

SecureSphere® Web Application Firewall

The Industry's Only Automated
Web Application Firewall

Are Your Web Applications Secure?

Web applications are a prime target for attacks; 92% of businesses have suffered from a successful Web application attack over the past twelve months according to a 2006 FBI survey. These attacks can produce devastating results ranging from high profile data breaches to brand damage, lawsuits and fines.

Security administrators and regulators have taken note. Since traditional security products do not stop Web application attacks, new compliance regulations now mandate application layer protection. Meeting today's security and compliance requirements can be a daunting challenge for many businesses.

Protect Your Applications and Your Business with Imperva

The SecureSphere® Web Application Firewall from Imperva protects Web applications and sensitive data. Plus, it offers drop-in deployment, automated, adaptable security, and low operational overhead. SecureSphere provides your business with a practical, highly secure solution to ensure that your business meets the modern challenges associated with transactional data security and compliance.



Automated Web Application Security

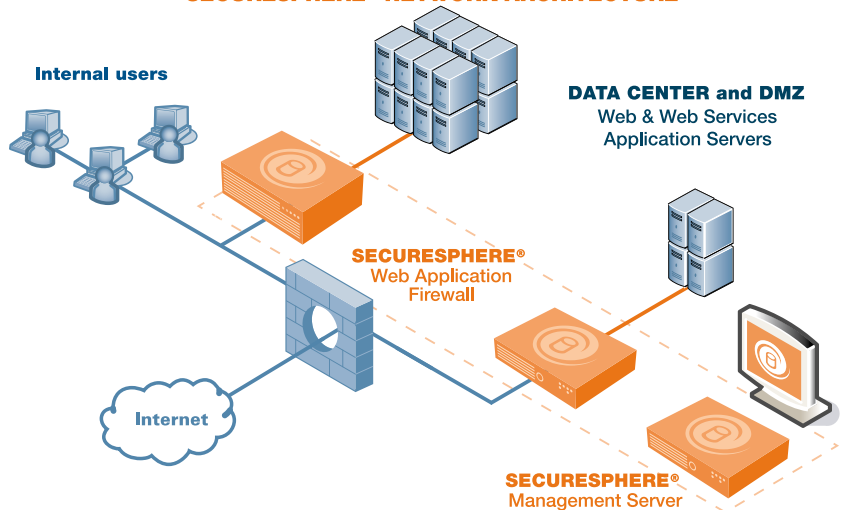
The SecureSphere® Web Application Firewall has transformed the way that businesses protect their applications and sensitive data by automating protection against Web attacks. Imperva's Dynamic Profiling technology automatically builds a model of legitimate behavior and adapts to application changes over time, keeping SecureSphere's application defense up to date and accurate without manual configuration or tuning.

Deployed in minutes with no changes to the existing infrastructure, SecureSphere protects the complete application stack, from the individual application to the server and network.

Imperva's Transparent Inspection technology delivers multi-gigabit

performance, sub-millisecond latency and options for high availability that meet the most demanding data center requirements. For large scale deployments, the SecureSphere MX Management Server centralizes and streamlines configuration, monitoring, and reporting.

SECURESPHERE® NETWORK ARCHITECTURE



Complete Attack Protection

The SecureSphere Web Application Firewall leverages multiple security defenses to provide the highest level of protection. These defenses include Dynamic Profiling, HTTP protocol validation, platform attack security, and Correlated Attack Validation.

Automated Application Learning – Imperva's Dynamic Profiling

SecureSphere's unique Dynamic Profiling technology automatically learns the structure, elements, and expected usage patterns of protected Web applications. Dynamic Profiling automatically detects and incorporates valid application changes

model: the need to manually create — and update — an enormous white list that can contain hundreds or even thousands of URLs, form fields, parameters and cookies. Dynamic Profiling automatically builds an accurate profile with no need for manual configuration or tuning.

Up-to-Date Security from the Imperva ADC

The Imperva Application Defense Center (ADC), an internationally recognized security research organization, continuously investigates new vulnerabilities reported around the world, analyzes exploit traffic from a diversity of real Web sites, and conducts primary vulnerability research to identify the latest threats. The results of this research are updated defenses at various layers within SecureSphere, including signature updates, protocol validation policies, and correlation rules.

In addition to updated attack defenses, the ADC offers optional ADC Insight Services. ADC Insights provide in-depth knowledge of business applications, pre-built compliance reports, and best practices from compliance and security experts.

Platform and Network Attack Protection

SecureSphere blocks attacks targeting known Web server, middleware and platform vulnerabilities. Over 4,000 signatures from sources like Bugtraq, CVE®, Snort®, and the Imperva ADC deliver comprehensive protection against such attacks. Besides known worms, SecureSphere identifies new, zero-day Web worms by detecting the unique combination of attributes that characterize Web worm attacks.

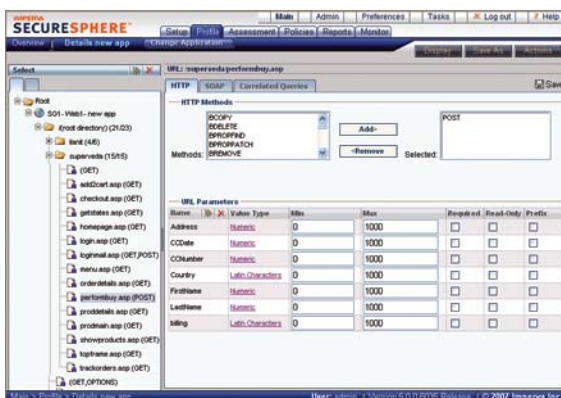
SecureSphere's integrated stateful network firewall protects against unauthorized users, protocols, and network attacks from both internal and external sources. It meets best practice security mandates to prevent nonessential protocols from reaching sensitive Web applications.

Web Services Protection

Leveraging its Dynamic Profiling technology, SecureSphere also profiles legitimate Web Services behavior including XML files, elements, attributes, schema, variables, and SOAP actions. Any attempt to tamper with normal Web services behavior is identified and blocked.

Unparalleled Accuracy

Imperva's unique Correlated Attack Validation technology correlates violations across security layers and over time to accurately identify the most complex attacks. Individual violations may not definitively indicate attack, but by correlating unique combinations of violations, attacks are validated beyond a doubt. No other solution can match the accuracy achieved through Correlated Attack Validation.



Dynamic Profiling automatically learns URLs, form fields, parameters, cookies, and expected user input.

into the application profile over time. By comparing Web requests to the profile, SecureSphere can detect unacceptable behavior and prevent malicious activity with pinpoint precision.

Dynamic Profiling overcomes the biggest drawback associated with a positive security

HTTP Protocol Validation

HTTP protocol validation prevents a myriad of protocol exploits including buffer overflow, malicious encoding, HTTP smuggling, and illegal server operations. Flexible policies enable strict adherence to RFC standards or allow minor variations for specific applications.

Transparent Deployment

No Changes to Application or Network

Transparent Inspection technology uniquely enables SecureSphere to be deployed into any environment without changing existing applications, servers or network. SecureSphere provides complete and accurate application security without forcing organizations to redesign their Web applications, change IP or DNS settings or update authentication schemes.

Kernel-based Transparent Inspection decouples security from deployment mode, so SecureSphere can support the following operation modes:

- **Transparent Layer 2 Bridge** – for drop-in deployment and industry-best performance
- **Layer Router** – for network segmentation, routing and network address translation
- **Reverse Proxy** – for content modification, such as cookie signing and URL rewriting
- **Transparent Proxy** – for fast deployment of content modification without network changes
- **Non-inline Monitor** – for zero-risk monitoring and forensics.

Gigabit Performance

SecureSphere delivers multi-gigabit throughput and tens of thousands of transactions per second while maintaining sub-millisecond latency. This level of performance is an order of magnitude better than competing approaches. It ensures completely transparent deployment. With SecureSphere, security will never impact data center service level agreements or application performance.

High Availability

SecureSphere supports a broad range of high availability options, enabling it to be deployed into some of the largest networks in the world. Availability options include:

- **Imperva High Availability (IMPVHA)** for sub-second failover
- **Virtual Router Redundancy Protocol (VRRP)** for router or proxy deployments
- **Active-Active and Active-Passive Redundancy** for external availability mechanisms
- **Fail-open interfaces** for single-gateway availability
- **Non-inline deployment** for zero risk monitoring and assessment

Operations

Automated Policy Maintenance

Implementing a white-list security model has traditionally required constant manual tuning. The application firewall's white list needed to be updated whenever the Web application changed. Dynamic Profiling eliminates manual tuning by automatically modeling Web applications and adapting to application changes. SecureSphere administrators still have full access to modify application profiles and create custom policies.

Centralized Management

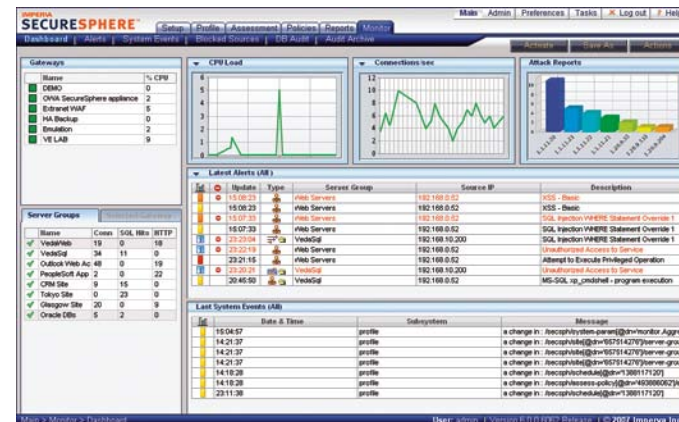
SecureSphere can be deployed as a standalone appliance or scale to protect distributed data centers. For larger environments, including mixed Web and database deployments, the SecureSphere MX Management Server offers centralized configuration, monitoring, and reporting. Management of large enterprise and ASP environments is streamlined through hierarchical organizational groupings, granular administrative permissions, and a unique task-oriented workflow.

Enterprise Class Reporting

SecureSphere offers rich graphical reporting capabilities, enabling customers to easily understand security status and meet regulatory compliance requirements. SecureSphere provides both pre-defined and fully-customizable Web based reports. Reports can be viewed on demand or emailed on a daily, weekly or monthly basis. SecureSphere's reporting platform provides instant visibility into security, compliance, and content delivery concerns.

Monitoring and Alerting

A real-time dashboard provides a high-level view of system status and security events. Alerts are easily searched, sorted, and directly linked to corresponding security rules. For flexible integration with Security Event Management products, SecureSphere supports syslog, SNMP, and direct ODBC access.



SecureSphere's real time dashboard

Automated and Accurate Protection Against:

- Web, HTTPS (SSL) and XML Vulnerabilities
- SQL Injection
- Session Hijacking
- Cross Site Scripting (XSS)
- Form Field Tampering
- Known Worms
- Zero Day Web Worms
- Buffer Overflow
- Cookie Poisoning
- Denial of Service
- Malicious Robots
- Parameter Tampering
- Brute Force Login
- Malicious Encoding
- Directory Traversal
- Web Server and Platform Attacks
- Site Recon
- OS Command Injection
- Cross Site Request Forgery (CSRF)
- Google Hacking
- Remote File Inclusion Attacks
- Illegal Encoding
- Credit Card Exposure
- Patient Data Disclosure
- Corporate Espionage
- Phishing
- Data Destruction

Application User Tracking

SecureSphere's Dynamic Profiling technology automatically captures Web application user names and associates all subsequent session activity with that specific user name. As a result, SecureSphere can uniquely monitor, enforce and audit policy on a per-user basis.

Optional Database Protection

The SecureSphere Web Application Firewall can be extended to monitor and protect Oracle, MS-SQL Server, DB2, Sybase, and Informix databases. The SecureSphere Database Security Gateway prevents external attacks and insider abuse providing end-to-end security for the data center. In addition, it leverages SecureSphere's Application User Tracking to trace individual SQL queries back to the Web user. This Universal User Tracking capability provides unparalleled visibility into database requests, changes and violations.

SecureSphere Features & Appliance Specifications

Web Security	Dynamic Profile (White List security), Web server & application signatures, HTTP RFC compliance, normalization of encoded data
HTTPS/SSL Inspection	Passive decryption or termination; optional HSM support for SSL key storage
Web Services Security	XML/SOAP profile enforcement, Web services signatures, XML protocol conformance
Content Modification	URL rewriting (obfuscation), cookie signing
Worm/Platform Security	Known and zero-day worm security / Operating system intrusion signatures
Network Security	Stateful firewall, DoS prevention
Advanced Protection	Pre-defined and custom correlation rules incorporate all security elements to detect complex, multi-stage attacks
Data Leak Prevention	Credit card numbers; PII (personally identifiable information); pattern matching
Policy/Signature Updates	New attack updates provided weekly or immediately for high threats
Deployment Modes	Transparent Bridge (Layer 2), Router/NAT (Layer 3), Reverse Proxy (Layer 7), Non-inline sniffer, Transparent Proxy (Layer 7)
Management	Web User Interface (HTTP/HTTPS), Command Line Interface (SSH/Console)
Administration	MX Server for centralized management, integrated management option (G4, G8), Hierarchical Management Groupings
Logging/Monitoring	SNMP, Syslog, Email, integrated graphical reporting, real-time dashboard
High Availability	IMPVHA (Active/Active, Active/Passive), fail open interfaces (bridge mode only), VRRP, STP and RSTP

Specification	SecureSphere G4	SecureSphere G8	SecureSphere G16 FTL	MX Management Server
Throughput	500 Mbps	1000 Mbps	2000 Mbps	N/A
Max Transactions/Sec	16,000	24,000	36,000	N/A
Latency	Sub-millisecond	Sub-millisecond	Sub-millisecond	N/A
Interfaces	6 x 10/100/1000 Mbps (max 4 fiber interfaces)	6 x 10/100/1000 Mbps (max 4 fiber interfaces)	6 x 10/100/1000 Mbps (max 4 fiber interfaces)	2 x 10/100/1000 Mbps (max 4 fiber interfaces)
Interface Types	Copper/Fiber SX/Fiber LX	Copper/Fiber SX/Fiber LX	Copper/Fiber SX/Fiber LX	Copper
Max Network Segments	(2)Bridge; (5)Router, Non-inline	(2)Bridge; (5)Router, Non-inline	(2)Bridge; (5)Router, Non-inline	N/A
Form Factor	1U; FTL Model: 2U	1U; FTL Model: 2U	2U	1U; FTL Model: 2U
Hard Drive	250GB SATA; FTL Model: (2) Hot-Swap 250GB SATA	250GB SATA; FTL Model: (2) Hot-Swap 250GB SATA	(2) Hot-Swap 250GB SATA	250GB SATA; FTL Model: (2) Hot-Swap 250GB SATA
External Drive	CD-ROM	CD-ROM	CD-ROM	CD-ROM
Enclosure	19 inch rack	19 inch rack	19 inch rack	19 inch rack
Weight	25 lbs; FTL Model: 65 lbs	25 lbs; FTL Model: 65 lbs	65 lbs	25 lbs; FTL Model: 65 lbs
Power Supply	350W; FTL Model: (2) Hot-Swap 750W total	350W; FTL Model: (2) Hot-Swap 750W total	(2) Hot-Swap 750W total	350W; FTL Model: (2) Hot-Swap 750W total
AC Power	100-240V, 50-60 Hz	100-240V, 50-60 Hz	100-240V, 50-60 Hz	100-240V, 50-60 Hz
Dimensions	16.93" x 25.51" x 1.67" FTL Model: 16.93" x 27.75" x 3.44"	16.93" x 25.51" x 1.67" FTL Model: 16.93" x 27.75" x 3.44"	16.93" x 27.75" x 3.44"	16.93" x 25.51" x 1.67" FTL Model: 16.93" x 27.75" x 3.44"
Operating Environment	10°C (50°F) to 35°C (95°F)	10°C (50°F) to 35°C (95°F)	10°C (50°F) to 35°C (95°F)	10°C (50°F) to 35°C (95°F)
Non-Operating Environment	-40°C (-40°F) to 70°C (158°F) relative humidity 90%, non-condensing at 35°C (95°F)	-40°C (-40°F) to 70°C (158°F) relative humidity 90%, non-condensing at 35°C (95°F)	-40°C (-40°F) to 70°C (158°F) relative humidity 90%, non-condensing at 35°C (95°F)	-40°C (-40°F) to 70°C (158°F) relative humidity 90%, non-condensing at 35°C (95°F)
EMC Certifications	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI

Imperva, Inc.

U.S. Headquarters
950 Tower Lane
Suite 1550
Foster City, CA 94404
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel-Aviv 67010
Israel
Tel: +972-3-6840100
Fax: +972-3-6840200



Network Computing
Editor's Choice
Web Application Firewall

Toll Free (U.S. only): +1-866-926-4678
www.imperva.com