



Conventional Web Server Protection is Not Enough –

Web servers are constantly in the line-of-fire as cyber-criminals prowl internal networks and the Internet searching for vulnerable systems. Hackers scan for open network doors, exploit custom code and commercial platform vulnerabilities and devise new techniques to disable web servers and steal or damage private information. Thwarting these evolving threats requires a multi-layered defense approach – one that combines the very best in conventional “rules-based” technologies to detect and block known threats with advanced behavioral components that can identify suspicious traffic and take immediate preventative action before the damage is done.

What is ThreatSentry?

ThreatSentry is a Web Application Firewall designed to protect Windows Web servers running Microsoft Internet Information Services (IIS). ThreatSentry is comprised of two powerful defense components – a **Web Application Firewall**, pre-configured with a dynamic and customizable knowledgebase of known attack characteristics and an advanced **Behavioral Engine** that profiles typical system activity to detect deviations from normal patterns as well as events that are similar to known attacks. Each server connection is scrutinized by both components to identify and take action against any activity falling outside trusted parameters. ThreatSentry’s intrusion prevention capabilities progressively improve as the baseline evolves automatically or based on input from the system administrator.

ThreatSentry Feature Matrix –

ThreatSentry Feature	
AI-Based neural behavioral engine	✓
State-of-the-art IIS Web Application Firewall	✓
Protection from known & unknown threats to IIS	✓
Protection from internal and external threats to IIS	✓
Comprehensive Intrusion & Threat Blocking options	✓
Extensive Requests rules control/management	✓
SQL Injection, XSS, DDOS, etc. protection	✓
Email/Pager/Cell Phone Security Alert notification	✓
Supervised and Self learning capabilities	✓
Security Alert/Training Data logs	✓
WHOIS database search	✓
On-screen & Audio Security Alert notification	✓
Adjust settings w/out IIS restart	✓
All-Port Firewall for Blocked IPs	✓
Extensive Blocked IP management options	✓
Intrusion Detection Only Mode	✓
Free install/evaluation session	✓
Technical Support	✓
HTML Reports	✓
Multi-server installation	✓
Centralized policy management	✓
Centralized Monitoring	✓
Remote/consolidated Security Alert log storage	✓
Price per server (includes 1 yr of support)	\$649

What Customers Say –

“ThreatSentry has become standard issue on all of the production servers that we design and implement. Being able to detect anomalies within data that flows from the Internet to IIS on the application layer is a very powerful feature that takes over where traditional stateful packet inspection firewalls leave off. The fact that ThreatSentry has the ability to intuitively “blacklist” the offending IP after it exceeds the preset thresholds really impressed us. This allows us to have a completely set and forget proactive security solution for our clients that run IIS.”

— Sean Furman, President, STF Consulting CEO, Rumson, NJ

“Threat Sentry has proved to be an invaluable tool for detecting and preventing malicious hack attempts on our public web server. It’s an extra layer of protection that allows us to analyze and track hack attempts without having to dig through IIS logs. It has already protected us from a scripted attack that -tried- to gain access to our server 76 times within a two minute period. Go ThreatSentry, Go!!!”

— Dave S., BSCS, MMCP, Database Programmer Analyst, Allentown, PA

Key Benefits

1

Increase System Availability

Surpasses the capabilities of conventional pattern matching, rules, and policy-based systems to better protect network weak points, and mitigate the impact of lapses in patch management, configuration errors, and the use of new and progressive attack techniques.

2

Reinforce Regulatory Compliance

ThreatSentry enables you to not only block unauthorized or unwanted activity but also better understand your web applications, web traffic, and vulnerabilities. Together, these capabilities enable you to demonstrate clear compliance with the regulatory demands of PCI DSS, SOX and HIPAA.

3

Maximize IT Budget

Implemented as an ISAPI extension and Snap-in in to the Microsoft Management Console (MMC), ThreatSentry is exceptionally easy to use and affordably priced for enterprises of any size.

Key Features

Unsurpassed Protection from Known/New, Internal/External Threats –

ThreatSentry is invaluable in protecting IIS servers from an array of vulnerabilities including SQL Injection, Cross Site Scripting, Directory Traversal, Parameter Manipulation, Buffer Overflow, Parser Evasion, High-bit Shellcode, Remote Data Services, and others.

Unparalleled Affordability and Ease-of-Use –

Implemented as an IIS ISAPI extension and manifested as a snap-in in to the Microsoft Management Console (MMC), ThreatSentry is exceptionally easy to use and affordably priced for enterprises of any size.

Logging, Reporting and Audit Features –

Review, sort, manage or export Security Alerts and Training Events. Track and audit reclassified events. Investigate security event details via ThreatSentry Event details. Integrated WHOIS lookup, logs and reports.

Breakthrough Combination of Advanced Technologies –

ThreatSentry is a hybrid solution, pre-configured with an extendable knowledgebase of known exploitive techniques and attack characteristics. ThreatSentry's behavioral engine detects any activity falling outside trusted parameters.

Centralized Network Management –

ThreatSentry snaps into the Microsoft Management Console (MMC) and features an intuitive user interface for multi-server management and configuration and reporting.

Security Alert Notification –

ThreatSentry Security Alerts can be transmitted to administrators via email, pager and/or cellular phone.

Expanded Security Modes –

In addition to Monitoring – Active, wherein ThreatSentry detects, alerts, and blocks untrusted requests, a Monitoring – Inactive Security Mode (Intrusion Detection only) is now available. In this mode, ThreatSentry detects and alerts when untrusted events are identified, but does not block or take any other preventative action.

Fully integrated Firewall – Blocks all network ports for Black Listed IPs.

Outlook Web Access Compatible – ThreatSentry is compatible with Outlook Web Access.

System Requirements

Microsoft Windows Server 2000/2003
Microsoft Internet Information Services 5.0/6.0
Intel processor (>700 MHz)
64 MB available RAM
20 MB of available disk space

Contact Information

Privacyware
Red Bank, NJ 07701
732-212-8110
info@privacyware.com

About Privacyware

Privacyware (www.privacyware.com) is an innovative provider of web application security, intrusion prevention and security data analytics software. Privacyware web application security and desktop defense offerings increase the level of protection from new and known malware, intrusions and other threats to individual, small business and large enterprise computing environments. Privacyware security data analytics products help enterprise security and compliance personnel overcome the increasingly critical challenge of security data overload, better understand the environments for which they are responsible and more effectively identify and comprehend malicious, unauthorized and/or deviant activity. Privacyware is a Microsoft Gold Certified Partner.



**Business Process and Integration
Data Management Solutions
ISV/Software Solutions**