Web

Protecting the Data That Drives Business®



Web Application Security

Protect Your Critical Web Applications

The market-leading Imperva SecureSphere Web Application Firewall:

- Automatically learns Web application structure and user behavior
- Updates Web defenses with research-driven intelligence on current threats
- Identifies traffic originating from malicious and fraudulent sources with ThreatRadar
- Virtually patches applications through vulnerability scanner integration
- Delivers high performance, drop-in deployment and clear, business-relevant reporting and alerts
- Fully addresses PCI DSS requirement 6.6

Products

SecureSphere Web Application Firewall

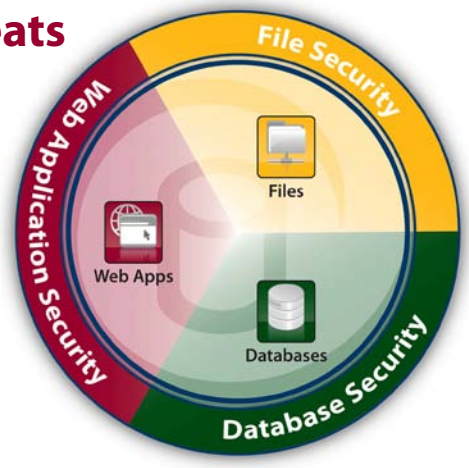
ThreatRadar Reputation Services

ThreatRadar Fraud Prevention Services

Protecting Web Applications from Online Threats

Web applications are a prime target for attack because they are easily accessible and they offer a lucrative entry point to valuable data. To combat complex and distributed attacks, organizations need to protect their Web sites from new and emerging threats without affecting application performance or uptime.

The market-leading SecureSphere® Web Application Firewall has transformed the way businesses protect their applications by automating Web security and providing flexible, transparent deployment. With its comprehensive protection and low administrative overhead, SecureSphere is the ideal solution to secure valuable Web assets and achieve PCI compliance.



Automated Learning of Applications and User 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 the Imperva Application Defense Center (ADC), an internationally recognized security research organization, SecureSphere offers the most complete set of application signatures and policies available. The ADC investigates vulnerabilities reported by Bugtraq, CVE®, Snort®, and underground forums and performs primary research to deliver the most current and comprehensive Web attack protection available.

Adaptable Protection from Large-Scale, Automated Attacks

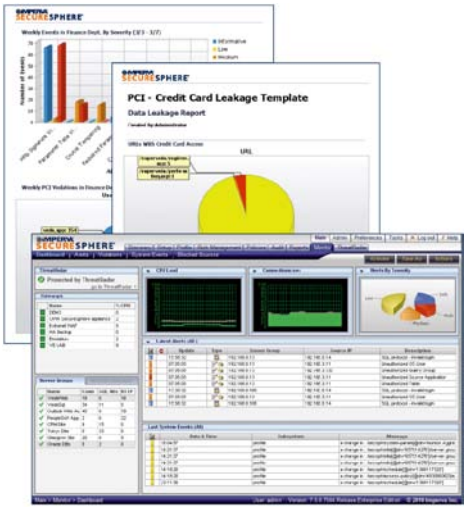
ThreatRadar Reputation Services identify and stop known attack sources. By integrating the foremost information about malicious IP addresses, bots, phishing URLs and anonymizing services, ThreatRadar can block bots and hackers before an attack can even be attempted. Up-to-date and accurate geolocation data allows businesses to monitor or restrict access by geographic location.

Virtual Patching Through Vulnerability Scanner Integration

For immediate patching of application vulnerabilities, SecureSphere can import assessment results from WhiteHat, IBM, Cenzic, NT OBJECTives, Qualys, and others and create custom policies to block known vulnerabilities. Virtual patching reduces the window of exposure and the cost of emergency fix and test cycles.

Protection Against Malware-based Fraud

ThreatRadar Fraud Prevention Services enable organizations to rapidly provision and manage fraud security without updating Web applications. By integrating with leading fraud security vendors, SecureSphere can transparently identify and stop fraudulent transactions. It also provides powerful monitoring and enforcement capabilities, allowing businesses to centrally manage WAF and fraud policies together.



PCI 6.6 Compliance Requirements

The SecureSphere Web Application Firewall helps thousands of enterprises meet PCI 6.6.

- Provides continuous and automated protection
- Offers pre-defined and custom reports that streamline compliance
- Virtually patches vulnerabilities for defense in-depth
- Satisfies PCI requirements for auditing and user access controls with optional Database Firewall

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, 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. This 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.

Customizable Reports for Compliance and Forensics

SecureSphere's rich graphical reporting capabilities enable customers to easily understand security status and meet regulatory compliance. SecureSphere provides both pre-defined and fully-customizable reports. Reports can be viewed on demand or emailed on a daily, weekly, or monthly basis.

Monitoring for In-Depth Analysis of Attacks

Alerts can be easily searched, sorted, and directly linked to corresponding security rules. SecureSphere's monitoring and reporting framework provides instant visibility into security, compliance, and content delivery concerns. A real-time dashboard provides a high-level view of system status and security events.

ThreatRadar: Reputation-based Security

- Integrate credible attack sources information into the WAF defenses
- Stop malicious visitors before they can launch an attack

Zero Impact Deployment and Ultra High Performance



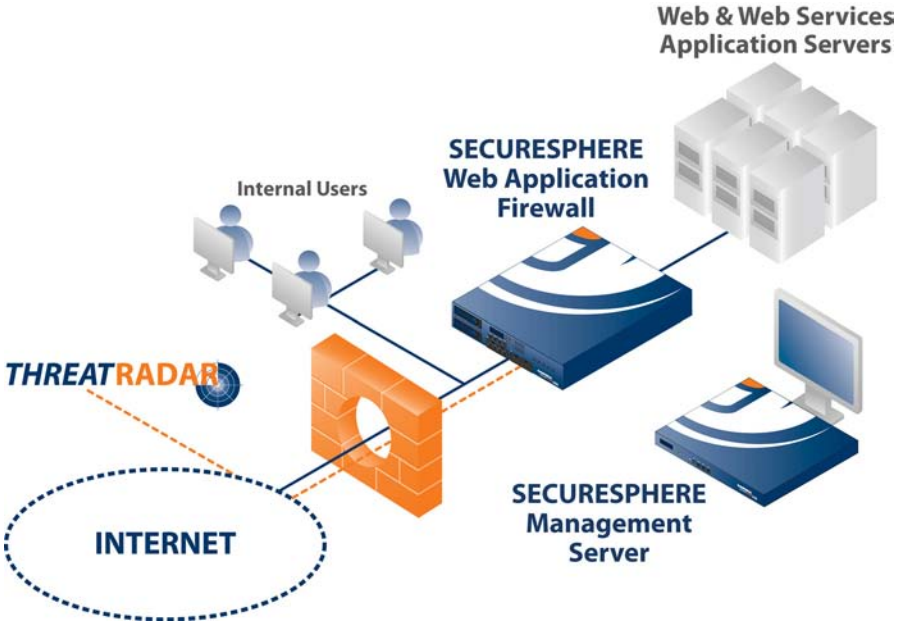
- **Hardware Appliances:** Offer multi-Gigabit throughput and sub-millisecond latency
- **Virtual Appliances:** Provide adaptable, reliable, and manageable security that grows with your business

Market-Leading Web Application Security

More organizations rely on Imperva to protect their critical Web applications than any other vendor. With drop-in deployment and low administrative overhead, SecureSphere provides a practical and highly secure solution to safeguard Web applications from online threats.

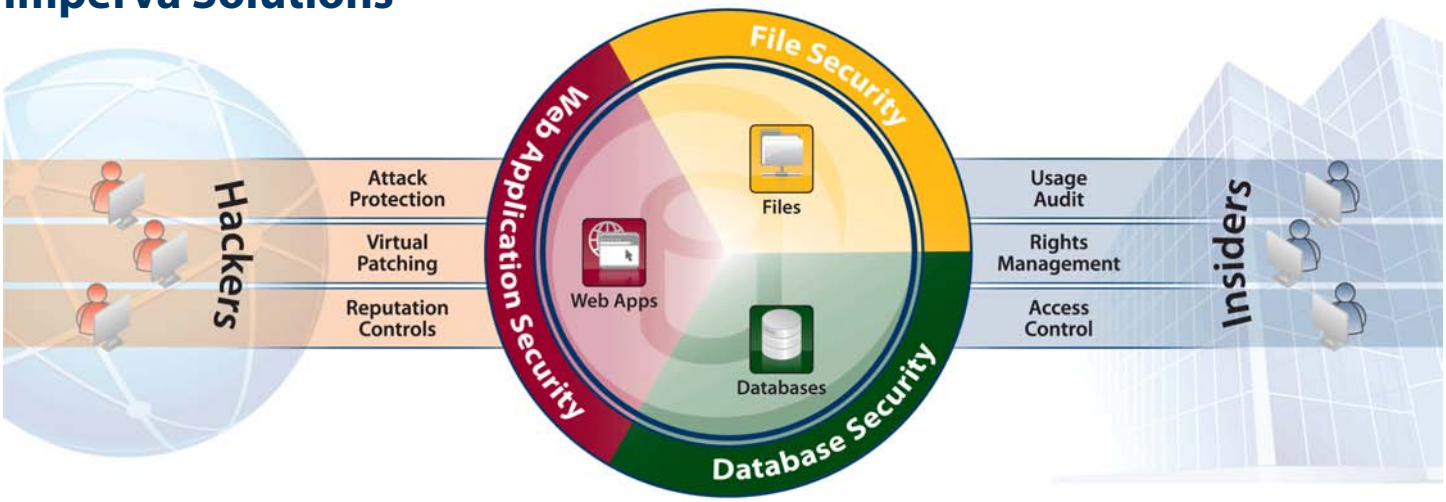
Multiple Deployment Options

- **Transparent Layer 2 Bridge:** Drop-in deployment and industry-best performance
- **Reverse Proxy and Transparent Proxy:** Content modification, such as cookie signing and URL rewriting
- **Non-inline Monitor:** Zero risk monitoring and forensics
- **High Availability:** IMPVHA, VRRP, fail open interfaces, existing redundancy options, non-inline deployment



Web

Imperva Solutions



Management Server	Family	SecureSphere Product
	Database	**Database Activity Monitoring** Full auditing and visibility into database data usage **Database Firewall** Activity monitoring and real-time protection for critical databases **Discovery and Assessment Server** 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	**File Activity Monitoring** 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 **SecureSphere for SharePoint** Visibility and analysis of SharePoint access rights and data usage, and protection against web-based threats
	Web	**Web Application Firewall** Accurate, automated protection against online threats **ThreatRadar** Fraud prevention and reputation-based security services that stop Web fraud and automated attacks

Family	Imperva Cloud Services
Web	**Cloud WAF** Easy and affordable cloud-based Web Application Firewall service **Cloud DDoS Protection** Safeguards businesses from the most debilitating and protracted DDoS attacks

Imperva is the global leader in data security

Thousands of the world's leading businesses, government organizations, and service providers rely on Imperva solutions to prevent data breaches, meet compliance mandates, and manage data risk.

ICSA labs CERTIFIED Web Application Firewall

Imperva
Headquarters
3400 Bridge Parkway, Suite 200
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

© Copyright 2011, Imperva
All rights reserved. Imperva, SecureSphere, and "Protecting the Data That Drives Business" are registered trademarks of Imperva.
All other brand or product names are trademarks or registered trademarks of their respective holders. #DS-WAS-1111rev1