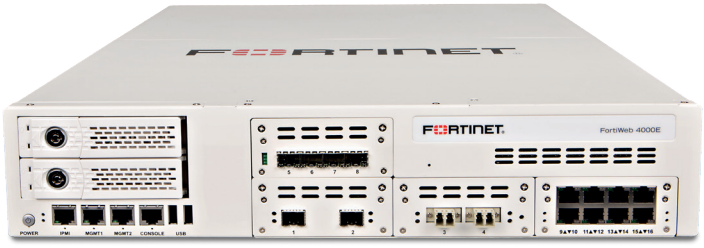
FortiWeb™

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

FortiWeb 是一款Web应用防火墙（WAF），可保护托管的Web应用免受针对已知和未知漏洞的攻击。FortiWeb 使用人工智能增强的多层次和关联检测方法，为应用程序提供针对已知漏洞和零日威胁的防护。



无以伦比的防护效能

多核处理器技术与基于硬件的SSL工具相结合，提供超高的 WAF 安全过滤吞吐性能 。

应用程序防护

防御 OWASP 排名前十的应用程序攻击，包括跨站点脚本攻击和 SQL 注入攻击 。

基于人工智能的机器学习威胁检测

采用双层机器学习引擎来检测应用请求异常并确定它们是否构成威胁。

亮点

- 运用基于人工智能的行为扫描关联威胁检测
- WAF 安全过滤吞吐性能高达 20 Gbps
- 通过与 Fortinet Security Fabric 集成提高防护能力
- 可视化分析工具发现高级威胁
- 第三方集成和虚拟补丁技术

FortiCare 全球全天支持
support.fortinet.com

FortiGuard 安全服务
www.fortiguard.com

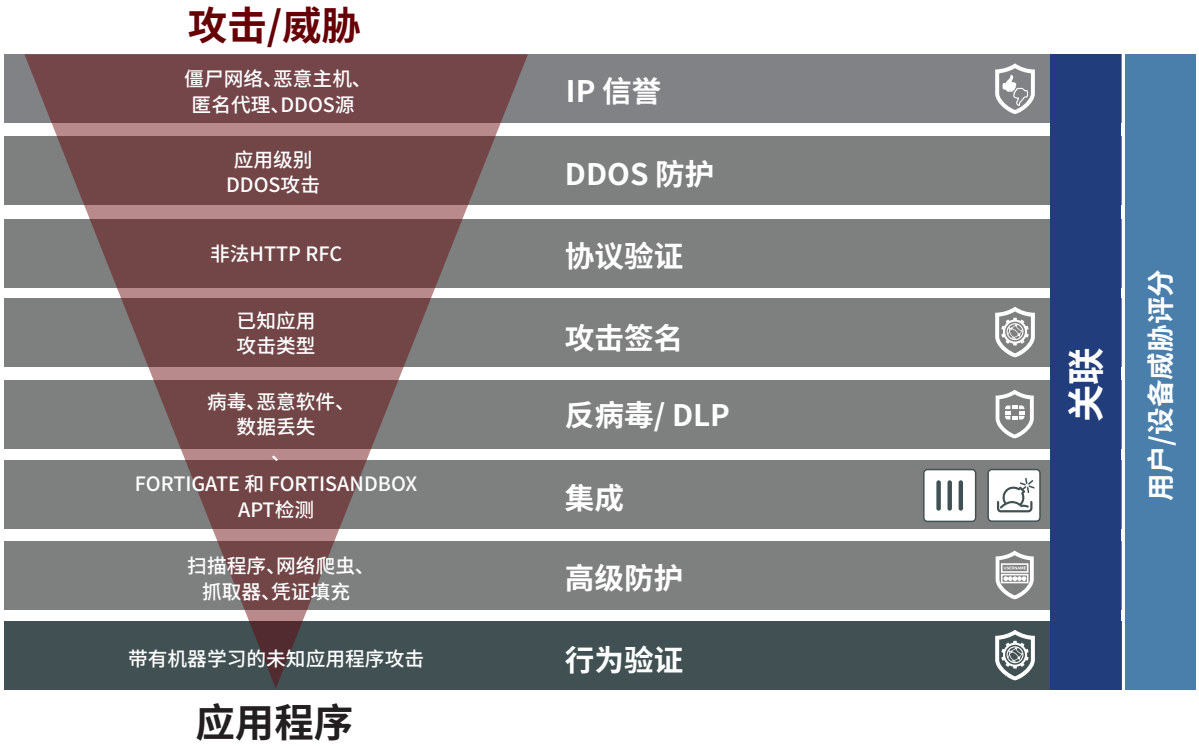
第三方认证

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

亮点

FortiWeb 提供全面的 Web 应用安全防护

FortiWeb 运用先进的多层次关联检测方法为您的外部和内部web应用提供完整的安全防护，防御 OWASP 排名前十的应用程序攻击和许多其他威胁。FortiWeb 的核心是基于人工智能的检测引擎使用机器学习来识别偏离正常模式的请求，并采取措施保护应用程序免受已知和未知的零日威胁。



FortiWeb 的多层次关联威胁检测方法可针对以应用程序漏洞为攻击目标的已知和未知零日威胁提供安全防护。

由FortiGuard威胁研究与响应实验室支持的双层机器学习模型

尽管 Web 应用防火墙是针对基于Web应用的攻击的最佳防御手段，但是为了防止 WAF 误判而进行的微调却会相当繁琐而耗时。FortiWeb 通过两个独立的检测引擎，使用基于人工智能的机器学习方法解决了这一难题。

第一层自动和动态地监视所有应用程序元素的活动是否偏离了预测的条目。如果第一个引擎标记出确定为异常的内容，则将其发送到第二层机器学习层，以评估它是威胁还是仅仅是一个此前未见的良性变化，例如输入错误或新字符。如果是攻击，那么 FortiWeb 可以采取行动，例如记录、警报和/或阻断请求。第二个机器学习层利用包含在 FortiWeb 解决方案中的威胁模型，并通过 FortiGuard WAF 安全服务进行更新，以提供需要模型重新训练和测试的新威胁保护。