

BIG-IP Application Security Manager

PRODUCT OVERVIEW



“F5 has really helped us become more aggressive in tuning our devices for our security needs. Now we do a much better job of blocking bad traffic while allowing valid traffic.”

Stuart Lyons, Security Engineer at Human Kinetics

Defend Against Web Attacks and Achieve Regulatory Compliance

Key benefits

- Ensure application availability by stopping attacks from any location
- Reduce the cost of security compliance
- Get out-of-the-box application security policies with minimal configuration
- Improve application security and performance
- Deploy flexibly for virtualized and private cloud environments
- Increase agility

With the continued growth of web application traffic, an increasing amount of sensitive data is exposed to potential theft, security vulnerabilities, and multi-layer attacks. Protect your organization and its reputation by maintaining the confidentiality, availability, and performance of the applications that are critical to your business.

F5 BIG-IP® Application Security Manager™ (ASM) is a flexible web application firewall that secures web applications in traditional, virtual, and private cloud environments. BIG-IP ASM provides unmatched web application and website protection, helps secure deployed applications against unknown vulnerabilities, and enables compliance for key regulatory mandates—all on a platform that consolidates application delivery with data center firewall capabilities, and network and application access control.



Deliver comprehensive security

BIG-IP ASM blocks web application attacks in minutes, to help protect against a broad spectrum of threats, including the latest distributed denial-of-service (DDoS) and SQL injection attacks. It also helps secure interactive web applications that use the latest coding, such as AJAX widgets and JSON payloads. Advanced vulnerability assessment integrations can scan web applications and BIG-IP ASM patches vulnerabilities in minutes to help protect against web threats. BIG-IP ASM stops hackers and attacks from any location and ensures that legitimate users can access applications.

Achieve compliance cost-effectively

Advanced, built-in security protection and remote auditing help your organization comply with industry security standards, including PCI DSS, HIPAA, Basel II, and SOX,

in a cost-effective way—without requiring multiple appliances, application changes, or rewrites. Detailed PCI reporting determines if PCI DSS compliance is being met and it guides administrators through the necessary steps to become compliant.

Get out-of-the-box protection

Equipped with a set of pre-built and certified application security policies, BIG-IP ASM gives you out-of-the box protection for common applications such as Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials, and Microsoft Office SharePoint. A rapid deployment policy secures any internal or third-party application.

Improve performance

Unlike many other security solutions, with BIG-IP ASM you don't have to choose between security and performance. The

F5 TMOS® architecture provides significant performance advantages, including SSL offload, caching, compression, TCP optimization, and more. BIG-IP® Local Traffic Manager™ integration enables protection from DDoS and other network attacks, and delivers data center firewall capabilities. And because BIG-IP ASM works on the same platform with other BIG-IP® modules, you can benefit from centralized, secure access control and even greater performance improvements.

Deploy flexibly and increase business agility

BIG-IP ASM Virtual Edition (VE) deploys in flexible environments, protecting your virtual and private cloud applications. By automatically building and managing security policies around newly discovered vulnerabilities, BIG-IP ASM deploys fast, agile business processes to secure your applications against constantly changing threats.

BIG-IP ASM features

Security and implementation

- Geolocation-based blocking
- Integrated XML firewall
- DataGuard™ and cloaking
- OneConnect™ aggregates requests to connections
- Live update for attack signatures
- Web scraping protection
- Data center firewall solution
- Application policy templates
- ICAP support for SMTP and SOAP files
- BIG-IP modules layering
- Session-based enforcement and reporting
- Advanced vulnerability assessment integrations
- BIG-IP ASM Virtual Edition
- Application security in the private cloud
- PCI reporting
- Incidents combined with violation correlation

Performance and configuration

- SSL offload
- Caching and compression
- iRules® and Fast Cache™
- TCP/IP optimization
- L7 Rate Shaping™
- Isolated resource allocation (vCMP™)
- iApps™ for pre-configured policies
- Application visibility and reporting

Comprehensive attack protection

- Cross-site request forgery
- Layer 7 DDoS
- Cross-site scripting
- SQL injection
- Parameter and HPP tampering
- Session highjacking
- Cookie manipulation
- Forceful browsing
- XML bombs/DoS

Learn more

For more information about BIG-IP ASM, use the search function on f5.com to find these resources.

Datasheets

[BIG-IP® Application Security Manager™](#)

[BIG-IP® Add-On Modules](#)

White papers

[Intelligent Layer 7 DoS and Brute Force Protection for Web Applications](#)

[Application and Data Security with F5 BIG-IP ASM and Oracle Database Firewall](#)

[Application Security in the Cloud with BIG-IP ASM](#)

Case study

[Human Kinetics Boosts Website Performance, Security, and Innovation with F5 Solution](#)

Article

[SC Magazine, 2010 Reader Trust Award for Best Web Application Security](#)

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com



IT agility. Your way.®