

產品 › 安全性

高級Web 應用防火牆 (WAF)

使用行為分析、主動式Bot 防禦和敏感數據應用層加密（例如憑據）抵禦最新一波攻擊。遭受到了攻擊？請撥打(866) 329-4253 或+1 (206) 272-7969

閱讀概述

獨一無二的功能
讓我們脫穎而出。

F5 高級WAF 可識別並攔截其他 WAF 解決方案遺漏的攻擊。

[觀看視頻](#) ›

高級應用防護

高級WAF 結合了機器學習、威脅智能及應用深層專業知識。

主動式Bot 防禦

保護應用免遭Bot 及其他惡意工具的自動攻擊。

防Bot 移動軟件開發工具包(SDK)

通過白名單、行為分析、安全Cookie 驗證和高級應用強化，保護移動應用。

瀏覽器內數據加密

在應用層加密數據，以抵禦數據提取惡意軟件和瀏覽器中間人攻擊。

行為DoS

API 協議安全

OWASP 十大防護

防護憑據盜竊

抵禦利用盜竊憑據發起的



行為分析和機器學習提供
高精度的應用層(L7) DoS
檢測和緩解。

部署用於保護
REST/JSON、XML 和
GWT API 的工具。

保護重要應用，對抗當今
最大的安全隱患（即
OWASP 十大漏洞）。

為何選擇高級 WAF？

保護您的應用免遭
最常見的攻擊，無
需升級應用本身

[閱讀白皮書](#) >

自動攻擊與Bot

自動攻擊與Bot 會耗盡
應用資源。

憑據盜竊

盜竊應用憑據或利用盜
用帳號的攻擊。

向移動客戶端 發起的攻擊

以基於瀏覽器的客戶端
和移動客戶端為對象的
Bot。

應用層攻擊

應用層攻擊可繞開簽名
和基於信譽的安全解決
方案。

Web 應用和API 攻擊

由於快速採用API 而產
生的新攻擊面和威脅。

有針對性的攻 擊活動

主動攻擊活動很難從單
一攻擊中檢測到。

F5 在“THE FORRESTER WAVE™：2018 年第二季度WEB 應用防火牆”(THE FORRESTER WAVE™: WEB APPLICATION FIREWALLS, Q2 2018) 中獲評為領導者

[獲取報告](#)

購買方式

多種靈活部署與管
理選項，滿足您的
特定需求

[查看購買選項](#) >



軟件

部署至您數據中心或您
私有云中的主流管理程
序。

[了解更多](#) >



公有云

適用於公有云優選提供
商，包括 [Amazon Web Services \(AWS\)](#)、
[Microsoft Azure](#)或
[Google Cloud Platform](#)。

[了解更多](#) >



作為服務

Silverline Web 應用防火
牆是一種基於雲的
WAF，可自託管或由F5



硬件



SOC 中的認證專家託管。

[了解更多 >](#)

運行於高性能硬件之上，以保護您的應用。

[了解更多 >](#)

阻止憑據盜竊

數據安全加密可阻止憑據和數據盜竊

[了解詳情>](#)

集中化安全管理

BIG-IQ 可實現對整個F5 高級WAF 部署的整體控制。

[探索BIG-IQ >](#)

阻止憑據盜竊

數據安全加密可阻止憑據和數據盜竊

[了解詳情](#)

立即開始

請求演示

查看實際使用中的高級WAF

即刻聯絡F5

開始試用

在您的環境中試用高級WAF

免費試用

準備好購買了嗎？

與F5 代表交流

聯繫F5 銷售人員

您的應用應該是- 快速、可用且安全- 可在任何云中配置。



F5 擁有20 餘年的應用交付服務經驗，無論在本地還是跨任何多雲環境，均可為企業級應用提供廣泛的服務和安全組合。

是否有疑問？
支持與銷售

關注我們

48 家財富50 強公司
仰賴F5

85 個辦事處分設於
43 個國家/地區

20 餘年堅持保護應用

關於F5

- 企業信息
- 新聞中心
- 投資者關係
- 就業機會
- 聯繫信息
- 通信偏好
- 認證
- 多元化與包容性

教育

- 培訓
- 認證
- LearnF5
- 免費在線培訓

F5 站點

- F5.com
- DevCentral
- 支持門戶
- 合作夥伴中心
- F5 實驗室

©2020 F5, Inc. 保留所有權利。