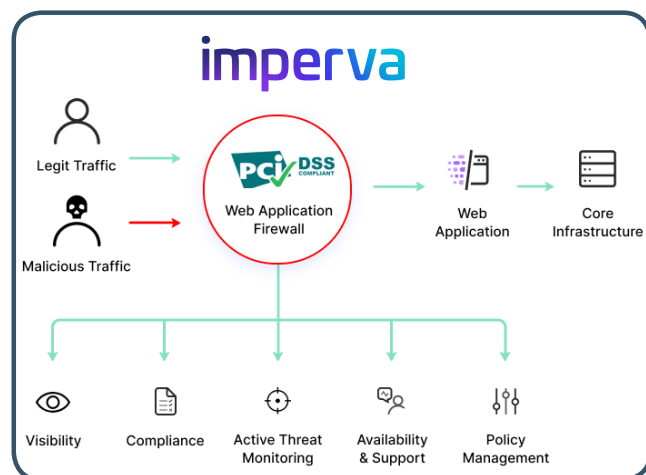


Imperva Cloud WAF

A real world test and evaluation of Imperva's cloud web application firewall



Key features

- **Fast deployment**
- **100% cloud hosted**
- **Single cloud admin portal**
- **Globally distributed CDN**
- **OWASP top 10 protection**
- **3-second DDoS mitigation SLA**
- **Sophisticated monitoring and alerting**
- **ML/AI powered attack analytics**
- **Advanced bot protection**
- **Smart AI Explain service**
- **Reputation intelligence dashboard**

The need for a web application firewall

Website attacks are increasing exponentially and businesses that want to survive and prosper cannot afford to let their defences down. Today's threat landscape is constantly evolving with AI now becoming the weapon of choice for organised gangs of cybercriminals as it allows them to create more advanced, scalable and automated attacks.

To counter these threats, businesses must implement a layered defence and a critical component of this strategy is a web application firewall (WAF). Traditional network firewalls cannot protect public-facing websites, web applications or APIs as they are not equipped to handle threats such as cross-site scripting (XSS), DDoS, SQL injection, local file inclusion (LFI) or brute force attacks.

A WAF is designed to monitor inbound and outbound web traffic, allow legitimate requests through and detect and block attacks before they can reach a web application. It keeps your company's websites running safely and smoothly while stopping malicious traffic from impacting on performance and data integrity.

There are plenty of choices on today's market and the Imperva WAF from Thales stands out from the crowd as its versatile Imperva WAF solution supports multiple deployment scenarios. It's available as a SaaS-based service, can be hosted locally on customer equipment, virtualised on a choice of cloud and on-premises hypervisors or delivered as a dedicated and hardened turnkey gateway appliance.

Clearly, Thales can deliver web application protection for virtually all business environments and this report focuses exclusively on its flagship Imperva Cloud WAF solution. Hosted on the Imperva globally distributed content delivery network (CDN), the Imperva Cloud WAF can protect any public-facing website along with its associated applications and APIs.

It's remarkably easy to deploy and the unified cloud portal provides a single pane of glass for configuring and managing all security components. Imperva offers an extensive range of optional protection features and these are all easily accessed from the same interface.

In this review, Binary Testing will not be using suites of simulated attacks in a synthetic environment as Imperva Cloud WAF will be used to protect our live web sites. The product will be configured to run in a real world scenario for three months allowing us to fully evaluate deployment, ease of use, features, management and monitoring – all threats and attacks it detects will be genuine and in real time.

How Imperva Cloud WAF works

At its foundation, Imperva Cloud WAF functions as a secure reverse proxy that intercepts and inspects all web traffic. It receives incoming user requests, completes a TCP three-way handshake, terminates the initial connection, connects with your web server(s) and forwards the request.

This all looks deceptively simple but there's a lot more going on in the background as the Imperva CDN employs a global network of data centres to host its reverse proxy services. Called points of presence (PoPs), Imperva Cloud WAF defaults to making all of them available to protect a customer's websites but automatically uses the nearest one to a user for request handling.

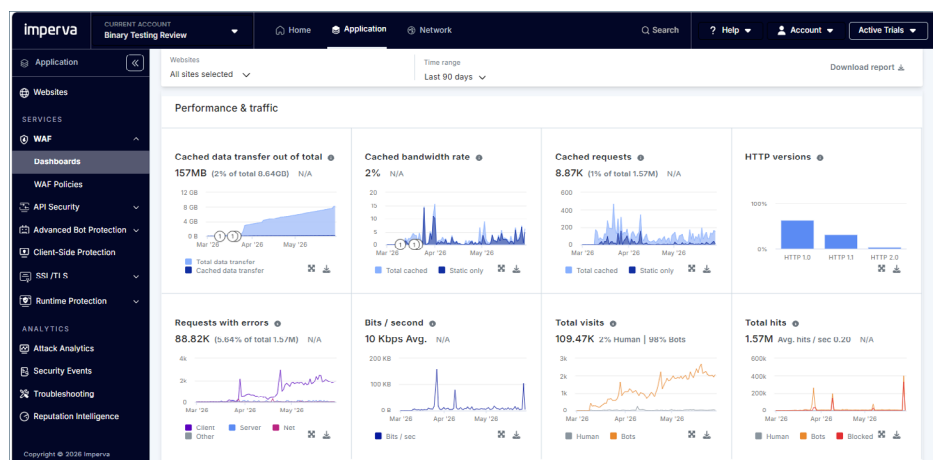
The benefits of this approach are manifold as Imperva Cloud WAF can significantly improve the user experience by optimising website performance and reducing latency. The CDN also delivers intelligent caching and integral load balancing while Anycast routing provides automated failover between PoPs without requiring changes to DNS resolution.

More importantly, it allows Imperva Cloud WAF to intercept all inbound traffic at the network edge before it gets anywhere near your web servers. It inspects each HTTP/S request at the connection, format/structure and content payload levels, and evaluates them using an extensive range of multi-layered checks including signature-based detection, behavioural analysis, reputation intelligence and advanced machine learning (ML) models.

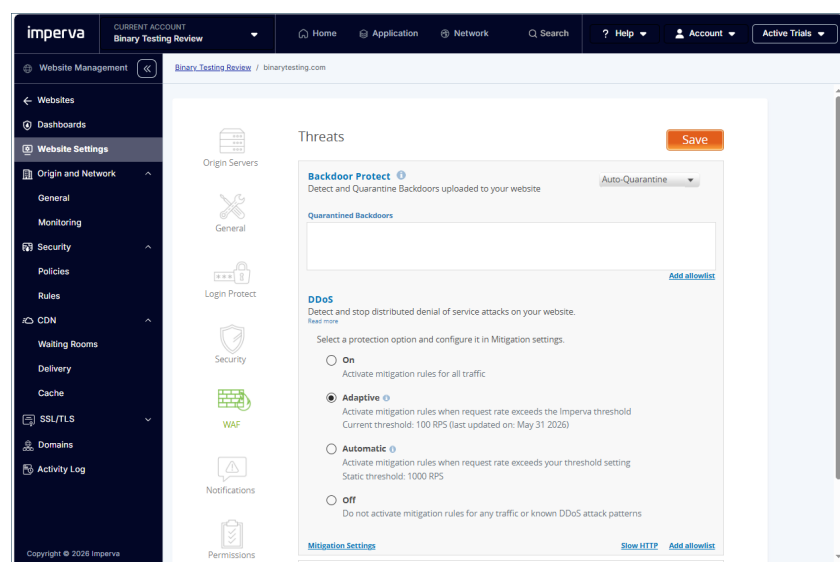
Connections are validated by comparing them with IP reputation databases of known bad actors plus malicious proxies and WAF policies can apply geo-blocking to restrict traffic from specific countries. Device fingerprinting and behavioural analysis are used to identify automated and AI-powered bots which recently surpassed human activity and currently account for more than half of all internet traffic.

Businesses that think Distributed Denial of Service (DDoS) attacks are a thing of the past are sadly misguided as they are getting a lot worse. Terabit-level, or volumetric, DDoS attacks are now commonplace and they are getting much smarter and faster requiring businesses to implement proactive, adaptive and self-defending systems that remove the human element from mitigation.

The DDoS Protection for Websites component is included with Cloud WAF and Imperva is so confident in its efficacy that it boasts a 3-second mitigation SLA (service level agreement) for any size, type and duration of attack. Imperva's global network of over 60 high-capacity PoPs offer a total 'scrubbing' capacity of 13Tbps and can process over 65 billion attack packets per second so are quite capable of handling the new breed of volumetric DDoS attacks.



The Imperva Cloud WAF dashboard provides plenty of information about PoP and website performance

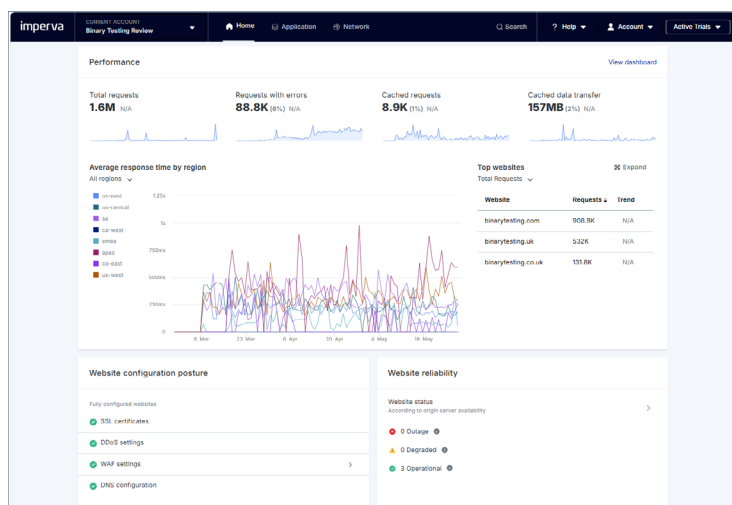


Imperva Cloud WAF provides integral L3/4/7 DDoS protection and mitigation with a 3-second SLA

Easy deployment

Imperva Cloud WAF deployment is swift as we added our websites in our account portal using their full domain names and opted to have Imperva manage all SSL certificates. The next step is very important as Imperva Cloud WAF requires you to prove you own the domains before it will issue site SSL/TLS certificates.

We used the automatically generated record name and CNAME record value to update the DNS services at our own website hosting provider and once Imperva Cloud WAF had validated domain ownership, we then added the A records it provided to route website traffic through Imperva's servers. The A record points to the nearest Cloud WAF PoP and Imperva generates two for redundancy.



Four green lights for the website configuration posture confirmed Imperva Cloud WAF was protecting our websites

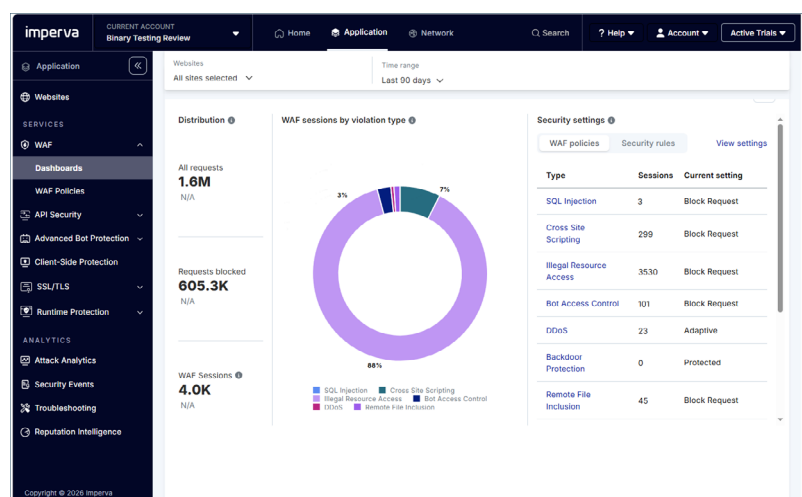
After updating our provider's DNS records, Imperva Cloud WAF ran a validation process to confirm traffic was being correctly routed. We checked the portal's website configuration posture status panel which shows green lights for SSL certificates, DDoS settings, WAF settings and DNS configuration and confirmed that all traffic to our websites was going through Imperva's servers.

Protection starts immediately as a default WAF policy is created, applied to all websites and set to block malicious visitors and requests. You can easily create your own custom policies and assign them to specific websites with each one containing rules that cover cross-site scripting (XSS), illegal resource access, remote file inclusion and SQL injection.

Attack surprise

The cloud portal is very well designed and provided a wealth of information about our website security posture. Businesses that think their websites are of no interest to cybercriminals will find these pages may well shake them out of their complacency.

The moment Imperva Cloud WAF had been activated, we could see that our websites were constantly under attack. Within the first day, Imperva Cloud WAF reported on illegal resource access, XSS, bad bot and DDoS bot attacks from multiple countries right across the globe and the alert list quickly grew to include SQL injection and remote file inclusion attacks.



The Imperva Cloud WAF portal clearly showed the sheer number of attacks our websites were being subjected to

Over the testing period of three months, Imperva Cloud WAF recorded a total of around 1.6M requests and blocked over 605,000 malicious requests with the majority of these being illegal resource access attacks from automated bots and hacking tools. Without Imperva Cloud WAF protecting our websites, we would have been blissfully unaware of this constant onslaught.

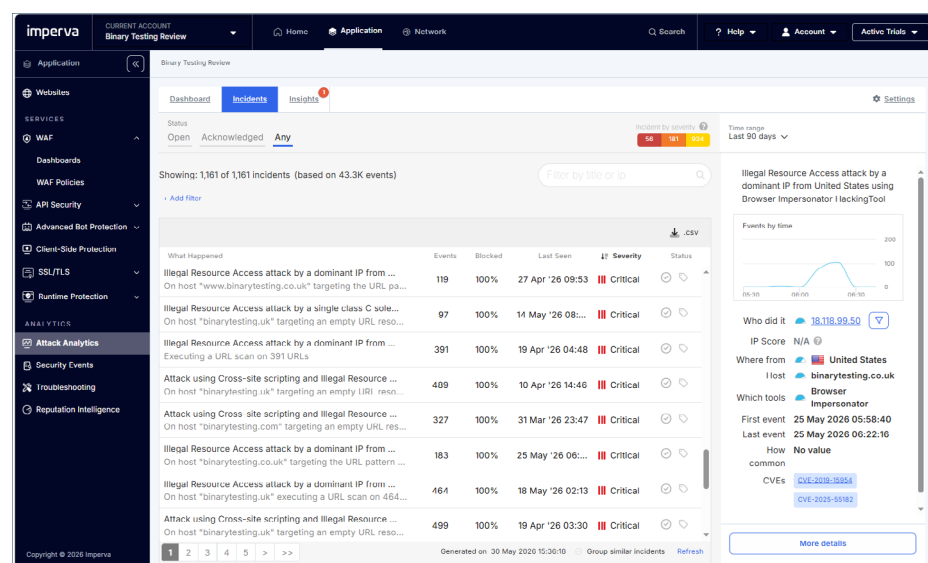
Attack analytics

The results from our three month live tests revealed an enormous number of attacks but Imperva Cloud WAF offers plenty of tools that can sort the wheat from the chaff and cut through the fog of alert smokescreens. The Attack Analytics service uses machine learning (ML) algorithms and artificial intelligence (AI) to sort and condense the many thousands of daily security alerts into concise and manageable lists of incidents prioritised by threat severity.

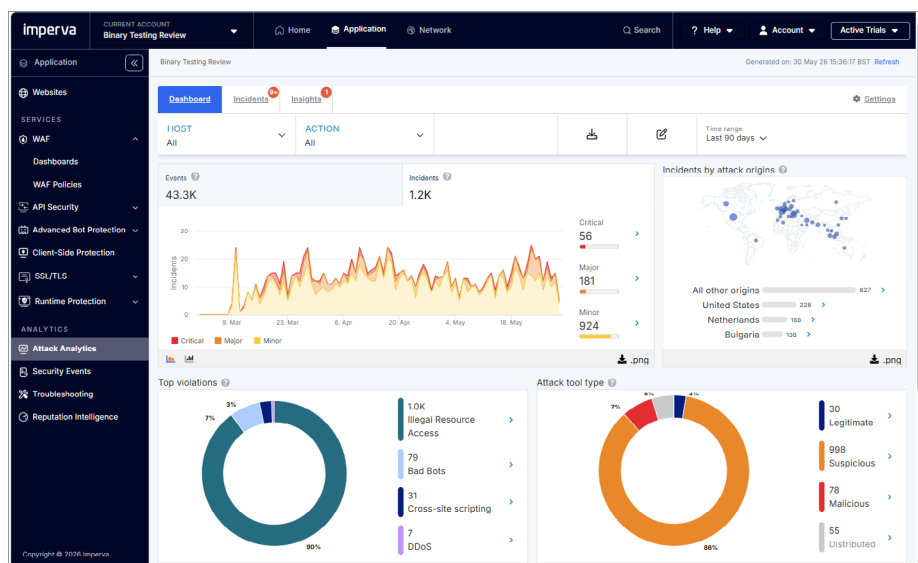
In practice, we found this partnership works extremely well with the customisable attack analytics dashboard presenting us with a tidy graphical overview of events and incidents over time which could be filtered to show all protected websites or specific ones along with all, blocked or alerted events. More charts showed the dominant attack origin countries, the top violations, the most popular attack tools, the most attacked websites and a highlight chart that shows the number of similar incidents identified by Imperva across its entire customer base and those associated with known CVEs.

Moving to the incidents panel reveals a list of all attacks and showed Imperva's ML and AI services in action as they condensed over 43,000 events down to just over 1,144 incidents. This can be reduced further by applying up to eight filters such as the country, action, frequency and bad bots.

Selecting an incident provides a wealth of information in the right pane as we could see the originating IP address of the attacker, the country, the tool used, the website being attacked and any associated CVEs. You can drill down further into individual incidents by clicking on the 'More details' button below this display and see the discovered violations, a list of resources that were attacked, the website hosts being targeted and all IP addresses used by the attacker.



The Attack Analytics Incidents page provides everything you need to know about each detected attack

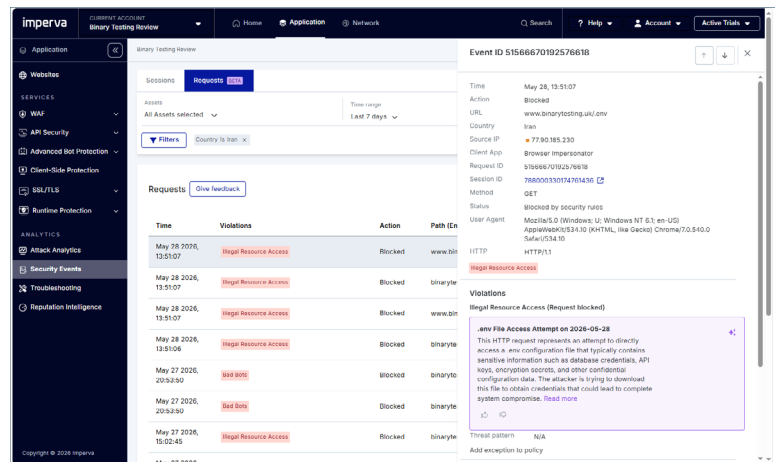


The Attack Analytics dashboard uses ML and AI to condense all detected threats into actionable insights

Security events and AI Explain

The security events dashboard provides a complete rundown on all activities that have triggered an Imperva Cloud WAF security rule and presents an events snapshot chart at the top for quick views of overall event classifications. Down below, we could view all security events in more detail and see the client type and app used by the hacker, the entry point, the source IP address, the number of hits and the country of origin.

An extensive range of filters is provided to fine-tune the information with options including the violation type, security action, country, client app, URL and CVE. We could drill down into selected events and see every request made by the attacker, the violation type and a full breakdown of the HTTP request being used.



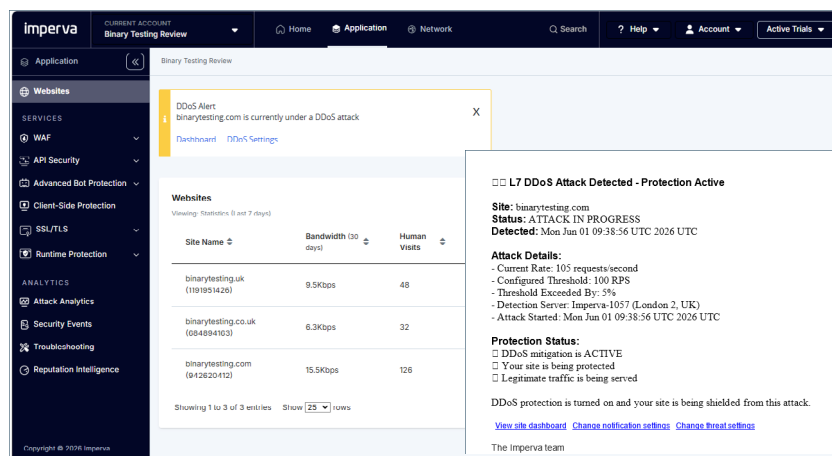
The smart AI Explain service uses generative AI to provide a clear description of a violation and remediation advice

This is a lot of information to digest but the smart AI Explain feature simplifies analysis immensely as it uses Amazon Bedrock generative AI to produce a clear explanation of the selected event and provide sage advice on remediation. AI Explain can currently analyse XSS, illegal resource access and SQL injection attacks and has an account limit of 100 queries per month which can be increased if required.

DDoS protection

Imperva Cloud WAF protects websites from all malicious DDoS activity including volumetric attacks at Layer 3 and 4 and application level attacks at Layer 7. Protection is easily configured for each website with options to enable mitigation rules for all traffic, use adaptive protection with automatic RPS (request per second) thresholds adjusted on a daily basis or fully automated using a specific RPS threshold.

To test our website protection, we used the HOIC (High Orbit Ion Cannon) stress-testing tool on multiple Windows clients to generate Layer 7 DDoS attacks. We own the websites so there are no issues of legality but you should be aware that unauthorised use of HOIC to attack websites is a serious crime and may result in a criminal conviction.



Imperva's DDoS Protection for Websites provides plenty of warnings and alerts when an attack is detected

Imperva Cloud WAF passed our tests with flying colours as it blocked all attack traffic and posted alerts in the portal summary page advising on which website was under attack. It issued email alerts within a minute of the attack starting and also sent another to confirm the attack had stopped.

From a legitimate user's perspective, they would have been none the wiser that an attack was taking place. During our tests, we were able to access all three websites with no indication of any performance issues.

Advanced bot protection

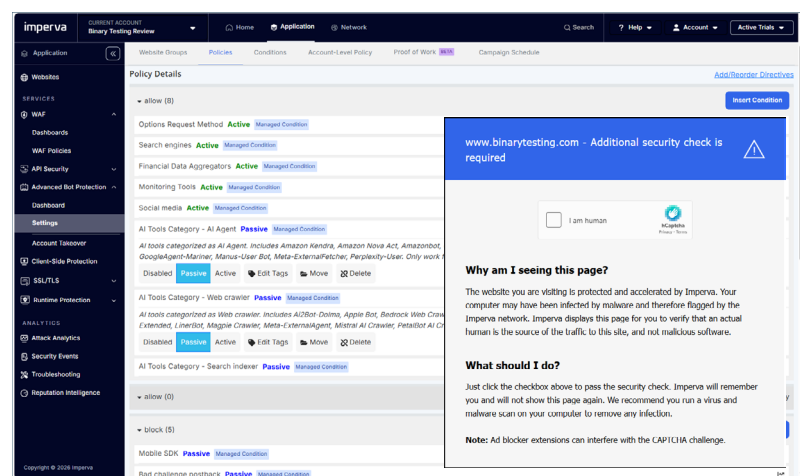
Imperva Cloud WAF includes sophisticated bot protection for smaller organisations which employs signature, IP reputation and rate limiting detection methods and is designed to block vulnerability scanners, simple scrapers, known bad bot and DDoS attacks. The Advanced Bot Protection (ABP) add-on targets larger businesses and goes much further by dynamically sorting the good bots from the bad using behavioural analysis, ML, device fingerprinting, threat intelligence feeds and progressive challenges.

ABP works hand in glove with Imperva Cloud WAF as it analyses each client request header to determine its source and asks two fundamental questions - who are you and what are you trying to do? Using over 700 parameters to create unique traffic fingerprints, ABP instructs Imperva Cloud WAF to allow human visitors and good bots through, block malicious bots and serve a Captcha challenge page for suspicious traffic.

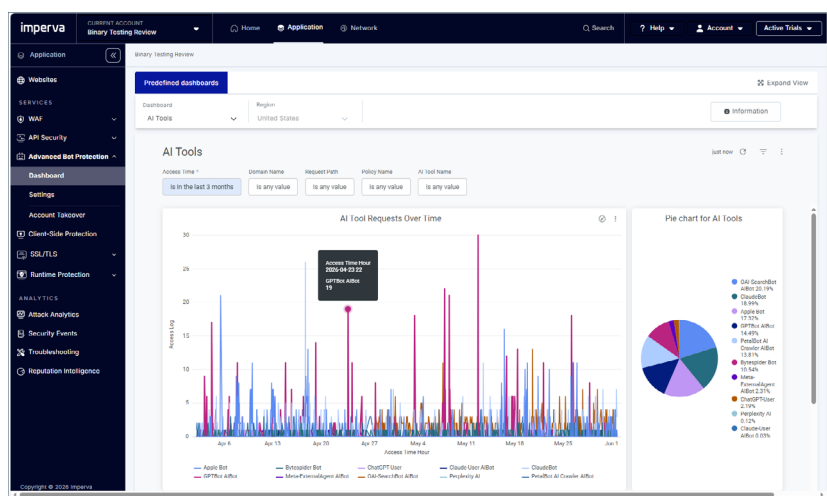
Accessed from a dedicated section in the cloud portal, the ABP dashboard provides an incredible amount of information on bot activity. There is a lot of data to digest but, as we've come to expect from Imperva, plenty of filters are provided to hone the data presented.

The AI Tools page was of particular interest as this provided us with graphical views of all detected AI tools, agents and web crawlers accessing our websites along with the number of requests being made by each one. They showed how our website data was being scraped to train LLM (large language models) and from our graphs, we could see plenty of AI bot activity such as ClaudeBot, Applebot, PetalBot, GPTBot and Bytespider.

One of the biggest issues with bot scrapers, and particularly the more aggressive AI models, is they could be costing you money by inflating cloud and website hosting charges. Along with high levels of visibility into AI bot activity, ABP gives you the tools to control access at a granular level and provides a default policy to protect against the majority of bot attacks



Advanced bot protection policies provide granular control of bot activity and can issue Captcha challenges



The AI Tools graph revealed all the AI tools, agents and web crawlers accessing our websites

Policies contain rulesets applied to website groups and can be customised with paths to protect specific pages. Groups of directives within a policy are defined with actions and use conditions that if met, will trigger actions which could be to allow, block, challenge or throttle. ABP is one of the more complex components of the Imperva solution but we found it a very powerful tool clearly capable of providing deep protection against threats such as web scraping, scalping, data mining, account takeover, API abuse and much more.

Conclusion

It became abundantly clear to us during testing that businesses must consider a web application firewall as a critical component in their website and data protection strategy. During our three month evaluation of the Imperva Cloud WAF, we were staggered by the number and type of attacks it detected on our websites that were occurring on a daily basis and from multiple geographical locations across the globe.

We modestly consider our websites as comparatively low-key affairs and yet they received an alarming amount of attention from automated bots and hacking tools with attacks including illegal resource access, XSS, bad bot, DDoS bot, SQL injection and remote file inclusion. Scale this up to high-profile corporate websites and it's clear that the number and type of attacks are going to be exponentially greater as they offer cybercriminals a highly lucrative target.

And it's only going to get worse with the advent of dark LLMs heralding a 'fifth wave' of cybercrime and the use of weaponised AI with no ethical restrictions. DDoS attacks are evolving just as quickly and are changing from at-scale attacks to those that are simpler to launch and easily repeatable with targets expanding to any business that relies on an online presence.

Imperva Cloud WAF is an undeniably powerful website security solution but Binary Testing found it extremely simple to deploy and we were impressed with its cloud portal which provides a single pane of glass for monitoring and managing all suite components. The default WAF policy ensured protection started immediately but we found it easy to create custom policies and apply them to specific websites.

The level of attack information provided is truly remarkable but the combination of the Imperva ML and AI services plus the Attack Analysis, Security Event and AI Explain dashboards condensed it down to manageable lists of actionable events. The DDoS Protection for Websites component performed flawlessly when subjected to our live tests and Imperva's global PoP network clearly has the capacity to mitigate very high attack volumes and keep your websites running smoothly.

We consider the optional Advanced Bot Protection module a must-have feature as it showed us precisely which bots were scraping our websites. It provided the insights and tools to create granular policies to protect them from malicious bots and automated attacks whilst allowing good bots through.

Imperva Cloud WAF is an ideal security solution for enterprises that need to protect critical web applications from advanced and evolving cyber threats while its 100% cloud deployment makes it simple to deploy and highly scalable. Imperva offers a free 30-day trial of Cloud WAF – try it out and you too, can see just how popular your websites are with cybercriminals.

