threatsentry

✧ **State-of-the-art IIS Web Application Firewall –** Configurable 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 brute force, DoS and DDoS attacks.

✧ **Physical systems or in the Cloud** – Application layer protection designed for physical or virtual infrastructures.

"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 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 – ThreatSentry supports Windows Server 2019, 2016, 2012/R2, 2008/R2, 2003 and 2000 and IIS versions 5 – 7-10 (native IIS module), 6 (ISAPI Extension) and 5 (ISAPI Filter) on 32 and 64 bit systems. 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	About Privacyware
Windows Server 2000 through 2019 Internet Information Services 5-10 Prerequisites: Microsoft SQL Server or Microsoft SQL Express	Privacyware (www.privacyware.com) develops the leading software–based Web Application Firewall and Host IPS for Microsoft Internet Information Services (IIS). Privacyware products leverage conventional and advanced analytics technologies to help systems administrators, IT security and compliance personnel more effectively identify, understand and prevent malicious and/or unauthorized computing system activity. Privacyware is a member of the Microsoft Partner Network with a Silver Application Development competency.

Contact Privacyware for more information and free evaluation software: 614-656-1956 x235, info@privacyware.com

Microsoft Partner
Silver Application Development