DATASHEET

Web Application Security

Protect Your Critical Web Applications

Products

SecureSphere Web Application Firewall

ThreatRadar Reputation Services

ThreatRadar Fraud Prevention

DDoS Protection Service

Imperva Incapsula

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 websites from new and emerging 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 security capabilities, updated with threat intelligence based on research and big data analytics.

Imperva SecureSphere

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. Imperva SecureSphere is available on physical and virtual appliances, and on Amazon Web Services.

Imperva SecureSphere Capabilities

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

An add-on service to the SecureSphere Web Application Firewall, ThreatRadar Reputation Services offers powerful protection against automated attacks and botnets. ThreatRadar aggregates near real-time feeds of known attack sources, bots, phishing URLs, and anonymizing services to block malicious traffic before an attack can be attempted. Up-to-date geolocation data enables businesses to restrict access by geographic location.

ThreatRadar Community Defense provides crowd-sourced threat intelligence to stop emerging threats by collecting attack data from SecureSphere Web Application Firewalls.

DDoS Protection Service

SecureSphere Web Application Firewall stops application-layer DDoS attacks, but massive network-based DDoS attacks can still saturate your Internet connection and prevent traffic from ever reaching your site. The best place to combat network DDoS threats is in the cloud – before the attack can clog your network. DDoS Protection Service for SecureSphere is a secure, ultra-high capacity service that safeguards organizations from crippling DDoS attacks. DDoS Protection Service for SecureSphere can be deployed quickly and can scale on demand to mitigate multi-gigabit DDoS attacks.

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, an add-on service to the SecureSphere Web Application Firewall, enables 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. SecureSphere's 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

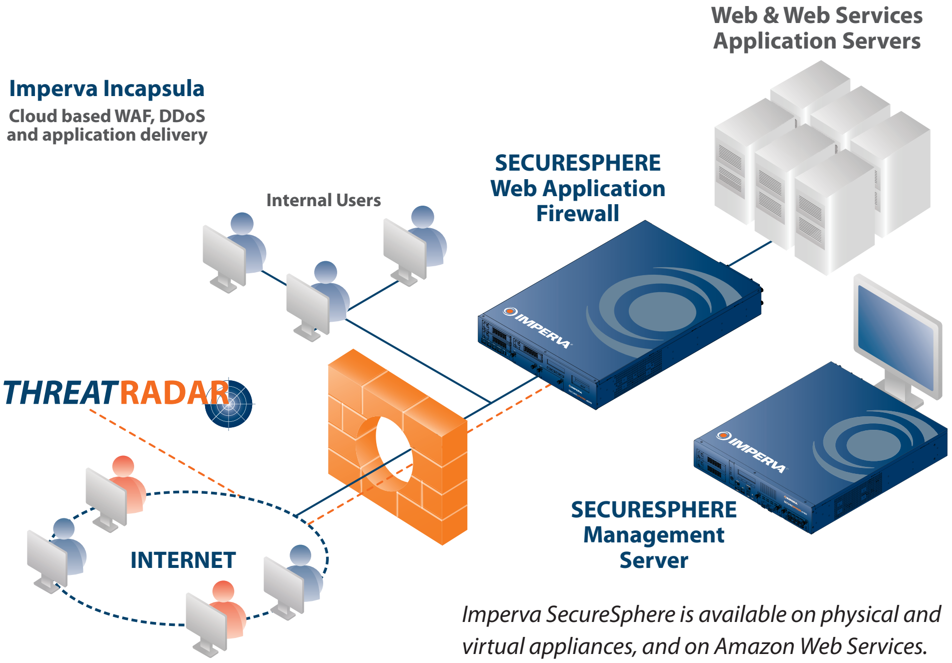
SecureSphere's rich graphical reporting capabilities enable customers to easily understand security status and meet regulatory compliance. SecureSphere provides both pre-defined and fully-customizable reports. Reports can be viewed on demand or emailed on a daily, weekly, or monthly basis.

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.

Imperva Incapsula

Imperva Incapsula is an easy and affordable service that integrates a PCI-certified Web Application Firewall, DDoS protection, load balancing and failover on top of a global content delivery network. Imperva Incapsula requires no hardware or software installations, and no web application changes, only a simple DNS change, so even business units or other organizations without dedicated security or IT staff can rest assured that their web applications and data are safe.



Imperva SecureSphere is available on physical and virtual appliances, and on Amazon Web Services.

Multiple SecureSphere Deployment Options

- **Transparent Layer 2 Bridge.** Drop-in deployment and industry-best performance
- **Reverse Proxy and Transparent Proxy.** Provide 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

Imperva SecureSphere Data Center 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 the Imperva Application Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.

WEB APPLICATION SECURITY PRODUCTS

Web Application Firewall
Accurate, automated protection against online threats

ThreatRadar Reputation Services
Leverage reputation data to stop malicious users and automated attacks

ThreatRadar Community Defense
SecureSphere deployments around the world provide crowd-sourced threat intelligence to subscribers

ThreatRadar Fraud Prevention
Stop fraud malware and account takeover quickly and easily

Incapsula SaaS WAF and DDoS Protection
Best-of-breed web application security and content delivery as a service

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

IMPERVA®

www.imperva.com