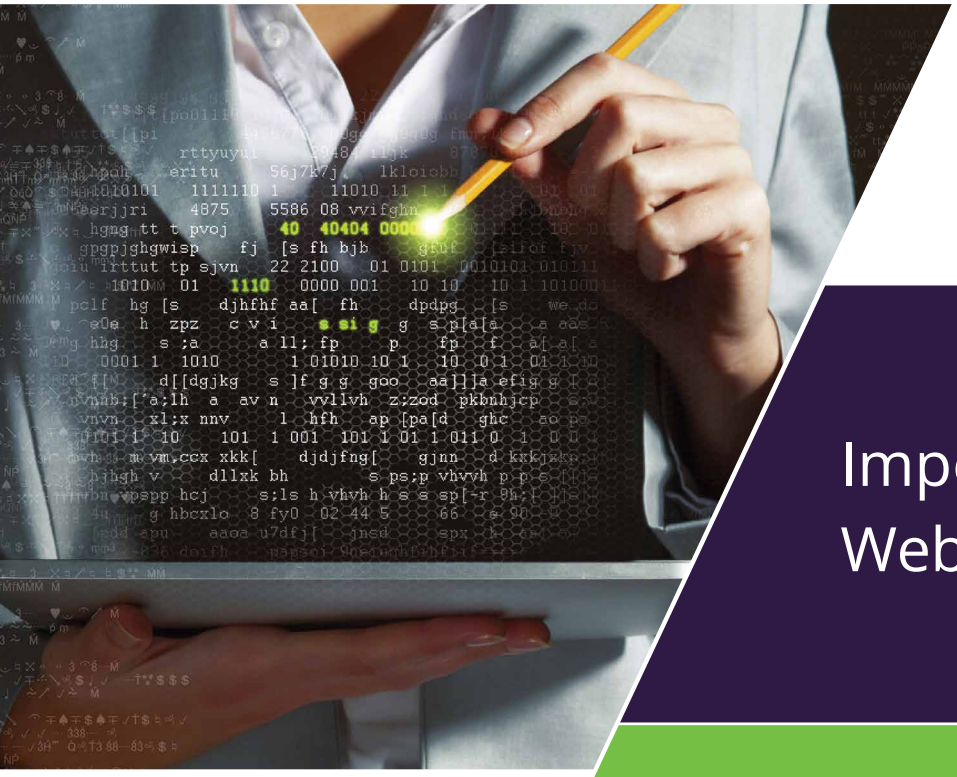
IMPERVA®



Imperva SecureSphere Web Application Firewall

DATASHEET

Protect Your Critical Web Applications and Data

Web applications are a prime target of cyber attacks because they are readily accessible and offer an easy entry point to valuable data. To combat cyber attacks, organizations need to protect websites and applications from existing and emerging cyber threats without affecting application performance or uptime.

More organizations rely on Imperva to protect their critical web applications than any other vendor. Imperva web application security solutions fit seamlessly into physical, virtual and cloud-based data centers, and deliver the market's most advanced web application security, constantly updated with threat intelligence curated by the renowned Imperva Application Defense Center research team.

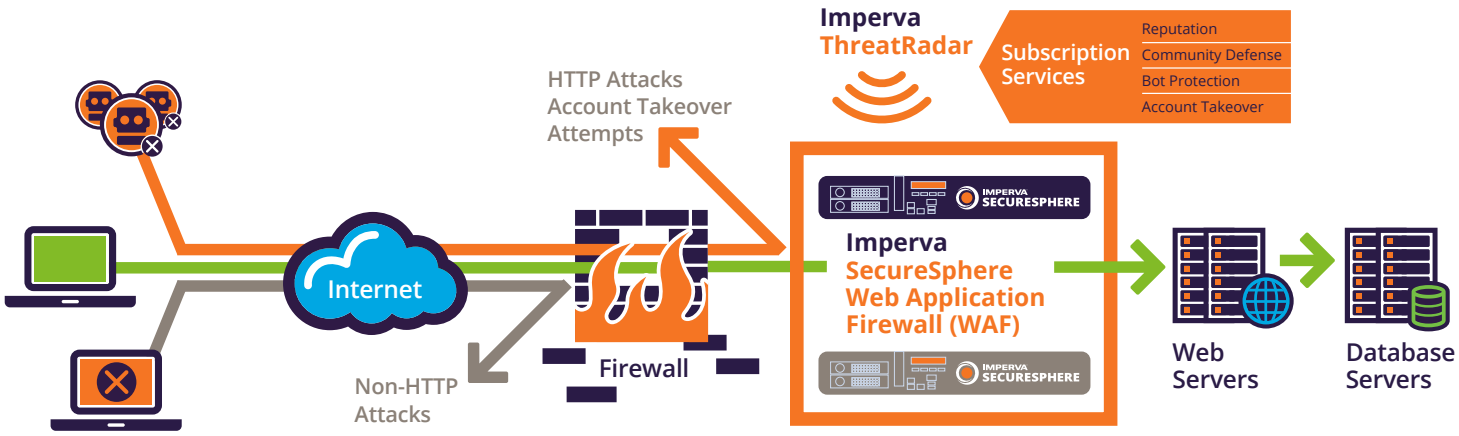
SecureSphere Web Application Firewall analyzes all user access to your business-critical web applications and protects your applications and data from cyber attacks.

Imperva SecureSphere Web Application Firewall

SecureSphere Web Application Firewall analyzes all user access to your business-critical web applications and protects your applications and data from cyber attacks. SecureSphere Web Application Firewall dynamically learns your applications' "normal" behavior and correlates this with the threat intelligence crowd-sourced from around the world and updated in real time to deliver superior protection.

Imperva was recognized as the only leader in Gartner's Magic Quadrant for Web Application Firewalls.[1] The industry-leading SecureSphere Web Application Firewall identifies and acts upon dangers maliciously woven into innocent-looking website traffic; traffic that slips right through traditional defenses. This prevents application vulnerability attacks such as SQL injection, cross-site scripting and remote file inclusion; business logic attacks such as site scraping and comment spam; botnet and DDoS attacks; and account takeover attempts in real-time, before fraud can be performed.

[1] Gartner Magic Quadrant for Web Application Firewalls, Jeremy D'Hoinne, Adam Hils, Claudio Neiva, 19 July 2016.



The following ThreatRadar intelligence feeds are available:

- **Reputation Service**–Filters traffic based upon latest, real-time reputation of source
- **Community Defense**–Adds unique threat intelligence crowd-sourced from Imperva users
- **Bot Protection**–Detects botnet clients and application DDoS attacks
- **Account Takeover Protection**–Protects website user accounts from attack and takeover
- **Fraud Prevention**–Simplifies deployment of best-in-class partner fraud prevention solutions

Imperva SecureSphere Capabilities

Automated Learning of User and Application Behavior

To accurately detect attacks, a web application firewall must understand application structure, elements, and expected user behavior. Imperva's patent-pending Dynamic Profiling technology automates this process by profiling protected applications and building a baseline or "white list" of acceptable user behavior. It also automatically learns application changes over time. Dynamic Profiling eliminates the need to manually configure–and update–innumerable application URLs, parameters, cookies, and methods.

Research-Driven Security Policies

Powered by Imperva Application Defense Center (ADC) - an internationally recognized security research organization - SecureSphere offers the most complete set of application signatures and policies available. Imperva ADC investigates vulnerabilities reported by Bugtraq, CVE®, Snort®, and underground forums, and also performs primary research to deliver the most current and comprehensive threat intelligence and web application attack protection available.

Flexible Deployment Options

SecureSphere can be deployed as a physical appliance, a virtual appliance, via Amazon Web Services, or as a hybrid of these. Deployments are particularly flexible in that SecureSphere can be deployed transparently, requiring virtually no changes to the network. Additionally granular policy controls enable superior accuracy and unequaled control to match each organization's specific protection requirements.

Deep Threat Intelligence

To protect against today's well-resourced cyber criminals, it is vital to have an advanced warning system that is aware of and protects against constantly evolving web-based attacks. Imperva ThreatRadar[2] updates SecureSphere Web Application Firewall with real-time threat intelligence crowd-sourced from around the world and curated by Imperva Application Defense Center. ThreatRadar provides better protection, improves WAF accuracy, and makes the security team more efficient by proactively filtering traffic from known bad sources so the security team can focus on what is really important.

Virtual Patching

SecureSphere can perform "virtual patching" for your web applications via vulnerability scanner integration. Instead of leaving a web application exposed to attack for weeks or months while code is modified after discovering a vulnerability, virtual patching actively protects web applications from attacks to reduce the window of exposure, and decreases the costs of emergency fix cycles until you are able to patch them.

HTTP Protocol, Platform, and XML Protection

SecureSphere enforces HTTP standards compliance to prevent protocol exploits and evasion techniques. Fine-grained policies allow administrators to enforce strict adherence to RFC standards or allow minor deviations. With over 8,000 signatures, SecureSphere safeguards the entire application infrastructure including applications and web server software. Flexible, automated XML security policies protect web services, SOAP, HTML 5 Web Sockets and Web 2.0 applications.

Granular Correlation Policies Reduce False Positives

SecureSphere distinguishes attacks from unusual, but legitimate, behavior by correlating web requests across security layers and over time. SecureSphere Correlated Attack Validation capability examines multiple attributes such as HTTP protocol conformance, profile violations, signatures, special characters, and user reputation, to accurately alert on or block attacks with the lowest rate of false positives in the industry. ThreatRadar threat intelligence can be included as an attribute, ensuring policies evaluation includes the very latest on the global threat landscape.

Customizable Reports for Compliance and Forensics

The rich graphical reporting capabilities offered by SecureSphere enable customers to easily understand security status and meet regulatory compliance. SecureSphere provides both pre-defined and fully-customizable reports. This enables you to quickly assess your security status and streamline demonstration of compliance with PCI, SOX, HIPAA and FISMA and other compliance standards.

Out-of-the-box SIEM Integration

SecureSphere WAF easily integrates with most of the leading Security Information and Event Management (SIEM) systems such as Splunk, ArcSight, RSA enVision and others. SecureSphere WAF events in any SIEM are intuitively indexed and are easily searchable for quick incident response. SecureSphere WAF exports events as syslog messages in Common Event Format (CEF) and JSON format.

[2] ThreatRadar Threat Intelligence feeds are available as annual subscriptions

Imperva SecureSphere Cyber Security

Imperva SecureSphere is a comprehensive, integrated security platform that includes SecureSphere Web, Database and File Security. It scales to meet the data center security demands of even the largest organizations, and is backed by Imperva Application Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.

IMPERVA SECURESPHERE

WEB APPLICATION SECURITY PRODUCTS	
SecureSphere Web Application Firewall	Accurate, automated protection against online threats
SecureSphere ThreatRadar	Global, real-time threat intelligence for detection, filtering and blocking of known bad traffic
DATABASE SECURITY PRODUCTS	
Database Activity Monitor	Full auditing and visibility into database data usage
Database Firewall	Activity monitoring and real-time protection for critical databases
Database Assessment	Vulnerability assessment, configuration management, and data classification for databases
User Rights Management for Databases	Review and manage user access rights to sensitive databases
ADC Insights	Pre-packaged reports and rules for SAP, Oracle EBS, and PeopleSoft compliance and security
FILE SECURITY PRODUCTS	
File Activity Monitor	Full auditing and visibility into file data usage
File Firewall	Activity monitoring and protection for critical file data
User Rights Management for Files	Review and manage user access rights to sensitive files
Directory Services Monitor	Audit, alert, and report on changes made in Microsoft Active Directory
SHAREPOINT SECURITY PRODUCTS	
SecureSphere for SharePoint	Visibility and analysis of SharePoint access rights and data usage, and protection against Web based threats
MANAGEMENT PRODUCTS	
MX Management Server	Single interface for managing, monitoring, and reporting on the activities of multiple SecureSphere gateways
Manager of Managers	Federates multi-domain and multi-tenant environments that are deployed with multiple MX Management Servers