winner of the "why WAFs suck" prize with 25% of responses. What's difficult about implementation and management of WAFs? Survey respondents noted:

- "Writing rules"
- "Time-consuming configurations and administration"
- "Having to manually test our applications after every change to make sure it still works the way it needs to work, not the way the WAF thinks it does"
- "It takes a lot of time to fine-tune WAF rules."
- "Building advanced rule sets that allow for use of IPS, IDS software"

A lot of the responses mentioned rules and set-up woes. We've been there, and that's why we're on a mission to take rule tuning and cumbersome set-up off your plate. Our solution uses an attacker-centric approach and behavioral analytics to monitor all user interactions and determine the appropriate response based on risk. Although the ability to write custom

If you've used legacy or traditional WAFs, you know that creating less than 100 rules is rare, and having up to 500 rules can be quite common. Managing those 100s and 100s of rules is extremely complex, especially as applications and the environment are constantly changing. For comparison, ThreatX has only one customer that has more than 10 custom rules in their instance (most often triggered by the need to factor specific business logic requirements). That customer has only 31 rules. And, as far as I'm concerned, that's about 31 too many.

Because of our breadth of detection capabilities and deep visibility into the kill chain, we provide accurate results and actionable and prioritized responses and insights. As the applications and attack vectors change, the solution dynamically adapts to keep up. In addition, our application security experts act as an extension of your security team and help you act upon the findings, without an additional charge.

Although this may sound like a very complex solution, the approach actually simplifies the deployment and configuration required. Customers deploy ThreatX in hours, not days. And they enable the full force of ThreatX protection in days, not weeks, months, or years.

Poor visibility

"Poor visibility" came in at 14%, and comments included:

> "Not enough context to investigate incidents"
>
> "My biggest complaint in a WAF is visibility on what is blocked and actionable response."
>
> "Weak context around alerts"
>
> "Web application firewalls do not offer enough context to investigate incidents."

You can't secure what you don't know about, and you can't act on incident data without the right context. ThreatX covers *all* your apps and APIs, against all threats — not only signature-based. The ThreatX platform automatically classifies and correlates all suspicious behavior for each unique entity. This includes attack data from multiple IPs that are correlated to

how they are being attacked in real time. ThreatX puts the insights into visibility.

False positives

12% of respondents highlighted "false positives," and comments included:

> "Sometimes blocks legit content"
>
> "Way too many false positives, low value alerts"
>
> "They block legitimate traffic and let through malicious traffic!"

Don't waste your time chasing down false-positive results. ThreatX goes far beyond the signatures and anomaly detection used in other AppSec tools today. By tracking and compiling a complete picture of an entity's suspicious behavior, we can gather threat intelligence on patterns and techniques during early stages of the attack while blocking at the entity level as the attack intensifies. The result is enforcement that is both highly accurate and laser-focused on the threats that matter most. The added benefits include the audit trail to justify the response and key insights on what is being targeted.

There are a lot of ways that WAFs suck. You know it; we know it, and that is exactly why we built ThreatX from the ground up to turn things around. WAFs don't have to suck. Check out our demo video to find out how we can make your life easier, or schedule a demo with us to see our solution live.

Tags

APPLICATION SECURITY WAF

Bret Settle

Bret has served in multiple executive roles for Corporate Express/Staples and BMC Software and has extensive knowledge of the software development and security products industries. Bret has been responsible for enterprise security in multiple roles and has been an innovator throughout his career and has a proven track record of building and developing high performing organizations and dynamic cyber security teams.

SHARE

Subscribe for updates

Sign up for exclusive threat research, company and content updates, and the occasional fun contest.

JOIN OUR NEWSLETTER

SRC CYBER SOLUTIONS LLP THREATX REQUEST A DEMO

Ready to get started?

REQUEST A DEMO

Contact Us
www.srccybersolutions.com
+91 120 232 0960 / 1
sales@srccybersolutions.com

Newsletter Sign Up →