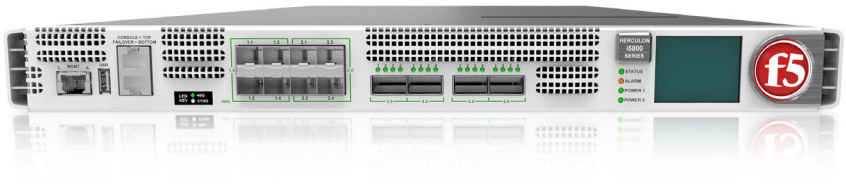
F5 Herculon DDoS Hybrid Defender

DATASHEET



What's Inside

Securing the Data Center with Next-Generation DDoS Protection

Distributed denial-of-service (DDoS) attacks remain a top concern and leading cause of business service outages facing organizations today. Often used as a smoke screen for more dangerous hacks or theft, DDoS attacks threaten businesses of all sizes. Free or moderately priced DDoS attack resources available online enable even the most novice attackers to assemble electronic armies (bots) focused on weakness in protocols, firewalls, and applications that can be difficult to defend against. How quickly you discover and stop DDoS attacks is the key to overcoming the potential for monumental costs, damage to critical resources, and loss of important data.

F5® Herculon™ DDoS Hybrid Defender™ provides next-generation hybrid DDoS defense to ensure real-time coverage against ever-changing network attacks, sophisticated application attacks, volumetric DDoS threats, and those that hide behind SSL. This hybrid solution creates signatures automatically—enabling faster and more accurate threat identification and blocking of evasive threats. These include low-and-slow patterns and short sporadic bursts of 100+ Gb traffic that may go undetected. Herculon DDoS Hybrid Defender discovers and fingerprints new and unusual traffic patterns without human intervention, distinguishing and isolating potential malicious traffic from legitimate traffic almost instantaneously. With a combination of application stress-level context and behavior analytics, Herculon DDoS Hybrid Defender can accurately detect and mitigate the attack in progress.

Key benefits

Comprehensive DDoS coverage

Herculon DDoS Hybrid Defender leverages dynamic intelligence services, behavioral analytics, and event correlation. It also features unique anti-bot defense to secure against non-human threats including web scraping, brute force attacks, and application DDoS attacks.

Seamless hybrid defense

Protect the network with automated settings for DDoS threshold values, IP intelligent feeds, IP black listing, and remote trigger black-holing that blocks known bad actors immediately without wasting mitigation cycles.

Flexible deployment options

Seamlessly integrate on-premises DDoS protection that supports both inline or out-of-band processing with a cloud-based volumetric scrubbing service—for sub-second attack detection and a low total cost of ownership (TCO).

Why Herculon DDoS Hybrid Defender?

- Complete coverage in a single offering with combined network and application DDoS defense, SSL decryption, behavioral analysis, and cloud scrubbing
- Sub-second attack detection with geotracking, intelligent signaling, and hardware assist—inline or in out-of-band mode
- In-depth and real-time attack visibility for more effective decisions with 3000+ L3–L4 metrics, detailed logging, actionable reports, and intelligence sharing
- Proactive bot defense that discovers malicious bot activity in advance of attacks

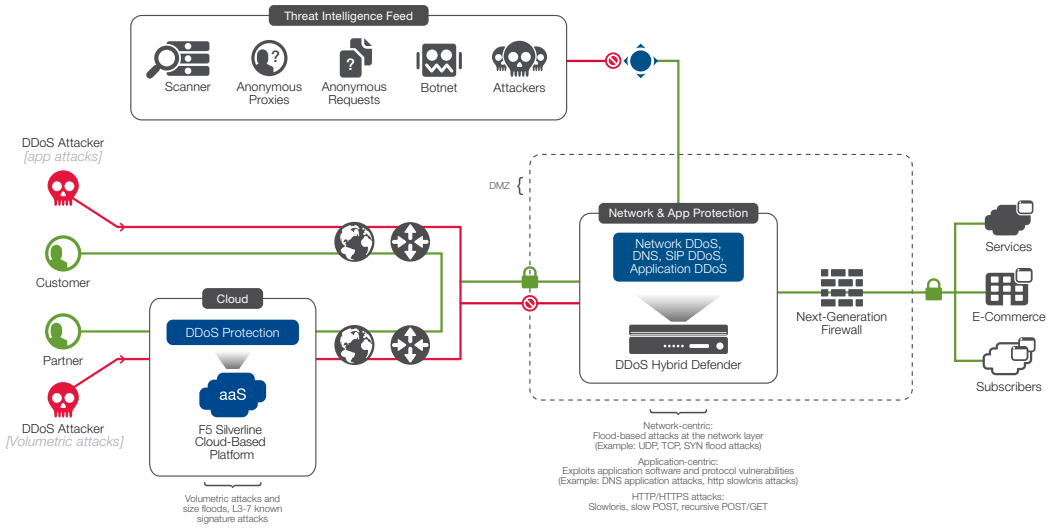
Comprehensive DDoS Coverage

Herculon DDoS Hybrid Defender provides the broadest attack coverage in any single offering. The proven technology ensures continuity of business services, which are threatened by hacktivists, cyber vandals, extortionists, and more. It speeds discovery of highly advanced DDoS attacks and provides fast detection and mitigation of network and application-based DDoS attacks. For attacks causing WAN bandwidth saturation, Herculon DDoS Hybrid Defender provides automated signaling to redirect traffic to a cloud scrubber.

Seamless Hybrid Defense

Designed to integrate with the F5 Silverline® DDoS Protection cloud-based service, Herculon DDoS Hybrid Defender ensures fast activation of on-demand, cloud-based scrubbing to mitigate bandwidth saturation attacks. Unlike other hybrid DDoS approaches, the F5 solution is seamless, transparent, and managed to reduce errors and IT overhead. It enables a smooth and immediate transition back to on-premises protection once attack traffic has subsided to normal levels.

Herculon DDoS Hybrid Defender prevents saturation of inbound pipes by redirecting volumetric attack traffic to Silverline cloud services. In addition, information from all DDoS attacks discovered and mitigated by on-premises devices can be automatically communicated to F5 Security Operations Centers (SOCs) for expert research and global threat analysis. This information drives standard signature updates and security enhancements, while enabling accurate discovery of future threats based on trend analysis.



Herculon DDoS Hybrid Defender deployment: on-premises appliance and cloud scrubbing.

Deploy Where You Need It Most

Herculon DDoS Hybrid Defender eliminates common concerns with deployment, especially where network architectures are more complex. It offers a simplified user interface and an "out-of-the-box" experience—with automatic sizing and configuration of DDoS protection features. The flexible deployment options enable DDoS protection services to be easily deployed within the data center as a physical or virtual appliance, directly in the path of traffic or out of band for analysis of traffic behavior.

Herculon DDoS Hybrid Defender Specifications

This solution defends the most complex infrastructures, enabling organizations to improve data center and application level security, protect customer data and access, and enhance overall security postures.

DDoS Mitigation:	All layer 3, 4, & 7 DoS/DDoS threats including flood/sweep with Src/Dst IP address awareness, UDP/DNS/HTTP/TCP/SIP/SYN/ACK/RST/FIN using sub-second detection, network behavior analysis, 120+ DDoS vectors, application anomaly detection, dynamic filtering, protocol analysis, source tracking, control policies, and more
DDoS Auto-Threshold Setting:	Automatically generated and adjusted for all DDoS network and application threshold values for TPS, PPS, and requests per second
Malicious Bot Defense:	Proactive bot defense, captcha challenges, headless browser detection, bot categorizations identifying severity and good/bad bots, device fingerprinting
IP Intelligence:	Bad actor information can be communicated across other DHD devices; F5 IP Intelligence licensed services provide global DDoS threat intelligence feeds
DDoS Detection:	Out-of-band SPAN port, Netflow monitoring
SSL Inspection (Decryption):	Tamper-proof enclosure and safety: up to 80 Gbps Inspected throughput, up to 22M HTTPS connections, up to 100M concurrent sessions
Reporting and Forensics:	Dashboard summary current attack and drill-down reporting, standard and customizable charts and graphs; blocked/passed traffic; app health, bot signatures; Top 10 threats/destination IPs/source_IPs; sys mon; max # of attacks; IPs participating in attack (dashboard)
Mitigation Techniques:	Rate limiting/blocking, connection limiting, source limiting, shunning/blacklisting/whitelisting, BGP routing and RTBH (source and destination), cloud scrubbing, manual or automated
Management:	REST; CLI, Web UI; RBAC management
Deployment Modes:	Asymmetric Inline active/inactive; VLAN bridge mode; OOB Span/TAP monitoring with Netflow, packet data; appliance or virtual edition (software)
Event Notifications:	SNMP, Syslog, email
Cloud Signaling:	BGP routed automatic triggering with licensed F5 Silverline DDoS Protection cloud-based scrubbing, collaborative manual triggering with third-party services
High Performance (HA):	Support HA active/passive

Specifications	i10800	i5800
Traffic Performance		
L4/L7 Max Throughput:	160 Gbps/80 Gbps	60 Gbps/35 Gbps
L4 Max Concurrent Connections:	100M	40M
L4 Connections/sec:	1.5M	900K
SSL TPS Throughput:	ECC: 48K TPS (ECDSA P-256) RSA: 80K TPS (2K Keys) 40 Gbps bulk encryption	ECC: 20K TPS (ECDSA P-256) RSA: 35K TPS (2K Keys) 20 Gbps bulk encryption
L4 Latency:	<10 us	<10 us
PPS (TCP/UDP):	44M/140M	14M/115M
Attack Mitigation Performance		
H/W SynCookies/sec:	130M SYN cookies/sec	50M SYN cookies/sec
Network DDoS Detection Speed:	<1s	<1s

Specifications	i2800
Traffic Performance	
L4/L7 Max Throughput:	10 Gbps/5 Gbps
L4 Max Concurrent Connections:	14M
L4 Connections/sec:	250K
SSL TPS Throughput:	ECC: 3.5K TPS (ECDSA P-256) RSA: 4.3K TPS (2K Keys) 8 Gbps bulk encryption
L4 Latency:	<10 us
PPS (TCP/UDP):	2M/3M
Attack Mitigation Performance	
H/W SynCookies/sec:	0.8M SYN cookies/sec
Network DDoS Detection Speed:	<1s

More Information

To learn more about F5 security products, visit f5.com to find these and other resources:

Web pages

Herculon DDoS Hybrid Defender
Herculon SSL Orchestrator
Security Operations Center
Silverline Platform

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com

Solutions for
an application world.