



# IT Services Company Achieves 360° Web Application Security with Imperva SecureSphere Virtual Appliances

## Overview

An IT services and business software company with more than 20,000 employees provides data center hosting services for its own financial applications and for third-party Web applications. Many of these Web applications are Internet-facing and are regulated by the Sarbanes-Oxley and Gramm-Leach-Bliley Acts. The Company needed to protect sensitive data in its custom and packaged Web applications.

With dynamic, highly-customized applications, it was difficult for the Company's security team to stay on top of application changes and enforce vulnerability remediation. While security is a top priority, continually scanning applications after every change was burdensome. It required significant coordination between application developers and security engineers. Both groups needed to investigate assessment results, identify real, exploitable threats, and then developers needed to code and apply fixes. While security is essential, it had to be balanced with application features, usability, and other business requirements.

The Security Officer for the business software unit realized that a Web Application Firewall could satisfy the Company's security requirements without impacting release schedules. It would provide instant vulnerability remediation, enabling the Company to roll out new application releases without disruptive emergency fix cycles. While the Company would continue to perform application scans and fix discovered vulnerabilities, these processes would not slow down release cycles.

## Imperva SecureSphere Meets and Exceeds Company's Requirements

The security team realized that a Web Application Firewall would be a strategic investment for the Company. Therefore, they established detailed product requirements and laid out a thorough evaluation process that would include a hands-on proof of concept and application penetration tests. Based on an internal analysis, the security team developed the following criteria:

- **Accurate Web application protection**

The Web Application Firewall had to stop all application attacks without blocking legitimate traffic. Therefore, the security team would perform extensive vulnerability assessments against potential solutions to ensure that they correctly detected attacks.

- **Easy deployment in a virtualized environment**

The Company had moved much of its infrastructure, including Web applications, databases, and load balancers, to VMware. They maintained a remote disaster recovery site that mirrored the infrastructure at their primary site. With a completely virtual architecture, the Web Application Firewall would also need to be a virtual appliance.



### Customer

Fortune 500 IT Services and Business Software Company

### Requirements

- Protect internally-developed and hosted Web applications
- Meet SOX and GLBA compliance requirements
- Integrate seamlessly into virtualized environment
- Provide detailed, clear log messages for security and forensics

### Solution

Imperva SecureSphere virtual appliances provides comprehensive protection and granular security policies for a corporate data center and disaster recovery site

### Bottom Line

- SecureSphere provides continuous, real-time Web application security
- New Web applications can be brought to market faster because emergency application fix cycles are eliminated
- Centralized management enables wide-scale deployment and accelerates data restoration

- **Granular security policies**

Security engineers at the Company needed to be able to fine tune policies based on specific application requirements. Because the Company would be protecting both packaged and internally developed applications, the security engineers would need to be able to create different policy sets per application.

- **Detailed, relevant alerting and reporting**

The Web Application Firewall would be used not only to block attacks, but also to monitor application usage and improve application development processes. Therefore, the Web Application Firewall had to provide comprehensive alerts that contained the full HTTP request and clearly identified what part of the request violated a security policy.

- **Virtual patching**

The Company uses IBM AppScan and HP WebInspect to detect Web application vulnerabilities. The Web Application Firewall should be able to integrate with these tools to virtually patch application vulnerabilities. Virtual patching would allow the Company to enforce stricter security rules for known vulnerable application elements.

The Company performed an in-depth evaluation of several Web Application Firewalls. Security engineers conducted penetration tests and analyzed product management and usability. The Imperva SecureSphere Web Application Firewall performed exceedingly well in security tests, but it especially outshone alternative solutions with its comprehensive logging and its custom security policies. According to the Security Officer, "SecureSphere provided the best logging, capturing the entire request and pinpointing the exact string that triggered an alert or block action. With SecureSphere, we have the detail necessary to investigate and act on security events."

## **Flexible Deployment into a Virtualized Environment**

For the Company, a virtual appliance form factor is essential. The Company has migrated their applications to VMware and designed high availability into every aspect of their application infrastructure. At each site, multiple load balancing virtual instances are configured to monitor application availability and reroute traffic if an application server became unavailable. If, for any reason, the SecureSphere Web Application Firewall is unresponsive, the load balancing virtual instance can route traffic around the virtual instance—providing cost-effective high availability.

In the event that the entire primary site went down, all traffic can be routed to a disaster recovery site. The Company automatically replicates its virtual infrastructure from the primary site to the disaster recovery sites. Because SecureSphere is available as a virtual appliance, it can easily be re-deployed to the Company's redundant virtual data centers.

SecureSphere also offers several features that address management and scalability requirements. First, SecureSphere supports centralized management, so all policy configuration, Web application profile management, signature updates, and monitoring

*"Application security is essential for our organization. The SecureSphere virtual appliance enables us to protect our Web applications and improve our development processes—without slowing down our application development schedules."*

**SECURITY OFFICER,  
FORTUNE 500 IT SERVICES AND  
BUSINESS SOFTWARE COMPANY**

and alerting functions can be managed from one location. This enables the Company to easily manage and configure multiple virtual appliances, streamlining administrative tasks.

The Company also needed to protect multiple Web applications, including in-house applications and packaged third party applications. Using SecureSphere's hierarchical management features, the Company can configure policies at the application, group or global level. Out-of-the-box security policies protect the Company's applications against Web attacks like SQL injection, cross-site scripting, and directory traversal. However, the security team really appreciates SecureSphere's granular custom policies. The security team can build custom policies based on a myriad of conditions—source IP address, violation type, destination URL, header information, cookies, number of occurrences, and many more—to address unique requirements.

### **SecureSphere Enhances SDLC with Monitoring and Virtual Patching**

The Company has begun to incorporate SecureSphere into its software development processes. Both security engineers and application developers examine security alerts to understand how hackers are attacking the site. Graphical reports identify application errors, most attacked Web pages, and other security statistics. Before deploying Imperva SecureSphere, the security team knew that its sites were getting attacked. But now, security engineers and developers have a clearer picture of the attacks and probes that are targeting their applications.

The Company also virtually patches vulnerabilities found by its application assessment solution. While security engineers are just beginning to leverage these capabilities in production, they are already realizing the benefits. According to the Security Officer, "Virtual patching protects our applications in that critical time between when a vulnerability is discovered and it is patched in the application."

Imperva SecureSphere is the optimal choice for the Company because it offers accurate Web application protection, virtual patching, enterprise-grade policy control, and detailed alerts—all while supporting the organization's virtual appliance requirements. "When combined with vulnerability scanning, Imperva provides 360° application security and it offers us cost savings because we can bring applications to market faster, knowing that they are protected."

