

# 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

## Protect Your Business with High Performance Application Security

### Key benefits:

- Ensure application availability by stopping hackers and attacks
- Handle changing threats with greater agility
- Reduce the costs of meeting security compliance requirements
- Improve application security and performance
- Get out-of-the-box application security policies with minimal configuration

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

F5's 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 end-to-end application protection, advanced monitoring, and centralized reporting, and it addresses key regulatory mandates.

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

## Deliver comprehensive security

With BIG-IP ASM, you get integrated attack prevention from the latest layer 7 DoS and brute force attacks, along with advanced protocol protection. BIG-IP ASM mitigates a broad spectrum of attacks like SQL injection and cross-site scripting and provides a comprehensive set of pre-defined, validated Application Ready Solution security policy templates. As an advanced, application layer gateway, BIG-IP ASM stops hackers and attacks while ensuring that legitimate users can access the applications they need.

## Increase business agility

BIG-IP ASM automatically builds and manages security policies around newly discovered vulnerabilities, deploying fast, agile business processes without manual intervention. Running on F5's intelligent and powerful TMOS™ architecture,

BIG-IP ASM gives you unprecedented control and flexibility in securing your applications against constantly changing threats.

## Achieve compliance cost-effectively

Advanced, built-in security protection helps your organization comply with industry security standards, including PCI DSS, HIPAA, Basel II, and SOX, in a cost-effective way—without requiring multiple appliances and with no application changes or rewrites.

## Improve performance

Unlike many other security solutions, with BIG-IP ASM you don't have to choose between security and performance. TMOS architecture provides significant performance advantages, including SSL offload, caching, compression, TCP optimization, and more. And because

BIG-IP ASM works on the same platform with BIG-IP® WebAccelerator™, you can gain even greater performance improvements while benefitting from optimized server utilization and cost savings.

## 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.

## BIG-IP ASM Features

- Real-time traffic policy builder
- Integrated XML firewall
- Data guard and cloaking
- WhiteHat Sentinel integration
- Live update for attack signatures
- SMTP and FTP security
- Application Ready Solution policy templates
- URI latency monitoring and reporting
- BIG-IP WebAccelerator integration
- F5 TMOS architecture
  - SSL offload
  - Caching
  - Compression
  - iRules™
  - TCP/IP optimization
  - L7 Rate Shaping™
- IPv6 Gateway™
- IP/port filtering
- Comprehensive attack prevention
  - Layer 7 DoS
  - Brute force
  - Cross-site scripting
  - SQL injection
  - Parameter tampering
  - Session highjacking
  - 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](http://F5.com) to find these resources.

### Datasheets

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

[BIG-IP® Add-On Modules](#)

### White Paper

[Web Application Vulnerabilities and Avoiding Application Exposure](#)

### Case Study

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

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 [www.f5.com](http://www.f5.com)

F5 Networks, Inc.  
Corporate Headquarters  
[info@f5.com](mailto:info@f5.com)

F5 Networks  
Asia-Pacific  
[info.asia@f5.com](mailto:info.asia@f5.com)

F5 Networks Ltd.  
Europe/Middle-East/Africa  
[emeainfo@f5.com](mailto:emeainfo@f5.com)

F5 Networks  
Japan K.K.  
[f5j-info@f5.com](mailto:f5j-info@f5.com)



IT agility. Your way.