IMPERVA®

SecureSphere® SE
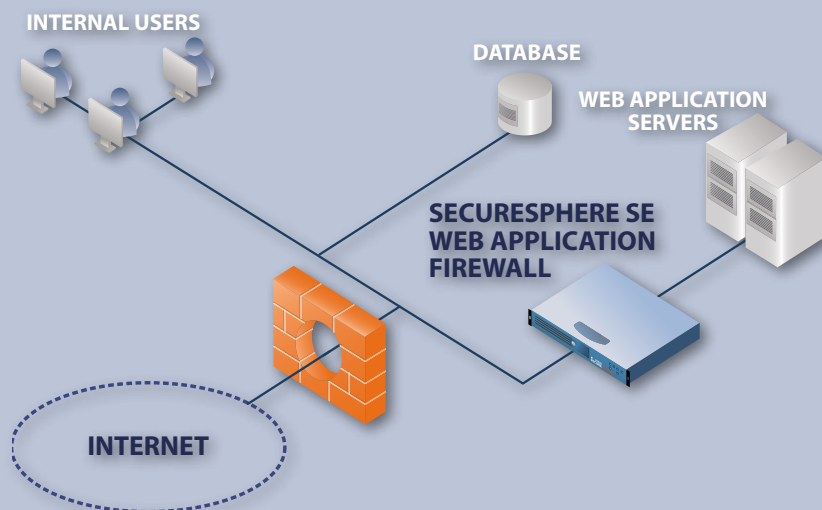## Web Application Firewall

Market Leading Web Application Security
for the Medium Enterprise

Web application attacks pose a real threat to online data for businesses of every size, making it critical for you to protect your online applications.

Imperva delivers the most proven, most recognized, and most trusted solution for protecting Web applications. Based on the market-leading Imperva Web Application Firewall, SecureSphere SE WAF is designed specifically for medium enterprises. With so much at stake, why go with anything but the best?

IMPERVA™
SECURESPHERE™ G2 Gateway

Market-Leading Web Application Firewall for Medium Enterprise

Based on Imperva's enterprise-class SecureSphere Web Application Firewall, the Standard Edition Web Application Firewall is designed for medium enterprises, providing the industry's best and only automated protection for critical applications. It combines superior application data security with proven performance, ease-of-use, and automatic security updates demanded by medium enterprise with limited IT resources. The Imperva SecureSphere SE Web Application Firewall delivers enterprise-class security at an affordable cost for medium enterprises.

INTERNAL USERS

DATABASE

WEB APPLICATION SERVERS

SECURESPHERE SE WEB APPLICATION FIREWALL

INTERNET

Automated Protection and Easy Deployment

The SecureSphere SE Web Application Firewall uniquely addresses the key business needs of medium enterprises: reliable protection of online applications and data against all types of application attacks, ease of deployment, and automated security policy configuration. Through Imperva's kernel-based Transparent Inspection, SecureSphere supports multiple deployment modes for varying needs without degradation of performance and with minimal latency in all modes. With Imperva's Dynamic Profiling, SecureSphere removes the need for constant manual tuning of application monitoring and security policies, making it easy for medium enterprises to maintain security without a large support staff.

Protects Confidential Data from Breaches and Leakages

The SecureSphere SE Web Application Firewall leverages multiple inspection layers and security defenses to secure Web applications from sophisticated attacks and malicious hackers.

Accurate Application Protection

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.

Reliable Data Leakage Prevention

SecureSphere inspects outbound traffic to identify potential leakage of sensitive data such as cardholder data and social security numbers. In addition to reporting on where sensitive data is used in the application, SecureSphere can optionally prevent this information from leaving the organization.

Automated Application Learning

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 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 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.

Provides Easy Deployment with Minimal Configuration

SecureSphere provides flexible deployment options and through Dynamic Profiling entails minimal configuration and policy definition by the SecureSphere administrator.

Flexible Deployment

Based on Imperva's kernel-based Transparent Inspection technology, SecureSphere enables high-performance, high-availability deployment into finely-tuned data centers without any impact on existing databases, applications, or network infrastructure.

» Transparent Layer 2 Bridge – for drop-in deployment and industry-best performance

» 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

Automated and Accurate Protection Against:

- Web, SSL, and XML Vulnerabilities
- SQL Injection
- Session Hijacking
- Cross-Site Scripting (XSS)
- Form Field Tampering
- Worms
- Buffer Overflow
- Cookie Poisoning
- Denial of Service
- Brute Force Login
- Parameter Tampering
- Malicious Encoding

- Directory Traversal
- Web Server and Platform Attacks
- Credit Card Exposure
- Patient Data Disclosure
- US SSN Leakage
- Attack Reconnaissance
- Command Injection
- Cross Site Request Forgery (CSRF)
- Google Hacking
- Illegal Encoding
- Phishing
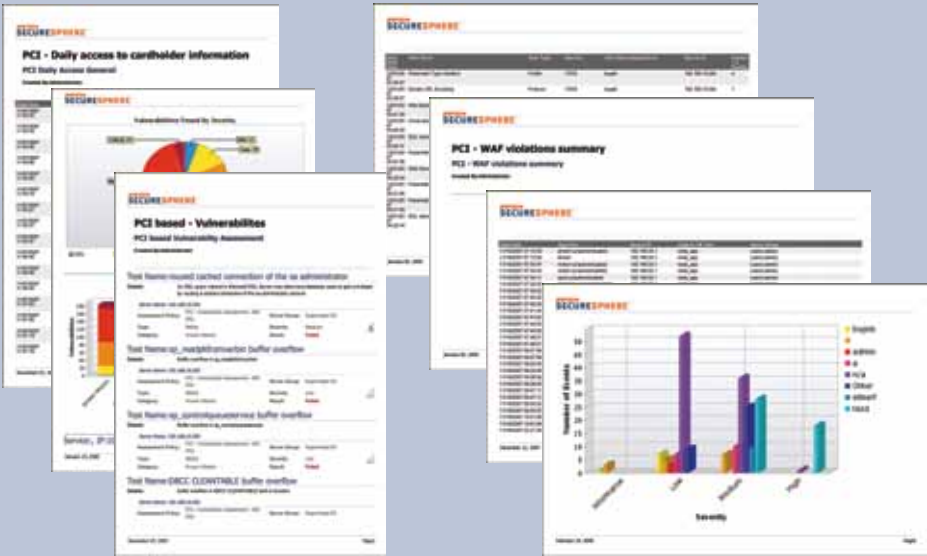
Ease of Monitoring and Alerting

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.

Business Relevant Reporting

SecureSphere includes reporting for specific business applications and regulatory mandates. SecureSphere provides a number of pre-defined and customizable Web based reports. Periodic updates from compliance and security experts at the Imperva ADC ensure reporting is up-to-date and relevant.

Scalable Management

SecureSphere can be deployed as a standalone appliance and can also scale to protect a cluster of Web servers. The SecureSphere SE Management Server offers a centralized configuration, monitoring, and reporting infrastructure to manage multiple SecureSphere WAF appliances and many applications from a single console.

SecureSphere's real time dashboard

SecureSphere SE Features

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, custom error messages, error code handling
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; Social Security Numbers; PII; NPI; HPI; pattern matching
Policy/Signature Updates	New attack updates provided weekly or immediately for high threats
Deployment Modes	Transparent Bridge (Layer 2), Reverse Proxy (Layer 7), Non-inline sniffer , Transparent Proxy (Layer 7)
Management	Web User Interface (HTTP/HTTPS), Command Line Interface (SSH/Console)
Administration	SecureSphere SE Management Server for centralized management, integrated management option
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

Most Proven Solution

Imperva is the market leader in Web Application Firewalls. Over 4,500 organizations are protected by Imperva solutions.

Most Recognized Solution

Imperva SecureSphere has won over 20 product awards in the last 5 years, far more than any other solution on the market.

Most Trusted Solution

More revenue and online assets are entrusted to Imperva SecureSphere than any other solution.

Delivers Dynamic Up-to-Date Security Protections

SecureSphere provides real-time security updates to protect against the latest threats based on feeds from its own premier research organization, the Imperva Application Defense Center (ADC). The Imperva ADC 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.

Upgradeable to Enterprise Edition

SecureSphere SE has everything you need to protect your online-applications, packaged in a solution for small IT staff. To provide maximum flexibility, SecureSphere SE deployments are upgradeable to the Enterprise Editions as organizations grow their needs.

Appliance Specifications

Specification	SecureSphere SE G2 Appliance	SecureSphere SE Management Server
Throughput	100 Mbps	N/A
Latency	Sub-millisecond	N/A
Interfaces	4 x 10/100/1000 Mbps	2 x 10/100/1000 Mbps (max 4 fiber interfaces)
Interface Types	Copper	Copper
Max Network Segments	(1)Bridge; (3)Router, (2) Non-inline	N/A
Form Factor	1U	1U; FTL Model: 2U
Hard Drive	250GB SATA	250GB SATA; FTL Model: (2) Hot-Swap 250GB SATA
Enclosure	19 inch rack	19 inch rack
Weight	9.9 lbs (4.5 kg)	25 lbs; FTL Model: 65 lbs
Power Supply	250W	350W; FTL Model: (2) Hot-Swap 750W total
AC Power	90-264V, 47-63 Hz	100-240V, 50-60 Hz
Dimensions	16.9" x 14.5" x 1.7" (430mm x 369mm x 42.4mm)	16.93" x 25.51" x 1.67", FTL Model: 16.93" x 27.75" x 3.44"
Operating Environment	0°C (32°F) to 40°C (104°F)	10°C (50°F) to 35°C (95°F)
Non-Operating Environment	-20°C (-4°F) to 75°C (167°F) relative humidity 5% to 95%	-40°C (-40°F) to 70°C (158°F) relative humidity 90%, non-condensing at 35°C (95°F)
EMC Certifications	FCC, CE-EMC	FCC, CISPR 22, CE, VCCI