

BIG-IP Application Security Manager

PRODUCT OVERVIEW



“At the time of deployment, we can secure critical applications proactively and rapidly, directly through BIG-IP ASM, which saves us a lot in terms of rollout time and resources.”

Philippe Bossut, Network System Manager, Crédit Coopératif

Achieve Compliance with High Performance Application Security

Key benefits

- Reduce the cost of security compliance
- Ensure application availability by stopping hackers and attacks

- Get out-of-the-box application security policies with minimal configuration
- Improve application security and performance

- Handle changing threats with greater agility

As more application traffic moves over the web, sensitive data is exposed to theft, security vulnerabilities, and attacks, especially at the application layer.

F5 BIG-IP® Application Security Manager™ (ASM) is an advanced web application firewall that significantly reduces and mitigates the risk of loss or damage to data, intellectual property, and web applications. BIG-IP ASM provides unmatched application and website protection, a complete attack expert system, and compliance for key regulatory mandates—all on a platform that consolidates application delivery with network and application acceleration and optimization.

The result is the industry's most comprehensive web application security and application integrity solution. The award-winning BIG-IP ASM solution protects your organization and its reputation by maintaining the confidentiality, availability, and performance of the applications that are critical to your business.

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 provides steps required to become compliant if not.

Deliver comprehensive security

BIG-IP ASM patches web application vulnerabilities in minutes to protect from a broad spectrum of threats, including the latest (D)DoS, brute force, and SQL injection attacks as well as cross-site request forgery. A complete attack expert system provides on-the-spot attack details, staging of new policies for testing, and

quick administrator notification. This advanced application-layer gateway stops hackers and attacks and ensures legitimate users can access applications.

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 with zero configuration time.

Improve performance

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

F5 TMOS® architecture provides significant performance advantages, including SSL offload, caching, compression, TCP optimization, and more. Fast Cache™ integration enables cache blocking to save time and expense. And because BIG-IP ASM works on the same platform with other BIG-IP® modules, you can benefit from centralized access control and even greater performance improvements.

Increase business agility

BIG-IP ASM automatically builds and manages security policies around newly discovered vulnerabilities, deploying fast, agile business processes without manual intervention. TMOS architecture gives you unprecedented control and flexibility in securing your applications against constantly changing threats.

BIG-IP ASM features

- PCI reporting
- Integrated XML firewall
- DataGuard™ and cloaking
- Live update for attack signatures
- Web scraping protection
- Human readable policies (remote audit)
- Web services encryption/decryption and digital signature verification
- Application Ready Solution policy templates
- ICAP support
- BIG-IP modules layering
- iRules™ and Fast Cache integrations
- WhiteHat Sentinel integration
- F5 TMOS architecture
 - SSL offload
 - Caching
 - Compression
- iRules™
- TCP/IP optimization
- L7 Rate Shaping™
- IPv6 Gateway™
- Comprehensive attack protection
 - Cross-site request forgery
 - Layer 7 DoS
 - Brute force
 - Cross-site scripting
 - SQL injection
 - Parameter and HPP tampering
 - Session hijacking
 - Buffer overflows
 - Cookie manipulation
 - Various encoding attacks
 - Forceful browsing
 - XML bombs/DoS

Learn more about BIG-IP ASM

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 paper

[Manageable Application Security](#)

Case study

[Crédit Coopératif Secures Its Online Banking Services](#)

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.