aptum imperva

Service Guide

Aptum Managed WAF

Version 2.1

About Aptum Managed WAF

Aptum's Managed WAF provides Web Application Firewalling (a/k/a WAF) as a service (the "Services") to Aptum's customer (the "Customer") web-based applications and websites for which the Services are provisioned and configured. The WAF services provide a Cloud-based Web Application Firewall with available DDoS protection, resilient globally deployed data centers to deliver the Services (which are monitored continuously), with Bot Management and protection against many web-based threats that face businesses today.

The Services are backed by Aptum's 24x7 Managed Service team, which means you just make one call to our support team, and we'll keep you informed as we work on the Service issue through to resolution. Unless otherwise expressly defined herein, capitalized terms referenced in this Service Guide shall have the meanings ascribed to them elsewhere in the Agreement (as this term is defined in Aptum's Terms of Business, available at https://aptum.com/legal/, or a Master Services Agreement executed by the Parties (these are referred to herein as the "MSA"). To the extent that there is a conflict between any term in this Service Guide and any term in the MSA, the term in the MSA shall take precedence, govern, and control the subject matter. By way of reference, this Service Guide forms part of the Agreement.

Customer Responsibilities

Both the Customer and Aptum are responsible for collaborating on the execution of the Services. This Service Guide describes Aptum's Managed WAF (the "Managed WAF" or the "Services") and provides an overview of the Services, which may be modified by Aptum from time to time upon reasonable notice to the Customer. The Customer agrees to reasonably cooperate with Aptum to ensure that the Services are successfully provisioned as follows:

1. Before the commencement of the Services, the Customer will indicate to Aptum in writing a person to be the single point of contact, according to the project plan, to help ensure that all tasks can be completed within the specified time. All Services communications will be addressed to such point of contact (the "Customer Contact"). Failure to do so may result in an increase in scope and/or duration in scheduling.

2. The Customer will provide technical points-of-contact ("Technical Contacts"), who have a working knowledge of the environment in scope for the Services. Aptum may request that meetings be scheduled with Technical Contacts.

3. The Customer Contact will have the authority to act for the Customer in all aspects of the Services including bringing issues to the attention of the appropriate persons within the Customer's organization and resolving conflicting requirements.

4. The Customer Contact will ensure that any communication between the Customer and Aptum, including any scope-related questions or requests, is made through the appropriate Aptum representative.

5. The Customer Contact will provide timely access to technical and business points of contact and required data/information for matters related to the scope of Services.

6. The Customer Contact will ensure attendance by key Customer contacts at Customer meetings and deliverable presentations.

7. The Customer Contact will obtain and provide project requirements, information, data, decisions, and approvals within one working day of the request unless both parties agree to a different response time.

8. The Customer may be responsible for developing or providing documentation, materials, and assistance to Aptum promptly. Aptum shall not be responsible for any delays in completing its assigned tasks to the extent that they result from the Customer's failure to provide such timely documentation, materials, and assistance.

9. The Customer is responsible for providing all hardware, software, internet access, and facilities for the successful completion of the Services.

10. The Customer will conduct regular and timely backups of all its systems, software, and data which may be subject to, or in connection with the Services so that the Customer possesses full restoration capabilities.

11. Tickets opened by the Customer directly with Aptum's vendor (Imperva™) are outside the scope of the Services and shall not constitute notice or communication of any kind to Aptum and shall result in delays in resolving Services-related issues.

Introduction

Web Application security is a growing area of concern for enterprise organizations. Half of all attacks are directed at web applications and that rate is increasing. Factors such as the rise of cloud computing, the increase in data processing requirements, the complexity of web applications, and an increase in the overall sophistication level of attackers have led to an extremely challenging environment for IT security leadership. Data security standards such as PCI DSS and the NIST Cyber Security Framework also present significant hurdles for security teams. Each standard is rigorous, requiring hundreds of controls to achieve compliance. The fact is, when a breach occurs, it could often have been prevented. However, security budgets are not keeping up. IT leaders struggle to keep pace with innovation and the growing costs of breach mitigation, prevention, post-breach remediation, and cleanup. Our Managed WAF is an enterprise-grade web application security PaaS (Platform-as-a-Service) that was designed to address today's cyber security challenges.

Managed WAF At-a-Glance

Managed WAF is a Web Application Firewall solution designed to protect your platform and services hosted with Aptum (in our Cloud, Hyperscale, Colocation, or Hosted environments), protecting your most critical web applications against security threats. Utilizing Imperva's Application Security Suite, your web applications will have the benefit of DDoS Protection, Application Firewalling against security threats, protection against emerging attack vectors, and protection against malicious Bot activity, all while having a tremendous amount of information and analytics at your fingertips.

Cloud-based, best-in-class Web Application Firewall and available DDoS protection for Layer 7 Applications. By default, Managed WAF includes up to 1Gbps of DDoS Protection and up to 5k packets per second of attack protection. Additional protection options are available as well.

Large global infrastructure with 51 DDoS-resilient data centers with over 9 Tbps capacity

Monitored and managed 24x7 by top cybersecurity experts

Aptum partners with Imperva™ to deliver a comprehensive solution for your Aptum Managed Environment

Imperva™ has millions of web applications and networks under WAF protection

Companies who can benefit from our Managed WAF include those in the eCommerce, Gaming, Energy, Government, Technology, Hospitality, and Financial Services Industries

Imperva's Bot Management includes some of the industry's best bot detection and defense techniques such as sender reputation, statistical analysis, client validation, including CAPTCHA protection and JavaScript Challenge to identify and block bad and/or suspicious bot activity

Multiple Certifications
- Level 1 PCI DSS v3.2.1 Certified
- ISO 27001

Our Technology Partner: Imperva™

We've partnered with Imperva™ to provide complete end-to-end protection using their best-in-class technology. The Imperva™ technology platform creates a protective shell around our clients' security perimeters, adding a critical layer of web application and IP protection. All traffic flows through the Imperva™ platform before arriving at the origin server infrastructure. Traffic is directed to the nearest Imperva™ POP which is connected to the Aptum Network.

How It Works

Our cloud-based Web Application Firewall platform and managed service ensure the protection of your web applications and network.

Enterprise-Grade Web Application Firewall

Designed to address today's cyber security principles of global distribution, optimized performance, scalable architecture, and adaptive learning.

DDoS Attack Mitigation

Distributed Denial of Service (DDoS) attacks are commonplace in today's cyber security landscape. The Managed WAF App Protect Professional, App Protect Enterprise, and App Protect 360 options include automated DDoS attack protection against Application Layer 7 DDoS attacks. DDoS Protection can be added to App Protect Essentials for an additional service charge.

Content Distribution Network (CDN)

Our Managed WAF solution includes access to a CDN to help ensure your site's content is delivered as quickly as possible to your end customers.

Real-Time Updates

Because our Managed WAF is delivered as a Platform-as-a-Service, we are constantly delivering improvements and new security features to all clients through a robust and rapid deployment process.

Intuitive Portal

Designed to deliver all the details and information about your site's protection and the blocked attacks against your site.

Benefit from a Globally Distributed Infrastructure

Well-intended security controls end up becoming an enterprise security chokepoint when cyber attackers can leverage global networks and continuously change the threat locations. Eventually, the enterprise origin becomes overwhelmed and breached, resulting in cybercriminals having an unfair advantage over an organization's perimeter-only defenses. A global security platform extends the enterprise's defenses. Organizations must embrace globally scalable and distributed solutions as a starting point to thwart attacks.

Imperva's network consists of 51 DDoS-resilient data centers with over 9 Tbps capacity.

For details and exact city locations, please see: https://www.imperva.com/products/global-network-map/

Managed WAF Service Offering

There are technical functions that are critical to delivering robust and effective security services. Elements key to our Managed WAF service performance are:

An intuitive user interface, and role-based access supporting strong authentication services.

Traffic to origin is universally inspected, and the security system does not pose a single point of failure thanks to HA, load balancing, and dynamic DNS routing.

DDoS mitigation protecting at layer 7. Mitigation that is highly scalable, quick attack detection and response. (*DDoS Protection beyond attacks greater than 1Gbps or 5k packets-per-second requires upgrading to App Protect Professional, App Protect Enterprise, or App Protect 360).

Attack Analytics and SIEM logs to assist with compliance reporting and attack response.

Support application architecture-specific requirements for flexible and granular custom rule configuration capability.

Protection from industry-standard vulnerabilities such as OWASP Top 10 and Automated Top 20.

API Security to help protect your application from new vectors of attacks and improper access to your sensitive applications.

24x7 security operations with global researchers and analysis capabilities to provide site-specific services and consider global activities on the dark web to proactively prepare before attacks happen.

Third-party support through API integration and data export to leading SIEM vendors (optional).

Managed WAF Control Center

Security data can be overwhelming and almost unusable if not presented in a simple, consumable format with actionable controls for fine-tuning. The Managed WAF Control Center presents an intuitive interface to look at vulnerability data from a high-level perspective, then drill down into specific date ranges and vulnerability types down to detailed security events. The Control Center allows users and administrators to view, create, and manipulate data through applications or reporting modules:

Dashboards and Aggregated Metrics

Web Application Firewall Attack Logs and Filters

Detailed Event Incidents

Correlated Web Application Request Logs

The Managed WAF portal enables you to configure traffic and alerts, block requests, and fine-tune your WAF to your application's needs.

Security best practices, regulations, audit requirements, and compliance that dictate user controls must be in place to safeguard the use and management of security applications. The Managed WAF portal user admin includes the following must-have functions:

1. Ability to implement two-factor authentications for strong access control
2. Ability to create role-based permissions then assign and group users
3. Separation of duties with view-only and administrative rights
4. User activity logging
5. Change management and rollbacks

Flexible Deployment Options

Our Managed WAF offers flexible types of deployment depending on your needs. Some of these deployment paths are:

1

Secured Deployment

Our Managed WAF isolates your web application and protects you from attacks, operating as a security shield between your Origin and your CDN. Your Origin server is firewalled to permit only our Managed WAF to communicate with the system, and your DNS is updated accordingly to your new protected location.

2

Secured Deployment + CDN

Our Managed WAF isolates the origin and protects from all attacks, operating as a security shield. We additionally configure the CDN function in your WAF, providing security, scalability, and performance. Adding the CDN capabilities will not only help accelerate your site's responsiveness; it will also help ensure the security of your information and data.

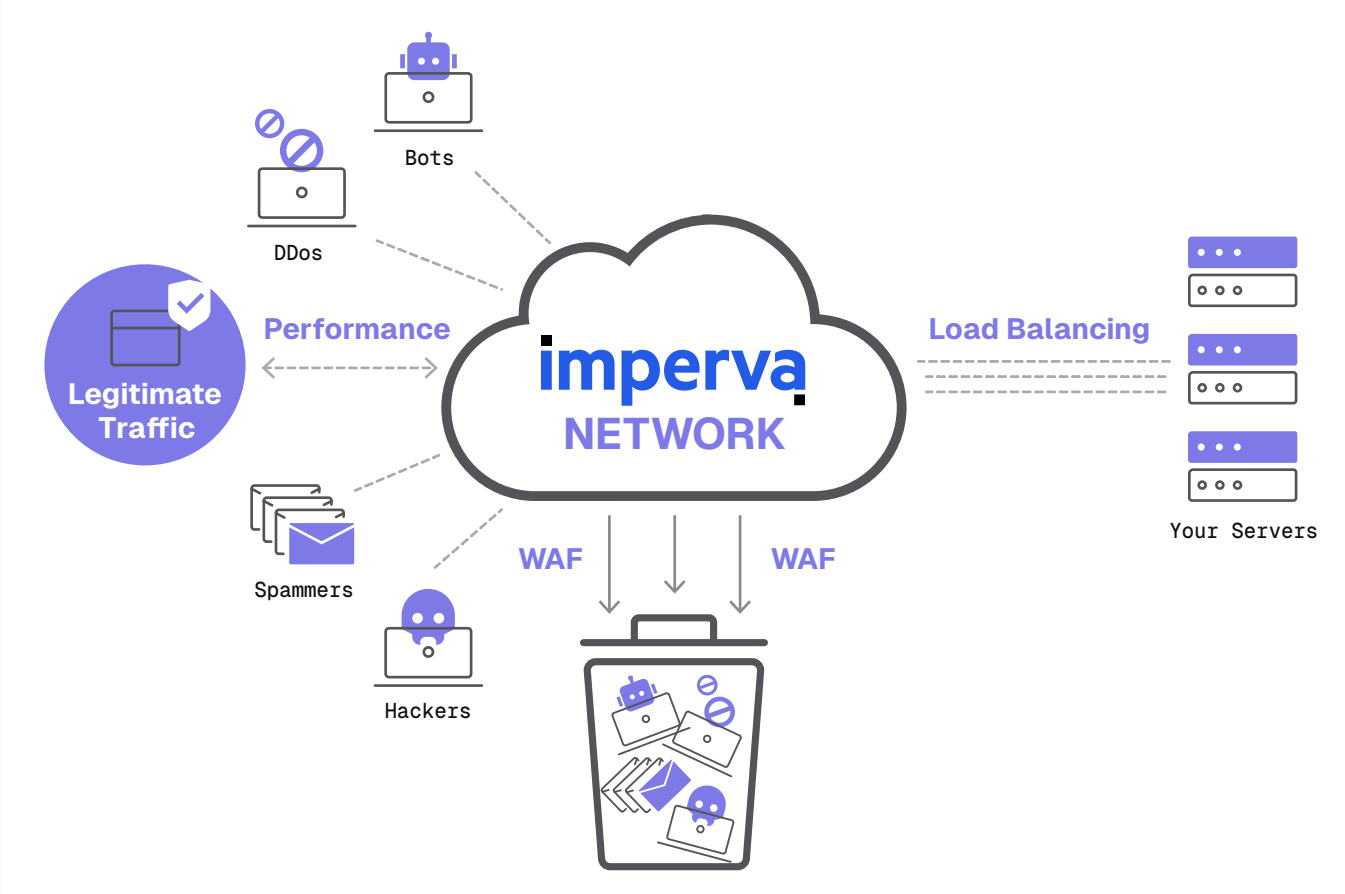
3

No Change to Your Infrastructure

Our Managed WAF is enabled through a simple DNS change, without the need for any change to your perimeter-based security or CDN provider. Once activated, our Managed WAF watches and filters all traffic to your web applications, automatically filtering out known vulnerabilities as well as the latest zero-day threats.

Managed WAF Traffic Flow

Imperva's Web Protection is a 100% cloud-based solution for protecting websites and applications from external threats including OWASP top 10 threats, hacking attempts, malicious bots, scraping, and DDoS attacks.



At the core of Imperva's Web Protection is their security reverse proxy and Web Application Firewall (WAF) in the cloud, which are deployed across their globally distributed CDN network. Organizations using Web Protection route their website traffic through the Imperva network by performing a simple DNS change. This enables Imperva to inspect each request sent to the website and filter out any kind of malicious activity.

Benefits

PCI certified Web Application Firewall

Backed by Imperva's security team for updating and tuning security rules

Easy and quick implementation - usually no rule tuning is required

Bot mitigation using Imperva's advanced client classification technology

Backdoor Protection to identify and quarantine backdoors planted on your website

Custom security logic using security rules

Granular access controls based on IPs, URLs, location, and client type

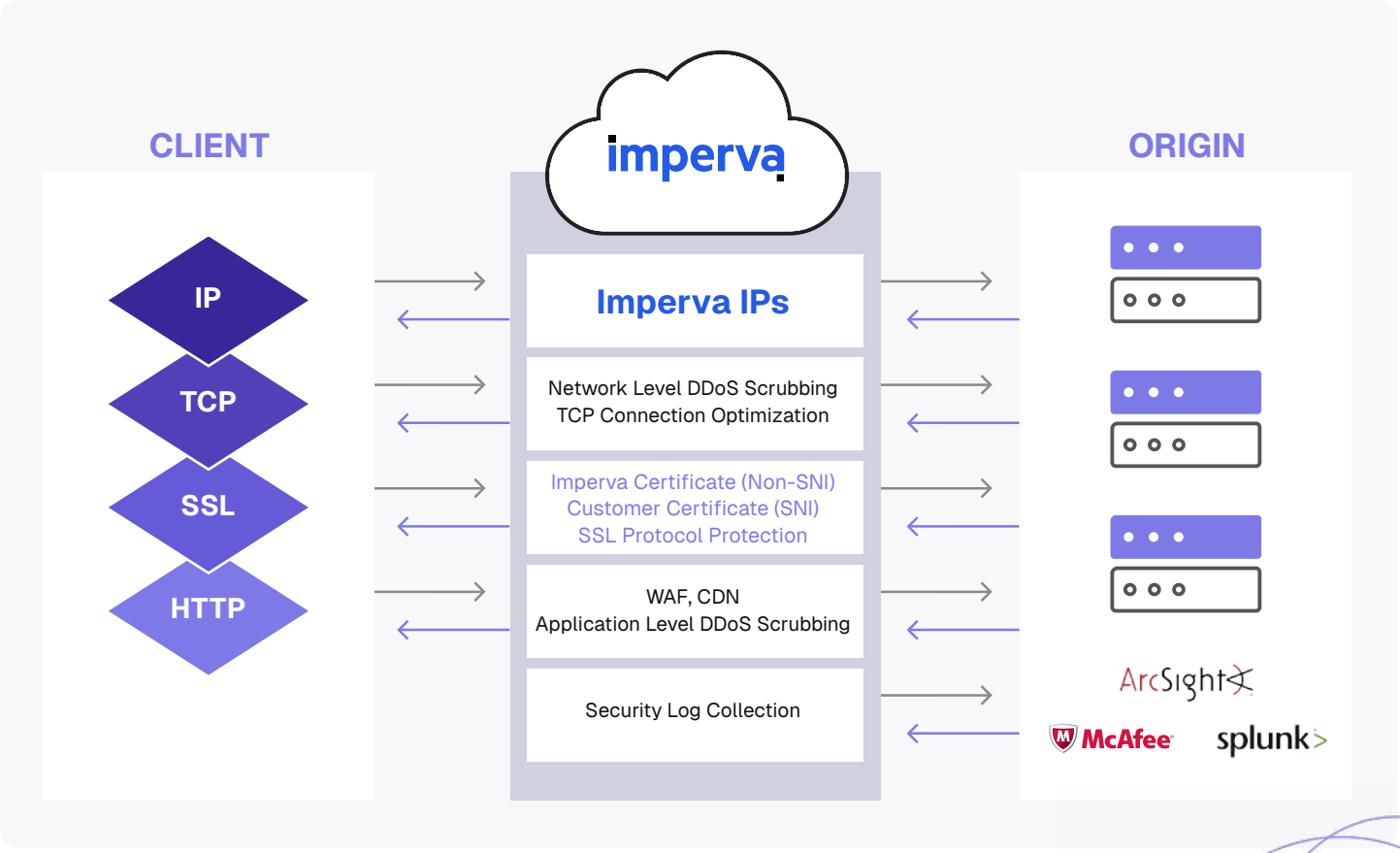
Seamless implementation of two-factor authentication

Real-time dashboard for traffic monitoring and event analysis REST

API and SIEM integration of access and security logs

How Does Web Protection Work?

Imperva's Web Protection is based on a network of secure reverse proxies deployed on their globally distributed CDN. Web traffic that is routed through the Imperva network is terminated by those proxies, allowing Imperva to inspect each request to the website and identify and block any malicious activity.



Organizations using Web Protection update their domain DNS to point to a unique hostname (CNAME) provided by Imperva (e.g. mysite.incapdns.net). This hostname is dynamically resolved for every website visitor, making sure each visitor is served by the closest Imperva data center.

Service Options

Four different levels of service are available for our Managed WAF depending upon your solutions needs:

App Protect Essentials

For businesses looking for essential application security protection in an easy to deploy platform.

App Protect Professional

For IT teams seeking sophisticated threat detection including advanced DDoS, account takeover, and formjacking.

App Protect Enterprise

For IT security teams looking to prevent business abuse by bots and client-side attacks.

App Protect 360

For security professionals requiring on-premises WAF and runtime protection from supply chain attacks using RASP.

Each level of WAF includes certain features and capabilities, and can have capabilities added for an additional fee as noted in the following features table.

	App Protect Essentials	App Protect Professional	App Protect Enterprise	App Protect 360	Definition
Web Application Firewall					
Cloud WAF	☑	☑	☑	☑	A cloud WAF that protects applications against all attacks wherever they're located
WAF Gateway (On-Premises & Customer-managed)			☑	☑	An appliance or virtual WAF that protects applications against all attacks wherever they're located
API Security					
API Schema Protection	☑	☑	☑	☑	Protects websites and APIs with an intuitive single-stack approach
BOT Protection					
Client Classification	☑	☑	☑	☑	A multilayered system to block simple bots
Rate Limiting	☑	☑	☑	☑	Prevents automated bots from rapidly traversing through the website by applying rate limits
CAPTCHA Insert	☑	☑	☑	☑	Inserts CAPTCHA tests into the workflow to mitigate automated bot traffic
Multi-factor Authentication	ADD-ON	ADD-ON	☑	☑	Inserts multi-factor authentication into the workflow to mitigate automated bot traffic
Advanced Bot Protection - Account Takeover Detection		☑	☑	☑	Detects credential stuffing and cracking advanced bots from performing account takeover attacks
Advanced Bot Protection		ADD-ON	☑	☑	Protects websites, mobile applications, and APIs from automated threats (bad bots) without affecting traffic

	App Protect Essentials	App Protect Professional	App Protect Enterprise	App Protect 360	Definition
Client-Side Protection					
Client-Side Protection – Detection	ADD-ON	☑	☑	☑	Detects JavaScript services used in client-side attacks
Client-Side Protection - Mitigation	ADD-ON	ADD-ON	☑	☑	Prevents JavaScript services from being used for data theft from client-side attacks (formjacking, digital skimming, and Magecart)
Runtime Protection					
Runtime Application Self-Protection				☑	Detects and blocks attacks from inside the application
Reporting & Analytics					
SIEM Integration	☑	☑	☑	☑	Turnkey integrations with leading SIEM solutions
Attack Analytics	☑	☑	☑	☑	A service that uses machine learning to distill thousands of events into a single, actionable attack narrative
Reputation Intelligence Feed	☑	☑	☑	☑	A security reputation feed that combines research from Imperva security researchers
Data Retention	30 DAYS	90 DAYS	90 DAYS	90 DAYS	The number of days the data will be available on the Imperva System
DDoS Protection					
Basic Website Protection	☑	☑	☑	☑	An always-on DDOS mitigation service that manages any type, size, or duration of attack with near-zero latency
Standard Website Protection	ADD-ON	☑	☑	☑	An always-on DDOS mitigation service that manages any type, size, or duration of attack with near-zero latency in under 3 sec (backed by SLA)
Individual IP Protection	ADD-ON	ADD-ON	ADD-ON	ADD-ON	An on-demand or always-on mitigation service that protects individual IP addresses against DDOS attacks
DNS Protection					
Managed DNS Protection	☑	☑	☑	☑	An Imperva hosted and secured DNS service providing optimal DNS availability and response time
DNS Zones Protection	☑	☑	☑	☑	An always-on cloud mitigation service that protects DNS servers and provides optimal DNS performance and caching capabilities
Content Delivery Network (CDN)					
Dynamic Content Acceleration	☑	☑	☑	☑	Network acceleration boosts response times to the origin
Frontend Compression and Minification	☑	☑	☑	☑	Reduces file size and trims code to its essentials for faster delivery
Session Optimization	☑	☑	☑	☑	Uses techniques like TCP connection pools and session reuse for faster content delivery
Smart Caching	☑	☑	☑	☑	Intelligent profiling of content that determines cache frequency to optimize content for faster delivery
Edge Cache Rules	☑	☑	☑	☑	Provides caching control with high granularity via programmable edge rules
Origin Cache Shield	☑	☑	☑	☑	Provides the Imperva CDN with an intermediate cache layer to optimize infrastructure capacity

	App Protect Essentials	App Protect Professional	App Protect Enterprise	App Protect 360	Definition
Application Delivery					
Edge Delivery Rules	☑	☑	☑	☑	Edge programmability for granular control of security, processing, and delivery of the content
Edge Load Balancing	ADD-ON	ADD-ON	ADD-ON	☑	A cloud-based load balancer that supports local and global server load balancing across on-premises and public
Services					
Advanced Reporting	☑	☑	☑	☑	Suite of reports that highlights strengths, weaknesses, risk levels, and improvement opportunities within your implementation
Proactive Monitoring	ADD-ON	☑	☑	☑	Proactive notifications by Imperva with insights into protected assets and recommended actions using statistical analysis
Enterprise Services	ADD-ON	ADD-ON	ADD-ON	ADD-ON	Staff augmentation by a team of Imperva security experts who provide ongoing consultation and operational assistance

Roles and Responsibilities

The following table illustrates some of the responsibilities of Aptum and our customers regarding Aptum's Managed WAF solution.

Activity	Customer	Aptum
Managed WAF Solution Installation		
Install and configure Managed WAF Solution	☑	☑
Configuration Management		
Create company records and site		☑
Enable caching and WAF protection		☑
Install SSL certificate(s)		☑
Assign a record IP and CNAME	☑	☑
DNS switch and global test	☑	☑
Event Monitoring		
Cache and WAF tuning	☑	
Notify Aptum's customers of DDoS attacks or WAF threats		☑
Provide email addresses for notifications	☑	☑
Maintenance Management		
Schedule patch/software updates through change a management procedure		☑
Implement patch updates		☑
Access Management		
Maintain administrative access to Managed WAF solution		☑
Incident Management		
Troubleshoot and diagnose incidents		☑
Change Notification		
Notify Aptum of any pending or anticipated changes to their internet hosts, applications, CDN, DNS, services, or planned events that have the potential to impact their established baseline traffic profile	☑	

Possible Overage Fees

Throughput Overage

It is possible to incur overages for bandwidth subscribed to on your Managed WAF Solution. Imperva measures the amount of utilization for the subscribed service level (i.e. 20Mbps, 50Mbps, 100Mbps, etc.). If your utilization as measured at the 95th Percentile for the month is more than the subscribed level, you could be charged for that overage in 10Mbit increments the following month. The rate per 10Mbit increment is as follows:

	USD	CAD	GBP
10 Mbits Overage	**$ 500**	**$ 679**	**£ 399**

You can configure alerts within the Imperva portal for potential overages. The system provides the capability to configure a warning if your utilization exceeds the subscribed level. To avoid overage fees, you can subscribe to a higher-tier service when needed. You cannot lower your tier of service until the expiration of your contract. Please contact your account management team if you wish to discuss this further.

SLA, SLO, and Service Credits

The following service level agreement ("SLA") applies only to the provision of Managed WAF. If Aptum does not achieve any applicable service levels set forth in this SLA, then the Customer may be eligible to receive a Service Credit(s) as specified in this SLA.

DEFINITIONS

A. Network Infrastructure ("NI") shall mean the group of Imperva controlled systems (servers, hardware, and associated software) that are used by Imperva in delivering the Services.

B. Network Infrastructure Outage ("NI Outage") shall mean any contiguous period when the Imperva NI does not direct traffic to the Customer network.

C. Peripheral Infrastructure ("PI") shall mean the Imperva Management Console and APIs of the Services.

D. Peripheral Infrastructure Outage ("PI Outage") shall mean any contiguous period when the Imperva PI is unavailable, outside of a Scheduled Maintenance window.

E. "Outage" shall mean a NI Outage or PI Outage, as applicable.

F. "Scheduled Maintenance" shall mean maintenance performed by Imperva on the PI (a) in which the Customer is provided electronic notice at least 48 hours in advance (notice of Scheduled Maintenance shall be provided to Customer Contacts by email), and (b) which is a recurring weekly maintenance window pertaining to the PI every Sunday between 12:00 AM EST and 7:00 AM EST. During this maintenance window, the PI may be intermittently unavailable.

G. "Credit(s)" shall mean the entitlements available to the Customer under this SLA, as calculated by the Managed WAF Service Levels below.

H. "DDoS Event" shall mean a Surge (as defined below) continuing for five (5) consecutive minutes or more, of which at least 30%, measured in Mbps, is considered malicious by Imperva, in its sole discretion. A DDoS Event shall be deemed to have ended when for at least three (3) consecutive hours, 10% or less of traffic to the Customer website, measured in Mbps, is considered malicious by Imperva, in its sole discretion.

I. "Surge" shall mean peak traffic to the Customer's website and/or network calculated by the 95th percentile of bandwidth usage for clean traffic.

UPTIME COMMITMENT

Except as otherwise defined in this SLA, Aptum commits to a NI annual uptime of 99.999%. and a PI annual uptime of 99.95%. In the event of a NI Outage longer than five (5) minutes or a PI Outage longer than four (4) hours, the Customer will be eligible to receive Credits as described below. Aptum makes no uptime commitment, and the Customer is not eligible to receive Credits for beta, evaluation, or other trial services.

DDOS MITIGATION

Managed WAF is designed to mitigate Layer 7 DDoS Attacks against your protected website(s) using industry-leading technology quickly and providing an always-on DDoS Protection service.

The included protection for App Protect Essentials is up to a 1Gbps attack and/or 5,000 packets per second of attack. Additional protection can be added to App Protect Essentials for an additional monthly fee. Managed WAF App Protect Essentials does not have an SLA against DDoS Attacks unless an additional Website DDoS Protection service is subscribed to by our customer.

App Protect Professional, App Protect Enterprise, and App Protect 360 include unlimited DDoS attack protection levels.

The SLA for mitigation of a DDoS attack is within three seconds of detection for App Protect Professional, App Protect Enterprise, and App Protect 360, and for App Protect Essentials when subscribed to the optional Website DDoS Protection for App Protect Essentials Service. If the detected attack is not mitigated within three seconds of detection, then the following SLA applies, as described below.

MANAGED WAF SERVICE LEVELS

SERVICE	SERVICE LEVEL	SERVICE CREDIT
Managed WAF – Includes DDoS Protection for App Protect Professional, App Protect Enterprise, and App Protect 360 Managed WAF – Add-on: Website DDoS	Mitigation of automatically detected DDoS attacks within three seconds	Five percent (5%) of the Net monthly recurring Fees for the Managed WAF Services for each hour (or fraction thereof) of Downtime. The maximum Credit issuance to the Customer shall not exceed one hundred percent (100%) of the Net monthly recurring Fees for the affected Managed WAF for the then-current monthly billing period.
App Protect Essentials, App Protect Professional, App Protect Enterprise, and App Protect 360	Managed WAF NI annual uptime of 99.999% and a PI annual uptime of 99.95%	

EXCEPTIONS

NI and PI downtime due to the following events shall not be considered a NI Outage or a PI Outage:

- Cases in which the Customer was not routing traffic to the Imperva network, or no Customer traffic was affected by the Outage.
- Use of the Services in a manner inconsistent with the terms of the Agreement, including Aptum's AUP.
- Problems with the Customer's or a third party's hardware or software, or problems caused by third parties who gain access to the Service by means of the Customer's accounts or equipment.
- Problems with the Customer's registrar or DNS provider.
- Network unavailability outside of the NI.
- Any Force Majeure Event.

SUBMISSION OF CLAIMS

To submit a claim for a Credit, the Customer must open a support request ticket in Aptum's support ticketing system no more than five (5) calendar days after the outage event and must include details describing the outage, network traceroutes, the site(s) affected, and any attempts made to resolve the outage.

REVIEW OF CLAIMS

Aptum will use the information included with the ticket by the Customer to reasonably validate the Customer's claims in order to make a good faith judgment on whether there was an outage, and if the issuance of Credit(s) is warranted.

EXCLUSIVE REMEDY AND LIMITATIONS

The issuance of Credits to the Customer as set forth in this SLA shall be the Customer's sole and exclusive remedy for Services not achieving the performance levels specified in this SLA. Credits shall only be applied against payable Fees associated with the Service that gave rise to this issuance of such Credits. The Customer's entitlement to Credits shall be forfeited if the Customer is not current on the payment of Fees for the Services at the time that such Credits would have been issued. Upon termination of the Services, any unused Credits remaining in the Customer's account shall automatically expire.

SERVICE LEVEL OBJECTIVE (SLO)

For issues the Customer raises via Aptum's support ticketing system, our support team will review your request and assign a priority for the issue based on the type of impact on the Services. Issues regarding Managed WAF that are escalated to our support team will be assigned a response time SLO as follows:

PRIORITY	PRIORITY DEFINITION	RESPONSE TIME SLO
Urgent – P1 Progressed 24 x 7	The most severe type of problem. It can be described as a showstopper, a critical failure in an operational activity where no workaround is available.	30 Minutes
Medium – P2 Progressed 24 x 7	The problem limits the functionality or usefulness of the application, but the condition is not critical to the continued operation of the Service. A workaround is readily available and can be applied or used with little or no operational impact.	2 Hours
Low – P3 Progressed 24 x 7	The least severe type of problem. It can be described as a problem causing minimal or no business impact or arising from an unsatisfactory component or configuration. The problem can be circumvented with no operational impact and there are no data integrity issues. Deferred maintenance of the "low" problem is acceptable.	8 Hours

SLO response times are performance targets only and do not have associated remedies. However, incidents can be escalated by calling our service desk at any time. For further information on Aptum's SLA and the definitions of capitalized words, please visit Aptum's website: https://aptum.com/legal/