THREATX

CASE STUDY

Global Marketing Company Blocks Suspicious Traffic Without Excessive Rule Tuning

The Challenge

Before partnering with ThreatX, a global marketing company was experiencing significant problems with the legacy web application firewall (WAF) it had deployed. The team had several production workloads on that solution and experienced a "catastrophic impact" when they tried to enable any kind of blocking mode. "The rules and signatures required extensive tuning to attain even a minimum level of confidence that moving to block mode would not impact production," said the Director of Security Architecture and Engineering. "The one time we tried to enable blocking mode with our legacy WAF on one of our large production platforms, we broke the entire environment." After that, the company decided to avoid moving into blocking mode altogether. "We had a WAF," said the Director of Security Architecture and Engineering, "that was there to check a box, but didn't do anything."

"The tuning work was excessive," said the Director. "It would take roughly two weeks of manually poring over huge Excel spreadsheets that contained dumps of the log files to look at the traffic and try to come up with a tuning selection or tuning suggestions. Then we had to work with the client teams and the external client to review their application traffic to make sure that we weren't going to break something."

Another challenge with the legacy WAF was that the team didn't have an automated way to detect anomalous behavior. At one point, they were being targeted by a malicious actor, but their current security solution couldn't identify the behavior as malicious. "We had a site that was being targeted by a bot," said the Director of Security Architecture and Engineering, "it was attempting to log in with rotating usernames and passwords. However, this threat actor was crafting a properly formed interaction with the API. So, there was nothing malicious. It was using proper user agents and properly formed headers – nothing about it was out of the ordinary." Unfortunately, attempts to thwart the behavior didn't work either. "No matter how much we implemented rate limiting," he said, "the attacking entity would always go below the rate limit, and so you got to a point where you couldn't rate limit it any further until you broke legitimate traffic."

> "We had a site that was being targeted by a bot, attempting to log in with rotating usernames and passwords. However, this threat actor was crafting a properly formed interaction with the API. So, there was nothing malicious. It was using proper user agents and properly formed headers – nothing about it was out of the ordinary. ThreatX's ability to recognize anomalies that indicate suspicious behavior is game-changing."

The Solution

Based on their challenges, the global marketing company set out to find a SaaS-based solution, so they wouldn't have to manage an on-prem solution, and a solution that could analyze and block attacker behavior. "We wanted to find something that would enable us to have rules and signatures," said the Director of Security Architecture and Engineering, "because that's necessary, but then something else that would allow us to very quickly move into blocking mode." The Director and his team had heard that ThreatX could move into blocking mode in 72 hours, which piqued their interest in the solution. During the POC with ThreatX, they deployed the platform in front of one of their largest client team's staging environments. "We deployed it in learning mode," he said. "We moved to blocking mode about three weeks later, and it has remained in blocking mode for almost three years."

Since then, the marketing company has onboarded over 70 additional sites and platforms onto the ThreatX solution. Some of them are web applications, some of them are individual APIs.

> “ Within 72 hours, we implemented ThreatX and successfully moved into blocking mode with no production impact. That's a major game-changer for us."

The Benefits

No maintenance

One of the biggest benefits the marketing company has realized from deploying ThreatX is the lack of maintenance. They don't need to spend time tuning it as they did with other security solutions. "After we put it in the blocking mode, we never had to turn it off." said the Director of Security Architecture and Engineering. "Never in the history of any of our security tools have we ever been able to enable blocking and just leave it without having to go back and turn it off or tune it constantly."

"If we were trying to use that old WAF provider for all the sites that we have now it would have taken us 10 years [to tune it] unless we'd hired a whole bunch of engineers," he said.

The Director noted that a big benefit of the ThreatX solution is freeing his team to focus on what they do best. "Something that can scale automatically, dynamically adjust to the volume of traffic, and can look at that traffic and recognize anomalies that indicate suspicious behavior is game-changing," he said. "It allows my team to focus on higher-value activities that only humans can do."

> “ We never have to turn it off. Never in the history of any of our security tools have we ever been able to enable blocking and just leave it without having to go back and turn it off or tune it constantly."

Unparalled time-to-blocking

Another major benefit of working with ThreatX has been the speed of deployment. "In most scenarios, we implemented ThreatX and successfully moved into blocking mode within 72 hours, with no production impact," said the Director of IT Architecture and Engineering. "That's a major game-changer for us." In fact, ThreatX and the marketing company worked together to make the onboarding process even more streamlined and optimized. "If there's a security incident, we can move a site to ThreatX within four hours," the Director said. "We assemble the necessary teams, gather all the data, engage ThreatX, get it built, ready, and make changes. We've done that on a number of occasions."

The Director of Security Architecture and Engineering sums it up like this: "The value of ThreatX isn't around one particular point, but if I were going to pick one, it is the fact that we can move into blocking mode within 72 hours with very, very high confidence that we will not be blocking legitimate traffic, and false positives will be minimal. And we can pass along that same assurance to our stakeholders to their environment without breaking their operations."

> “ The WAF becomes security theater, to be honest with you. There was no real security value from having a WAF deployed in front of your environment that is incapable of enabling blocking mode."

More effective security:

The global marketing company's previous WAF solution simply couldn't protect the organization against the types of attacks they were seeing, primarily because they couldn't put it in blocking mode because of the number of false positives. "It becomes security theater, to be honest with you," said the Director of Security Architecture and Engineering. "There was no real security value from having a WAF deployed in front of your environment that is incapable of enabling blocking mode."

ABOUT THREATX

ThreatX's API protection platform makes the world safer by protecting APIs from all threats, including DDoS attempts, BOT attacks, API abuse, exploitations of known vulnerabilities, and zero-day attacks. Its multi-layered detection capabilities accurately identify malicious actors and dynamically initiate appropriate action. ThreatX effectively and efficiently protects APIs for companies in every industry across the globe. For more information, visit: www.threatx.com.

To learn more **REGISTER FOR A DEMO**

www.threatx.com/request-a-demo

THREATX

www.threatx.com | info@threatx.com | +1 888.303.5580