SANS

Analyst Program

Product Overview

Safeguard Your Business-Critical Web Apps and APIs with a WAF

Written by **Dave Shackleford**

November 2023

FORTINET

Introduction

The use cases for cloud services continue to expand rapidly. Organizations realize that many types of access scenarios are shifting as platform-as-a-service (PaaS) usage and cloud infrastructure deployments increase, and interconnectivity models among users, remote offices, and data centers change. With this shift, organizations also realize that web services and APIs are becoming the standard for application deployments. Traditional security measures that focus on networking, servers, and operating systems are no longer adequate, and bad actors are targeting this new attack surface that many security teams aren't even aware of.

The rapid maturation of the cloud is driving a convergence of many elements of cloud services and security into a unified fabric. Fortunately, one of the cloud-based controls that can help protect application workloads and access in both on-premises and cloud hosting environments is web application firewalls (WAFs). WAFs are used to filter and monitor traffic to and from web application infrastructure. These tools are similar to application proxies in many ways, focusing only on web app traffic and applying application-layer filtering and rulesets to prevent attacks. Most WAFs are used to detect and block common web app attacks such as cross-site scripting (XSS), SQL injection, command injection, directory traversal, and others. Mature WAFs come with a starting ruleset that includes standard blocking and detection rules for attacks of these types, although most organizations will want to modify these rules and add their own. WAFs are often used to "fingerprint" application traffic and identify unusual behavior patterns. As examples, an uptick in transaction attempts by a specific user could be considered odd, or certain users clicking links they normally wouldn't could be out of character. When setting up WAFs to perform this type of monitoring and filtering, it's critical to involve application developers so that false positives are reduced and the monitoring effort is as accurate as possible. Today, though, there are many more threats to application environments, including malicious botnets and denial-of-service attacks, as well as attempts to exploit exposed APIs (which are on the rise).

Traditional security measures that focus on networking, servers, and operating systems are no longer adequate.

Improved and more well-integrated protection for applications running in the cloud is one of the major use cases for adopting cloud edge services and tools. In the cloud, where applications are often deeply integrated into numerous cloud fabric services, employing security and networking controls that are closer to the applications and integrate more natively with the cloud provider environment make much more sense.

SANS recently reviewed Fortinet's FortiWeb Cloud service, which offers a wide range of security capabilities and controls in a brokered model to protect applications from web application attacks, API attacks, malicious bots, and much more. Although we did not onboard applications to the platform during this review, we did walk through an onboarding demonstration that showed the process to be relatively simple and straightforward. FortiWeb checks the domain, network ports, content delivery networks (if in place), DNS and blocking/monitoring configuration, and more. Altogether, the process of onboarding our sample app took roughly five minutes.

FortiWeb's General WAF Controls

First, we reviewed some of the FortiWeb WAF security policies and controls, which can be configured to alert security teams, deny silently, or both. The essential signature-based detection includes controls for SQL injection, XSS, generic attacks, known exploits, and trojan malware. Customers can search for specific signatures based on common vulnerabilities and exposures (CVE) number, keywords, attack categories, signature IDs, and attack severity levels. Figure 1 shows the configuration we enabled for this review.

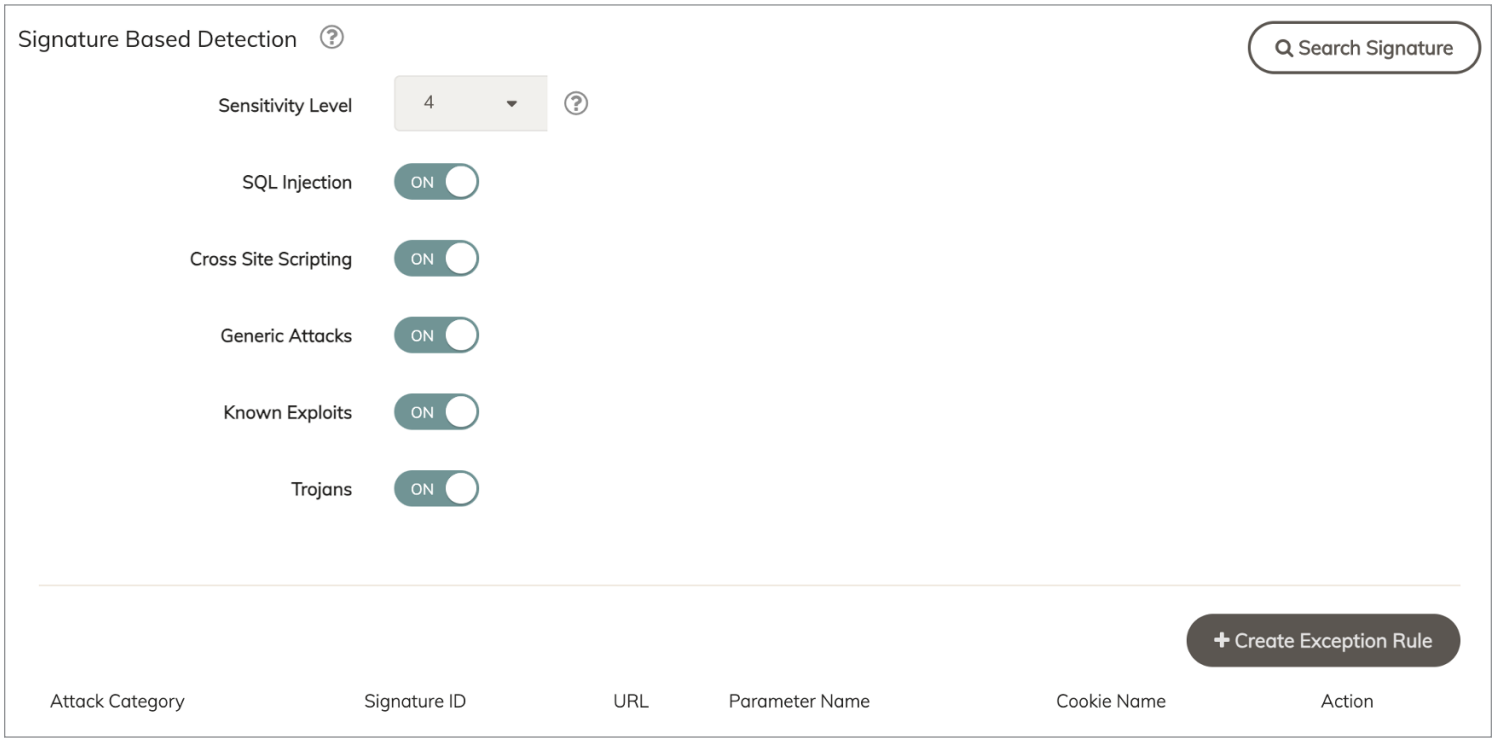

Figure 1. Known Attack Security Rules from FortiGuard Labs[1]

[1] FortiGuard Labs, www.fortinet.com/fortiguard/labs

FortiGuard Labs also provides a wide range of detection signatures focused on SQL and XSS injection, which we universally enabled during the review, as shown in Figure 2.

Fortinet WAF rules are easy to configure and well-suited to defend applications from common Open Web Application Security Project (OWASP) Top 10 attack variations.[2] We ran several web application scans and attacks against our sample application, and all were detected and blocked by FortiWeb Cloud with no issues.

Bot Mitigation

Given the prevalence of sophisticated botnets today, many organizations are concerned about malicious bots targeting applications for denial of service, fraud, injection attacks, and more. FortiWeb Cloud has distinct categories of bot protection available. One of them, "Known Bots," focuses on bot families and campaigns observed and detected by Fortinet threat intelligence. These bot families range from DoS to spam and fraud, and each category can include custom allow/block parameters, as well. See Figure 3.

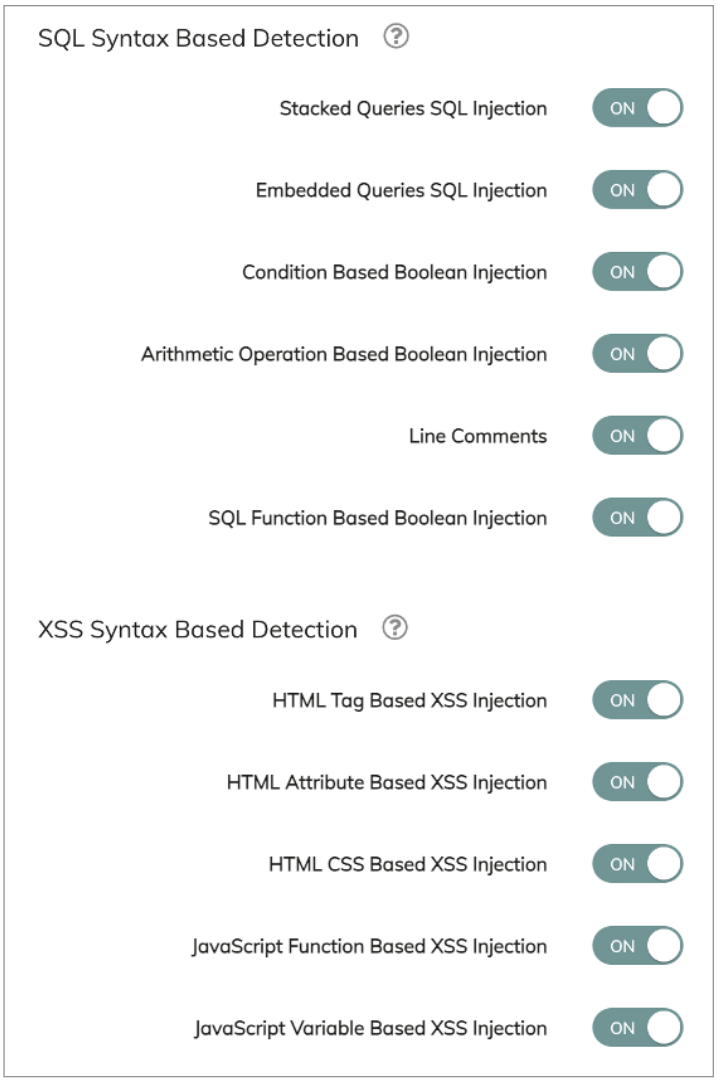

Figure 2. FortiGuard Labs WAF Rules

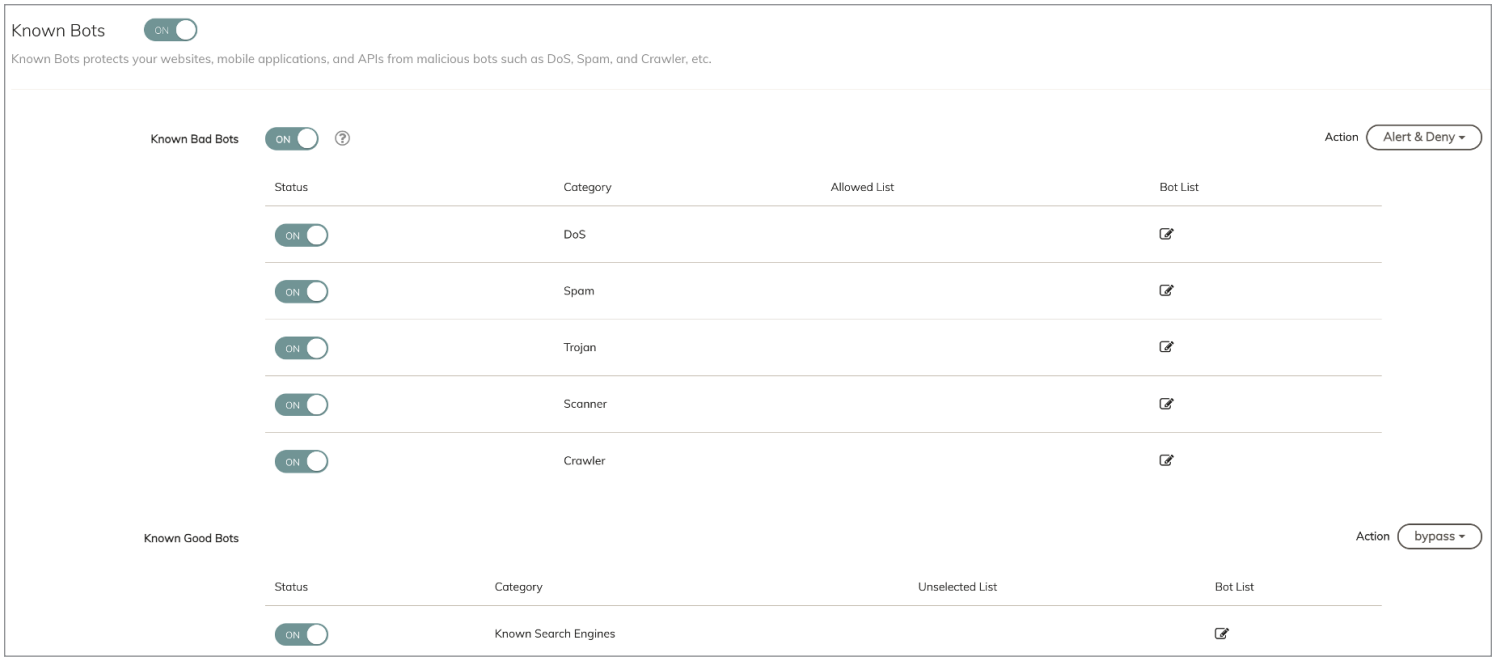

Figure 3. Known Bot Detection and Prevention

[2] "OWASP Top 10," https://owasp.org/www-project-top-ten

FortiWeb Cloud also can detect bots based on access thresholds (looking for crawlers, vulnerability scans, "low and slow" attacks, credential brute forcing, and more) and machine learning–based patterns. The machine learning (ML) capabilities are also closely related to anomaly detection (covered in the "Anomaly Detection" section of this review). The Fortinet team has developed a sophisticated catalog of 14 client identification methods to determine whether a request is legitimate or coming from an automated bot. Enforcement actions can be selected (e.g., sending bot traffic to a CAPTCHA) with a specific blocking duration, or source IP addresses and URLs can be deliberately allowed for unusual client types. Options for machine learning–based bot detection are shown in Figure 4.

Figure 4. Machine Learning-Based Bot Detection

Additional controls include biometric monitoring (mouse movement, clicks, keyboard interaction, etc.) and bot deception that injects a hidden link into response pages. (Any interactions with these links likely indicate bot scanning.)

Anomaly Detection

One of the more important types of detection capabilities for online applications today is behavioral analysis of unusual or anomalous traffic. FortiWeb Cloud has a highly tuned machine learning engine that can scan all incoming traffic for unusual patterns with several layers of detection technology.

FortiWeb Cloud first scans all incoming traffic against the FortiGuard Labs signatures for malicious traffic patterns. As a secondary measure, FortiWeb Cloud scans traffic using sophisticated ML algorithms to look for known and suspected patterns of access that may indicate attacker probes or exploit attempts. The primary dashboard for anomaly detection shows a list of the URLs accessed (or where access was attempted), violations triggered based on the Fortinet team signatures and threat intelligence, learning progress based on known detection and continuous analysis, and more, as shown in Figure 5.

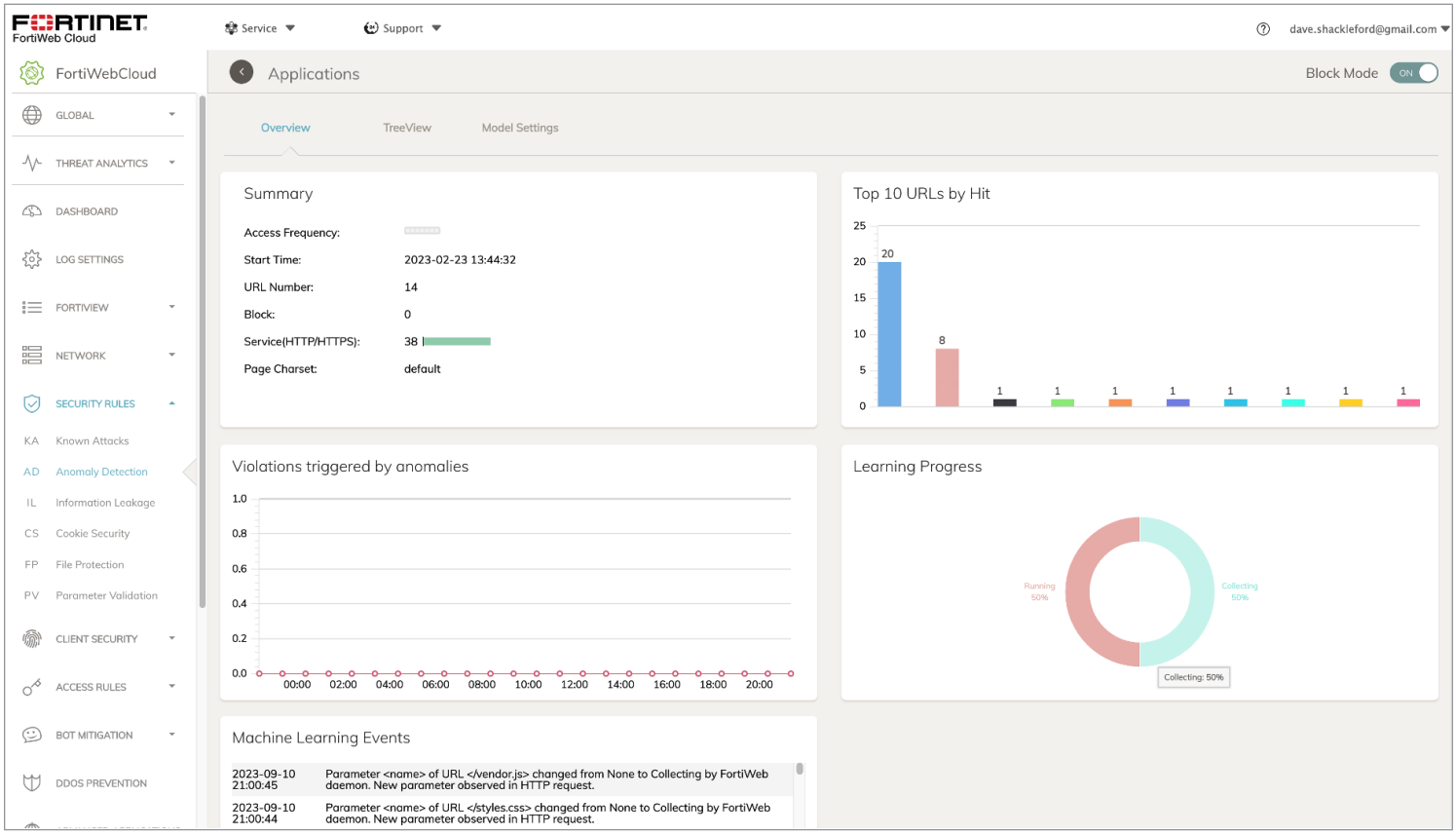

Figure 5. Anomaly Detection Dashboard

The FortiWeb platform also leverages machine learning to analyze incoming requests and potential malicious attacks and traffic patterns for all protected assets. Within the Anomaly Detection engine, we reviewed the "TreeView" visualization model, which shows application content with an analysis of machine learning coverage. Figure 6 shows that the "Search" parameter in our Juice Shop application is still being analyzed by the core Fortinet machine learning algorithms.

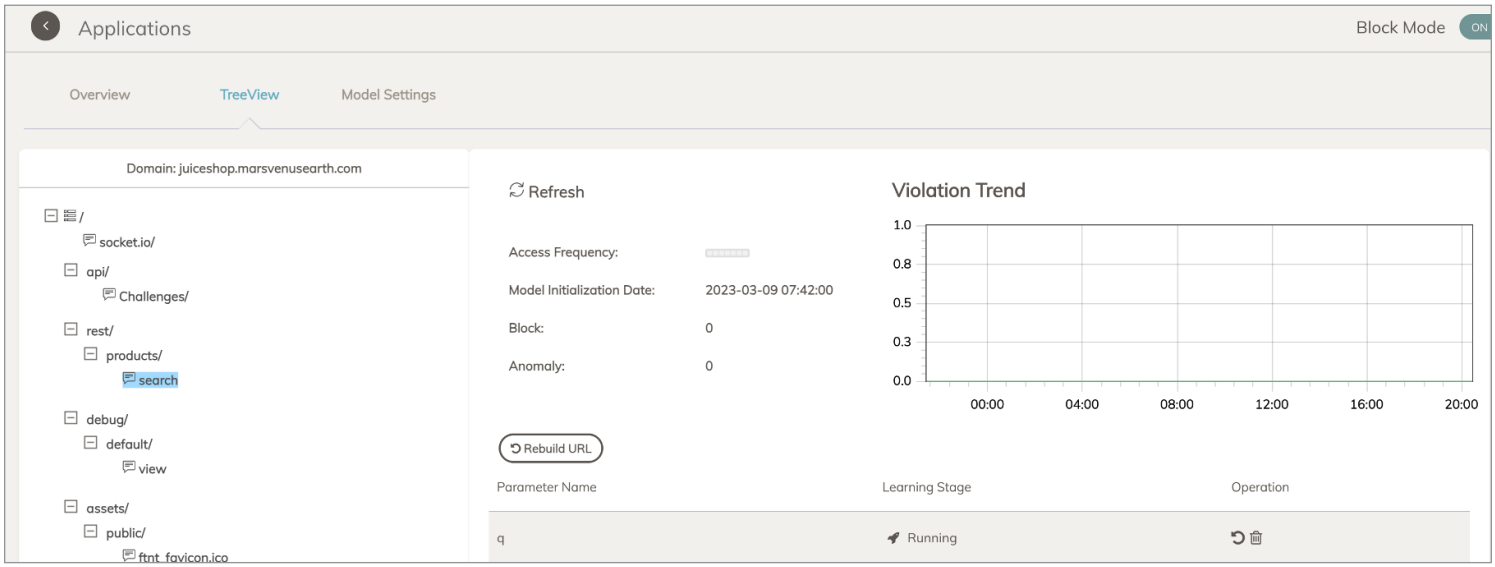

Figure 6. Machine Learning in the "Search" Parameter

To test the FortiWeb detection capabilities, we sent some simple SQL injection attempts into the "Search" parameter of the application. FortiWeb detected this attack and redirected us to a default block page, as shown in Figure 7. (This also can be customized.)

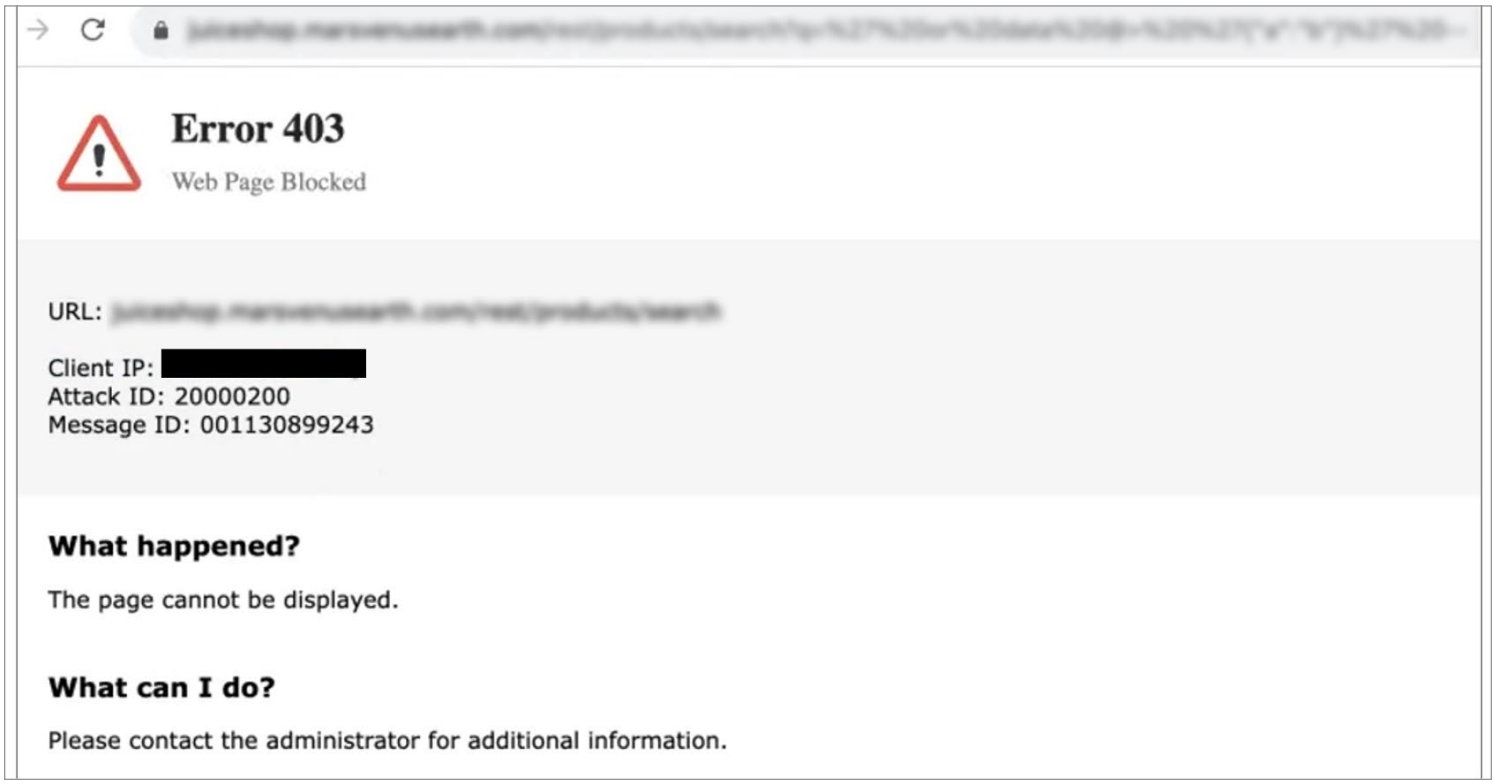

Figure 7. Blocking SQL Injection with Anomaly Detection

The ML engine within FortiWeb Cloud takes in domain and network address reputation, antimalware processing, and sandboxing to look for indicators of compromise and credential stuffing attempts, among other factors.

In addition to these anomaly detection capabilities, FortiWeb Cloud offers information leakage monitoring, validation and analysis of cookie attributes, input validation for parameters (primarily through regular expression pattern matching), and file protection that can perform antivirus scanning analysis, looking for known trojans and backdoors, and full-fledged malware sandboxing with a license for FortiSandbox (shown in Figure 8).

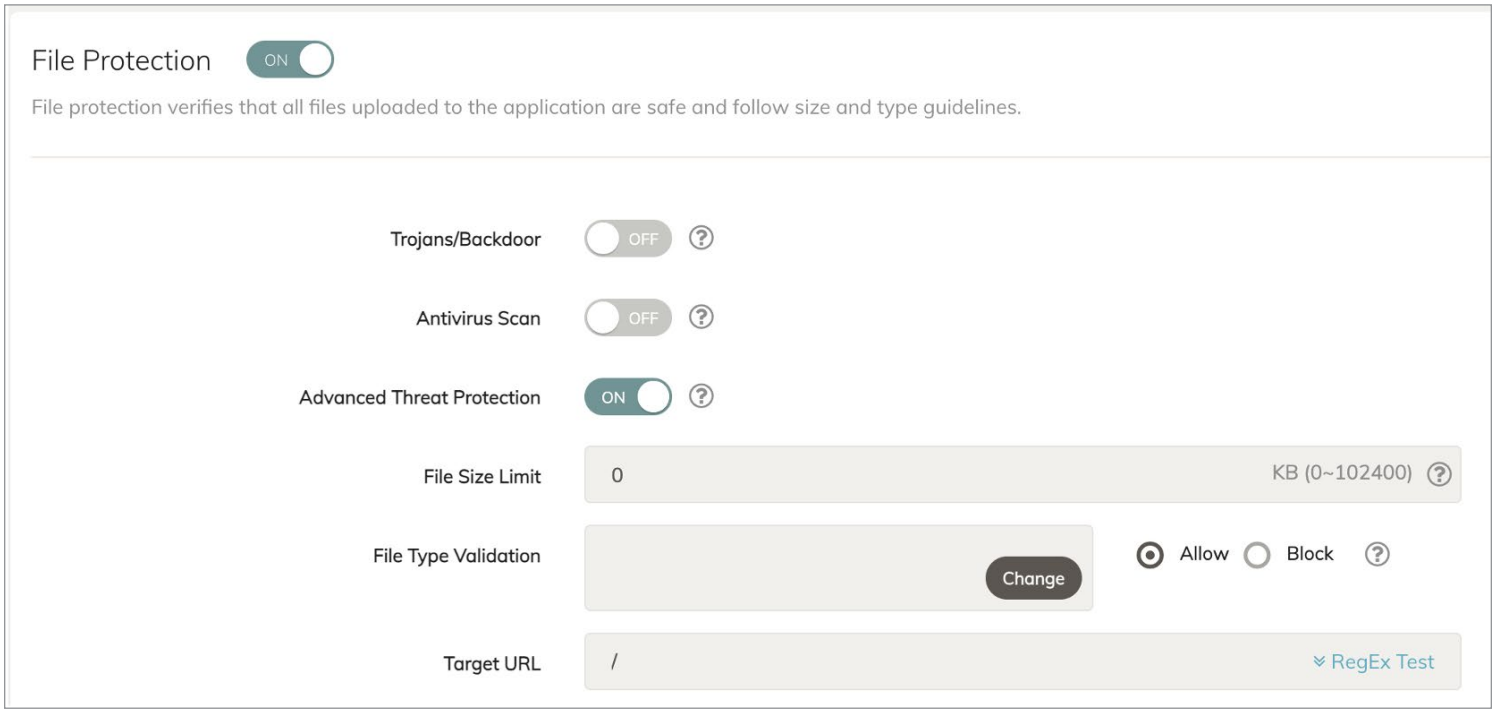

Figure 8. FortiWeb File Protection

The evolution of ML and request analysis at massive scale can help services like FortiWeb Cloud rapidly build threat profiles that customers can implement quickly, versus relying on on-premises solutions that don't have constant updates and analytics in the background to ensure threat models are as up-to-date as possible. This capability to build threat profiles quickly is an important feature of cloud-based security controls and brokering models because it allows customers get real-time updates and threat intelligence that can be leveraged very quickly.

API Protection

As more applications and web services shift to the cloud, there's also major growth in open and extensible APIs between applications and cloud services for all manner of enhanced capabilities and features (such as client features, integration and automation, monitoring and information queries, and many more). Unfortunately, many of these APIs are exposed and largely unprotected, and attackers are actively targeting them today. FortiWeb Cloud supports rules using the OpenAPI standard, JSON, and XML/SOAP frameworks, and clients can easily upload API description files that can be used to create new policy definitions. A sample YAML file with API specifications and definitions for our test site is shown in Figure 9.

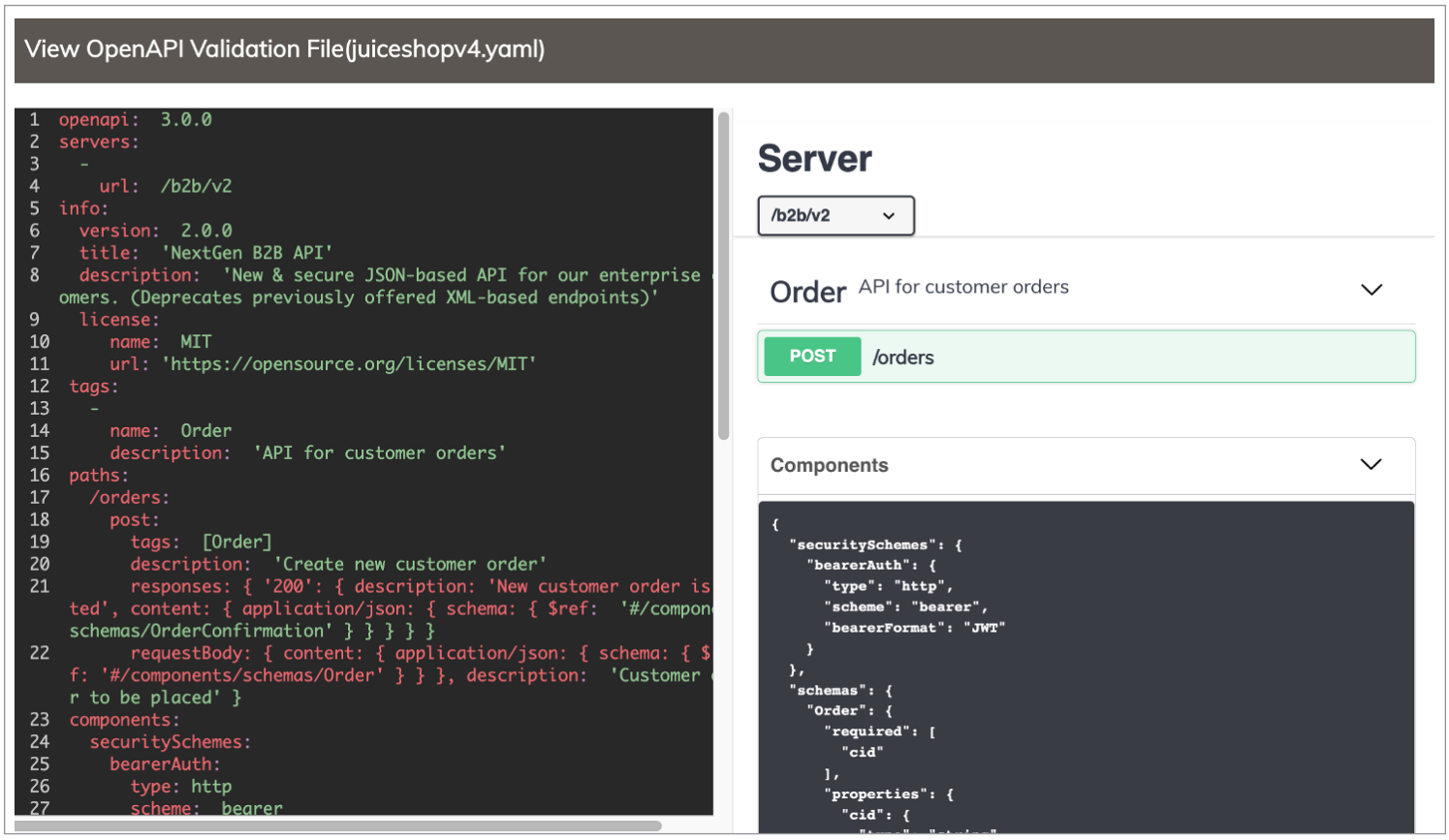

Figure 9. OpenAPI Definitions and Validation in FortiWeb Cloud

With a defined API model in place, FortiWeb then looks for attempts to inject malicious content, manipulate API capabilities and functions, and more. FortiWeb Cloud also includes an ML model for protecting APIs, where the API parameters, requests, and responses are all analyzed by FortiWeb security analytics to detect unusual or malicious interactions with APIs. The ML model can also produce Swagger templates for OpenAPI, as shown in Figure 10.

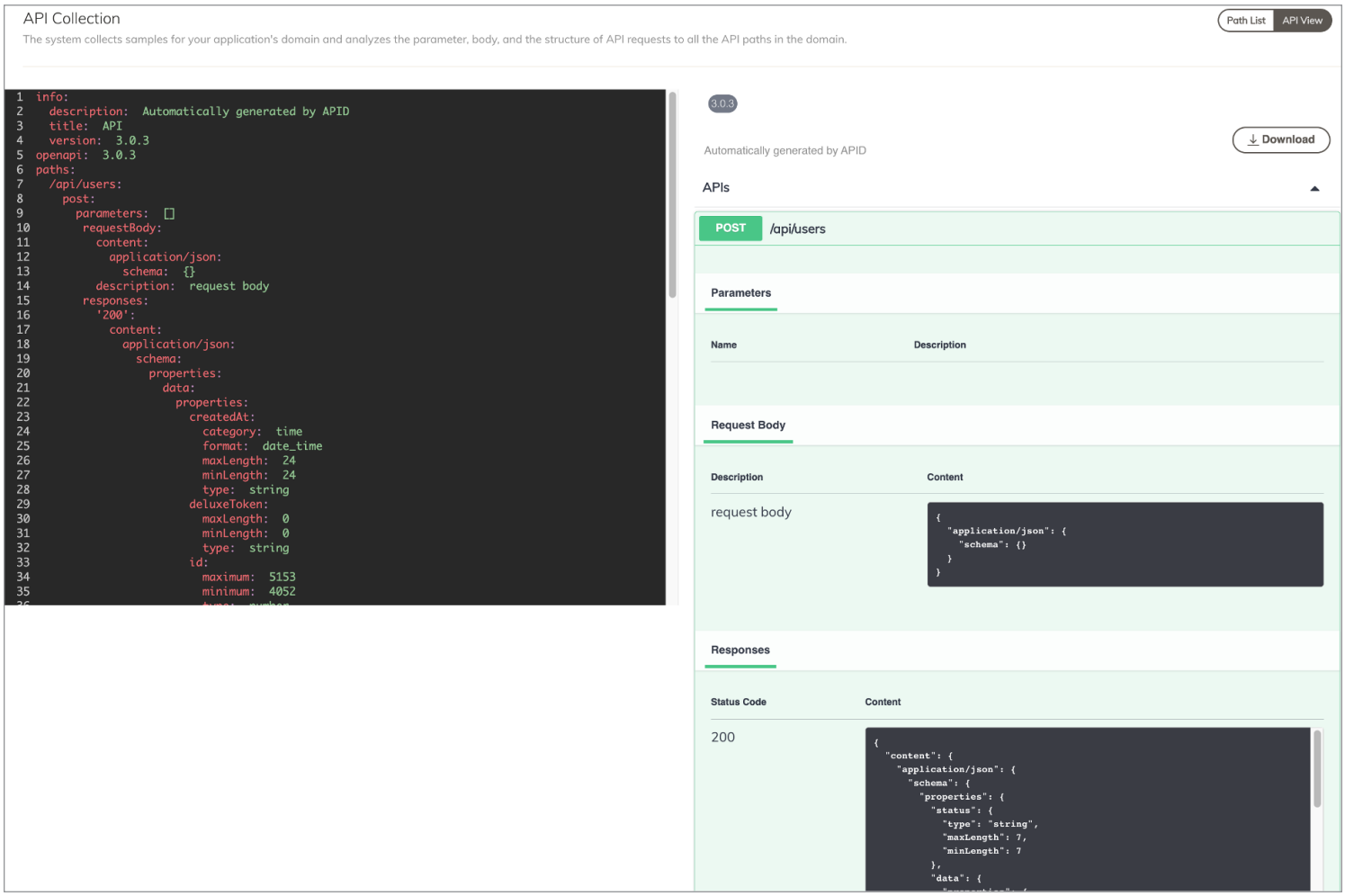

Figure 10. FortiWeb Cloud Machine Learning Protection for APIs

The API protection capabilities provide schema protection to validate expected data types and formats, as well as threat protection against OWASP API threats. Although we didn't configure or test API Gateway functionality, FortiWeb Cloud does also offer the capability to provision API keys, manage API users, control API access, and rewrite API calls.

Threat Analytics

The Threat Analytics monitoring and alerting capabilities in FortiWeb Cloud enable security operations teams to better visualize the types of threats detected categorically as well as potential incidents that may occur as a result of ongoing attacks. The dashboard was easy to navigate, including information about top attack types, origin of attacks geographically, and more, all aggregated and compiled with Fortinet ML technology in the background. See Figure 11.

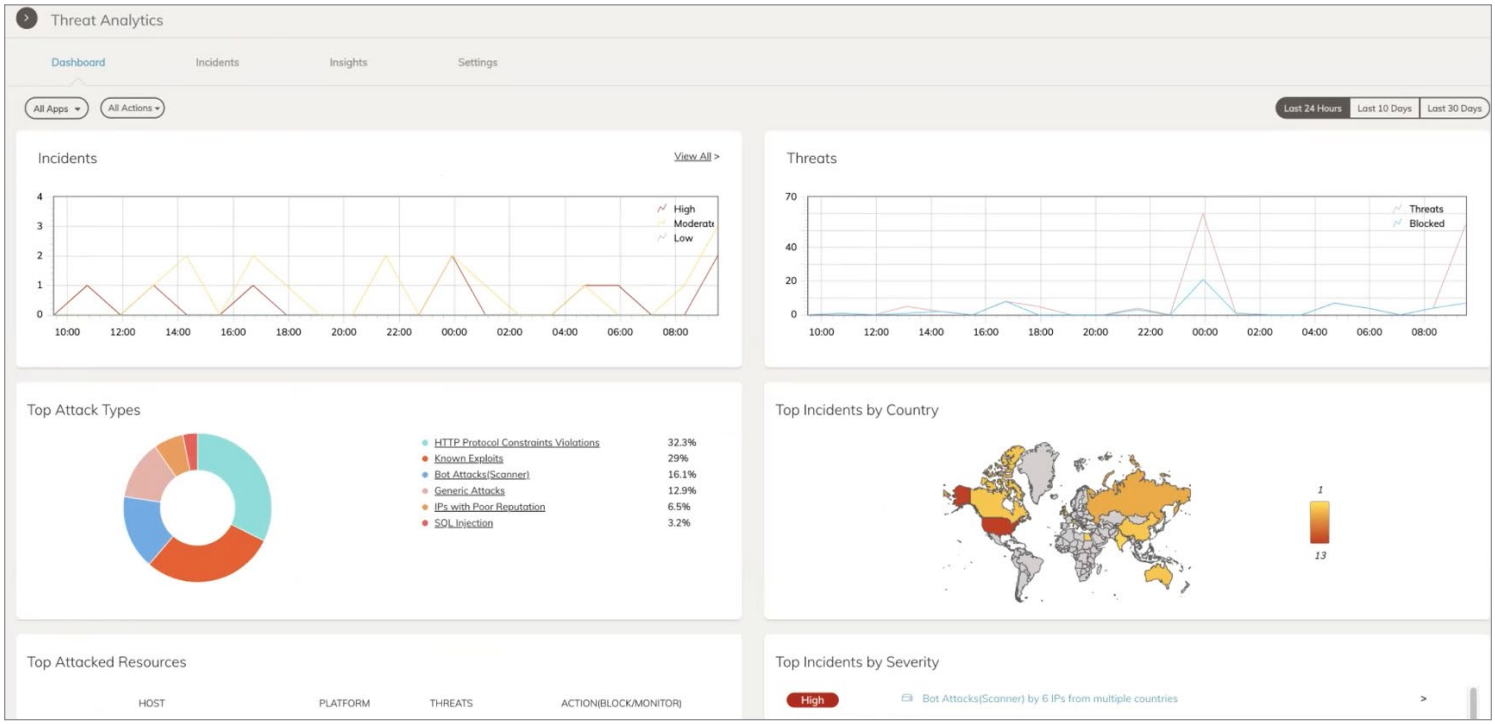

Figure 11. FortiWeb Cloud Threat Analytics Dashboard

Threat Analytics also compiles incidents based on aggregate traffic and attacks that are coordinated or appear to come from the same source. In Figure 12 on the next page, we see that numerous threats in the same category, from the same source, or both can easily be compiled into an incident to be analyzed uniquely. This functionality could help SOC analysts dig more deeply into attack details and tune detection and prevention policies more effectively.

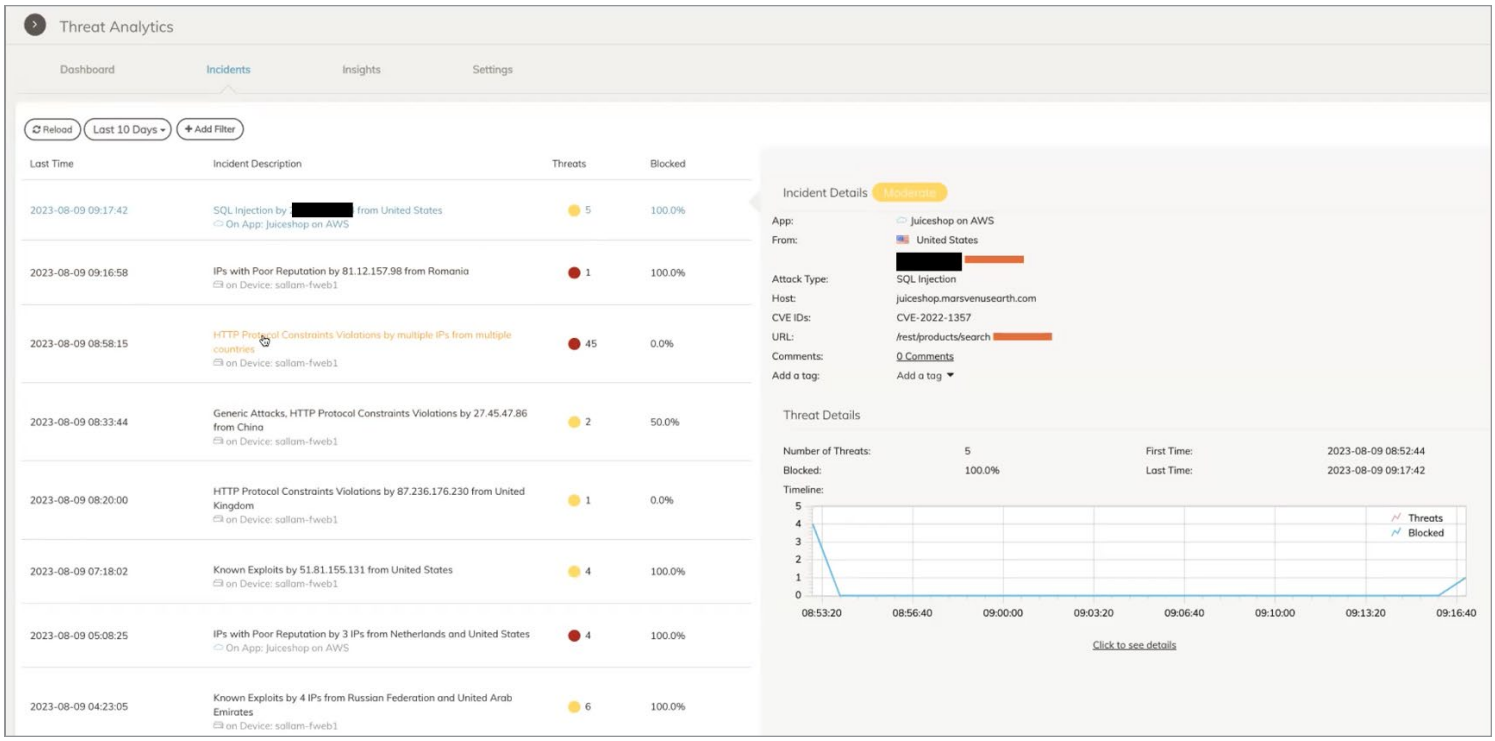

Figure 12. Threat Analytics Incident Reporting

In addition, a more granular view of specific attack detections is shown in the Attack Logs dashboard, which highlights specific attacks, sources, and the severity of these attacks, and offers granular filtering to look for particular elements of the attacks such as CVE IDs, source and destination ports, addresses, domains, and much more. See Figure 13.

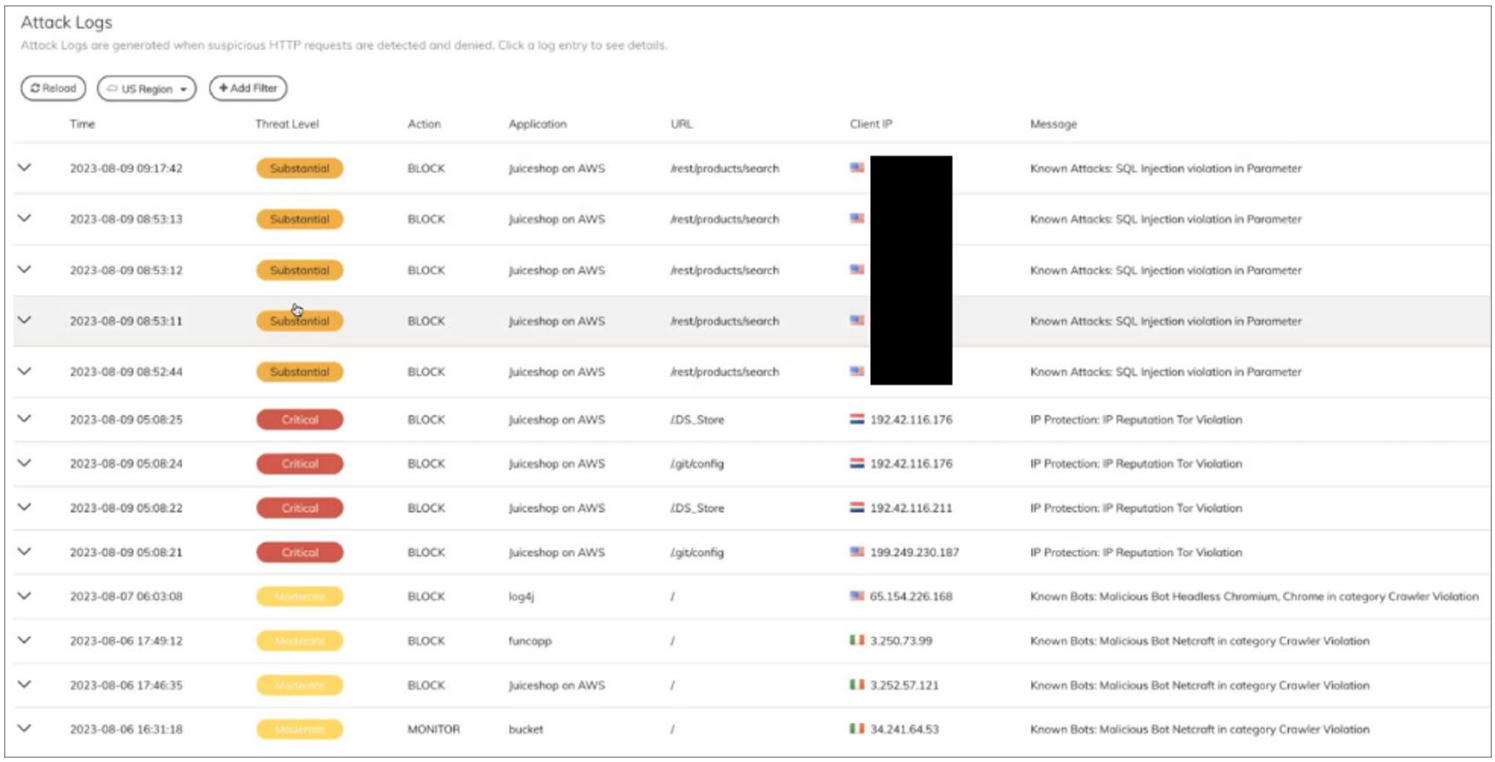

Figure 13. FortiWeb Cloud Threat Analytics Attack Logs

The Threat Analytics capability can also provide more detailed insights into WAF-specific policies and alerts (not reviewed here), as well as risks based on exposed APIs and application services. Alerting can be easily integrated into JIRA and ServiceNow workflows, as well.

Client Security and Access Rules

We didn't explore these features in detail, but FortiWeb Cloud does offer client-centric security controls such as HTTP header validation and analysis (looking for known clickjacking attacks and others), cross-site request forgery (CSRF) detection that inspects user requests and parameters looking for unusual access to and potential manipulation of session tokens, and possible man-in-the-browser (MITB) attacks that attempt to intercept client-to-server content requests.

Some additional security features added to FortiWeb Cloud include IP protection policies that allow blocking of entire geographic spaces (countries), as well as trusted and untrusted IP source addresses and ranges, and IP reputation analysis, as shown in Figure 14.

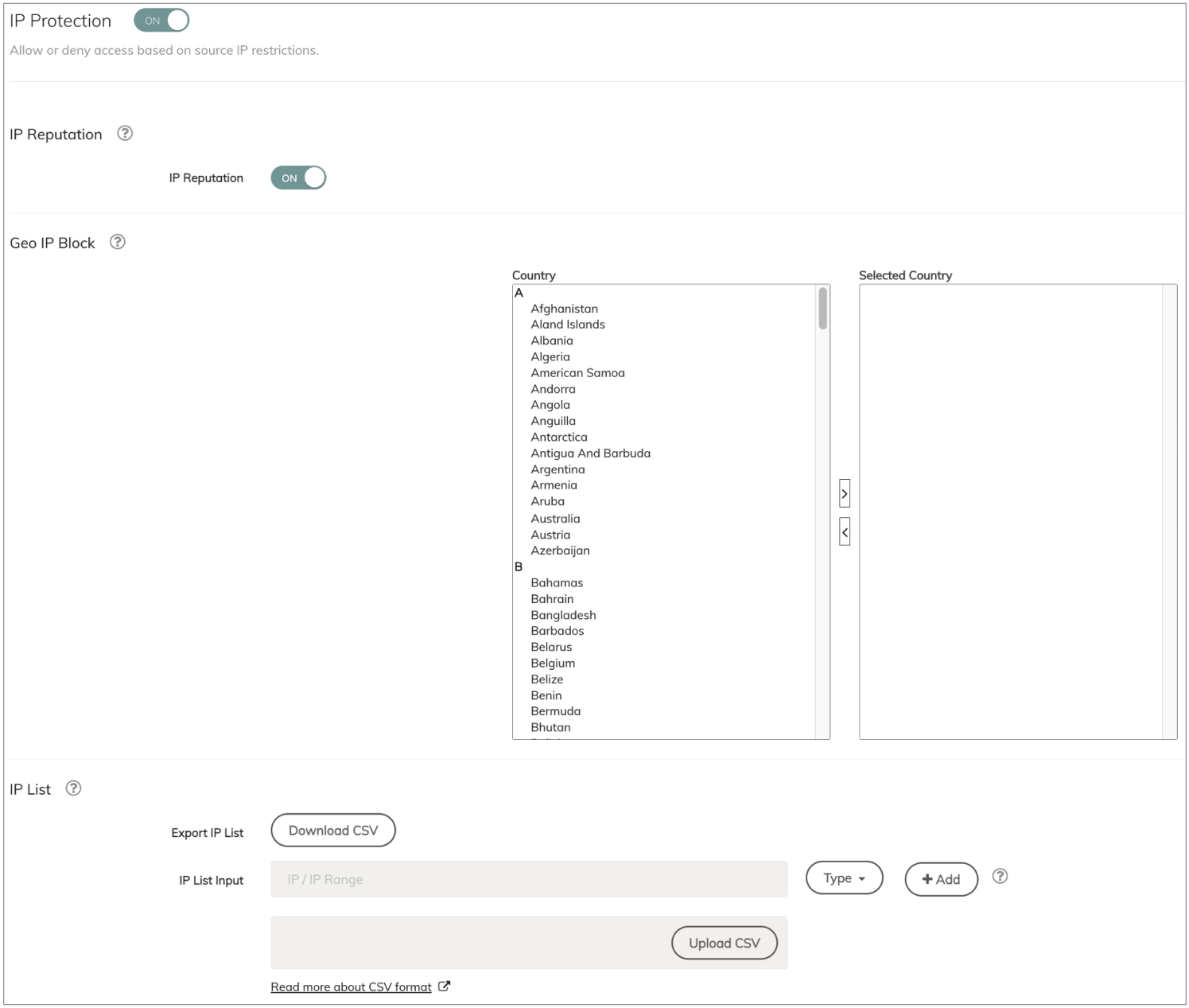

Figure 14. IP Protection Features in FortiWeb Cloud

DDoS Protection

Many organizations have faced DDoS attacks in their own data centers; these can be notoriously difficult to defend against using existing network perimeter technologies. Many on-premises tools and controls are not capable of wholly protecting applications and network services, and the variety and types of attacks are changing as well. Although most attacks are still volume-based (primarily SYN floods and ICMP and UDP traffic), more and more application-level traffic is seen today, primarily HTTP, HTTPS, and DNS queries. Some of these are much "slower" in nature and focus more on connection handling at the application/service layer than on pure volume. Also, many DDoS attacks now target stateful network devices, looking to fill connection queues and cause slowdown and loss of availability. New types of criminal activity are being seen related to DDoS attacks. In addition to the classic extortion and political focus, DDoS attacks are now being used as a distraction mechanism while other attacks (such as data exfiltration and privilege escalation attempts) are underway, making the need to defend against DDoS efficiently and effectively even more pronounced.

FortiWeb Cloud can impose limits on the number of HTTP requests that a client can make within a specified time frame. This helps prevent HTTP-based DDoS attacks that overload a web application with excessive requests.

FortiWeb Cloud's DDoS protection capabilities include the features listed below (and shown in Figure 15):

- **HTTP access and request limits—**FortiWeb Cloud can impose limits on the number of HTTP requests that a client can make within a specified time frame. This helps prevent HTTP-based DDoS attacks that overload a web application with excessive requests.
- **Blocking known malicious IP addresses—**FortiWeb Cloud can leverage threat intelligence data to identify and block known malicious IP addresses that are involved in DDoS attacks or other malicious activities.

Figure 15. FortiWeb Cloud DDoS Prevention

- **Session and cookie-based limitations and enforcement—**By monitoring user sessions and cookies, FortiWeb Cloud can identify anomalies and enforce session and cookie-based limitations to protect against DDoS attacks that attempt to exploit application vulnerabilities.
- **"Roadblock" measures such as CAPTCHA—**FortiWeb Cloud employs additional security measures such as CAPTCHA challenges to verify whether incoming traffic is from legitimate users or bots. CAPTCHA challenges are often used to block or restrict automated traffic that may be part of a DDoS attack.

It is likely that DDoS attacks will continue in the future, whether fueled by criminal goals, political mischief, or other motives. At the same time, the severity and sophistication of these attacks is growing, and many organizations are not well equipped to handle them. Using a cloud-based solution with DDoS defense may prove to be an effective security control for preventing, detecting, and responding to these attacks, whether you have on-premises protection or not.

Conclusion

This was a focused and targeted review, but FortiWeb Cloud offers a wide range of cloud security brokering controls and capabilities, such as WAF policies, API security, access controls and account takeover policies, and much more. The solution was easy to navigate, and policies were simple to create and modify.

For organizations deploying cloud-based applications and looking to protect all manner of web services via a cloud-based security brokering platform, FortiWeb Cloud deserves a look. There are numerous integrations with other Fortinet products such as the FortiSandbox malware analysis platform, and the API analysis and protection service is highly intuitive and capable. More ML capabilities are being integrated all the time, as well, helping organizations to better defend against both known and unknown threats.

Sponsor

SANS would like to thank this paper's sponsor:

FORTINET®