



Comparison

SecureSphere Vs. Intrusion Prevention Systems

Web applications are a prime target for attack. Ninety two percent of businesses have suffered from a successful Web application attack in the past twelve months according to an FBI survey.¹ And twenty one percent of organizations had experienced a data breach due to an application attack.² Traditional network security products such as deep-inspection firewalls and intrusion prevention systems (IPS) cannot prevent application layer attacks.

New compliance regulations such as the PCI Data Security Standard now mandate application layer protection. Businesses that process, store or transfer credit card data must install a Web application firewall in front of their Internet facing Web applications or undergo a source code audit.

The SecureSphere Web Application Firewall protects Web applications and sensitive data. It provides your business with a practical, highly-secure solution to ensure that your business meets today's application security and compliance requirements.

SecureSphere Overview

The SecureSphere Web Application Firewall delivers accurate and comprehensive protection for Web applications and Web Services (XML) applications. SecureSphere leverages multiple security defenses simultaneously—including Dynamic Profiling, up-to-date security content, protocol validation, session tracking, and platform attack prevention—to provide the highest level of Web application security available.

With SecureSphere, organizations are protected against dangerous and costly attacks such as SQL injection, session hijacking, parameter tampering, and cross-site scripting. SecureSphere also inspects sensitive data sent over HTTPS (SSL), communications that are typically ignored by network security devices.

Intrusion Prevention Systems (IPS)

Intrusion Prevention Systems were developed to detect and optionally block the types of attacks not visible to a standard network firewall. Intrusion Prevention Systems look at the contents of a packet's data payload and compares it to a list of known attack patterns (or signatures) that are derived from documented vulnerabilities. IPS products can also enforce protocol restrictions to protect against known protocol vulnerabilities.

¹ CSI/FBI Computer Crime and Security Survey, 2006

² Aberdeen Group, "Developing Secure Applications: Built-in or Bolted On?", May 2007

Why are Intrusion Prevention Systems (IPS) insufficient at providing total application security?

Intrusion Prevention Systems are ineffective against targeted Web hacks and unauthorized database breaches. Web attacks target vulnerabilities that are unique to the individual application and the internally developed application logic. Since each vulnerability is unique to the targeted application, known signatures and protocol restrictions will not prevent these types of threats.

How is Web application security different from Intrusion Prevention?

Solving application security issues requires a deep understanding of all the elements of the application and database, including URL parameters, cookies, form field inputs, and SQL queries, among others. IPS products do not track this application information and do not protect against attacks against the application or database. SecureSphere offers a unique value in protecting actual applications and databases themselves (as opposed to just the supporting platforms and infrastructure software). The primary security benefit of application security is preventing malicious users from abusing legitimate applications to access or change critical business information.

Does SecureSphere replace an Intrusion Prevention System (IPS)?

It depends. In the data center, where companies are primarily focused on protecting sensitive Web and database applications, SecureSphere will replace existing IPS products by delivering full application level security. However, SecureSphere's deep inspection firewall is focused primarily on protecting applications and databases as opposed to departmental servers or client computers on user segments. IPS products focus primarily on users and departmental segments and can protect many different types of protocols. Therefore, IPS products still play a valuable role because they inspect can mail, FTP, Windows file sharing, Microsoft RPC communications, and many other protocols from attacks and intrusions.

Both SecureSphere and a network Intrusion Prevention System (IPS) offer the following features:

- Signature-based protection from known network, operating system, and Web server software attacks
- Signature-based protection from generic Web application attacks like SQL injection and directory traversal
- Automated security content updates
- Behavior-based policies and analysis

Security and Feature Comparison

The table on the following page compares the security and features of the SecureSphere Web Application Firewall and an Intrusion Prevention System.

	SecureSphere	IPS
Inspect TCP handshake	✓	✓
Normalize traffic ¹	✓	
Decrypt and inspect SSL ²	✓	
Enforce protocol conformance	✓	✓
Session/cookie protection	✓	
Input validation (White List)	✓	
Attack detection (Black List) ³	✓	✓
Correlated Attack Validation	✓	Limited
Block attacks	✓	✓
Block user sessions	✓	
Block data leaks ⁴	✓	Limited
Rewrite content	✓	
Application level auditing ⁵	✓	
Application user tracking	✓	
Optional database security and auditing	✓	

¹ **Normalize traffic:** Decode encoded content, such as URL encoded or UTF encoded content

² **Decrypt and inspect SSL:** SecureSphere can interface to a FIPS-certified HSM or store a copy of the SSL key. Most IPS products cannot inspect SSL/HTTPS traffic. However, McAfee IntruShield is one exception.

³ **Attack detection (Black List):** Includes application, Web server, operating system, and network attacks

⁴ **Block data leaks:** Inspects outbound traffic for credit card numbers, CVV, SSN, custom signatures.

SecureSphere Advantages

SecureSphere was designed from the ground up to protect Web applications from every kind of security threat. Intrusion Prevention Systems cannot deliver this level application security.

- Only SecureSphere tracks and maintains session state information.
- Only SecureSphere profiles protected Web applications. It compares cookies, parameters, form fields, referrers, and user behavior to expected behavior.
- Only SecureSphere protects HTTP, HTTPS (SSL) and XML traffic. IPS's like Tipping Point cannot decrypt and inspect HTTPS (SSL) traffic. So the most sensitive transactions are completely unprotected.
- Therefore, SecureSphere alone can prevent:
 - Parameter tampering
 - Session hijacking
 - Session replay
 - Cookie injection
 - Cookie poisoning

- Brute force login attempts
- Illegal HTTP encoding (double encoding, malicious encoding)
- XML and SOAP attacks

An IPS detects some intrusion signatures, but it cannot place those signatures in context because it cannot parse HTML for the individual elements, fields, JavaScript, cookies or compare behavior to expected, profiled behavior. So, unlike SecureSphere, an IPS cannot accurately block:

- SQL injections
- Cross-site scripting attacks
- Application specific buffer overflow attacks
- Unknown, zero-day web worms
- Site scanning and reconnaissance
- OS command injections in form fields

SecureSphere automatically profiles web applications to model the structure and all of the elements of protected applications. By analyzing web traffic over time, it also develops a baseline of standard behavior. SecureSphere correlates deviations from expected behavior with attack signatures to accurately block all types of application threats.

Because of these advantages, SecureSphere delivers complete application protection. That is why the SecureSphere Web Application Firewall is the only choice to meet organizations application security and compliance requirements.



US Headquarters
950 Tower Lane
Suite 1550
Foster City, CA 94404
Tel: +1-650-345-9000
Fax: +1-650-345-9004
www.imperva.com

International Headquarters
125 Menachem Begin Street
Tel-Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200