



threatsentry

Multi-Layered Defense for IIS

- ❖ **State-of-the-art Web Application Firewall** – Provides configurable and extensible rules-based control over HTTP/HTTPS request methods (OPTIONS, GET, POST, HEAD), URL Paths, URL Path Request Frequency, URL Query String length, and HTTP Request Headers.
- ❖ **Behavior-based Intrusion Prevention Component** – Adaptive, behavior-based engine (with sensitivity control) analyzes Web traffic patterns to detect new threats and behavioral deviations.
- ❖ **Fully integrated Firewall** – Proprietary NDIS driver delivers flexible network IP blocking (featuring white list, black list and duration control) at TCP/IP and UDP layers for all ports.
- ❖ **Anti-DoS/DDoS** - Configurable request frequency monitor blocks successive requests to individual or all site pages to reduce the risk of DoS and DDoS attacks.

"ThreatSentry is working beautifully. We are now PCI compliant, thanks to your software." – Leading US Electronic Payments Processor

Key Features & Benefits

PCI DSS Section 6.6 Support – Fulfills the web application layer firewall (WAF) requirement in [PCI DSS 6.6](#) and aids in the web application code review process by revealing vulnerabilities embedded within the software.

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 can be installed and deployed in minutes, is exceptionally easy to use and affordably priced for enterprises of any size.

Attack Detail – Comprehensive detail regarding all blocked requests, including time stamp, source/destination IP address, blocking Type (WAF, BE, Network Firewall), Parameter, Target URL path, HTTP method, WHOIS data, etc. are provided within the Management Console's integrated Security Alert Log.

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.

Technical Compatibility – Compatible with IIS Lockdown, URLScan, and major third party server-side scripting platforms like ASP, ASP.NET, PHP, JSP, ColdFusion, and Perl.

Management and Configuration Tools – Email alert notification, compliance and security reporting, Regular Expression support, Active and Passive security modes.

"Threat Sentry has proved to be an invaluable tool for detecting and preventing malicious hack attempts on our public web server. 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

| | |
|--|--|
| System Requirements Microsoft Windows Server 2000/2003/2008 Internet Information Services 5.0/6.0/7.X Intel processor (>700 MHz) 64 MB available RAM 20 MB of available disk space | About Privacyware Privacyware (www.privacyware.com) is an innovative provider of award-winning pc security, web application firewall and security data analytics software. Privacyware products leverage conventional and advanced behavioral technologies to help systems administrators, IT security and compliance personnel more effectively identify, understand and prevent malicious, unauthorized and/or deviant computing system activity. |
| Contact Information Privacyware Red Bank, NJ 07701 732-212-8110 info@privacyware.com |  Business Process and Integration Data Management Solutions ISV/Software Solutions |