FÜRTINET®

FortiWeb™

FortiWeb 100D, 400D, 600D, 1000E, 2000E, 3000E, 3010E, 4000E and VM

FortiWeb is a web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. Using multi-layered and correlated detection methods, FortiWeb defends applications from known vulnerabilities and from zero-day threats.

Acceleration and Performance

Multi-core processor technology combined with hardware-based SSL tools deliver blazing fast protected WAF throughput.

Application Protection

Protection from the OWASP Top Ten application attacks including Cross Site Scripting and SQL Injection.

Enhanced Detection

Built-in advanced detection tools monitor and track usage, users, devices and sessions, and intelligently evaluate suspicious requests to detect sophisticated attacks.

Highlights

- Up to 20 Gbps protected WAF throughput
- Correlated threat detection with behavioral scanning
- Enhanced protection with FortiGate and FortiSandbox integration
- Advanced tools that minimize false positive detections
- Third-party integration and virtual patching

FortiCare Worldwide 24/7 Support

support.fortinet.com

FortiGuard Security Services

www.fortiguard.com

Third-Party Certification

ICSAlabs
CERTIFIED WEB APPLICATION FIREWALL

Corporate Armor

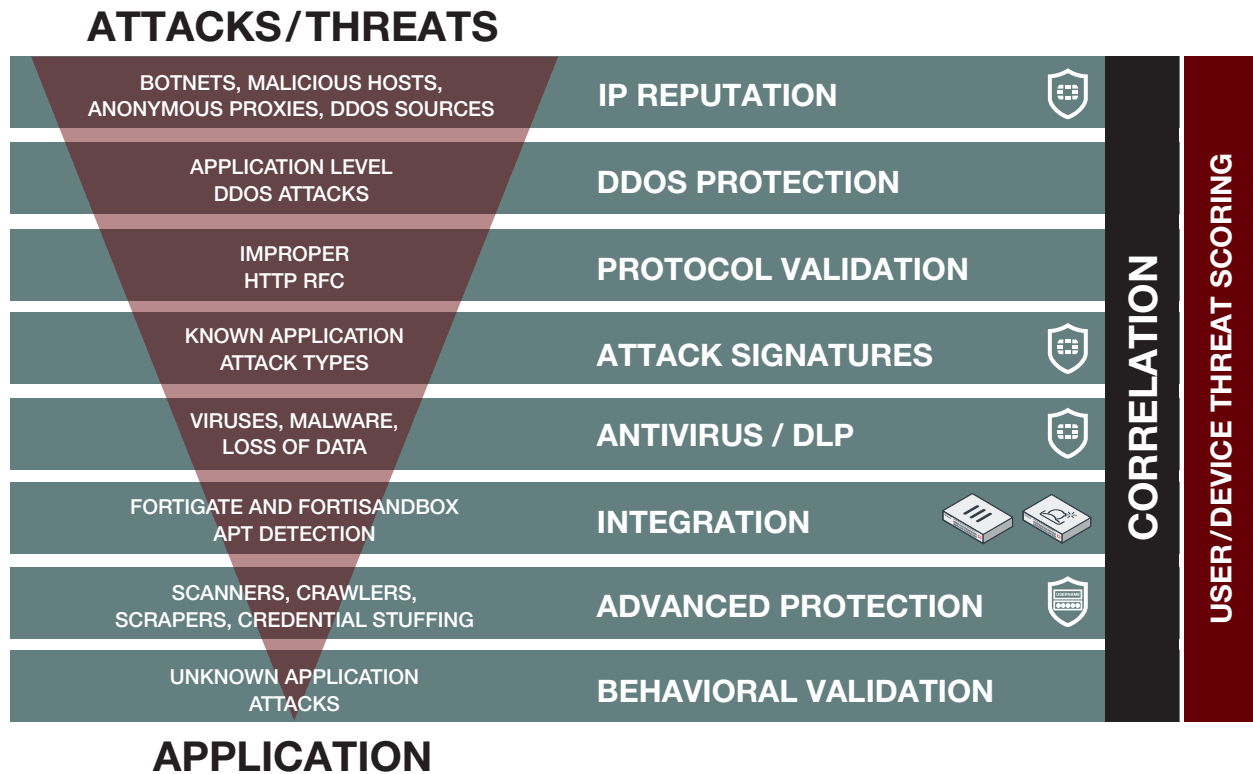sales@corporatearmor.com
877.449.0458

DATA SHEET

HIGHLIGHTS

Comprehensive Web Application Security with FortiWeb

Using an advanced multi-layered and correlated approach, FortiWeb provides complete security for your external and internal web-based applications from the OWASP Top 10 and many other threats. At the heart of FortiWeb is its behavior-based detection engine that intelligently detects threats that stray from normal patterns and takes action to protect applications from known and unknown zero-day threats.

ATTACKS/THREATS

BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	**IP REPUTATION**	
APPLICATION LEVEL DDOS ATTACKS	**DDOS PROTECTION**	
IMPROPER HTTP RFC	**PROTOCOL VALIDATION**	
KNOWN APPLICATION ATTACK TYPES	**ATTACK SIGNATURES**	
VIRUSES, MALWARE, LOSS OF DATA	**ANTIVIRUS / DLP**	
FORTIGATE AND FORTISANDBOX APT DETECTION	**INTEGRATION**	
SCANNERS, CRAWLERS, SCRAPERS, CREDENTIAL STUFFING	**ADVANCED PROTECTION**	
UNKNOWN APPLICATION ATTACKS	**BEHAVIORAL VALIDATION**	

CORRELATION

**USER/DEVICE THREAT SCORING**

APPLICATION

FortiWeb's layered and correlated approach to threat detection provides nearly 100% protection from known and unknown zero-day threats that target application vulnerabilities.

Deep Integration into the Fortinet Security Fabric and Third-Party Scanners

As the threat landscape evolves, many new threats require a multi-pronged approach for protecting web-based applications. Advanced Persistent Threats that target users can take many different forms than traditional single-vector attack types and can evade protections offered only by a single device. FortiWeb's integration with FortiGate and FortiSandbox extend basic WAF protections through synchronization and sharing of threat information to both deeply scan suspicious files and share infected internal sources.

FortiWeb also provides integration with leading third-party vulnerability scanners including Acunetix, HP WebInspect, IBM AppScan, Qualys, IBM QRadar, and WhiteHat to provide dynamic virtual patches to security issues in application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules by FortiWeb to protect the application until developers can address them in the application code.

HIGHLIGHTS
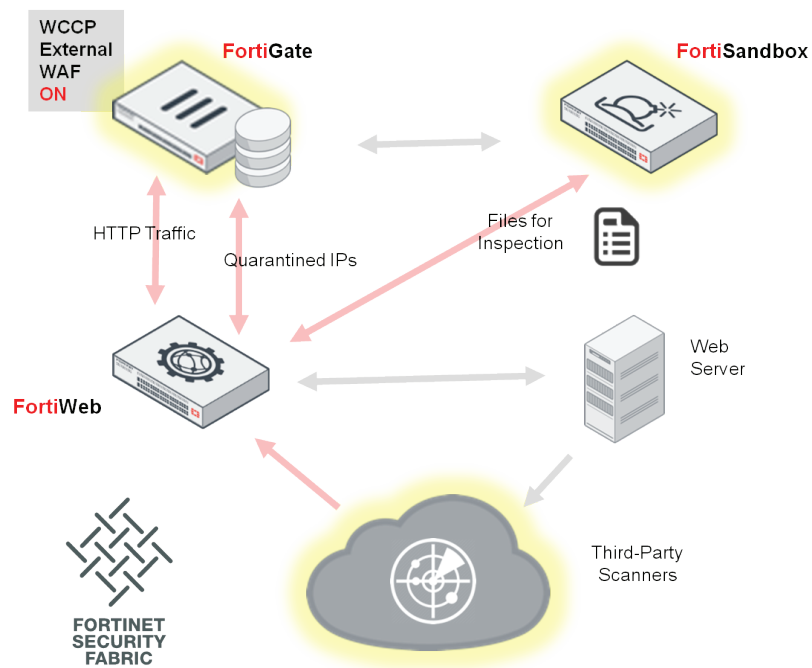
Integration with other Fortinet Security Fabric elements, including FortiGate and FortiSandbox, delivers APT protection and extends vulnerability scanning with leading third-party providers.

Solving the Challenge of False Threat Detections

False positive threat detections can be very disruptive and force many administrators to loosen security rules on their web application firewalls to the point where many often become a monitoring tool rather than a trusted threat avoidance platform. The installation of a WAF may take only minutes, however fine tuning can take days, or even weeks. Even after setup, a WAF can require regular check ups and tweaks as applications and the environment change.

FortiWeb takes this challenge head-on with advanced tools that can dramatically reduce incorrect event triggering due to false detections. Building on basic WAF protections such as whitelists, learning exceptions, user tracking, and alert tuning, FortiWeb adds new features including device fingerprinting/tracking, threat weighting, and syntax-based attack analysis that nearly eliminates many common false detection scenarios.

Secured by FortiGuard

Fortinet's Award-winning FortiGuard Labs is the backbone for many of FortiWeb's layers in its approach to application security. Offered as 5 separate options, you can choose the FortiGuard services you need to protect your web applications. FortiWeb IP Reputation service protects you from known attack sources like

botnets, spammers, anonymous proxies, and sources known to be infected with malicious software. FortiWeb Security Service is designed just for FortiWeb including items such as application layer signatures, malicious robots, suspicious URL patterns and web vulnerability scanner updates. Credential Stuffing Defense checks login attempts against FortiGuard's list of compromised credentials and can take actions ranging from alerts to blocking logins from suspected stolen user ids and passwords. The FortiSandbox Cloud subscription enables FortiWeb to integrate with Fortinet's cloud-sandbox service. Finally, FortiWeb offers FortiGuard's top-rated antivirus engine that scans all file uploads for threats that can infect your servers or other network elements.

VM and Cloud Options

FortiWeb provides maximum flexibility in supporting your virtual and hybrid environments. The virtual versions of FortiWeb support all the same features as our hardware-based devices and work with all the top hypervisors including VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen and KVM. FortiWeb is also available for Amazon Web Services and Microsoft Azure. Additionally, FortiWeb fully supports Fortinet's VM On-Demand Program for organizations that need maximum flexibility for virtual deployments.

FEATURES

Deployment options

- Reverse Proxy
- Inline Transparent
- True Transparent Proxy
- Offline Sniffing
- WCCP

Web Security

- Automatic profiling (white list)
- Web server and application signatures (black list)
- IP Reputation
- IP Geolocation
- HTTP RFC compliance
- Native support for HTTP/2

Application Attack Protection

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking
- Built-in Vulnerability Scanner
- Third-party scanner integration (virtual patching)

Security Services

- WWeb services signatures
- XML and JSON protocol conformance
- Malware detection
- Virtual patching
- Protocol validation
- Brute force protection
- Cookie signing and encryption
- Threat scoring and weighting
- Syntax-based SQLi detection
- HTTP Header Security
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- L4 Stateful Network Firewall
- DoS prevention
- Advanced correlation protection using multiple security elements
- Data leak prevention
- Web Defacement Protection

Application Delivery

- Layer 7 server load balancing
- URL Rewriting
- Content Routing
- HTTPS/SSL Offloading
- HTTP Compression
- Caching

Authentication

- Active and passive authentication
- Site Publishing and SSO
- RSA Access for 2-factor authentication
- LDAP and RADIUS support
- SSL client certificate support

Management and Reporting

- Web user interface
- Command line interface
- Central management for multiple FortiWeb devices
- Active/Active HA Clustering
- REST API
- Centralized logging and reporting
- User/device tracking
- Real-time dashboards
- Bot dashboard
- Geo IP Analytics
- SNMP, Syslog and Email Logging/Monitoring
- Administrative Domains with full RBAC

Other

- IPv6 Ready
- HTTP/2 to HTTP 1.1 translation
- HSM Integration
- High Availability with Config-sync for syncing across multiple active appliances
- Auto setup and default configuration settings for simplified deployment
- Setup Wizards for common applications and databases
- Preconfigured for common Microsoft applications; Exchange, SharePoint, OWA
- OpenStack support for FortiWeb VMs
- Predefined security policies for Drupal and Wordpress applications
- WebSockets support

SPECIFICATIONS

	FORTIWEB 100D	FORTIWEB 400D	FORTIWEB 600D	FORTIWEB 1000E
Hardware				
10/100/1000 Interfaces (RJ-45 ports)	4	4 GE RJ45, 4 SFP GE	4 GE RJ45 (2 bypass), 4 SFP GE	6 (4 bypass), 4x SFP GE (non-bypass)
10G BASE-SR SFP+ Ports	0	0	0	2
SSL/TLS Processing	Software	Software	Software	Hardware
USB Interfaces	2	2	2	2
Storage	16 GB	240 GB SSD	240 GB SSD	2x 2 TB
Form Factor	Desktop	1U	1U	2U
Power Supply	Single	Single	Dual	Dual Hot Swappable
System Performance				
Throughput	25 Mbps	100 Mbps	250 Mbps	1.3 Gbps
Latency	Sub-ms	Sub-ms	Sub-ms	Sub-ms
High Availability	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	0	32	32	64

All performance values are "up to" and vary depending on the system configuration.

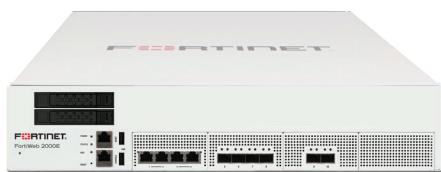|	FORTIWEB 100D	FORTIWEB 400D	FORTIWEB 600D	FORTIWEB 1000E
Dimensions				
Height x Width x Length (inches)	1.61 x 8.27 x 5.24	1.73 x 17.24 x 16.38	1.73 x 17.24 x 16.38	3.46 x 16.93 x 19.73
Height x Width x Length (mm)	41 x 210 x 133	44 x 438 x 416	44 x 438 x 416	88 x 430 x 501.20
Weight	2.3 lbs (1.1 kg)	22 lbs (9.97 kg)	22 lbs (9.97 kg)	28 lbs (12.8 kg)
Rack Mountable	Optional	Yes	Yes	Yes, with flanges
Environment				
Power Required	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Maximum Current	110V/1.2A, 220V/1.2A	100V/5A, 240V/3A	100V/5A, 240V/3A	100V/5A, 240V/3A
Power Consumption (Average)	18 W	109 W	109 W	140 W
Heat Dissipation	74 BTU/h	446.3 BTU/h	446.3 BTU/h	471 BTU/h
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-4–158°F (-20–70°C)
Humidity	10–90% non-condensing	10–90% non-condensing	10–90% non-condensing	5–90% non-condensing
Compliance				
Safety Certifications	FCC Class A Part 15, C-Tick, VCCI, CE, UL/cUL, CB	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL

FortiWeb 100D

FortiWeb 400D

FortiWeb 600D

FortiWeb 1000E

SPECIFICATIONS

	FORTIWEB 2000E	FORTIWEB 3000E	FORTIWEB 3010E	FORTIWEB 4000E
Hardware				
10/100/1000 Interfaces (RJ45 ports)	4 bypass, 4 SFP GE (non-bypass)	8 bypass, 4 SFP GE (non-bypass)	8 bypass, 4 SFP GE (non-bypass)	8 bypass, 4 SFP GE (non-bypass)
10G BASE-SR SFP+ Ports	2	4	4 (2 bypass)	4 (2 bypass)
SSL/TLS Processing	Hardware	Hardware	Hardware	Hardware
USB Interfaces	2	2	2	2
Storage	2x 1 TB	2x 2 TB	2x 2 TB	2x 2 TB
Form Factor	2U	2U	2U	2U
Power Supply	Dual Hot Swappable	Dual Hot Swappable	Dual Hot Swappable	Dual Hot Swappable
System Performance				
Throughput	2.5 Gbps	5 Gbps	5 Gbps	20 Gbps
Latency	Sub-ms	Sub-ms	Sub-ms	Sub-ms
High Availability	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	64	64	64	64

All performance values are "up to" and vary depending on the system configuration.

	FORTIWEB 2000E	FORTIWEB 3000E	FORTIWEB 3010E	FORTIWEB 4000E
Dimensions				
Height x Width x Length (inches)	3.5 x 17.2 x 20.8	3.5 x 17.5 x 22.6	3.5 x 17.5 x 22.6	3.5 x 17.5 x 22.6
Height x Width x Length (mm)	88 x 438 x 530	88 x 444 x 574	88 x 444 x 574	88 x 444 x 574
Weight	33 lbs (15 kg)	56.2 lbs (22.5 kg)	56.2 lbs (22.5 kg)	56.2 lbs (22.5 kg)
Rack Mountable	Yes	Yes	Yes	Yes
Environment				
Power Required	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Maximum Current	120V/6A, 240V/3A	120V/2.6A, 240V/1.3A	120V/2.6A, 240V/1.3A	120V/3A, 240V/1.5A
Power Consumption (Average)	200 W	200 W	200 W	248.5 W
Heat Dissipation	1433 BTU/h	1045.5 BTU/h	1045.5 BTU/h	1219.8 BTU/h
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)
Humidity	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing
Compliance				
Safety Certifications	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL,	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL,

FortiWeb 2000E

FortiWeb 3000E

FortiWeb 3010E

FortiWeb 4000E

www.fortinet.com

SPECIFICATIONS

	FORTIWEB-VM (1 VCPU)	FORTIWEB-VM (2 VCPU)	FORTIWEB-VM (4 VCPU)	FORTIWEB-VM (8 VCPU)
System Performance				
HTTP Throughput	25 Mbps	100 Mbps	500 Mbps	2 Gbps
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	4 to 64 based on the amount of memory allocated			
Virtual Machine				
Hypervisor Support	VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure. Please see FortiWeb VM Installation Guide for versions supported.			
vCPU Support (Minimum / Maximum)	1	2	2 / 4	2 / 8
Network Interface Support (Minimum / Maximum)	1 / 4 (10 VMware ESX)	1 / 4 (10 VMware ESX)	1 / 4 (10 VMware ESX)	1 / 4 (10 VMware ESX)
Storage Support (Minimum / Maximum)	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB
Memory Support (Minimum / Maximum)	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit
Recommended Memory	4 GB	4 GB	4 GB	4 GB
High Availability Support	Yes	Yes	Yes	Yes

Actual performance values may vary depending on the network traffic and system configuration. Performance metrics were observed using a Dell PowerEdge R710 server (2x Intel Xeon E5504 2.0 GHz 4 MB Cache) running VMware ESXi 5.5 with 4 GB of vRAM assigned to the 4 vCPU and 8 vCPU FortiWeb Virtual Appliance and 4 GB of vRAM assigned to the 2 vCPU FortiWeb Virtual Appliance.

ORDER INFORMATION

Product	SKU	Description
FortiWeb 100D	FWB-100D	Web Application Firewall — 4x GE RJ45 ports, 16 GB storage.
FortiWeb 400D	FWB-400D	Web Application Firewall — 4x GE RJ45 ports, 4x GE SFP ports, 240 GB SSD storage.
FortiWeb 600D	FWB-600D	Web Application Firewall — 4x GE RJ45 ports (2x bypass), 4x GE SFP ports, 240 GB SSD storage.
FortiWeb 1000E	FWB-1000E	Web Application Firewall — 2x 10 GE SFP+ ports, 2x GE RJ45 ports, 4x GE RJ45 bypass ports, 4x GE SFP ports, dual AC power supplies, 2 TB storage.
FortiWeb 2000E	FWB-2000E	Web Application Firewall — 2x 10 GE SFP+ ports, 4x GE RJ45 bypass ports, 4x GE SFP ports, dual AC power supplies, 2 TB storage.
FortiWeb 3000E	FWB-3000E	Web Application Firewall — 4x 10 GE SFP+ ports, 8x GE RJ45 bypass ports, 4x GE SFP ports, dual AC power supplies, 2x 2 TB storage.
FortiWeb 3010E	FWB-3010E	Web Application Firewall — 8x GE RJ45 bypass ports, 4x GE SFP ports, 2x 10G SFP+ bypass ports, 2x 10G SFP+ ports, dual AC power supplies, 2x 2 TB HDD storage.
FortiWeb 4000E	FWB-4000E	Web Application Firewall — 8x GE RJ45 bypass ports, 4x GE SFP ports, 2x 10G SFP+ bypass ports, 2x 10G SFP+ ports, dual AC power supplies, 2x 2 TB HDD storage.
FortiWeb-VM01	FWB-VM01	FortiWeb-VM, up to 1 vCPU supported. 64-bit OS.
FortiWeb-VM02	FWB-VM02	FortiWeb-VM, up to 2 vCPUs supported. 64-bit OS.
FortiWeb-VM04	FWB-VM04	FortiWeb-VM, up to 4 vCPUs supported. 64-bit OS.
FortiWeb-VM08	FWB-VM08	FortiWeb-VM, up to 8 vCPUs supported. 64-bit OS.
Central Manager 10	FWB-CM-BASE	FortiWeb Central Manager license key, manage up to 10 FortiWeb devices, VMware vSphere.
Central Manager Unlimited	FWB-CM-UL	FortiWeb Central Manager license key, manage unlimited number of FortiWeb devices, VMware vSphere.