SecureSphere®
Web Application Firewall

Protect Your Critical Web Applications

Safeguard Web applications from attacks and data breaches with the market leading Web Application Firewall. SecureSphere helps businesses:

- *Monitor and protect Web applications*
- *Directly address PCI 6.6 compliance*
- *Automate security operations with Dynamic Profiling*
- *Transparently protect Web applications with virtual patching*
- *Deliver high performance, sub-millisecond latency, and enterprise-class management and reporting*

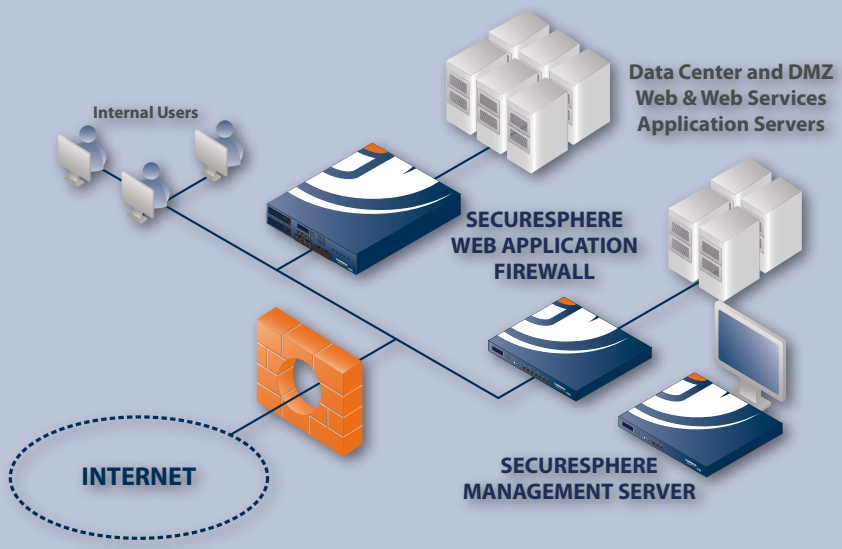
Only the market leading SecureSphere Web Application Firewall offers automated, non-intrusive, and scalable Web application security.

Web Application Firewall

Market-Leading Web Application Security

The SecureSphere® Web Application Firewall protects Web applications against sophisticated attacks, stops online identity theft, and prevents data leaks from applications. Multiple configuration options, including layer 2 bridge, proxy, and non-inline monitor enable drop-in deployment with no changes to existing applications or networks.

As the market-leading Web application firewall, more organizations rely on Imperva to monitor and protect their critical Web applications than any other vendor. Imperva SecureSphere provides your business with a practical and highly secure solution to ensure that your Web applications and data are safe.



Accurately Monitor and Protect Web Applications

The SecureSphere Web Application Firewall leverages multiple inspection layers and security defenses to provide the highest level of protection.

HTTP Protocol Validation

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

Data Leak 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.

Network and Platform Protection

SecureSphere detects and blocks attacks that target Web server, middleware, and platform vulnerabilities based on over 6,500 signatures from the Imperva Application Defense Center (ADC). The ADC investigates vulnerabilities reported by Bugtraq, CVE®, Snort®, and underground forums and performs primary security research to deliver the most up-to-date and comprehensive Web attack protection available.

SecureSphere's integrated stateful firewall protects applications and data from unauthorized users, protocols, and network layer attacks. SecureSphere also defends against new, zero-day Web worm attacks by identifying the unique combination of attributes that characterize Web worm attacks.

Reputation-based Security

ThreatRadar, an optional, automated security service, can block traffic originating from known attack sources. ThreatRadar monitors live feeds from around the world and continuously updates the WAF protection policies with the most recent list of malicious IPs to ensure the highest level of protection. ThreatRadar also alerts on phishing incidents and extended forensics information on geographic location of suspicious activity.

Unparalleled Accuracy

Imperva's unique Correlated Attack Validation 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.

Web 2.0 and XML Protection

SecureSphere protects dynamic Web 2.0 and Web Services by learning how these applications behave. It learns and protects XML files, elements, attributes, schema, variables, and SOAP actions. SecureSphere also prevents threats common to Web 2.0 applications, including SQL injection, XSS, and CSRF.

Automate Security Operations

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.

Application User Tracking

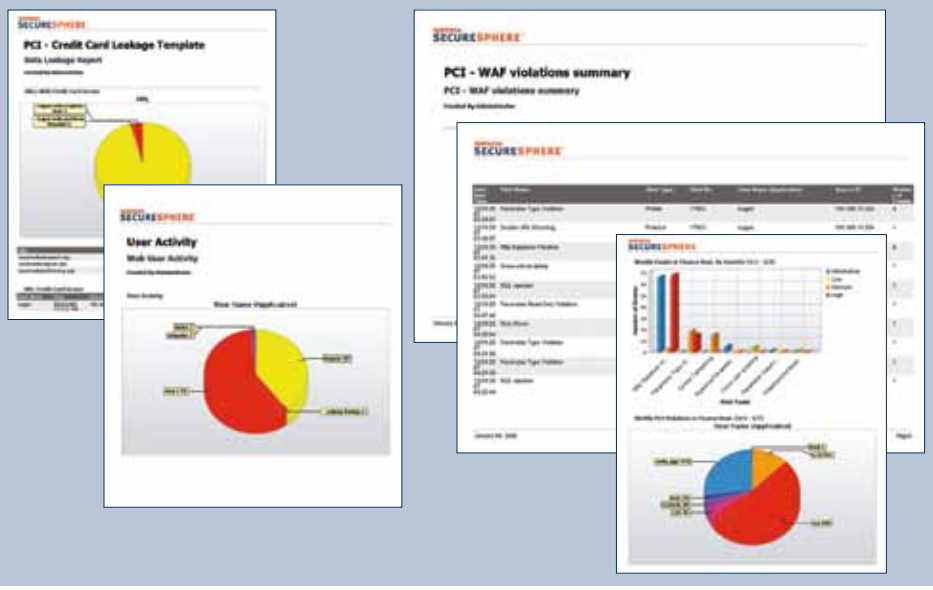
Using Dynamic Profiling, SecureSphere automatically captures Web application user names and associates all subsequent session activity with that specific user name. As a result, SecureSphere can uniquely monitor, enforce, and audit policy on a per user basis.

Up-to-Date Security from the ADC

The Imperva ADC, an internationally recognized security research organization, continuously investigates new vulnerabilities reported worldwide, analyzes exploit traffic from many different Web sites, and conducts primary vulnerability research to identify the latest

SecureSphere protects against many application attacks, including:

- Web, HTTPS(SSL) and XML Vulnerabilities
- SQL Injection
- Session Hijacking
- Cross Site Scripting (XSS)
- Form Field Tampering
- Web Worms
- Buffer Overflow
- Cookie Poisoning
- Denial of Service
- Malicious Robots
- Parameter Tampering
- Brute Force Login
- Malicious and Illegal Encoding
- Directory Traversal
- Web Server and OS Attacks
- Site Reconnaissance
- OS Command Injection
- Cross-Site Request Forgery (CSRF)
- Google Hacking
- Remote File Inclusion Attacks
- Phishing
- Sensitive Data Leakage (SSNs, Cardholder data, PII, HPI)
- Data Destruction
- Anonymous Proxy Vulnerabilities



PCI 6.6 Compliance Requirements

SecureSphere Web Application Firewall helps thousands of Enterprise organizations, including e-commerce, retail, banking, education, technology, and gaming companies meet PCI 6.6.

SecureSphere includes over 300 pre-defined reports to automate compliance mandates, including PCI. SecureSphere offers business relevant reporting so technical, business unit owners, and PCI auditors can view the right report for their specific need.

threats. The results of this research are updated defenses at various layers within SecureSphere, including signature updates, protocol validation policies, and correlation rules.

Enable Non-Intrusive Deployment

No Network or Application Changes

SecureSphere provides the most deployment options of any WAF in the industry, including a unique transparent deployment option that enables deployment without requiring any network or application changes.

SecureSphere delivers multi-Gigabit throughput and tens of thousands of transactions per second while maintaining sub-millisecond latency.

- Transparent Layer 2 Bridge – drop-in deployment and industry-best performance
- Layer 3 Router – network segmentation, routing, and network address translation
- Reverse Proxy – content modification, such as cookie signing and URL rewriting
- Transparent Proxy – fast deployment of content modification without network changes
- Non-Inline Monitor – zero-risk monitoring and forensics

Flexible High Availability Options

SecureSphere supports a broad range of high availability options:

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

Provide Enterprise-Grade Centralized Management

Support for Large, Distributed Deployments

SecureSphere can be deployed as a standalone appliance or scale to protect large and/or distributed data centers. The SecureSphere MX Management Server offers a centralized configuration, monitoring, and reporting infrastructure to manage multiple appliances and applications from a single console.

Best-in-Class Monitoring and Reporting

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. SecureSphere offers rich graphical reporting capabilities, enabling customers to easily understand security status and meet regulatory compliance requirements. There are both pre-defined and fully-customizable Web based reports. These can be viewed on demand or emailed on a daily, weekly, or monthly basis.

Hierarchical Management

Management of large enterprise and ASP environments is streamlined through hierarchical organizational groupings, granular administrative permissions, and a unique task-oriented workflow.

Integrate with 3rd Party Enterprise Applications

SecureSphere integrates with large scale enterprise applications to integrate Web Application Firewall with overall security activities. This includes leading SIEM and Log Management solutions, directory solutions for role based authentication, and Web Application Scanning solutions for vulnerability assessment.

Dynamic Profiling for Accurate Protection and Automated Policy Configuration

Accurate Web application security requires understanding hundreds of thousands of constantly changing variables including URLs, parameters, form fields and cookies. Imperva's innovative, patent-pending, Dynamic Profiling technology automatically profiles all Web application elements and builds a baseline of acceptable user behavior. By building an accurate profile or "white list" of application usage, Dynamic Profiling streamlines monitoring and security policy configuration without requiring extensive manual configuration or tuning. Plus, SecureSphere automatically detects and incorporates valid application changes into the application profile over time. Dynamic Profiling can also generate a complete profile report of your applications with real usage statistics that can be used to audit whether actual application usage matches intended usage.

SecureSphere Features and Appliance Specifications

Web Security
- » Dynamic Profile (White List security)
- » Web server & application signatures
- » Reputation-based security
- » HTTP RFC compliance
- » Normalization of encoded data

See list of attacks prevented on page 2

HTTPS/SSL Inspection
- » Passive decryption or termination
- » Optional HSM for SSL key storage

Web Services Security
- » XML/SOAP profile enforcement
- » Web services signatures
- » XML protocol conformance

Content Modification
- » URL rewriting & obfuscation
- » Cookie signing
- » Cookie encryption
- » Custom error messages
- » Error code handling

Platform Security
- » Operating system intrusion signatures
- » Known and zero-day worm security

Network Security
- » Stateful firewall
- » DoS prevention

Advanced Application Protection
- » Correlation rules incorporate all security elements (white list, black list) to detect complex, multi-stage attacks

Data Leak Prevention
- » Credit card number
- » PII (Personally Identifiable Information)
- » Pattern matching

Policy/Signature Updates
- » Security updates provided weekly or immediately for critical threats

Authentication
- » All authentication methods supported transparently and inspected in bridge and non-inline monitor modes. Can actively authenticate users in proxy mode.
- » Support for RSA Access Manager for two-factor authentication
- » Support for LDAP (Active Directory)
- » Support for SSL client certificates

User Awareness
- » Automated Tracking of Web Application Users

Deployment Modes
- » Transparent Bridge (Layer 2)
- » Router/NAT (Layer 3)
- » Reverse Proxy and Transparent Proxy (Layer 7)
- » Non-inline Sniffer (Monitoring only)

Management
- » Web User Interface (HTTP/HTTPS)
- » Command Line Interface (SSH/Console)

Administration
- » MX Server for centralized management
- » Integrated management option (all models except G16 FTL)
- » Hierarchical management groupings

Logging/Monitoring/Reporting
- » Real-time dashboard
- » Integrated graphical reporting (HTML, PDF, CSV formats)
- » SNMP
- » Syslog
- » Email
- » Common Event Format (CEF)

High Availability
- » IMPVHA (Active/Active, Active/Passive)
- » Fail-open interfaces (bridge mode only)
- » VRRP
- » STP and RSTP

Integration with 3rd Party Enterprise Applications
- » SIEM/SIM tools: ArcSight, RSA enVision, Prism Microsystems, Q1 Labs, TriGeo, NetIQ
- » Log Management: CA ELM, SenSage, Infoscience Corp.
- » Web application vulnerability scanners: WhiteHat, IBM, Cenzic, NT OBJECTives, and others

ICSA labs CERTIFIED www.ICSALabs.com Web Application Firewall

TECHWORLD.COM AWARDS 2008 WINNER

InformationWeek Editor's Choice

SAP® Certified Integration

iMPERVA®

Imperva
Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

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