# The Imperva Story

*Imperva's mission is simple:*

**Protect the data that drives our customers' business**

*In achieving this, Imperva is leading the creation of a new category:*

**Data Security**

## Who We Are

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.

Underscoring Imperva's commitment to data security excellence, the Imperva Application Defense Center (ADC) is a world-class security research organization that maintains SecureSphere's cutting edge protection against evolving threats.

## The Problem We Solve

Data drives business, making it the ultimate prize for hackers and malicious insiders as well as the subject of intense regulatory scrutiny. Organizations are challenged with securing their data and maintaining regulatory compliance, while controlling cost, complexity, and risk.

## How We Solve It

Imperva SecureSphere is the market leading data security and compliance solution. SecureSphere protects sensitive data from hackers and malicious insiders, provides a fast and cost-effective route to regulatory compliance, and establishes a repeatable process for mitigating data risk.

### Database Security

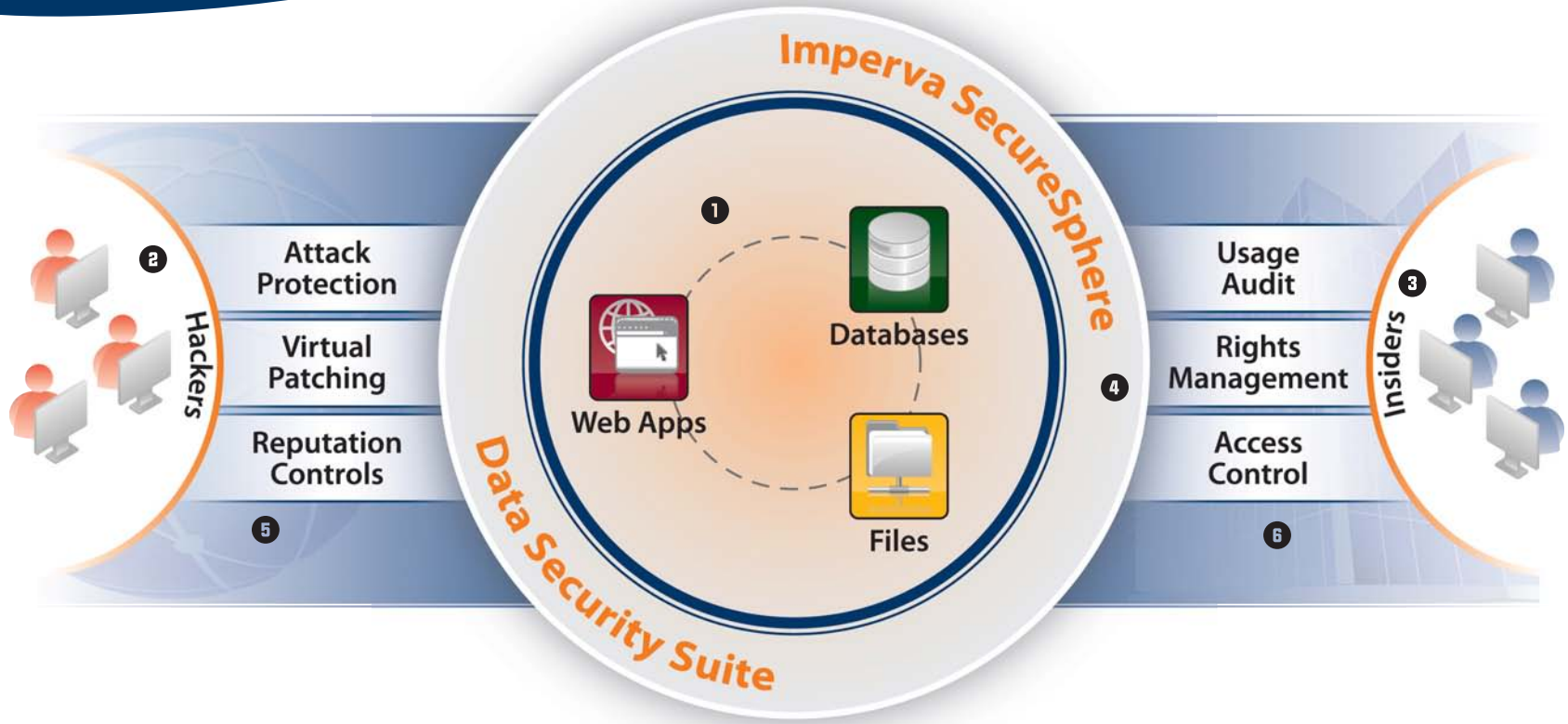
Award-winning database security and compliance solutions, audit database access, and deliver real-time protection against database attacks

### File Security

Cutting edge auditing, protection and rights management for unstructured data on file servers and network attached storage devices

### Web Application Security

Market-leading protection against large-scale Web attacks with reputation controls, automated management, and drop-in deployment




1. Your sensitive data lives in databases and files and is often accessible to the world via web apps.
2. This data is at risk from hackers that launch advanced, automated, and large scale attacks.
3. …and from malicious and privileged insiders that may abuse their privileges for economic or personal gain.
4. Imperva SecureSphere is the only comprehensive solution for data security and compliance of sensitive web, database, and file assets.
5. Imperva addresses the external threat with:
   - » Attack protection from both known and zero day attacks
   - » Virtual patching for mitigating vulnerabilities
   - » Reputation controls that stop malicious visitors from accessing the site
6. Imperva addresses the internal threat with:
   - » Comprehensive auditing of application and privileged access to sensitive data
   - » Elimination of excessive and unused access rights
   - » Enforcement of access control policies and separation of duties

# Comprehensive Data Security

# Business Drivers

| Data Breach Prevention | Real-time protection from hackers and malicious insiders to mitigate the data breach risk |
|---|---|
| Hacking and External Threats | Protect against large scale, automated attacks by hackers |
| Insider Threats | Detect and stop insiders' abuse of privileged access to sensitive data |
| Secure Web Development | Mitigate risk of application vulnerabilities exploits through virtual patching |

| Regulatory and Industry Compliance | Fast, cost-effective route to regulatory compliance via full visibility into data usage, vulnerabilities, and access rights |
|---|---|
| Sensitive Data Usage Auditing | Complete audit trail of all access to sensitive data as required by regulations |
| Privileged User Monitoring | Audit privileged user activity on database hosts, ensuring separation of duties |
| Web & Enterprise Application Controls | Protect and audit Web and Enterprise application data access |

| Data Risk Management | Automated, repeatable process for analysis of risk to sensitive data |
|---|---|
| Data Classification | Identify sensitive data in scope for security and compliance initiatives |
| Vulnerability Assessment | Detect and mitigate applications and system vulnerabilities to reduce the risk of data breach |
| User Rights Management | Review and restrict user access rights to a business need-to-know |



# Solutions

## Data Breach Prevention

Imperva SecureSphere provides real-time protection against data breaches by hackers and malicious insiders. SecureSphere enables executives, risk officers, auditors, and security professionals to mitigate the financial and reputation damage of data loss.

SecureSphere will:

- Alert or block access requests that deviate from normal application and data usage; or violate corporate practices
- Update defenses with research-driven intelligence on current threats and vulnerabilities
- Virtually patch application and database vulnerabilities to reduce the window of exposure and impact of ad-hoc fixes

## Regulatory and Industry Compliance

Imperva SecureSphere accelerates time to compliance by providing full visibility into data usage, vulnerabilities, and access rights. SecureSphere enables executives, risk officers, auditors, and security professionals to quickly and cost-effectively meet regulatory mandates.

SecureSphere will:

- Audit all sensitive data access including privileged and application users
- Identify and mitigate application and database vulnerabilities
- Automate the labor intensive process of reviewing and approving user access rights

## Data Risk Management

Imperva SecureSphere automates the risk analysis of sensitive data. SecureSphere enables executives, risk officers, auditors, and security professionals to establish a continuous and repeatable process for reducing data risk.

SecureSphere will:

- Continuously scan databases and file systems for sensitive data
- Prioritize vulnerability mitigation by data sensitivity and severity of exposure
- Accelerate the detection and revocation of excessive rights and dormant users

# SecureSphere Data Security Suite

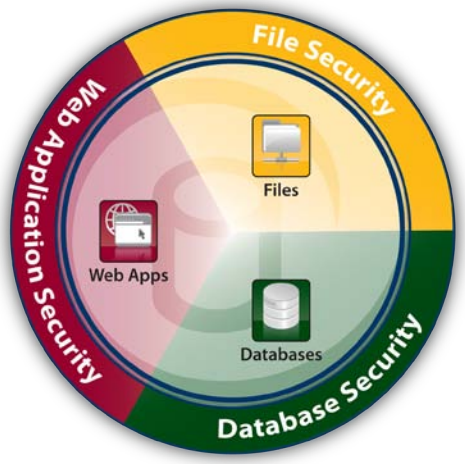
## Comprehensive Web, Database, and File Security

**SecureSphere Data Security Suite** is the market-leading data security and compliance solution. SecureSphere protects sensitive data from hackers and malicious insiders, provides a fast and cost-effective route to regulatory compliance, and establishes a repeatable process for data risk management.

Powering the SecureSphere Data Security Suite is a common platform that provides flexible deployment options, unified management, deep analytics, and customizable reporting. The SecureSphere platform enables enterprise scalability and accelerates time to value.

SecureSphere Data Security Suite:

- Protects web applications from complex, large scale online attacks
- Secures and audits access to business-critical databases and files
- Focuses forensic analysis for effective incident response
- Reduces data risk by detecting sensitive data, mitigating vulnerabilities, and removing excessive rights




### Address the Full Variety of Information System Deployment Modes

As the information technology industry turns to cloud computing, virtualization and outsourcing, a third requirement of covering a wide range of deployment models has become critical for many organizations. To meet this need, Imperva delivers not just traditional enterprise products, but also large-scale solutions for service providers and cloud infrastructure services as well as product and service options to scale down to mid-market and small businesses.



# Database Security

SecureSphere Database Security solutions secure sensitive data stored in databases. SecureSphere provides full visibility into data usage, vulnerabilities, and access rights. It enables security, audit, and risk professionals to improve data security and meet compliance mandates.


SecureSphere will:

- Audit all access to sensitive data by privileged and application users
- Alert or block database attacks and abnormal access requests, in real time
- Detect and virtually patch database software vulnerabilities based on Imperva ADC research – reducing the window of exposure
- Identify excessive and dormant user rights to sensitive data
- Accelerate incident response and forensic investigation with advanced analytics

### SecureSphere Database Activity Monitoring (DAM)

Delivers automated scalable activity monitoring, auditing, and reporting for heterogeneous database environments. SecureSphere helps organizations demonstrate regulatory compliance through automated processes, analysis, and reporting. SecureSphere accelerates incident response and forensic investigation with centralized management and advanced analytics.

### SecureSphere Database Firewall (DBF)

Provides real-time database protection against internal and external threats by alerting or blocking attacks and abnormal access requests. SecureSphere provides virtual patching for database software vulnerabilities, reducing the window of exposure and impact of long patch cycles. DBF includes the auditing and analytics capabilities offered by DAM.

### User Rights Management for Databases (URMD)

Enables automatic aggregation and review of user access rights. SecureSphere helps identify excessive rights and dormant users based on organizational context and actual data usage. Using URMD, organizations can demonstrate compliance with regulations such as SOX, PCI 7, and PCI 8.5 and reduce the risk of data breach.

### SecureSphere Discovery and Assessment Server (DAS)

Provides vulnerability assessment and configuration audits allowing users to measure compliance with industry standards and best practices. Data discovery and classification enable organizations to accurately scope security and compliance projects. With a combined analysis of sensitive data and vulnerabilities, SecureSphere helps prioritize and better manage risk mitigation efforts.

# File Security

SecureSphere File Security solutions protect sensitive files on file servers, storage devices, and content repositories. SecureSphere provides full visibility into data ownership, usage, and access rights and enables executives, auditors, security, and IT managers to improve data security and meet compliance mandates.


SecureSphere will:

- Audit all access to sensitive files by privileged and application users
- Alert on or block file access requests that violate corporate policies
- Identify excessive user rights to sensitive files and enable a complete rights approval cycle
- Accelerate incident response and forensic investigation through centralized management and advanced analytics

## SecureSphere File Activity Monitoring (FAM)

Delivers real-time monitoring and auditing of access to files stored on file servers and network attached storage (NAS) devices. SecureSphere file auditing provides flexible alerting, analytics, and reporting so administrators can document and communicate access activity to key stakeholders, and demonstrate regulatory compliance. FAM includes User Rights Management for Files for file rights auditing.

## SecureSphere File Firewall (FFW)

Prevents internal abuse and unauthorized access of sensitive file data, and helps ensure file integrity. SecureSphere monitors access activity, generates alerts based on user-defined rules, and blocks access that violates business policy. Centralized management, analytics, and reporting accelerate forensic investigations and security incident response. FFW includes User Rights Management for Files for file rights auditing.

## SecureSphere User Rights Management for Files (URMF)

Identifies existing user access rights and facilitates a complete rights review cycle. SecureSphere file rights auditing ensures sensitive file data is accessible only by those with a business need to know. SecureSphere facilitates rights review cycles by creating a baseline of existing rights, identifying excessive and unused rights, and providing workflow capabilities to specify and communicate changes between all participants in the review process. URMF is included as part of SecureSphere FAM and FFW.



# Web Application Security

SecureSphere Web Application Security solutions protect Web applications from cyber attacks. SecureSphere continuously adapts to evolving threats and enables security professionals, network managers, and application developers to mitigate the risk of a data breach and address key compliance requirements such as PCI 6.6.


SecureSphere will:

- Model legitimate Web application usage
- Alert or block access requests that:
  - Deviate from normal application and data usage
  - Attempt to exploit known and unknown vulnerabilities
  - Originate from malicious sources
  - Violate corporate policies
  - Are part of a sophisticated multi-stage attack
- Update Web defenses with research-driven intelligence on current threats
- Virtually patch application vulnerabilities through integration with Web application vulnerability scanners, reducing the window of exposure and impact of ad-hoc application fixes

## SecureSphere Web Application Firewall (WAF)

The market-leading Web Application Firewall delivers automated protection against current application attacks, including SQL injection, XSS, and CSRF. SecureSphere combines automated application learning with up-to-date protection polices and signatures from the Imperva Application Defense Center to accurately identify and stop attacks. Granular correlation rules, reputation-based security, and a powerful reporting framework complete SecureSphere's superior multi-layer protection. With multi-gigabit inline and non-inline configuration options, SecureSphere offers drop-in deployment and ultra high performance meeting the most demanding data center requirements.

## ThreatRadar

As an add-on security service for the Web Application Firewall, ThreatRadar bolsters defenses against large-scale automated attacks. ThreatRadar enables timely, real-world protection from known attack sources, such as malicious IP addresses and phishing URLs, as well as identifies source reputation and geographic location for forensics. By transmitting attack source feeds in near real time to SecureSphere WAFs, ThreatRadar can quickly and accurately stop malicious users before an attack can be launched.

# SecureSphere Platforms

The SecureSphere platform is the cornerstone of Imperva's award-winning data security products. The SecureSphere platform includes centralized management and reporting framework, physical and virtual appliance delivery options, and server agent software that extends data security to host systems. The SecureSphere platform, with its flexible deployment options and administration capabilities, provides organizations the scalability, adaptability, and management needed to deploy state of the art data security solutions.

## Management, Analytics, and Reporting

The SecureSphere MX Management Server is a centralized management platform for multiple SecureSphere gateways. It provides a single point for aggregating security policy, hierarchical security management, real-time monitoring, logging, auditing, and compliance reporting. The SecureSphere MX Management Server can simultaneously manage SecureSphere Database, File, and Web Security gateways from a single console.

## Hardware and Virtual Appliances

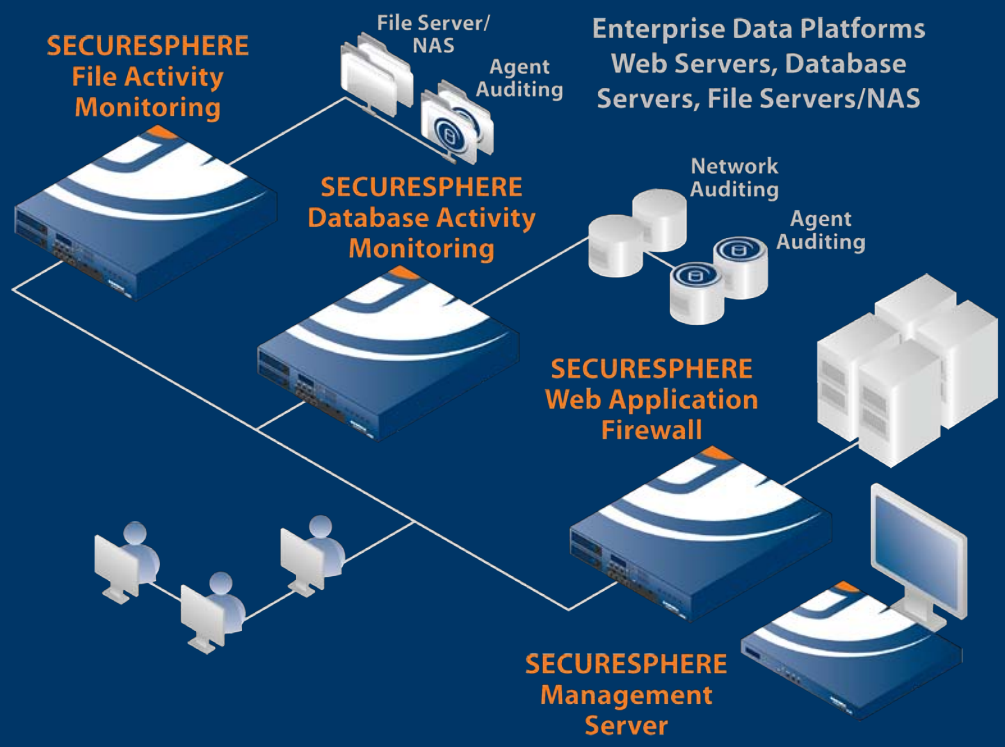
SecureSphere hardware appliances provide superior performance, scalability, and resiliency for demanding network environments. Fail-open interfaces offer fast, cost-effective high availability. For the most demanding applications, Imperva offers appliance models featuring redundant, hot-swappable power, fans and drives. SecureSphere virtual appliances provide the complete SecureSphere product line in a flexible, easy to install software solution. Virtual Appliances allow organizations to use existing server hardware and cut power, cooling, and support costs.

## Agents

For 360 degree visibility into user activity, SecureSphere extends its monitoring, auditing, and enforcement capabilities to host servers. The light weight SecureSphere agent can be used to audit database activity and protect sensitive data with minimal impact to the server performance. Agent communications to the SecureSphere appliance are buffered and encrypted to prevent data loss or compromise. SecureSphere agents can optionally block user activity and quarantine user accounts in the event of a security violation.



# Imperva SecureSphere Data Security Suite




*SecureSphere Data Security Suite is the market leading data security and compliance solution. SecureSphere protects web applications and sensitive file and database data from hackers and malicious insiders, provides a fast and cost-effective route to regulatory compliance and establishes a repeatable process for data risk management.*


**Imperva**

3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
Tel: +1-650-345-9000

www.imperva.com