

**Current Methods of Server Protection are Incomplete**

Web server applications such as Microsoft IIS are constantly in the line-of-fire as hackers and others intent on malicious activity prowl internal networks and the Internet searching for their next unsuspecting victims.

In a battle of wits and creativity, hackers are always on the lookout for open network doors, exploitable vulnerabilities or new techniques to outfox their victims. New and hybrid strains of known viruses, intrusion techniques and other misuse originating from inside and outside the network are continuously concocted and launched. Thwarting these attacks requires more than an array of firewalls and ant-virus solutions splayed across the network. Today, IT managers need the ability to stay one step ahead of the attackers.

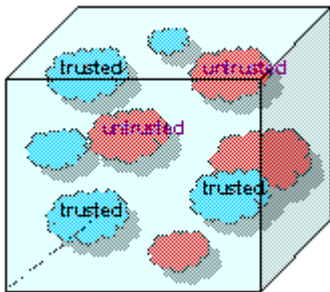
**What is ThreatSentry?**

ThreatSentry™ is an advanced neural application that uses a complex automated learning process, a knowledge-base of documented exploits, and an analysis model specifically designed for Microsoft® Internet Information Services (IIS), to continuously collect, analyze and organize server events into an evolving baseline of acceptable activity. Each server connection is compared against this baseline to identify and take action against any activity falling outside of acceptable parameters. Because ThreatSentry is founded on a breakthrough machine-learning convention, it is remarkably easy to deploy and maintain.

**How Does It Work?**

ThreatSentry is comprised of two key components. The first is implemented as an ISAPI filter which collects and feeds data to the Adaptive Security Engine (ASE). Leveraging a breakthrough combination of applied mathematic and cybernetic approaches that enable machine learning and analysis of the network security information, ASE continuously monitors the vital aspects of IIS operation. ASE detects abnormal requests and other unusual traffic enabling ThreatSentry to prevent any type of activity that could be harmful to the network.

1

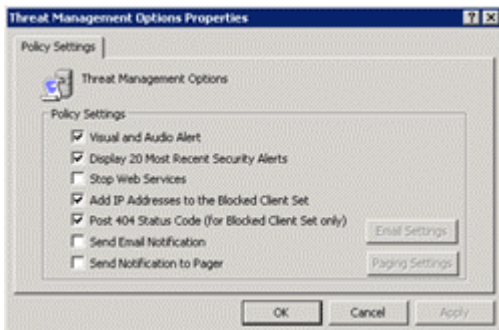


Upon installation ThreatSentry begins to collect and organize IIS-specific data into clusters that reflect the normal use patterns (both trusted and untrusted) within the server environment, ("Training Mode"). The process of organizing these clusters is guided through the use of a built-in knowledgebase of published attack signatures. Once the required number of training events has been collected, ThreatSentry shifts automatically into "Monitor" mode.

**Maintenance Tip #1:** To ensure optimized accuracy and effectiveness, it is important to review the classification of events in the **training database** to validate that they have been classified correctly.

2

In "Monitor Mode" ThreatSentry compares all incoming requests to IIS against the Training Database to determine whether it falls within acceptable distance of trusted activity. If it does, the process continues. If it does not, ThreatSentry initiates whatever action/s have been configured, ranging from posting an on screen alert, to blocking the untrusted connection, or shutting down IIS.



3

Maintaining ThreatSentry is simple. As described in the maintenance tips above, proper classification of events is essential and can be accomplished as Security Alerts are displayed, or during periodic review of the Security Alert Log. After one or more events have been reclassified, the Training Database should be "Re-Trained" upon which ThreatSentry will remember not only the correct classification of the particular event/s, but also its various characteristics which will be applied to the analysis of subsequent events.



**Maintenance Tip #2:** To ensure progressively improved accuracy and effectiveness, it is important to review the classification of events in the **Security Alert Log** to validate that they have been classified correctly.

## Key Benefits

- 1 **Unsurpassed detection of known, unknown and hybrid attacks:** ThreatSentry leverages security data and attack signatures in a new way that eliminates the limitations inherent in simple pattern matching and provides flexibility beyond rules-based systems. ThreatSentry applies cognitive reasoning to the analysis of server events thereby improving the ability to detect new or novel threats.
- 2 **Progressively improved system accuracy and effectiveness:** ThreatSentry can be retrained at any time to reflect its own (unsupervised) or user-influenced (supervised) classification of events. Event classification is always based on the current status of the environment being monitored ensuring progressively improved accuracy and effectiveness.
- 3 **Reduced costs and increased operational efficiency:** ThreatSentry automates and refines some of the most critical tasks performed by experienced system and security administrators freeing them up to focus on other responsibilities.  
  
ThreatSentry eliminates efforts and costs associated with maintaining attack signatures and configuration rules.
- 4 **Easy to deploy and use:** ThreatSentry is pre-configured for Microsoft IIS and during installation, automatically adjusts certain settings specific to the environment it will protect.  
  
ThreatSentry provides an intuitive management console that allows administrators to quickly and easily manage settings on any number of servers, adjust threat classifications and retrain without impeding system or network performance.

## Key Features

- Neural Protection & Approach** – overcomes limitations and operational burden of solutions that rely solely on rules & signatures.
- Comprehensive non-intrusive protection** – provides maximum protection against buffer overflow, parser evasion attacks, directory traversal attacks, general exploitation, in addition to other attacks and security breaches targeted at IIS.
- Management** - features a central console for multi-server management and an intuitive user interface for rich configuration and reporting options. Provides complete security event detail and convenient WHOIS lookup for further investigation of untrusted events.
- Self-configures** – pre-configured analytic model for IIS. Automatically determines size of training database. Powerful default settings.
- Adaptive** – baseline can adjust based on most recent experience to provide immediate attack detection and mitigation.
- Integrated mitigation policy module** – allows ThreatSentry to not only provide attack alerts but also initiate preventative response.
- Unsupervised learning technology** – teaches itself, adapts and reacts as new events are analyzed and classified.
- Supervised learning technology** – allows system administrator intervention to reclassify events, thereby reinforcing system intelligence and accuracy.
- Security Alert Notification** - Security Alerts can be transmitted to administrators via pager and/or cellular phone.
- Server specific configuration** – optimizes system resources and eliminates wasteful analysis, preserves system integrity and enhances system performance.
- Ease of use** – simple to install and configure with low ongoing support, maintenance & TCO.

## System Requirements

Windows 2000/2003 Server w/ IIS 5.0 or higher installed.  
 Intel processor (>700 MHz)  
 64 MB minimum RAM  
 200 MB of free disk space

## Contact Information

Privacyware  
 125 Half Mile Road, Suite 104  
 Red Bank, NJ 07701  
 732-212-8110  
[info@privacyware.com](mailto:info@privacyware.com)

## About Privacyware

Privacyware is the leading provider of advanced threat prevention and security intelligence solutions. The combination of advanced competencies in non-linear mathematics, neural networks and self-learning systems, and proficiency in complex software and systems development allows us to create innovative and intelligent security solutions that are distinguished by their ease of use, advanced analytic capabilities, and the value they deliver to security staff and the greater enterprise. Privacyware solutions fuel the organization's ability to make better decisions and remain a step ahead of hackers and others seeking to compromise critical systems.