haltdos

DATASHEET

# Managed Security-as-a-Service

## Overview

With the increasing use of web applications for everything from online banking to e-commerce, personal and sensitive data is being transmitted and stored online at an unprecedented scale. As a result, the need for security in web applications cannot be overstated. Securing web application is an ever-evolving challenge, as cyber-criminals constantly develop new and sophisticated methods to attack web applications.

Organizations need a proactive and ongoing effort to identify and mitigate vulnerabilities, and stay up-to-date with the latest threats and security measures. Without the right protection, they can become an attack vector that may ultimately lead to a data breach.

Haltdos Managed Security-as-a-Service empowers organizations to protect their infrastructure and applications through state-of-the-art AI powered product backed by automation, global threat-intel, and artificial intelligence. The solution offers comprehensive protection and fine-grained control, making it the ideal solution to secure network and applications, enforce compliance, and provide iron-clad protection against a wide variety of attacks.

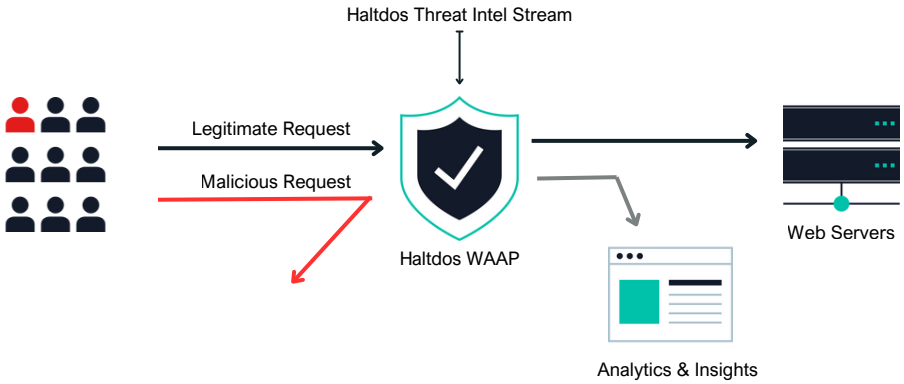
**Prevent Data Breach**

**Non-Stop Protection**

**AppSec Made Easy**

### KEY CAPABILITIES:

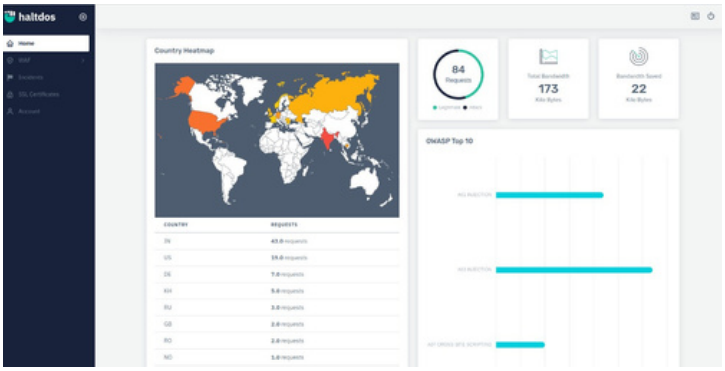
- Pre-built security templates
- Best in class, fully PCI compliant
- Deploy in blocking mode with near zero false positives
- Backed by research-driven intelligence on current threats
- Easy to configure with user defined rules
- Automatic learning user and application behaviour
- Delivers actionable insights into Attack analytics
- Correlation engine that detects sophisticated, multi-stage attacks
- Dedicated infrastructure over multiple cloud service providers
- 24/7 Security Operations and Support Team




## BEYOND OWASP TOP 10 PROTECTION

Haltdos WAAP solution protects against OWASP Top 10 security threats like cross-site scripting, SQL Injection, remote file inclusion, and illegal resource access, blocking attacks in real time. The solution uses different mitigation techniques that different attacks require - whether it's a DDoS attack, or a bot utilizing a SQL injection to attack your API. Moreover, the team at Haltdos Labs actively discovers emerging threats to provide up-to-date security protection you need in today's fast-changing attack landscape. Security experts monitor external sources like new vulnerability disclosures, and help you reduce the risk of third-party code. New security signatures that defend against recently discovered threats are added daily.

### Dynamic Profiling & API Discovery



Fueling the digital transformation, APIs have become increasingly popular, providing the backbone for mobile applications, automated business to business operations, and ease of management across applications. However, with their popularity, they also increase the attack surface with additional exposed application surfaces that organizations must secure. Haltdos WAAP provides the right tools to address threats to APIs. Our Dynamic Profiling Technology automatically discovers APIs by continuously evaluating application traffic. Discovery plays an integral role in building a baseline or "whitelist" of acceptable user behaviour, and for establishing a positive security model. Positive security model approach is benefited by automatic incorporation of valid changes on the application profile over time. This eliminates the need to manually configure and update countless application URLs, parameters, cookies, and methods in your security rules.

### Bot Management

Haltdos WAAP solution protects against automated bots, webs scrapers, crawlers, data harvesting, credential stuffing, and other automated attacks, to protect your web assets, mobile APIs, applications, users, and sensitive data. Combining machine learning with bot deception and client fingerprinting, Haltdos WAAP is able to block malicious bot attacks while reducing friction on legitimate users. With advanced tracking techniques, Haltdos WAAP can differentiate between humans, automated requests, and repeat offenders, track behavior over time to better identify humans from bots and enforce CAPTCHA challenges when required.

### Network Optimization & DDoS Protection

Haltdos WAAP solution is an effective tool for protecting web applications from DDoS attacks by monitoring traffic, rate limiting and throttling traffic, blocking traffic from malicious sources, caching content, and automatically filtering out malicious traffic. Capable of mitigating attacks in real-time (less than 30 seconds), the solution also offers TCP and HTTP optimizations such as content compression, congestion control, TCP multiplexing techniques, and built-in load balancing. Haltdos Cloud WAAP solution can help improve performance, reliability and availability of Web Applications & APIs.

## NEXT-GEN APPLICATION PROTECTION

### Correlation Technology

Haltdos Correlation technology addresses complex attacks that are ambiguous in nature. Correlation engine examines multiple pieces of information at the network, protocol, and application levels across multiple requests and users sessions to distinguish between attacks and legitimate traffic. By basing decisions on multiple observations, rather than a single incident, Haltdos WAAP solution delivers a highly accurate and completely automated application protection, achieving high degree of accuracy with zero false negatives and reduced false positives in the process.

### Deception Technology

Taking deception to the attackers, Haltdos WAAP solution is an Industry First solution capable of creating decoys targeting attackers and bots. By embedding invisible decoys as fake links and forms inside web pages of the application, Haltdos WAAP can accurately detect malicious bots, and web scrapers during reconnaissance phase, and take pro-active measures to block them even before they launch any attack. The technology makes it possible for WAAP to make Java based application appear as a PHP based application - making it harder for bots and attackers to launch successful attack campaigns.

### Mobile App Security

Current security and anti-fraud measures do not adequately address the needs of the mobile app world. Sensitive data that is being shared through APIs are still subject to exploits such as app impersonation, reverse engineering of API protocols, spoofing transactions, and using bots and emulators to access backend API servers. Haltdos Secure Mobile App Protection creates a trusted environment that protects your APIs and your business by providing additional authentication- authenticating app instances, not users. By ensuring that the mobile app connecting through an API is a genuine untampered instance, fraudulent transactions, malicious scripts, and bot attacks are blocked at the source.

### Data Leak Prevention

Web Data Leak Prevention policies in Haltdos WAAP solution detects and prevents sensitive data and personal identifiable information (PII) from leaving the application. These policies can include regular expressions, predefined patterns (such as credit card numbers or Social Security numbers), or custom patterns specific to the application's data types. By enforcing encryption for data in transit, and masking or redacting certain portions of data to limit exposure (such as hiding credit card numbers except for the last four digits), Haltdos WAAP can enforce Privacy and sensitive data breaches.

### AI / ML Anomaly Engine

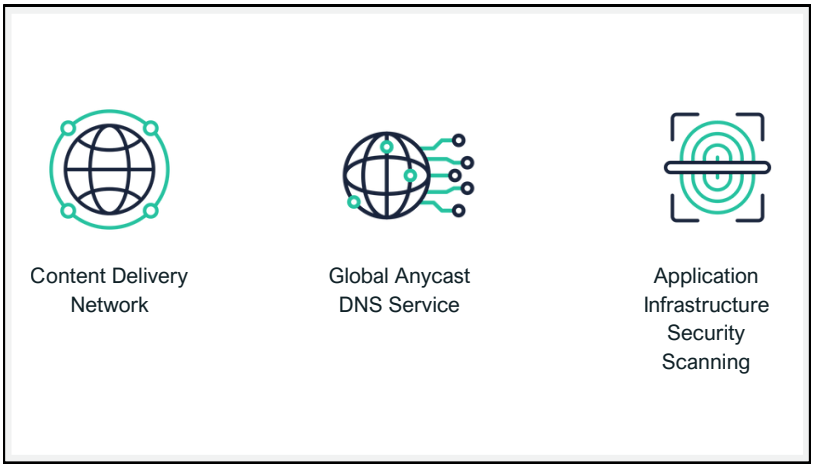
With a state of the art anomaly detection engine, Haltdos WAAP accurately identifies misbehaviors, misuse, and unauthorized access to critical resources. The solution establishes a baseline of normal behavior by analyzing historical data and user behavior patterns to establish normal patterns. This baseline is continuously updated and adapted based on the evolving traffic patterns and user behavior. The solution also supports custom user-defined behaviour policies for protected web assets and resources.

### API Gateway

Haltdos WAAP can act as a full fledged API Gateway that acts as an entry point for client applications to access and interact with a collection of microservices or backend APIs. It provides a centralized point of control, security, and management for API calls, enabling efficient and secure communication between clients and backend services. The solution provides authentication, routing and composition, request and response transformation, API discovery and payload verification.

## EXTEND YOUR CLOUD SECURITY POSTURE

Haltdos Cloud Services comes with built-in DDoS mitigation from network to application layer attacks. The service provides the following add-ons to improve security, reliability and performance of your infrastructure.



# Globally Distributed DNS Service

## Fast, Secure & Fully Managed

An authoritative DNS solution is essential for managing and securing domain name resolution, ensuring high availability and optimal performance for global applications. It efficiently handles large volumes of DNS queries while providing robust protection against threats such as DDoS attacks and cache poisoning. The solution leverages scalable architecture and advanced security features to guarantee rapid and reliable DNS responses. By optimizing the delivery of applications across diverse environments, it maintains performance and reliability. Additionally, the solution includes comprehensive monitoring and management tools to ensure continuous application health and performance.

### Global Network

Global Network of 180+ PoPs powered by Anycast routing for reduced response time

### Fully Managed

Fully managed DNS infrastructure backed offered as SaaS service with easy to use Graphical User Interface

### DDoS Protection

Fully automated, advanced traffic monitoring and filtering to reliably protect against any DDoS attacks

### Low TTL

DNS service that supports low TTL values to boost change propagation across the world

### Failover Management

Make your DNS record dynamic with automatic DNS update based on periodic health monitoring of your endpoints

### Geo DNS

Global Traffic Director that responds to DNS queries based on user location to redirect user to the nearest servers

### IPv4 & IPv6

Fully operational and support for modern networks via IPv4 and IPv6 protocols.

### Instantly Updated

All DNS record changes are applied instantly to all our authoritative DNS servers across the globe

# Content Delivery Service

## Fast, Secure & Fully Managed

Haltdos offers a premier Content Delivery Network (CDN) service engineered to enhance performance, security, and reliability for your digital content. Our cutting-edge CDN infrastructure is designed to provide seamless and secure content delivery worldwide, ensuring optimal user experiences and robust protection for your online assets.

### Enhanced User Experience

Experience faster load times, reduced latency, improved responsiveness, and seamless streaming for a superior browsing experience.

### Increased Security

Benefit from advanced DDoS protection, SSL/TLS encryption, a web application firewall, and bot management to keep your data secure.

### Cost Efficiency

Optimize bandwidth, save on infrastructure, reduce latency costs, and enjoy flexible pay-as-you-go pricing for cost-effective operations.

### Global Coverage

Ensure consistent performance worldwide with localized content delivery, global reach, and multilingual support for users everywhere.

### Scalability and Flexibility

Easily scale resources, customize configurations, and handle traffic spikes effortlessly for flexible and scalable solutions

### Advanced Analytics and Insights

Gain real-time monitoring, detailed reporting, and actionable insights to make data-driven improvements

### Simplified Integration and Management

Utilize a user-friendly dashboard, comprehensive API access, and seamless deployment for easy integration and management.

### Reliability and Continuity

Enjoy high availability, disaster recovery, and guaranteed performance with service level agreements for reliable and continuous service

# Solution Features

## TECHNOLOGY & CERTIFICATIONS

| | |
|---|---|
| Platform & Technology | Haltdos Platform with Signature from Threat Intelligence & Machine Learning |
| License | Fully Managed Services, Unlimited applications per zone. Zone and Bandwidth capping based on configured license |
| Support | 24x7 via Online, Email , Telephone and Dedicated Account Manager |
| Certifications | EAL 2+, ISO 9001, ISO 27001, ISO 45001, ISO 14001, IPv6 Ready Gold certifications |
| TAC Support | TAC support in India |

## OPERATION MODE

| | |
|---|---|
| Network Operations | Reverse Proxy |
| Protocols | HTTP 0.9/1.0/1.1/2.0/3.0 (QUIC) with translation, Web Socket, TCP |
| IP Stack | Dual IPv4 & IPv6 stack |
| Mitigation Modes | Bypass, Record (Report Only), Learning, Mitigation (Block and Report) |
| Block Actions | Drop Request, Terminate Connection or Session, Blacklist (temporary or permanent), Send Challenge (Captcha, JavaScript, Crypto), Rate Limiting, Tarpit or Custom Response |
| Brotli Compression | Compression for text-based content (HTML, CSS, JavaScript) for reduced payload sizes |

## INFRASTRUCTURE

| | |
|---|---|
| Infra | Global Multi-Cloud infrastructure with High Availability with over 30 Tbps of attack mitigation capacity |
| Elastic Scaling | Auto-scaling infrastructure to handle varying loads without manual intervention |

## MANAGEMENT FEATURES

| | |
|---|---|
| Graphical User Interface (GUI) | Secure web interface over HTTPs with support for all modern browsers |
| Logging | Centralized logging of system, services, MIS, incidents |
| Dashboards | Real-Time & historical dashboards with custom duration. Support for custom dashboards |
| RBAC Administration | Configurable user profiles with role based access control with MFA |

| | |
|---|---|
| Backup | Automatic backup and data retention for 12 months |
| Reporting | Periodic daily, weekly or monthly reports (predefined or custom) in PDF or Excel |
| Policy Management | On the fly configuration updates on mitigation appliances |
| Certificate Management | SSL certificate management with support for Let's Encrypt certificate generation |
| Events / Alerts | Detailed event and alert reporting on attack, health, etc. |
| Network Forensic | Network forensic with packet capture and traceroute |
| Attack Forensic | Built-in utilities for investigating attackers, attack payloads and identifying false positives |
| Whois & Threat Intel Portal | Support for users to upload malware, IP, domain, email, etc. to get detailed threat intel report |
| Updates, Upgrade & Threat Intel | Update and upgrade management on version releases and patch updates. Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Threat Stream |

## INTEGRATION FEATURES

| | |
|---|---|
| API | Yes (XML or JSON) |
| Custom Threat Intel | Integration with 3rd party Threat Intelligence (TI) feeds |
| Notification Integration | Notification & Logging via SNMP, SMTP, SMS Gateway and 3rd party integration via API hooks |
| SIEM Integration | Support for integration with SIEM via Syslog services or APIs |
| Identity Management | Inbuilt with support for integration with AD / SAML / LDAP |
| Security Tools Integration | Support for integration with SAST/DAST/IAST tools |
| DevOps Integration | Supports integration with Kubernetes, Terraform, AWS Cloud Formation, Ansible etc |

## LOAD BALANCING

| | |
|---|---|
| SSL/TLS Management | Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate based authentication also supported, proxy SSL/TLS connections |
| Load Balancing | Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported |
| Advanced Load Balancing | Content based load balancing with upstream rules |
| Load Balancing Algorithms | Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, etc. |

| | |
|---|---|
| Network Optimization | Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts |
| HTTP Optimization | Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients |
| Virtual Contexts | Support for multiple virtual contexts along with resource allocation |
| Failover Management | Automatic failover & recovery. Support for marking servers up / down / backup |
| Health Check | Periodic server or server group health check and alerting via TCP, SSL, ICMP, HTTP, DNS or custom script |
| Client Visibility | Embedding Real IP information in X-* headers, client cert information, etc |
| Redirection Rules | REGEX based redirection rules to rewrite URLs |
| Variable Rules | Support for embedding and using variables for A/B testing or custom load balancing |
| Script Rules | Embedding user defined custom code for advanced routing |
| Content Transformation | Transformation rules for data manipulation and Header rules for add / edit or delete headers in request or response |
| End-User Fingerprinting & Monitoring | Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring |

## SECURITY

| | |
|---|---|
| DDoS Protection | Instant protection against volumetric as well as Low & Slow Layer 7 DDoS attacks |
| API Security | Built-in API gateway for authentication, rate limiting, transformation, and documentation. Automatic discovery of API endpoints, identifies endpoints, methods, authentication status, sensitive data, and structural threats, protection against BOLA, BFLA and OWASP vulnerabilities. |
| Layer 7 Security | OWASP Top 10 Web Application Security Risks, OWASP Top 20 Automated Threats and SANS 25 Software Errors, WASC 50 |
| Security Profiles | Multiple security profiles with support for different security status per application based on url, source, country, regex, etc. |
| Positive Security Model | Support for Form Rules for positive security model |
| Negative Security Model | Support for user defined Firewall Rules for REGEX based negative security model |
| Virtual Patching | Support for virtual patching through built-in web security scanner or upload of 3rd party SAST / DAST / IAST scan results |

| | |
|---|---|
| Built-in Signatures | Over 4000+ built-in signatures on various technologies, platforms and frameworks with pre-defined templates. |
| 0-day Protection | Automatic learning and profiling application structure. Threat scoring and baseline creation for AI driven 0-day attack protection |
| Malicious Source Protection | Protection against TOR IP, Bad Reputation IP, dark IP, known Bots, proxies, spammers provided by Haltdos or user defined threat intel |
| Error Handling | Error rules for custom error handling |
| Bot Management | Anti-bot protection with AI classification and scoring of bots based on advanced browser fingerprinting |
| Anti-Automation Protection | Protection against known and 0-day bots, account takeover attempts, brute force attempts, scraping, reconnaissance, cloaking, etc |
| Mobile App Protection | Anti-Bot mobile SDK for Android & iOS for protecting mobile apps and communication between apps and web APIs |
| AV Scanning | Built-in AV scanner for malicious file upload. Support for ICAP integration for 3rd party scanners |
| Minimize False Positives | Support for REGEX based whitelist rules and signature staging and deploy policies to minimize signature based false positives |
| HTTP Validations | Protocol validations, request normalization (encoding & evasion techniques) before inspection, managing security headers and cookies etc. |
| Policy Inspection | Policy validation such as HTTP methods, file extension, request size, etc |
| Blacklist / Whitelist | Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, url, country, etc |
| Captcha Challenge | Support for JS or captcha challenge on suspicious user activity or known bots or malicious IPs |
| Rate Limiting | Rate Limit rules for implementing request, bandwidth or connection limits per source, IP prefix or user defined policy |
| API & WebSocket Protection | Built-in XML firewall, validation of XML / JSON / Ajax requests and WebSocket requests, GraphQL |
| Security Breach Prevention | Built-in support for data leak prevention, response filtering for sensitive personal identifiable information |
| Tamper Proofing | Tamper rules for URL/parameter tamper protection, website defacement, hidden form field protection, cookie signing and encryption, etc. |
| Correlation Engine | Advanced correlation engine with support for custom correlation rules for detecting attack across user requests and sessions |
| Automated Security Scanning | Add-on for automated security scanning for web infrastructure |
| Compliance | PCI-DSS 2.0 section 6.6, HIPAA, SOC2, GDPR enforcement |

| | |
|---|---|
| Deception Technology | Implement decoys in web application to protect against advanced bots, profile attacks and trap attackers |
| Sensitive Data Masking | Support for Log Rules for masking sensitive information such as passwords in logs and events |
| Enforced Browsing | Protection against forceful browsing, access to predictable resources, unauthorized navigation with additional security enforcement with Two factor authentication (2FA) |
| Misc. Protection | Support for protection against buffer overflow attacks, man-in-the-middle attacks, blocking malware payload, skimming, buffer overflow, SQL, SSI, LDAP injection, form jacking, etc |

## Global DNS Service

| | |
|---|---|
| Network | Global network with IP Anycast over 180+ PoP locations with IPv4 and IPv6 enabled |
| Network Security | Automated, Advanced DDoS Protection |
| DNS Security | Support for DNSSEC and protection against DNS poisoning |
| Failover Management | Support for Dynamic DNS Records with DNS health check. Also supports weighted DNS records |
| Traffic Director | Global Traffic director and load balancing with Geo DNS capability |
| DNS Propagation | Instant DNS propagation across entire network within seconds |
| TTL | Support for low TTL values upto 30s |
| Management | Easy to manage Centralized Management Console with RESTFul APIs for automation |

## Content Delivery Solution

| | |
|---|---|
| Network | Over 200 edge servers in major metropolitan areas and data centers worldwide |
| Optimized Routing | Anycast Routing for directing requests to the nearest edge server based on real-time network conditions. Algorithms that adapt to current network conditions, server health, and user location for optimal performance |
| Cache Types | Supports caching of static assets (images, videos, HTML, CSS) and dynamic content (API responses) |
| Caching Policies | TTL settings, cache purging, conditional caching based on headers and query strings |
| Edge Caching | Multi-level caching strategy, including edge-to-origin cache for frequently accessed content |

| | |
|---|---|
| Compression | Compression for text-based content (HTML, CSS, JavaScript) for reduced payload sizes |
| DDoS Protection | Multi-layered approach including rate limiting, IP blacklisting, and traffic analysis |
| Customizable Rules Engine | Custom traffic routing rules, geo-blocking, URL rewriting, and access control based on client attributes |
| Burst Handling | Instant scaling capabilities to manage unexpected traffic spikes |
| Real-Time Analytics | Live metrics on visitor behavior, traffic sources, and content performance |
| Performance Metrics | Detailed reporting on cache effectiveness, response times, error rates, and bandwidth usage |

## DNS Firewall Solution

| | |
|---|---|
| Network | Over 200 edge servers in major metropolitan areas and data centers worldwide |
| Global Load Balancing | Routing traffic across multiple data centres based on health checks |
| Load Balancing Algorithms | Support for Least connection, Proximity, Round Robin, Weighted RR, Persistent Hash, Geo, etc. |
| Operation Mode | Option for Authoritative or Recursive operational modes with support for various DNS record types such as A, AAAA, MX, TXT, PTR, etc. |
| Routing Rules | Custom rules for Static and Policy based routing |
| Network Mode | Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC |
| DNS Firewall | Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy, App Risk scoring and categorization |
| Rate Limiting | Controls and limits DNS query rates to prevent abuse and potential DDoS scenarios |
| Blacklist / Whitelist | Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc |
| Custom Signatures | Support for user defined custom rules with support for pattern, suffix, domain, etc. |
| Malicious Domain Blocking | Blocking malware domains, DGA domains, newly registered domains, homographic domains, cryptojacking, DDNS and category based domains (Adult, Social, etc.), Drive-by-Download, etc. |
| Multiple Security Profile | Support for multiple profile for selective security policy per network / IP address / user with detailed analytics |
| Web Filtering | Blocks or allows website access based on categories, redirecting restricted users to a customizable page for enhanced security and user experience. |