haltdos

Application Security + Delivery Platform

TECHNICAL SPECIFICATIONS

Web Application Security

SaaS or Virtual Appliance

Defend your applications against Web Attacks

Solution at a glance:

Multi-Layered Solution: Haltdos' AI-enhanced approach combines user behavior analysis, correlation, deception and reputation techniques to provide complete security for web-based applications from simple to 0-day attacks

Accurate Machine Learning: Haltdos' machine learning detection engine intelligently scores every request and bots to accurately detect threats with nearly zero false positive rate.

Built in Rules: Along with over thousands of built-in signatures, we operate 24x7 R&D operations looking out for new vectors of attacks and publish new signatures to mitigate them.

For any Application: With built-in templates for common CMS to custom designed applications, Haltdos protects any kind of web application with built-in support for websockets, HTTP 2.0, dual stack IPv4/IPv6, etc.

Advanced DDoS Protection: From volumetric to low & slow application DDoS protection with automatic trigger and remediation for 24x7 online presence.

Built-in API Gateway: With built-in load balancing, authentication and authorization capabilities API based XML / RESTFul / RPC web applications.

Managed Services

- 24 x 7 x 365 Telephonic Support
- 24 x 7 x 365 Email & Helpdesk
- Infra Monitoring & Attack Mitigation Support
- Policy Management & Fine-tuning Support

TALK WITH HALTDOS

Web www.haltdos.com
Call 1800-120-2394
Reach info@haltdos.com

Amidst fierce competition, your business cannot afford to slow down. With Haltdos, you don't have to sacrifice productivity and performance to get leading edges ecurity.

Haltdos provides multi-layer, multi-vector protection to ensure your website & web applications stays online, secure and always accessible to your customers.

Get peace of mind for your online business with Haltdos real-time, all the time network & application protection solution.

App Security : Feature Highlights

Constant Protection from Evolving Threats

Haltdos provides superior protection against data loss, DDoS, and all known application-layer attack modalities. Automatic updates provide defense against new threats as they appear and machine learning technology provides real-time zero-day attack protection.

Identity and Access Management

Haltdos has strong authentication and access control capabilities that ensure security and privacy by restricting access to sensitive applications or data to authorized users.

Built-in Load Balancer

Haltdos offers built-in load balancer for managing multiple application servers, periodic health checks and latency measurements from multiple global locations.

Self-Learning

Haltdos's security is adaptive through automated learning and can make policy recommendations by learning about application behavior, which can make it easier for security teams to manage policies. Administrators retain full control over the activation and deactivation of each ruleset, with the opportunity to screen for false positive before committing to production.

Content Protection

Haltdos Application Security monitors content in responses from web servers to detect defacement, sensitive data leaks such as credit card, PII information and application technology such as web server details, exceptions, etc.

Multi-Cloud Infrastructure

Haltdos Edge Security services leverages multiple Cloud Service Providers (CSPs) to provide redundant, reliable and consistent performance no matter where your web application resides.

Deception Technology

Haltdos Application Security combines industry first Deception Technology that accurately detects and identifies malicious bots, tracks their activity through dynamically generated decoys in web based applications.

Developer Scripts

Haltdos Application Security is the only WAF technology that allows users to write custom code that gets evaluated against incoming request or response for advanced mitigations that go beyond traditional regular expression based mitigations

Performance Monitoring

Haltdos Application Security provides comprehensive monitoring of web applications - checking latency, availability, performance and RUM metrics for every web page. This allows fine grained monitoring, failover and alerting for web applications

Anti-Bot Protection

Haltdos Application Security leverages machine learning to detect and classify bots by observing over 200 different browser parameters to help prioritize genuine users from crawlers, spammers and prevent account takeover, brute force login, carding, and other bot based attack vectors.

Haltdos also provides mobile SDK for protecting mobile applications and api based applications.

App Security : Feature Highlights

Easy to Use

Pre-built security templates and an intuitive web interface provide immediate security without the need for time-consuming tuning or training. Integration with security vulnerability scanners and SIEM tools automates the assessment, monitoring, and mitigation process.

Cross-Platform Portability

As IT architectures deploy more applications, they must also ensure that they are secure. Haltdos extends security policies to all corners of the data center. It can deploy common security policies across a mixture of cloud, software, virtual appliance, or even as a bare-metal server, integrating with existing systems with minimal disruption to the existing network.

Rapid Response

Haltdos can close application vulnerabilities faster, by importing ruleset recommendations from third-party vulnerability scanners and workflow tools such as ThreadFix. Automated learning is available to help security teams to manage policies. With full control over the activation of individual policies, organizations can maximize application security, while reducing the number of false positives.

Advanced Graphical Analysis and Reporting

Haltdos includes a suite of graphical analysis tools. It gives administrators the ability to visualize and drill-down into key elements of the solution such as server / IP configurations, attack and traffic logs, attack maps, and user activity. Haltdos UI lets administrators quickly identify suspicious activity in real time and address critical use cases such as origin of threats, common violations, and client / device risks.

Integration with Existing Technology

Haltdos connects with organizations' existing technology and business processes, and can integrate with Security Incident and Event Management systems (SIEMs).

Comprehensive Reporting & Logging

Haltdos includes a range of reporting options for threat analysis and data retention. This not only helps security professionals to see potential attacks developing, but also where policies are too restrictive. Also, data retention can help with local compliance requirements for record keeping, and also for auditing policy changes.

Dual-Mode Detection and Protection

Organizations can define security policies with the dual-mode "detect and protect" operation. Haltdos allows layered rulesets, maintaining a live ruleset to enforce policies which have been approved for production, and simultaneously operating a detection only ruleset which can include watch lists and trial policies. This enables new rulesets to be tested in a detection only mode, ensuring that new policies are not activated without approval from security administrators. With this feature, new layered rulesets can be tested without compromising existing policy enforcement, which helps to avoid false positives or weakened defenses, particularly in large-scale cloud applications.

PCI DSS Compliance

Haltdos helps compliance with PCI DSS, which is a key standard with for organizations which manage credit card payments. The standard defines a pragmatic set of security procedure: Section 6.6 of the standard mandates that a merchant must deploy and configure a web application firewall.

Subscription Options

Security Features	Essential	Premium	Enterprise
OWASP Top 10	Yes	Yes	Yes
Brute Force Protection	Yes	Yes	Yes
Geo / IP Reputation Blocking	Yes	Yes	Yes
Bot Protection	Yes	Yes	Yes
Data Leak Prevention	Yes	Yes	Yes
Website Scraping Protection	Yes	Yes	Yes
Basic DDoS Protection	Yes	Yes	Yes
Virtual Patching	Yes	Yes	Yes
Community Signatures	Yes	Yes	Yes
Malware Detection	Yes	Yes	Yes
Advanced Signatures		Yes	Yes
Advanced DDoS Protection			Yes
Zero-day Attack Protection			Yes
Developer Script			Yes
Deception Rules			Yes

Security Features			
Basic Load Balancing	Yes	Yes	Yes
Upstream Monitoring	Yes	Yes	Yes
Advanced Load Balancing		Yes	Yes
Websocket Support		Yes	Yes
API Gateway			Yes
Performance Monitoring			Yes
RUM Monitoring			Yes
Latency Monitoring			Yes

Security Features			
Email Support	Yes	Yes	Yes
Telephone Support	Yes	Yes	Yes
Dedicated Account Manager		Yes	Yes
SIEM Integration		Yes	Yes
Audit Logs			Yes
Reporting		Monthly	Daily / Monthly

Previous models mapped as HD-AIE-1G (HD-SFT-4100), HD-AIE-5G (HD-SFT-4600), HD-AIE-10G (HD-SFT-5100) and HD-AIE-50G (HD-SFT-6200)

SAFEGUARDING IT INFRASTRUCTURE

To learn more about Haltdos Enterprise Web & API Protection Solution and to ensure 360° protection for your critical website, APIs and mobile application, visit, www.haltdos.com or email us at sales@haltdos.com

Haltdos Edge Platform

version v5