haltdos

TECHNICAL SPECIFICATION

Haltdos Swift:
Web Application & API Protection

Fast . Scalable . Reliable

Haltdos hardware appliances deliver a hardened and scalable, reliable platform to power Haltdos solutions. Haltdos Hardware Appliances offer exceptional performance, allowing organizations to consolidate device management and address future bandwidth requirements. Haltdos appliances can manage heavy traffic loads without impacting application or network performance.

Fault Tolerant Hardware Design

With multi-gigabit throughput, fail open interfaces, secure out-of-band management, and low latency, Haltdos appliances are high assurance, fast and easy to manage. To maximize system uptime, Haltdos appliances offer redundant, hot-swappable components including redundant power supplies and hard drives. In the event of a hardware failure, the redundant component will automatically take over, providing continuous system operations

Support

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

CONNECT WITH HALTDOS

https://www.haltdos.com/appsec/enterprise-web-application-firewall

1800-120-2394

https://www.haltdos.com/contact

Flexible Expansion Options to Address Unique Business Needs

The appliances are built on a common hardware platform with flexibility in mind. Haltdos appliances can be extended to provide remote, out-of-band management and monitoring, performance acceleration, and more with expansion modules. Expansion modules include:

- Network Cards (copper or optical)
- Hardware Security Module (HSM) (non-FIPS and FIPS-140-2)
- SSL acceleration card
- Disk Space & RAM

Product Specifications

MITIGATION PERFORMANCE		HD-SFT-4100	HD-SFT-4600	HD-SFT-5100	HD-SFT-5400	HD-SFT-6200
1.1	Layer 4 Throughput (bps)	5 Gbps	24 Gbps	48 Gbps	72 Gbps	120 Gbps
1.2	Layer 7 Throughput (bps)	4 Gbps	20 Gbps	40 Gbps	60 Gbps	100 Gbps
1.3	SSL/TLS Throughput (bps)	4 Gbps	20 Gbps	40 Gbps	50 Gbps	100 Gbps
1.4	Compression Throughput (bps)	4 Gbps	20 Gbps	25 Gbps	37 Gbps	66 Gbps
1.5	Decompression Throughput (bps)	5 Gbps	20 Gbps	30 Gbps	54 Gbps	120 Gbps
1.6	SSL/TLS RSA 2K Rate (tps)	22K	40K	40K	100K	100K
1.7	SSL/TLS ECC Rate (tps)	15K	25K	25K	50K	50K
1.8	L4 Connections Rate (cps)	480 K	960 K	1.5 M	3 M	4.2 M
1.9	L7 Request Rate (rps)	750 K	3 M	7 M	10 M	15 M
1.10	Max Concurrent Connections	24 M	24 M	56 M	96 M	160 M
1.11	Induced Latency	< 1 ms				
HARDWARE SPECS						
2.1	Processor	Intel Xeon				
2.2	CPU Cores	8	20	32	40	64
2.3	Minimum Memory*	16 GB	32 GB	64 GB	128 GB	256GB
2.4	Minimum Hard Disk*	256 GB SSD	256 GB SSD	512 GB SSD	1 TB SSD	2 TB SSD
2.5	Form Factor	1U/2U/4U Rack Mount Server (19-inch mounting)				
2.6	Operating Temperature & Humidity	0 - 40 C with 8%-95% humidity (non-condensing)				
2.7	Power Supply and Fans	Redundant Power Supply (Hot Swappable)AC 170-240V,50 Hz and Redundant fans.				
2.8	Hardware Virtualization	N/A	Upto 15	Upto 25	Upto 30	Upto 50
2.9	Inspection Ports*					
	1 GE Ports	8	8	-	-	-
	10 GE Ports	-	2	4	8	8
	25 GE Ports	-	-	-	-	-
	40 GE Ports	-	-	2	2	4
	100 GE Ports	-	-	-	-	-
2.10	Out Of Band Ports					
	1 GE (RJ-45) Ports	2	2	2	2	2
	Console (RS232/RJ45) Ports	1	1	1	1	1
	HA Ports (RJ-45/SFP/SFP+)	1	1	1	1	1
	Input/Output (USB)	2	2	2	2	2

* Customizable Components

Centralized Management

Depending upon the chosen deployment as standalone or cluster, Haltdos also offers a centralized management solution for management of Haltdos products. The centralized management is API first solution that comes in the following flavors:

- HD-MGT-ST: This model is a single tenant centralized management solution that supports only one license dedicated to a single customer.
- HD-MGT-MT: This model is a multi-tenant centralized management solution that supports multiple licenses that can be used by one or more customers.

Like the products, Haltdos Centralized Management solution can be deployed in Hardware or virtual form factor.

Virtual Appliances

All Haltdos products are built on top of Haltdos Platform. This allows the platform to be installed in various flavors - SaaS, Hardware, or virtual form factor. Regardless of the form factor chosen, the product have same technical capabilities.

Cluster Virtual Models	Standalone Virtual Model	Throughput (Mbps)
HD-VC-25	HD-SFT-25/VM	25
HD-VC-50	HD-SFT-50/VM	50
HD-VC-100	HD-SFT-100/VM	100
HD-VC-200	HD-SFT-200/VM	250
HD-VC-500	HD-SFT-500/VM	500
HD-VC-750	HD-SFT-750/VM	750
HD-VC-1000	HD-SFT-1000/VM	1000
HD-VC-2500	HD-SFT-2500/VM	2500
HD-VC-7500	HD-SFT-7500/VM	7500

Cloud WAAP

EDGEO-WAAP is a cloud-delivered WAAP solution for securing web applications and APIs through a scalable, low-latency architecture. It is licensed based on the number of protected FQDNs and requires no customer-managed hardware or virtual appliance.

Product Model	Deployment	Licensing	Product
EDGEO-WAAP	Cloud / SaaS	FQDN Based	Web Application & API Protection (WAAP)

Product Features

TECHNOLOGY & CERTIFICATION

3.1	Platform & Technology	Haltdos Platform with Signature from Threat Intelligence & Machine Learning
3.2	License	Unlimited applications. Bandwidth capped by license. Upgrade possible without hardware replacement up to max supported hardware bandwidth.
3.3	Certifications	FCC, ROHS, CE compliant, EAL 2+, IPv6 Ready Gold certifications
3.4	Support	24x7 via Online, Email , Telephone and Dedicated Account Manager
3.5	Warranty	1 year warranty. Additional charges for extended warranty
3.6	TAC Support	TAC support in India
3.7	Training	OEM driven hands-on training

INTEGRATION FEATURES

4.1	API Integration	Supporting XML and RESTFul (JSON) APIs
4.2	Storage and Export	Local retention of logs, reports and events. Support for export to 3rd party storage
4.3	NIMS Integration	Support for SNMP, NTP / SNTP, DNS, Web Proxy integration
4.4	AAA Integration	Support for integration via RADIUS and TACACS+
4.5	Identity Management	Inbuilt with support for integration with AD / SAML / LDAP
4.6	Security Tools Integration	Support for integration with SAST/DAST/IAST tools. Integration with 3rd party Threat Intelligence (TI) feeds
4.7	SIEM Integration	Support for integration with SIEM and Syslog services
4.8	Export IOCs	Support for exporting attacking IOCs via STIX / TAXII
4.9	3rd Party Integration	Notification & Logging via SNMP, SMTP, SMS Gateway, and 3rd party integration via API hooks, CI/CD, Kubernetes

OPERATION MODE

5.1	Network Operations	Offline, Inline Reverse Proxy, Inline Forward Proxy, Inline Bridge, Inline Router Mode, Inline L2 Transparent
5.2	Inline Modes	Proxy or Direct Server Return, Immediate or Delayed Binding
5.3	Supported HTTP Protocols	HTTP 0.9,1.0,1.1,2.0,3.0 (QUIC) with translation
5.4	Deployment Modes	1-Arm or n-Arm, Support for Virtual Matrix Architecture & Direct Access Mode
5.5	IP Stack	Dual IPv4 & IPv6 stack
5.6	Web Socket Support	Yes
5.7	Mitigation Modes	Bypass, Record (Report Only), Learning, Mitigation (Block & Report)
5.8	Dynamic Routing	BGP, OSFP, RIPv1/v2
5.9	Networking	VLAN, VXLAN, Link Aggregation & Trunking (LACP), Multiple Routing Tables, ARP Table etc
5.10	Binding	Immediate or Delayed binding.
5.11	**Tunnelling Protocols**	VLAN, MPLS, GRE, L2TP, GTP, IPinIP
5.12	Block Actions	Drop Request, Terminate Connection / Session, Rate Limiting, Blacklist (Temporary or Permanent), Send Challenge, Tarpit
5.13	Virtual Matrix Architecture	Yes

5.14	Virtualization	Multi-tenancy with isolated VMs with dedicated CPU, RAM and Disk. Support for multiple OS templates for customized deployments
5.15	Direct Access Mode	Yes
HIGH AVAILABILITY		
6.1	Multiple Appliances	N + 1 Active - Active or Active – Passive (VRRP) with floating MAC
6.2	Management Modes	Standalone / Centralized Management (VM or appliance)
6.3	Secure Communication	Secure communication between centralized management and HA appliances for full state synchronization
MANAGEMENT FEATURES		
7.1	Graphical User Interface (GUI)	Secure web interface over HTTPs with support for all modern browsers
7.2	Command Line Interface (CLI)	Command Line Interface over SSH or console port
7.3	System Management	IPMI 2.0 Compliant
7.4	Audit Trail, Logging & Recovery	Centralized logging of system, services, MIS, incidents. Built-in MIS with policy recovery
7.5	RBAC Administration	Configurable user profiles with role based access control
7.6	Policy Management	On the fly configuration updates on mitigation appliances
7.7	Dashboards & Reporting	Real-Time & historical dashboards with custom duration. Support for custom dashboards. Status dashboard for 1-click health check. Periodic daily, weekly or monthly reports in PDF or Excel
7.8	API integration	Yes (XML or JSON)
7.9	Events / Alerts	Detailed event and alert reporting on attack, health, etc.
7.10	Haltdos Threat Stream	Periodic threat intel updates (signatures, Geo IP, Bad IP,TOR IP,Anon Proxy,etc.) from Haltdos.
7.11	Attack Forensic	Built in utilities for investigating attackers, attack payload and identifying false positives.
7.12	Backup, Restore & Snapshots	Automatic or manual backup and restore. CLI tool for pushing current snapshot to Haltdos Cloud for diagnostics
7.13	Certificate Management	SSL/TLS certificate management with support for Let's Encrypt certificate generation
7.14	Network Forensics	Network forensic with packet capture and traceroute. Built-in utilities for investigating attacks, payloads and managing false positives
7.15	Updates	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos. Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates
WAF FEATURES		
8.1	Comprehensive Security	OWASP Top 10 Web Application Security Risks, OWASP Top 20 Automated Threats and SANS 25 Software Errors
8.2	Security Profiles	Multiple security profiles with support for different security status per application based on url, source, country, regex, etc.

8.3	Positive Security Model	Support for Form Rules for positive security model
8.4	Negative Security Model	Support for user defined Firewall Rules for REGEX based negative security model
8.5	Virtual Patching	Support for virtual patching through built-in web security scanner or upload of 3rd party SAST / DAST / IAST scan results
8.6	Built-in Signatures	Over 4000+ built-in signatures on various technologies, platforms and frameworks with pre-defined templates
8.7	0-day Protection	Automatic learning and profiling application structure. Threat scoring and baseline creation for AI driven 0-day attack protection
8.8	Malicious Source Protection	Protection against TORIP, Bad Reputation IP, dark IP, known Bots, proxies, spammers provided by Haltdos or user defined threat intel
8.9	Bot Management	Anti-bot protection with AI classification and scoring of bots based on advanced browser fingerprinting
8.10	Mobile App Protection	Anti-Bot mobile SDK for Android & iOS for protecting mobile apps and communication between apps and web APIs
8.11	HTTP Validations	Protocol validations, request normalization (encoding & evasion techniques) before inspection, managing security headers and cookies etc
8.12	Script Rules	Embedding user defined custom code for advanced routing
8.13	Anti-Automation Protection	Protection against known and 0-day bots, account takeover attempts, brute force attempts, scraping, reconnaissance, cloaking, etc
8.14	AV Scanning	Built-in AV scanner for malicious file upload. Support for ICAP integration for 3rd party scanners
8.15	Minimize False Positives	Support for REGEX based whitelist rules and signature staging and deploy policies to minimize signature based false positives
8.16	Policy Inspection	Policy validation such as HTTP methods, file extension, request size, etc
8.17	Blacklist / Whitelist	Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, url, country, etc
8.18	Challenge-Response	Support for JS, Crypto and CAPTCHA challenge on suspicious user activity or known bots or malicious IPs
8.19	Rate Limiting	Rate Limit rules for implementing request, bandwidth or connection limits per source, IP prefix or user defined policy
8.20	API & WebSocket Protection	Built-in XML firewall, validation of XML / JSON / Ajax requests and WebSocket requests
8.21	API Security	Built-in API gateway for authentication, rate limiting, transformation, documentation and discovery
8.22	Variable Rules	Support for embedding and using variables for A/B testing or custom load balancing or implementing app specific security policy
8.23	End-User Fingerprinting & Performance Monitoring	Advanced user and device fingerprinting for user profiling, device authentication and Real User Metrics (RUM) for performance monitoring
8.24	Security Breach Prevention	Built-in support for data leak prevention, response filtering for sensitive personal identifiable information
8.25	Compliance	PCI DSS 2.0 section 6.6 enforcement
8.26	Captcha challenge	Support for JS or captcha challenge on suspicious user activity or known bots or maliciousIPs
8.27	Variables & Scripting	Support for user defined variables and scripts for building custom application specific security policy

8.28	Tamper Proofing	Tamper rules for URL / parameter tamper protection, website defacement, hidden form field protection, cookie signing and encryption, etc.
8.29	Client-Side Protection	Protection against key loggers, client side payload encryption, malicious plugin detection, etc
8.30	Enforce RFC Compliance	Protection against invalid HTTP requests
8.31	Correlation Engine	Advanced correlation engine with support for custom correlation rules for detecting attack across user requests and sessions
8.32	HTTP Validations	Protocol validations, request normalizations before inspection, managing security headers and cookies etc.
8.33	Policy Insprection	Policy insoection such as HTTP methods, files extension, request size, etc.
8.34	Deception Technology	Implement decoys in web application to protect against advanced bots, profile attacks and trap attackers
8.35	Sensitive Data Masking	Support for Log Rules for masking sensitive information such as passwords in logs and events
8.36	L3–L7 DDoS Protection	Protection against volumetric and low & slow DDoS attacks. Support for rate limiting based on connections and requests
8.37	Enforced Browsing	Protection against forceful browsing, access to pctable resources, unauthorized navigation with additional security enforcement with Two factor authentication
8.38	Misc. Protection	Support for protection against buffer overflow attacks,SQL, man-in-the-middle attacks, blocking malware payload, buffer overflow, SSI, LDAP injection, etc
8.39	NAT & Routing	Support for client, server or full NAT, static routing for IPv4 & IPv6
8.40	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
8.41	Load Balancing	Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.). Content based load balancing with upstream rules
8.42	Load Balancing Algorithms	Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc.
8.43	Optimization	TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts. Content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients
8.44	Virtual Contexts	Support for multiple virtual contexts along with resource allocation
8.45	Failover Management	Automatic failover & recovery. Support for marking servers up / down / backup
8.46	Health Check	Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script
8.47	Client Visibility	Embedding Real IP information in X-* headers, client cert information, etc
8.48	Redirection Rules	REGEX based redirection rules to rewrite URLs
8.49	Content Transformation	Transformation rules for data manipulation and Header rules for add / edit or delete headers in request or response
8.50	Authentication	Support for Single SignOn with multiple Auth type like Basic Auth, Form Auth, NTLM, LDAP, SAML, etc.
8.51	Error Handling	Error rules for custom error handling
8.52	Port Mirroring	Mirror traffic /specific traffic to another NIC port

HARDWARE FLEXIBILITY

Haltdos appliances are built on a common hardware platform with flexibility in mind. The appliances can be extended to provide remote, out-of-band management and monitoring, performance acceleration, and more with expansion modules

Expansion Module includes:

- Network Cards (copper or optical)
- Hardware Security Module (HSM) (non-FIPS and FIPS-140-2)
- SSL acceleration card
- Hard Disk & RAM

Hard Disk		
9.1	HD-DSK-128G-SSD	128 GB SSD Hard Disk
9.2	HD-DSK-256G-SSD	256 GB SSD Hard Disk
9.3	HD-DSK-512G-SSD	512 GB SSD Hard Disk
9.4	HD-DSK-1T-SSD	1 TB SSD Hard Disk
9.5	HD-DSK-1T-HDD	1 TB HDD Hard Disk
9.6	HD-DSK-2T-HDD	2 TB HDD Hard Disk
9.7	HD-DSK-4T-HDD	4 TBHDD Hard Disk

SSL Cards

	Part Code	Throughput			SSL TPS
10.1	HD-SSL-25G	SSL	25 Gbps	RSA	40
		Compression	20 Gbps	ECC	25K
10.2	HD-SSL-50G	SSL	50 Gbps	RSA	95K
		Compression	37 Gbps	ECC	48K

NIC Cards

11.1	Part Code	Description	Copper/Fiber	Hardware Bypass
11.2	HD-NIC-1x4C	Quad Port 1 Gbps	Copper	No
11.3	HD-NIC-1x4CB	Quad Port 1 Gbps	Copper	Yes
11.4	HD-NIC-1x4F	Quad Port 1 Gbps	Fiber (Single / Multi-Mode)	No
11.5	HD-NIC-10x2C	Dual Port 10 Gbps	Copper	No
11.6	HD-NIC-10x2CB	Dual Port 10 Gbps	Copper	Yes
11.7	HD-NIC-10x2F	Dual Port 10 Gbps	Fiber (Single / Multi-Mode)	No
11.8	HD-NIC-10x2FB	Dual Port 10 Gbps	Fiber (Single / Multi-Mode)	Yes
11.9	HD-NIC-10x4F	Quad Port 10 Gbps	Fiber (Single / Multi-Mode)	No
11.10	HD-NIC-10x4FB	Quad Port 10 Gbps	Fiber (Single / Multi-Mode)	Yes
11.11	HD-NIC-25x2F	Dual Port 25 Gbps	Fiber (Single / Multi-Mode)	No
11.12	HD-NIC-25x2FB	Dual Port 25 Gbps	Fiber (Single / Multi-Mode)	Yes
11.13	HD-NIC-25x4F	Quad Port 25 Gbps	Fiber (Single / Multi-Mode)	No
11.14	HD-NIC-25x4FB	Quad Port 25 Gbps	Fiber (Single / Multi-Mode)	Yes
11.15	HD-NIC-40x2F	Dual Port 40 Gbps	Fiber (Single / Multi-Mode)	No
11.16	HD-NIC-40x2FB	Dual Port 40 Gbps	Fiber (Single / Multi-Mode)	Yes
11.17	HD-NIC-40x4F	Quad Port 40 Gbps	Fiber (Single / Multi-Mode)	No
11.18	HD-NIC-40x4FB	Quad Port 40 Gbps	Fiber (Single / Multi-Mode)	Yes
11.19	HD-NIC-100x2F	Dual Port 100 Gbps	Fiber (Single / Multi-Mode)	No
11.20	HD-NIC-100x2FB	Dual Port 100 Gbps	Fiber (Single / Multi-Mode)	Yes
11.21	HD-NIC-100x4F	Quad Port 100 Gbps	Fiber (Single / Multi-Mode)	No
11.22	HD-NIC-100x4FB	Quad Port 100 Gbps	Fiber (Single / Multi-Mode)	Yes

RAM

12.1	HD-RAM-8G	8 GB DDR4 RAM
12.2	HD-RAM-16G	16 GB DDR4 RAM
12.3	HD-RAM-32G	32 GB DDR4 RAM
19.4	HD-RAM-64G	64 GB DDR4 RAM