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

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
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 |

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

APPLICATION

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.

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

**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.

**Advanced Graphical Analysis and Reporting**

FortiWeb includes a suite of graphical analysis tools called FortiView. Similar to other Fortinet products such as FortiGate, FortiWeb gives administrators the ability to visualize and drill-down into key elements of FortiWeb such as server/IP configurations, attack and traffic logs, attack maps, and user activity. FortiView for FortiWeb 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.

**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.

Also available as a cloud-based subscription service, FortiWeb Cloud is a convenient and easy-to-deploy WAF that’s always up-to-date. For organizations that need to quickly deploy a WAF and keep maintenance to a minimum, FortiWeb Cloud scales to meet traffic demands without the hassles of managing hardware and software. Nearly a “set-and-forget” WAF, FortiWeb Cloud delivers basic web application functionality for smaller applications and distributed applications that are difficult to manage. Please note that FortiWeb Cloud does not support the entire feature set included in the hardware and VM versions. Please contact us for more information.
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)
- File upload scanning with AV and sandbox

Security Services
- Web 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, RADIUS, and SAML support
- SSL client certificate support
- CAPTCHA and Real Browser Enforcement (RBE)

Management and Reporting
- Web user interface
- Command line interface
- FortiView graphical analysis and reporting tools
- 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
- Seamless PKI integration
- Attachment scanning for ActiveSync and OWA applications
- 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

<table>
<thead>
<tr>
<th></th>
<th>FORTIWEB 100D</th>
<th>FORTIWEB 400D</th>
<th>FORTIWEB 600D</th>
<th>FORTIWEB 1000D</th>
<th>FORTIWEB 1000E</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/100 Interfaces (RJ-45 ports)</td>
<td>4</td>
<td>4  GE RJ45, 4 SFP GE</td>
<td>4  GE RJ45 (2 bypass), 4 SFP GE</td>
<td>6 (4 bypass), 2x SFP GE (non-bypass)</td>
<td>6 (4 bypass), 2x SFP GE (non-bypass)</td>
</tr>
<tr>
<td>10G BASE-SR SFP+ Ports</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>High Availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Licenses</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Administrative Domains</td>
<td>0</td>
<td>32</td>
<td>32</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td><strong>System Performance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Throughput</td>
<td>25 Mbps</td>
<td>100 Mbps</td>
<td>250 Mbps</td>
<td>1 Gbps</td>
<td>1.3 Gbps</td>
</tr>
<tr>
<td>Latency</td>
<td>Sub-ms</td>
<td>Sub-ms</td>
<td>Sub-ms</td>
<td>Sub-ms</td>
<td>Sub-ms</td>
</tr>
<tr>
<td>High Availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Licenses</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Administrative Domains</td>
<td>0</td>
<td>32</td>
<td>32</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height x Width x Length (inches)</td>
<td>1.61 x 8.27 x 5.24</td>
<td>1.73 x 17.24 x 16.38</td>
<td>1.73 x 17.24 x 16.38</td>
<td>3.50 x 17.24 x 14.49</td>
<td>3.46 x 16.93 x 19.73</td>
</tr>
<tr>
<td>Height x Width x Length (mm)</td>
<td>41 x 210 x 133</td>
<td>44 x 438 x 416</td>
<td>44 x 438 x 416</td>
<td>86 x 438 x 368</td>
<td>88 x 430 x 501.20</td>
</tr>
<tr>
<td>Weight</td>
<td>2.3 lbs (1.1 kg)</td>
<td>22 lbs (9.97 kg)</td>
<td>22 lbs (9.97 kg)</td>
<td>27.6 lbs (12.5 kg)</td>
<td>28 lbs (12.8 kg)</td>
</tr>
<tr>
<td>Rack Mountable</td>
<td>Optional</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes, with flanges</td>
<td>Yes, with flanges</td>
</tr>
<tr>
<td><strong>Environment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Required</td>
<td>100–240V AC, 50–60 Hz</td>
<td>100–240V AC, 50–60 Hz</td>
<td>100–240V AC, 50–60 Hz</td>
<td>100–240V AC, 50–60 Hz</td>
<td>100–240V AC, 50–60 Hz</td>
</tr>
<tr>
<td>Maximum Current</td>
<td>110W/7.2A, 220V/1.2A</td>
<td>200W/5A, 240V/3A</td>
<td>300W/5A, 240V/3A</td>
<td>200W/5A, 240V/3A</td>
<td>300W/5A, 240V/3A</td>
</tr>
<tr>
<td>Power Consumption (Average)</td>
<td>18 W</td>
<td>109 W</td>
<td>109 W</td>
<td>115 W</td>
<td>140 W</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>74 BTU/h</td>
<td>446.3 BTU/h</td>
<td>446.3 BTU/h</td>
<td>471 BTU/h</td>
<td>471 BTU/h</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>32–104°F (-0°C–40°C)</td>
<td>32–104°F (-0°C–40°C)</td>
<td>32–104°F (-0°C–40°C)</td>
<td>32–104°F (-0°C–40°C)</td>
<td>32–104°F (-0°C–40°C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>10–90% non-condensing</td>
<td>10–90% non-condensing</td>
<td>10–90% non-condensing</td>
<td>5–95% non-condensing</td>
<td>5–90% non-condensing</td>
</tr>
<tr>
<td>Compliance</td>
<td>Safety Certifications</td>
<td>FCC Class A Part 15, C-Tick, VCCI, CE, UL/cUL, GB</td>
<td>FCC Class A Part 15, C-Tick, VCCI, CE, UL/cUL, GB</td>
<td>FCC Class A Part 15, C-Tick, VCCI, CE, UL/cUL, GB</td>
<td>FCC Class A Part 15, C-Tick, VCCI, CE, UL/cUL, GB</td>
</tr>
</tbody>
</table>

All performance values are “up to” and vary depending on the system configuration.
## SPECIFICATIONS

<table>
<thead>
<tr>
<th></th>
<th>FORTIWEB 2000E</th>
<th>FORTIWEB 3000E</th>
<th>FORTIWEB 3010E</th>
<th>FORTIWEB 4000E</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/100/1000 Interfaces (RJ45 ports)</td>
<td>4 bypass, 4 SFP GE (non-bypass)</td>
<td>8 bypass, 4 SFP GE (non-bypass)</td>
<td>8 bypass, 4 SFP GE (non-bypass)</td>
<td>8 bypass, 4 SFP GE (non-bypass)</td>
</tr>
<tr>
<td>SFP/GE Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USB Interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Form Factor</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Dual Hot Swappable</td>
<td>Dual Hot Swappable</td>
<td>Dual Hot Swappable</td>
<td>Dual Hot Swappable</td>
</tr>
<tr>
<td><strong>System Performance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Throughput</td>
<td>2.5 Gbps</td>
<td>5 Gbps</td>
<td>5 Gbps</td>
<td>20 Gbps</td>
</tr>
<tr>
<td>Latency</td>
<td>Sub-ms</td>
<td>Sub-ms</td>
<td>Sub-ms</td>
<td>Sub-ms</td>
</tr>
<tr>
<td>High Availability</td>
<td>Active/Passive, Active/Active Clustering</td>
<td>Active/Passive, Active/Active Clustering</td>
<td>Active/Passive, Active/Active Clustering</td>
<td>Active/Passive, Active/Active Clustering</td>
</tr>
<tr>
<td>Application Licenses</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Administrative Domains</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height x Width x Length (inches)</td>
<td>3.5 x 17.2 x 20.8</td>
<td>3.5 x 17.5 x 22.6</td>
<td>3.5 x 17.5 x 22.6</td>
<td>3.5 x 17.5 x 22.6</td>
</tr>
<tr>
<td>Height x Width x Length (mm)</td>
<td>88 x 438 x 530</td>
<td>88 x 444 x 574</td>
<td>88 x 444 x 574</td>
<td>88 x 444 x 574</td>
</tr>
<tr>
<td>Weight</td>
<td>33 lbs (15 kg)</td>
<td>56.2 lbs (25.5 kg)</td>
<td>56.2 lbs (25.5 kg)</td>
<td>56.2 lbs (25.5 kg)</td>
</tr>
<tr>
<td>Rack Mountable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Environment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Required</td>
<td>100–240V AC, 60–50 Hz</td>
<td>100–240V AC, 60–50 Hz</td>
<td>100–240V AC, 60–50 Hz</td>
<td>100–240V AC, 60–50 Hz</td>
</tr>
<tr>
<td>Maximum Current</td>
<td>120W/6A, 240W/3A</td>
<td>120W/6A, 240W/3A</td>
<td>120W/6A, 240W/3A</td>
<td>120W/6A, 240W/3A</td>
</tr>
<tr>
<td>Power Consumption (Average)</td>
<td>200 W</td>
<td>200 W</td>
<td>200 W</td>
<td>245.5 W</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>1433 BTU/h</td>
<td>1045.5 BTU/h</td>
<td>1219.8 BTU/h</td>
<td>1219.8 BTU/h</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>32–104°F (0–40°C)</td>
<td>32–104°F (0–40°C)</td>
<td>32–104°F (0–40°C)</td>
<td>32–104°F (0–40°C)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-13–158°F (-25–70°C)</td>
<td>-13–158°F (-25–70°C)</td>
<td>-13–158°F (-25–70°C)</td>
<td>-13–158°F (-25–70°C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>5–95% non-condensing</td>
<td>5–95% non-condensing</td>
<td>5–95% non-condensing</td>
<td>5–95% non-condensing</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All performance values are “up to” and vary depending on the system configuration.
## SPECIFICATIONS

### HTTP Throughput
<table>
<thead>
<tr>
<th>FORTIWEB-VM (1 VCPU)</th>
<th>FORTIWEB-VM (2 VCPU)</th>
<th>FORTIWEB-VM (4 VCPU)</th>
<th>FORTIWEB-VM (8 VCPU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 Mbps</td>
<td>100 Mbps</td>
<td>500 Mbps</td>
<td>2 Gbps</td>
</tr>
</tbody>
</table>

### Application Licenses
- VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure.

### Administrative Domains
- 4 to 64 based on the amount of memory allocated

### Virtual Machine
- **Hyervisor Support**: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure.

### System Performance

#### Storage Support
- Minimum / Maximum: 40 GB / 2 TB

#### Memory Support
- Minimum / Maximum: 1,024 MB / Unlimited for 64-bit

#### CPU Support
- Minimum / Maximum: 2 / 4

### ORDER INFORMATION

#### Product | SKU | Description
--- | --- | ---
FortiWeb 100D | FWA-100D | Web Application Firewall — 4x GE RJ45 ports, 16 GB storage.
FortiWeb 1000D | FWA-1000D | Web Application Firewall — 10 GE RJ45 ports, 4x GE SFP ports, dual AC power supplies, 2 TB storage.
FortiWeb 1000E | FWA-1000E | Web Application Firewall — 10 GE RJ45 ports, 4x GE SFP ports, dual AC power supplies, 2 TB storage.
FortiWeb 4000E | FWA-4000E | Web Application Firewall — 40 GE RJ45 ports, 4x GE SFP ports, dual AC power supplies, 2 TB storage.
FortiWeb 6000E | FWA-6000E | Web Application Firewall — 60 GE RJ45 ports, 4x GE SFP ports, dual AC power supplies, 2 TB storage.
FortiWeb 100D | FWA-100D | Web Application Firewall — 10 GE RJ45 ports, 4x GE SFP ports, 240 GB SSD storage.
FortiWeb 200D | FWA-200D | Web Application Firewall — 20 GE RJ45 ports, 4x GE SFP ports, 240 GB SSD storage.
FortiWeb 400D | FWA-400D | Web Application Firewall — 40 GE RJ45 ports, 4x GE SFP ports, 240 GB SSD storage.
FortiWeb 600D | FWA-600D | Web Application Firewall — 60 GE RJ45 ports, 4x GE SFP ports, 240 GB SSD storage.
FortiWeb 1000D | FWA-1000D | Web Application Firewall — 100 GE RJ45 ports, 4x GE SFP ports, 240 GB SSD storage.
FortiWeb 4000D | FWA-4000D | Web Application Firewall — 400 GE RJ45 ports, 4x GE SFP ports, 240 GB SSD storage.
FortiWeb 6000D | FWA-6000D | Web Application Firewall — 600 GE RJ45 ports, 4x GE SFP ports, 240 GB SSD storage.

#### Application Licenses
- FortiWeb Central Manager License — manage up to 10 FortiWeb devices, VMware vSphere.
- FortiWeb-VM — 1 VCPU, 2 VCPU, 4 VCPU, 8 VCPU.

#### Memory Support
- Minimum / Maximum: 4 GB / 4 GB

#### Recommended Memory
- 50 Mbps
- 500 Mbps

#### High Availability Support
- Yes

### Copyright Notice
Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet® and FortiGate® are registered trademarks of Fortinet, Inc. in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other claims herein were obtained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics. In such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant thereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.