haltdos

HaltDos Swift

Enterprise Application Firewall Solution

(Part of Application Delivery Controller)

DATASHEET

HaltDos Swift is a 360° protection for your websites and applications from cyber threats.

Defend Your Application Against Web Attacks Such as SQL Injections, Cross-Site Scripting Attacks Etc.

Swift at a glance:

Multi-Layered Solution: HaltDos AI-enhanced and multi-layered approach combine network behavioral analysis (NBA), heuristic and reputation techniques to provide complete security for both internal and external web-based applications.

Machine Learning Detection: HaltDos machine learning detection engine intelligently detects threats with nearly zero false positive detections. This ensures your applications remain secured against sophisticated threats like SQL injection, buffer overflows, zero-day attack, and DoS attacks.

Built in Rules: Our 24x7 R&D team is always on the lookout for new vectors of attacks and continuously publish signatures to mitigate them. HaltDos WAF uses best of signatures & Machine Learning to mitigate any attacks on your web applications.

Protect Your Website and Applications

HaltDos provides superior protection against application-layer DDoS and other attack vectors directed at web-facing applications while providing excellent protection against data loss. Automatic updates offer defense against new threats as they arise. As new threats emerge, it will acquire new capabilities to block them.

HaltDos has strong authentication as well as access control capabilities to ensure privacy and security. It restricts access to sensitive applications or data to authorized users. Our WAF uses state-of-the-art anomaly detection techniques to block application layer attacks along with ability for users to create custom set of rules to configure the solution as per organization's need.

Support

- 24 x 7 x 365 Support
- On-Site Warranty Support
- Twice a Year Site Visit Assurance
- Centralized Helpdesk

TALK WITH HALTDOS

Web haltdos.com/products/waf
Call 1800-120-2394
Reach haltdos.com/contact

Amidst fierce competition, your business cannot afford to slow down. With HaltDos, you don't have to sacrifice productivity and performance to get leading-edge security.

HaltDos provides multi-layer, multi-vector protection to ensure your website & applications stays online 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.

HaltDos Swift : Feature Highlights

Easy to Use

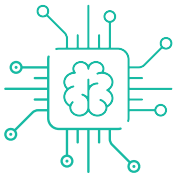
Pre-built security templates and an intuitive web interface provide immediate security without the need for time-consuming tuning or training. Integration with security vulnerability scanners and SIEM tools automates the assessment, monitoring, and mitigation process.

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.

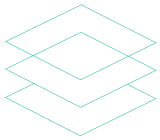
Constant Protection from Evolving Threats

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.



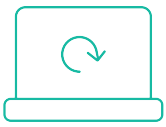
Self-Learning

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.



Massive Scalability

Organizations must scale dynamically to meet the needs of the largest global applications. HaltDos can extend seamlessly across CPU, computer, server rack, and data center boundaries. Organizations can use a combination of public and private cloud technologies, and be assured of common
application security.



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.

Distributed and Delegated Management

HaltDos includes a Web-based user interface to give security professionals full distributed access to centralized policy management and reporting. Organizations can now manage policies centrally and also delegate access to business partners to manage the security configurations of specific applications or domains, tailoring access rights granular settings for individual client applications.

HaltDos Swift : Feature Highlights

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.

PCI DSS Compliance

HaltDos helps compliance with PCI DSS, which is a key standard with for organizations which manage credit card payments. Failure to meet the requirements of PCI DSS exposes a merchant to a higher risk of fraud, potential liability for costs resulting from leakage of cardholder data, and incurs higher processing fees from credit providers. The PCI DSS standard defines a pragmatic set of security procedure: Section 6.6 of the standard mandates that a merchant must either perform regular security reviews of the source of all public-facing applications or deploy and configure an appropriate Web application firewall.

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.

Built-in Load Balancer

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

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.

How Swift Web Application Firewall Works

HaltDos supports best practices for application security. Due to its modular construction, organizations can deploy applications very easily in any IT environment, making it a scalable solution for application-level security. HaltDos can apply business rules to online traffic, inspecting and blocking attacks such as SQL injection and cross-site scripting, while filtering outgoing traffic to mask credit card data.

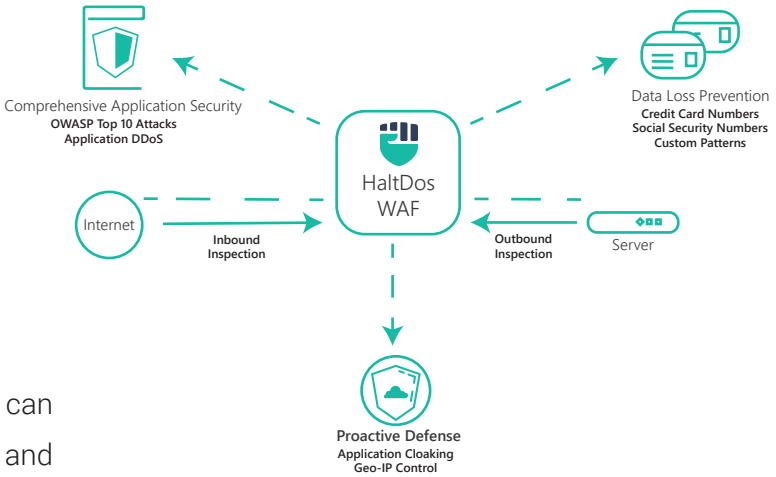
Response Analysis

HaltDos also monitors outgoing responses as they are returned to the client. Security-sensitive information can be filtered out from responses to ensure that data leakage is captured, even if the initial malformed request is successful. As a result, customer information such as credit card data, social security numbers, or healthcare related content can be screened out by using comprehensive security policies. HaltDos can monitor the behavior of the application and traffic patterns to help optimize protection and recommend additional policies.

Request Analysis

When activated, HaltDos receives and analyzes each request against the ruleset assigned to the application, and determines which of the following actions to take:

- Permitted requests are passed to the application
- Requests which are identified as known attacks are rejected, and logged with information to help trace the attacker
- Requests which cannot immediately be categorized can be rejected locally or passed on to the application, and depending on the security policy in force, they are logged and used to help classify future requests of this type



Mitigation Spotlight

Baseline Protection

HaltDos includes a Baseline Protection Wizard, which makes it easy to update policies. The baseline policies are a blacklist and regex-pattern match of known vulnerabilities and attacks: when HaltDos detects a suspicious pattern which matches the baseline policies, then the request is rejected without exposing the application.

HaltDos publishes regular baseline updates, and the HaltDos dashboard highlights the recommended updates. Note that the new baseline policies are NOT applied automatically - the new rules should be reviewed by the security team and activated through the management console.

Secure Entry Points

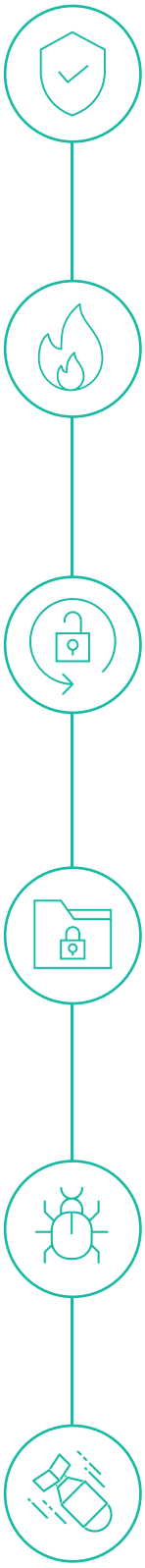
Similarly, many applications enforce authentication when a session is opened, but do not perform access control verification at each step or intermediate function. Attackers can manipulate workflow flaws to access data or bypass session authentication.

HaltDos offers an Entry Point Handler that can provide additional security by ensuring that new user sessions always start at a pre-determined entry point. This prevents attackers from deep linking into applications, bypassing entry points and authentication steps.

Resolving Third-Party Vulnerabilities

Modern online applications often include third -party libraries and tools, which may vulnerable to zero-day attacks. Third-party software providers may be unable to resolve flaws quickly, so attackers may be able to exploit these vulnerabilities before they are corrected. Known vulnerabilities within application components can be mitigated with HaltDos. Standard application attacks like SQL Injection or XSS can be mitigated using the Baseline Protection or the Whitelist Learning Capability.

Similarly, the pro-active features of the HaltDos can be used to identify and protect against vulnerabilities in the application logic of applications.



Secure Session Management

While many applications use secure passwords and authentication, it is possible for user and session data to be exposed through weak links such as session cookies and tokens. Attackers can use these weak links to create or modify sessions, and access live data.

HaltDos Secure Session Wizard can help to secure vulnerable sessions, using two important tools: the Session Handler can impose additional controls on user session timeouts and session limits, while the Cookie Jar Handler can be used to preserve vulnerable information by exchanging weak session cookies for more secure session management. With HaltDos, organizations can add an additional authentication layer in front of their applications.

Sensitive Data Masking

Attackers may attempt a variety of exploits to extract sensitive data, including payment card information, social security information, and security credentials.

This kind of sensitive data requires additional layers of protection beyond the encryption of stored data: for example, data in transit should be encrypted using secure transport, and active response filtering can mask out sensitive data which leaks through other defenses.

Forwarding and Redirecting Attack

Many Web applications use redirections and forwarding to transfer control within online services, and may be vulnerable when they use untrusted data or URL parameters to select the target Web page. Attackers may use weak validation of redirection criteria to trigger malware or phishing attacks by forwarding to unauthorized targets.

HaltDos Baseline Protection Wizard includes policies that check for fully-qualified URL references to protect against unwanted redirection. Security professionals can also define preferred redirection targets for when an invalid redirection target is detected.

STAY ONLINE AND ALWAYS AVAILABLE WITH HALTDOS SWIFT!

To learn more about our Enterprise WAF Protection Solution and to ensure 360° protection for your websites and applications, please visit: www.haltdos.com

HaltDos™ SWIFT

• *We are GDPR Compliant!* •