



## What's Inside:

- 1 Key Benefits
- 2 Real-Time Traffic Policy Builder
- 2 Out-of-the-Box Protection
- 2 Advanced Enforcement
- 2 Achieve Compliance with Security Standards
- 2 Cost Effective Application Security
- 3 Comprehensive Application Security and Acceleration
- 3 Integrated XML Firewall
- 3 DataGuard and Cloaking
- 3 Vulnerability Assessment
- 4 Live Update for Attack Signatures
- 5 SMTP and FTP Security
- 4 Centralized Advanced Reporting and Database Security
- 5 Architecture
- 6 BIG-IP ASM Platforms
- 6 More Information



## Protect Your Business with Next Generation Application Security

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 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.

### Key Benefits

#### Ensure application availability

Get comprehensive attack prevention from layer 7 DoS and brute force attacks, dangerous FTP and SMTP commands, and more.

#### Handle threats with greater agility

Focus on fast application development and deployment with automatic security policies.

#### Reduce costs and enable compliance

Achieve security standards compliance with built-in application security protection.

#### Get out-of-the-box application security policies

Provide protection with pre-built rapid deployment policies, and minimal configuration.

#### Improve app security and performance

Enable advanced app protection while increasing performance, and cost effectiveness with app security and acceleration.

According to the Web Application Security Consortium [96.85%](#) of websites have vulnerabilities providing immediate risk of attack while [69.37%](#) of the vulnerabilities are client-side. As more applications move to the web, data breach from web applications is a real concern. Once a breach occurs, the Ponemon Institute estimates the total average costs of a data breach is \$202 per record compromised and \$225 for malicious insiders or former workers.<sup>2</sup>

## Real-Time Traffic Policy Builder

At the heart of BIG-IP ASM is the dynamic policy builder engine, which is responsible for the automatic self-learning and creation of security policies. It automatically builds and manages security policies around newly discovered vulnerabilities, deploying fast, agile business processes without manual intervention. When traffic flows through BIG-IP ASM, the policy builder parses requests and responses, providing the unique ability to inspect the bi-directional flow of full client and application traffic—both data and protocol. By using the advanced statistics and heuristics engine, the policy builder can filter out attacks and abnormal traffic. The policy builder can also run in a mode in which it is made aware of site updates. By parsing responses and requests it can detect site changes and automatically update the policy accordingly, without any user intervention.

## Out-of-the-Box Protection

BIG-IP ASM is equipped with a set of pre-built application security policies that provide out-of-the box protection for common applications such as Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials, and Microsoft Office SharePoint. In addition, BIG-IP ASM includes a rapid deployment policy, which immediately secures any customer application. The validated policies require zero configuration time and serve as a starting point for more advanced policy creation, based on heuristic learning and specific customer application security needs.

## Advanced Enforcement

BIG-IP ASM can secure any parameter from client-side manipulation and validate log-on parameters and application flow to prevent forceful browsing and logical flaws. BIG-IP ASM also protects against OWASP Top Ten<sup>1</sup> and zero-day web application attacks.

## Achieve Compliance with Security Standards

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. BIG-IP ASM provides advanced reporting on new attacks such as layer 7 DoS and Brute Force. In addition, BIG-IP ASM integrates with WhiteHat, Splunk, and Secerno for vulnerability assessment, auditing, and real-time and database reporting to provide security breach reviews, attack prevention, and compliance.

## Cost Effective Application Security

Many websites and applications experience security threats that disrupt the business and damage the corporate brand. BIG-IP ASM reports previously unknown threats, such as brute force attacks, and mitigates web application threats, shielding the organization from data breaches. BIG-IP ASM helps prevent embarrassing and costly application breaches that cost millions of dollars in declining revenue, regulatory fines, and brand value.

<sup>1</sup> To read the OWASP Top Ten for BIG-IP ASM, contact your F5 representative.

<sup>2</sup> [“Data breach costs rise as firms brace for next loss,” Robert Westervelt, SearchSecurity.com.](#)

## Comprehensive Application Security and Acceleration

BIG-IP ASM and WebAccelerator™ can accelerate and secure applications while also enhancing performance. This provides an efficient multi-solution platform while adding security without performance reduction. Attacks are now filtered immediately and web applications are accelerated for improved user experience and application performance. Since there is no need to introduce a new appliance to the network, BIG-IP ASM and WebAccelerator running on BIG-IP® Local Traffic Manager™ enable an all-in-one appliance solution for maximum cost effectiveness.

## Integrated XML Firewall

BIG-IP ASM provides application-specific XML filtering and validation functions that ensure that the XML input of web-based applications is properly structured. It provides schema validation, common attacks mitigation, and XML parser denial-of-service prevention.

## DataGuard™ and Cloaking

BIG-IP ASM prevents the leakage of sensitive data (such as credit card numbers, social security numbers, and more) by stripping it out by masking the information. In addition, BIG-IP ASM hides error pages and application error information, preventing hackers from discovering the underlying architecture and launching a targeted attack.

## Vulnerability Assessment

Integration with WhiteHat's Sentinel Security offers a unique vulnerability assessment service that combines automated tools with dedicated, highly skilled application security experts. Through integration with BIG-IP ASM, the industry-leading WhiteHat Sentinel service can create BIG-IP ASM rules that specifically address the vulnerabilities discovered in a web application. The result is a validated and actionable vulnerability assessment with a near-instantaneous mitigation response, protecting the application while development corrects the vulnerable code.

BIG-IP ASM provides pre-built, validated application security policies requiring no configuration and giving out-of-the-box protection for mission-critical applications.

<input type="checkbox"/>	Name	Active Security Policy	Enforcement Mode	Logging Profile	State
<input type="checkbox"/>	OWA	OWA_default	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	Oracle_11i	Oracle_11i	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	PeopleSoft_Portal	PeopleSoft_Portal_default	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	SharePoint	SharePoint_Template	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	www.mycompany.com	www.mycompany.com_default	Blocking	Log all requests	VS1 Enabled

Delete Total Entries: 5

BIG-IP ASM provides comprehensive web application protection.

## Live Update for Attack Signatures

New signatures from new attacks are frequently required to ensure up-to-date protection. BIG-IP ASM queries the F5 signature service on a daily basis and automatically downloads and applies new signatures.



## SMTP and FTP Security

BIG-IP ASM eases the manageability of FTP server farms. BIG-IP ASM validates the FTP protocol, mitigates brute force attacks, and can also whitelist the enabled FTP commands. In addition, it can enforce command length limits and passive/active connections. For SMTP, BIG-IP ASM provides additional security checks at the perimeter. It also supports greylisting to prevent SPAM, enforces the SMTP protocol, blacklists dangerous SMTP commands, and mitigates directory harvesting attacks. The rate-limiting capabilities of BIG-IP ASM help to fight DoS attacks.

## Centralized Advanced Reporting and Database Security

Splunk, a large-scale, high-speed indexing and search solution, provides 15 different BIG-IP ASM specific reports. These reports provide visibility into attack and traffic trends, long-term data aggregation for forensics, acceleration of incident response, and identification of unanticipated threats before exposure occurs.

Secerno DataWall and BIG-IP ASM share common reporting for web-based attempts to gain access to sensitive data, subvert the database, or execute DoS attacks against the database. Malicious users can be isolated while reports and alerts provide immediate detection and information on the type and threat of such attacks.

## The BIG-IP ASM Architecture

BIG-IP ASM runs on F5's unique purpose-built TMOS® architecture. TMOS is an intelligent, modular, and high-performing platform that enhances every function of BIG-IP ASM. TMOS delivers insight, flexibility, and control, helping you intelligently protect your web applications.

### TMOS delivers:

- SSL offload
- Caching
- Compression
- The ability to manipulate any application content on-the-fly, regardless of in- or outbound traffic
- TCP/IP optimization
- Advanced rate shaping and quality of service
- IPv6 Gateway™
- IP/port filtering
- VLAN support through a built-in switch
- Resource Provisioning
- Route Domains (Virtualization)
- Remote Authentication
- Security
  - Display customized legal notices and security login banners
  - Enforce admin session timeouts
  - Securely logout of the BIG-IP system
  - Comply with enhanced auditing and logging requirements
  - Completely isolate and secure SSL certificates from being read or modified

### BIG-IP-ASM protects against various application attacks, including:

- Layer 7 DoS
- Brute Force
- Cross-site scripting
- SQL injection
- Parameter tampering
- Sensitive information leakage
- Session high-jacking
- Buffer overflows
- Cookie manipulation

- Various encoding attacks
- Broken access control
- Forceful browsing
- Hidden fields manipulation
- Request smuggling
- XML bombs/DoS

### Additional network security services include:

- SSL accelerator
- Stateful layer 3–4 firewall
- Transparent and non-transparent reverse proxy
- Key management and failover handling
- SSL termination and re-encryption to web servers
- VLAN segmentation
- DoS protection
- Client-side certificates support
- Client authentication via LDAP/RADIUS
- Dedicated management port
- Monitoring of URIs
- Centralized advanced reporting with Splunk
- Database Security with Secerno's DataWall

### Pre-built application security policies include:

- Lotus Domino 6.5
- OWA Exchange 2003
- OWA Exchange 2007
- Oracle 10g Portal
- Oracle Application 11i
- PeopleSoft Portal 9
- Rapid Deployment security policy
- SAP NetWeaver 7
- SharePoint 2003
- SharePoint 2007

## BIG-IP ASM Platforms

For detailed physical specifications, please refer to the BIG-IP System Hardware Datasheet. BIG-IP ASM is available as an add-on module for integration with BIG-IP Local Traffic Manager on the VIPRION, 8900, 8800, 8400, 6900, and 3600 platforms. BIG-IP ASM is available as a standalone solution on the 8900, 6900, and 3600 platforms.



VIPRION Chassis



8900 Series



8800 and 8400 Series



6900 Series



3600 Series

## More Information

Browse for these and other resources on F5.com to learn more about BIG-IP ASM.

### Product overview

[BIG-IP Application Security Manager](#)

### White paper

[Complying with PCI DSS Requirement 6.6](#)

### 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)

