



Welcome to the Detroit Tech-Security Conference

JCS Background

JCS & Associates, Inc. (JCS) was founded in 1991 as an I/T Security Sales and Marketing Company specializing in Endpoint Security Solutions.

JCS was McAfee's leading VAR in 1992 in NA and 1993 worldwide.

JCS began reselling Reflex Disknet Pro in 1995, and was named the exclusive North American Distributor by Reflex in 2002.

Reflex Magnetics was acquired by Pointsec in November of 2006. Pointsec was acquired by Check Point in February of 2007, and JCS was named "Check Point Endpoint Security Partner of the Year" for 2007 in March of 2008.

JCS currently has customers in every state and province in North America and offices located in Ann Arbor and Grand Rapids, MI, Minneapolis, MN, Sioux Falls, SD, Boulder, CO and Ottawa, Canada.

JCS has sold, installed and integrated more desktops with end-point security solutions than any other individual VAR in North America.

JCS' expertise helps customers accelerate the evaluation, proof of concept, executive buy-in cycle and installation for agent and non-agent based end-point security solutions.

- **The Network Challenge**
- **The Communications Challenge**
- **The Endpoint Challenge**

The Network Challenge

- ▶ Keep confidential data in

PCI, HIPAA, GLBA, legal liability

- ▶ Keep threats out

Malware, File Sharing Applications, Viruses, Porn

- ▶ Managing policy, procedure & controls

Defining Business Use and Entertainment

Technology Deployment

Training and Education

Regularly Monitor & Verify Technology Use

The Communications Challenge

▶ Everything in the Network is Communications

Packets, protocols, content

▶ Every hole (in/out) is a vector for attack & leaks

What's exposed?

Who's using it?

What's happening?

The Communications Challenge

Technology, by itself, doesn't keep you secure

- ▶ Rule-based systems control known traffic & content
- ▶ Static control vs. dynamic use = incompatible
- ▶ Systems can't tell you what they missed
- ▶ Abuses, errors, accidents, leaks = increased risk
- ▶ It's not technology, it's how it's used
- ▶ Must see actual technology use to determine status

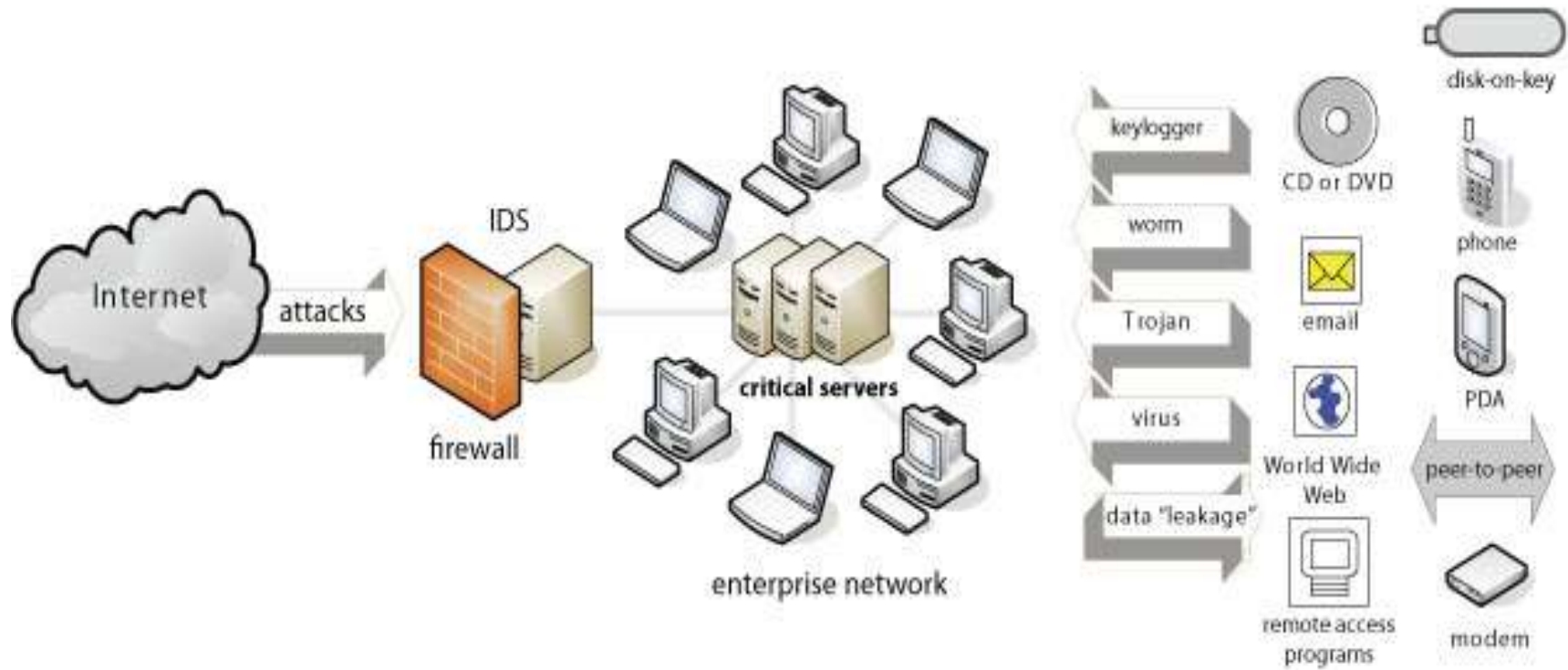
The Endpoint Challenge

- ▶ Endpoint agents are difficult to deploy and manage
- ▶ Endpoint (PCs, Servers, Mac, Linux) applications are inherently unstable
- ▶ Endpoint security applications are even more so
- ▶ Agent software conflicts leading to blue screens are a big issue with most Endpoint security tools
- ▶ Constant updates must be deployed
- ▶ Most security tools can be disabled or tampered with
- ▶ Each tool addresses only one part of the security puzzle
- ▶ Most Endpoint security tools do not have intuitive management consoles

The Endpoint Challenge

The firewall and IDS protect the network from threats through the Internet ...

... but not from threats through the endpoints.



The Endpoint Challenge – What's Out There?

File Sharing Application



Removable Media



Phones



Wireless Internet Cards



Internal and External Modems



Threat Inspector: The Solution to The Network and Communications Challenges

**Being Proactive:
See threats before they hit.**



Threat Inspector®

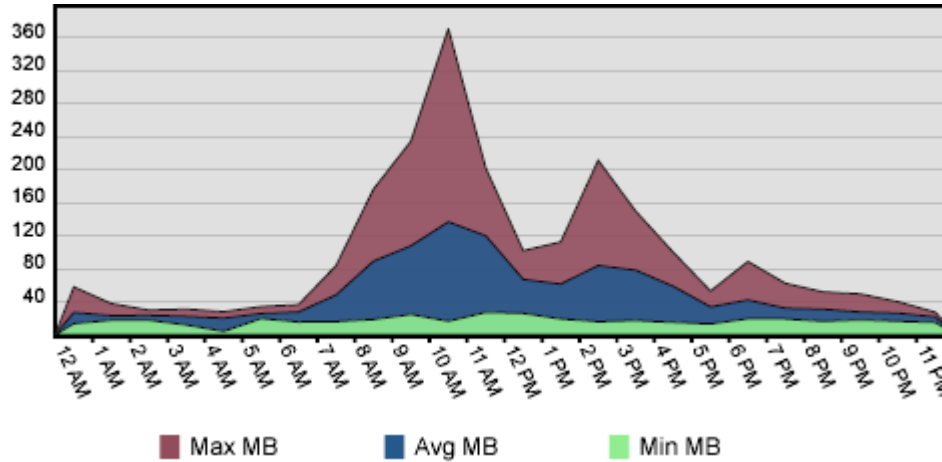
Affordable Security Information Management



What's Normal?

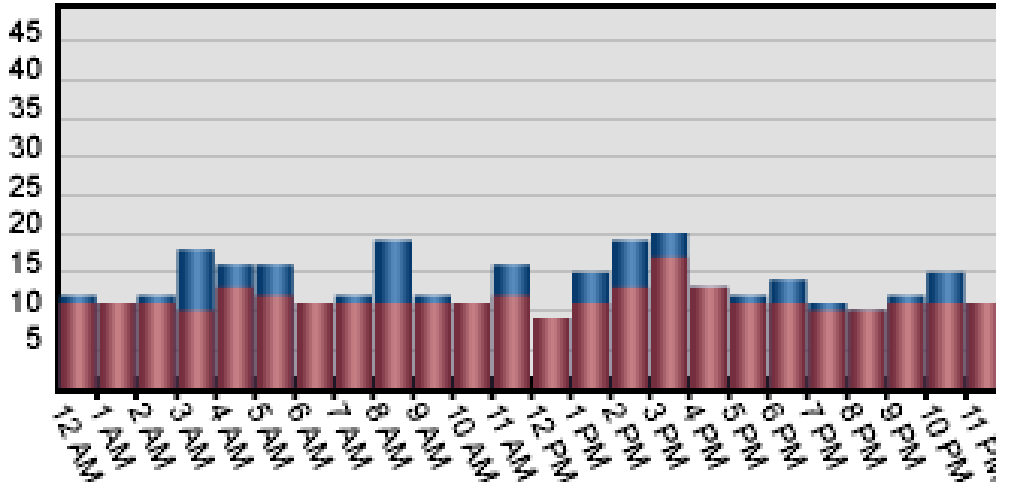
Trust, But Verify...

Threat Inspector

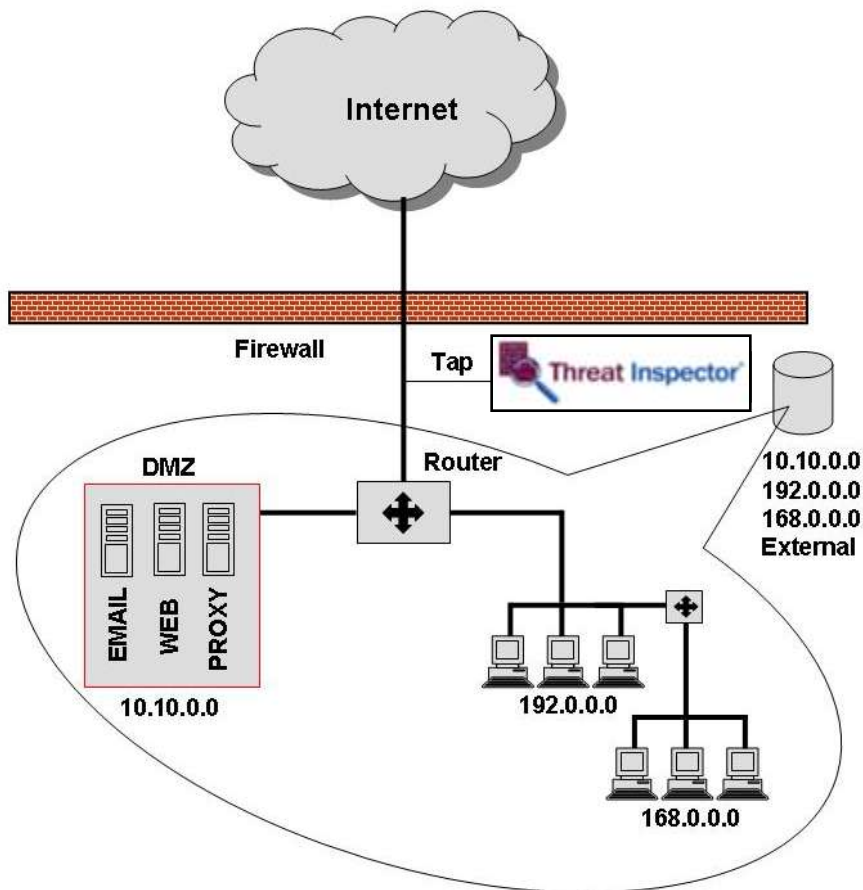


Normal Network Trend

Abnormal Trend



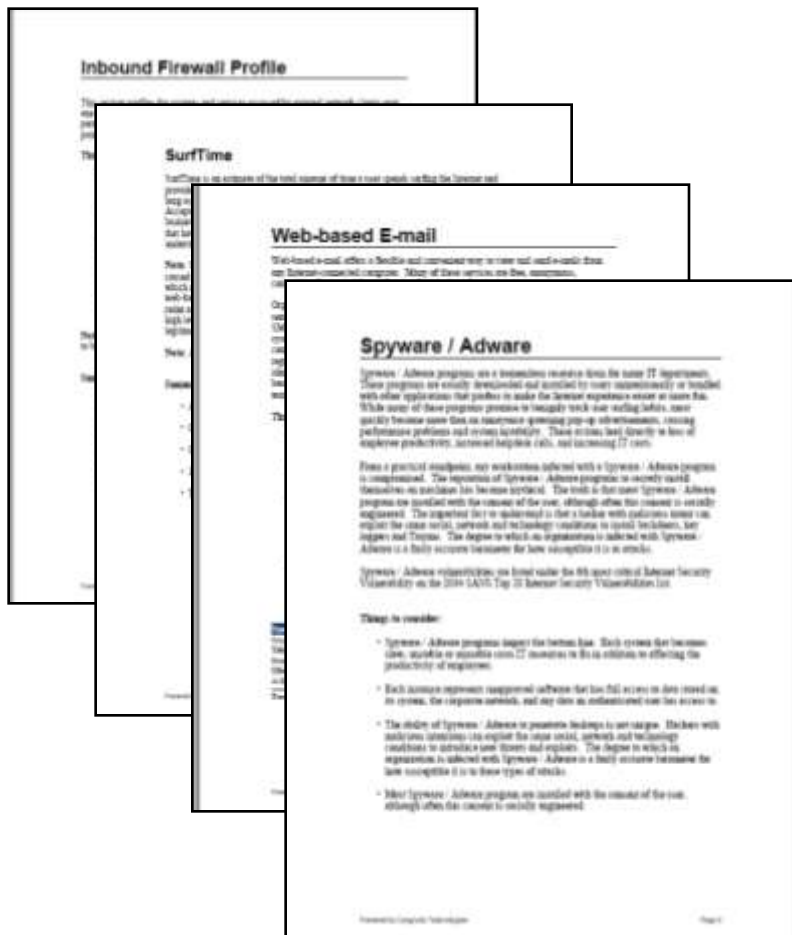
Threat Inspector



Passively monitors all inbound and outbound traffic activity

- Installs in minutes
- Non-disruptive to network
- Single PC network-level data source
- One-click risk assessment
- Objective network-level vantage
- Layered defense

Reports



- Firewall Report
 - Passive pen-test
- Web use report
- Email Systems report
- Spyware/Adware
- IM, P2P
- Data leakage
- Risk Exposure Rating
- Individual detailed device logs

Threat Inspector

Full Accounting



Internet-Exposed TCP/IP Services 6/22/2007 - 6/29/2007

This summary represents the **inbound network security policy**.

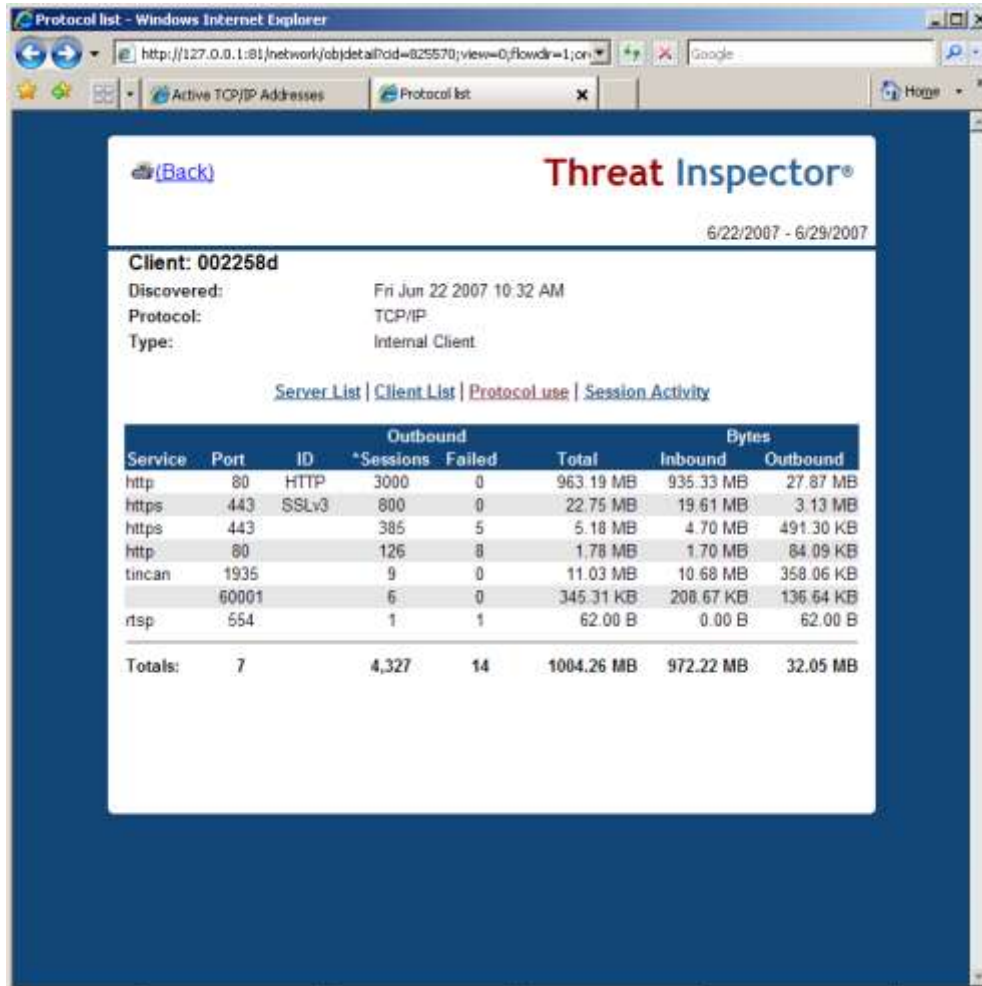
Top: Max

| Service | Port | ID | TCP/IP | | *Total | Bytes | |
|----------------|------|----------|----------|--------|-----------|------------|-----------|
| | | | Sessions | Failed | | Inbound | Outbound |
| smtp | 25 | EMAIL | 13201 | 0 | 762.11 MB | 731.11 MB | 31.00 MB |
| ms-sql-s | 1433 | | 14218 | 0 | 193.39 MB | 39.23 MB | 154.16 MB |
| vytaivaultbrtp | 2546 | | 12 | 0 | 134.15 MB | 130.33 MB | 3.82 MB |
| dmdocbroker | 1489 | FTP_data | 1 | 0 | 35.36 MB | 1.02 MB | 34.34 MB |
| t128-gateway | 1627 | FTP_data | 1 | 0 | 35.18 MB | 1.01 MB | 34.17 MB |
| sdsc-lm | 1637 | FTP_data | 1 | 0 | 34.94 MB | 1009.54 KB | 33.95 MB |
| https | 443 | SSLv1 | 1942 | 2 | 30.55 MB | 6.48 MB | 24.07 MB |
| | 3202 | | 469 | 0 | 22.91 MB | 1.83 MB | 21.08 MB |
| | 3204 | | 466 | 0 | 22.13 MB | 1.80 MB | 20.33 MB |
| | 3203 | | 472 | 0 | 21.26 MB | 1.82 MB | 19.44 MB |
| | 3561 | FTP_data | 1 | 0 | 7.95 MB | 172.01 KB | 7.78 MB |
| | 3571 | FTP_data | 1 | 0 | 7.90 MB | 169.72 KB | 7.73 MB |
| cnap | 1637 | FTP_data | 2 | 0 | 4.27 MB | 127.92 KB | 4.14 MB |
| laplink | 1547 | FTP_data | 1 | 0 | 4.18 MB | 121.86 KB | 4.06 MB |
| netmap_lm | 1493 | FTP_data | 1 | 0 | 4.16 MB | 120.18 KB | 4.04 MB |
| docstor | 1488 | FTP_data | 1 | 0 | 3.79 MB | 111.33 KB | 3.68 MB |
| ampr-inter | 1536 | FTP_data | 1 | 0 | 3.51 MB | 101.98 KB | 3.41 MB |
| shockwave | 1626 | FTP_data | 2 | 0 | 2.90 MB | 83.93 KB | 2.82 MB |
| https | 443 | | 181 | 0 | 1.06 MB | 225.53 KB | 863.23 KB |
| http | 80 | HTTP | 784 | 0 | 828.90 KB | 438.69 KB | 390.21 KB |

- Monitors & Decodes:
 - Every session
 - Data
 - Ports
 - Protocols
 - Applications
 - Communications
 - Files & Content
 - Source & Destination
 -for every workstation and server over 24 x 7 operational cycle

Threat Inspector

Simplifies Troubleshooting



The screenshot shows the Threat Inspector web interface in a browser window. The page title is "Protocol list - Windows Internet Explorer". The address bar shows the URL: <http://127.0.0.1:81/network/objectdetail?oid=825570;view=0;flowdir=1;on>. The page content includes a "Threat Inspector" logo, a date range "6/22/2007 - 6/29/2007", and client information for "Client: 002258d". The client was discovered on "Fri Jun 22 2007 10:32 AM" and is an "Internal Client" using "TCP/IP" protocol. Below this, there are navigation links for "Server List", "Client List", "Protocol use", and "Session Activity". The main content is a table showing network protocol activity.

| Service | Port | ID | Outbound | | Total | Bytes | |
|---------|-------|-------|-----------|--------|------------|-----------|-----------|
| | | | *Sessions | Failed | | Inbound | Outbound |
| http | 80 | HTTP | 3000 | 0 | 963.19 MB | 935.33 MB | 27.87 MB |
| https | 443 | SSLv3 | 800 | 0 | 22.75 MB | 19.61 MB | 3.13 MB |
| https | 443 | | 385 | 5 | 5.18 MB | 4.70 MB | 491.30 KB |
| http | 80 | | 126 | 8 | 1.78 MB | 1.70 MB | 84.09 KB |
| tincan | 1935 | | 9 | 0 | 11.03 MB | 10.68 MB | 358.06 KB |
| | 60001 | | 6 | 0 | 345.31 KB | 208.67 KB | 136.64 KB |
| rtsp | 554 | | 1 | 1 | 62.00 B | 0.00 B | 62.00 B |
| Totals: | 7 | | 4,327 | 14 | 1004.26 MB | 972.22 MB | 32.05 MB |

- Full accounting
- Detailed log files
- Hyper-linked data
- Start low with ports or start high with devices
- Tracks network flows
- Perimeter to endpoint

Summary

- Extremely easy-to-use & operate
- Centralized view of security operations
- Comprehensive reporting & forensics
- Objectively verify policies, procedures and controls
- Most cost-effective and affordable to own & operate
- Pricing
 - Up to 50 Endpoints \$1,495
 - Up to 100 Endpoints \$1,995
 - Up to 250 Endpoints \$2,995
 - Up to 500 Endpoints \$3,995
 - Up to 750 Endpoints \$4,995
 - Up to 1,000 Endpoints \$5,995
 - Up to 2,000 Endpoints \$6,995
 - Up to 3,000 Endpoints \$7,995
 - Up to 4,000 Endpoints \$8,995
 - Up to 5,000 Endpoints \$9,995



Promisec Spectator Professional: The Solution to The Endpoint Challenge

What is it?

Completely Clientless Endpoint Security Management (CESM)

Installs on a single PC or Server in under 10 minutes

Can inspect up to 250 PCs every 5 minutes

Each PC takes only 1 to 2 seconds to inspect

Black List (programs that shouldn't be on the Endpoints) and White List (programs that should or must be on the Endpoints) included in scan

Anti-Virus client verification, including signature file updates

Controls removable media devices

Repairs problems remotely

Ensures the availability of 3rd party security clients (Altiris, Zenworks, Tivoli, etc.)

Ensures compliance with SOX, HIPAA, GLBA, FISMA, SB1386

How Does It Work?

Single program running on one PC or Server

Uses 30+ documented and undocumented Microsoft APIs to communicate with endpoints

Uses credentials of local endpoint, or other credentials from credential manager to access endpoints

Inspects endpoints by host name, IP address, list of host names, IP address range or AD OU

Builds database of findings for immediate and historical reporting

Reports or alerts can be sent via Net Send, E-Mail or an external program can be run

Check Point Firewall-1 integration can block non-compliant machines from VPN access

IBM Tivoli Monitoring Server Integration

The Process

Install the software solution on a PC or Server

Define a baseline endpoint security policy

Inspect the enterprise endpoints for compliance with baseline. The first inspection usually identifies quite a bit more going on than the administrator originally thought, including:

- Unauthorized applications and processes
- Misconfigured Services
- Required applications that are not up-to-date or that have been disabled
- PCs without a third party desktop security agent
- Unauthorized shares that have been published to the world
- Unauthorized use of devices
- Suspicious Files and Registry Entries
- Remnants of deleted unauthorized applications
- Unknown Devices or evidence that these devices were attached recently

Promisec Spectator Professional

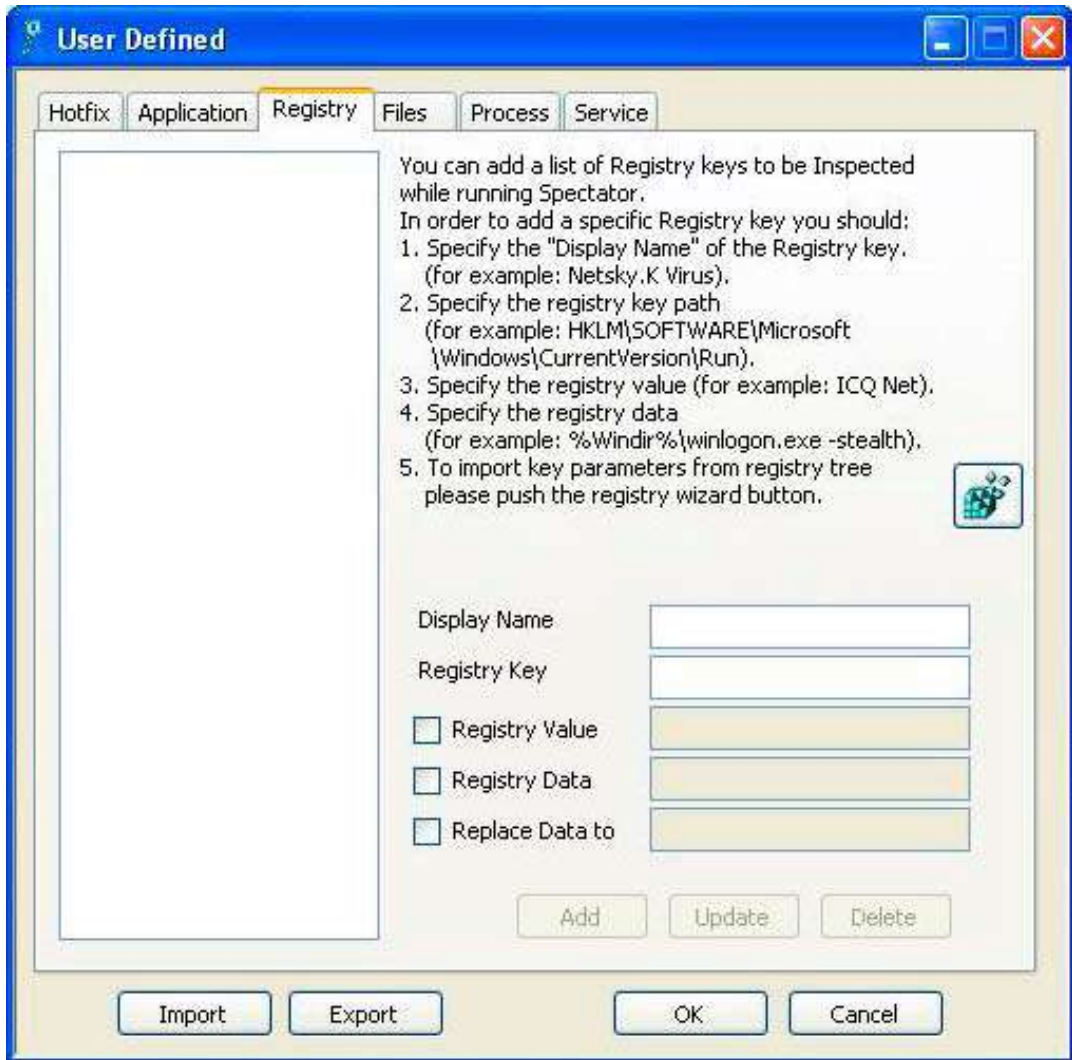
Intuitive, Easy to Use Interface

The screenshot displays the Promisec Spectator Professional interface. On the left, a panel titled 'Adding Hosts for Inspection' contains a list of hosts to be inspected, with a callout box labeled 'LIST OF HOSTS TO BE INSPECTED'. The main area is divided into several tabs: 'Anti Virus (35)', 'Service Packs (18)', 'Files (163)', and 'User Defined (4)'. A callout box labeled 'POLICY COMPLIANCE TABS' points to these tabs. Below the tabs is a table of inspection results, with a callout box labeled 'INSPECTION RESULTS' pointing to the table. The table has columns for Host Name, IP Address, Last Logged-On User, Object, Status, and Details. A callout box labeled 'REMEDIAL ACTIONS' points to a panel on the right side of the interface, which contains a list of actions such as 'Show Running Processes', 'Uninstall Application', and 'Send Message'.

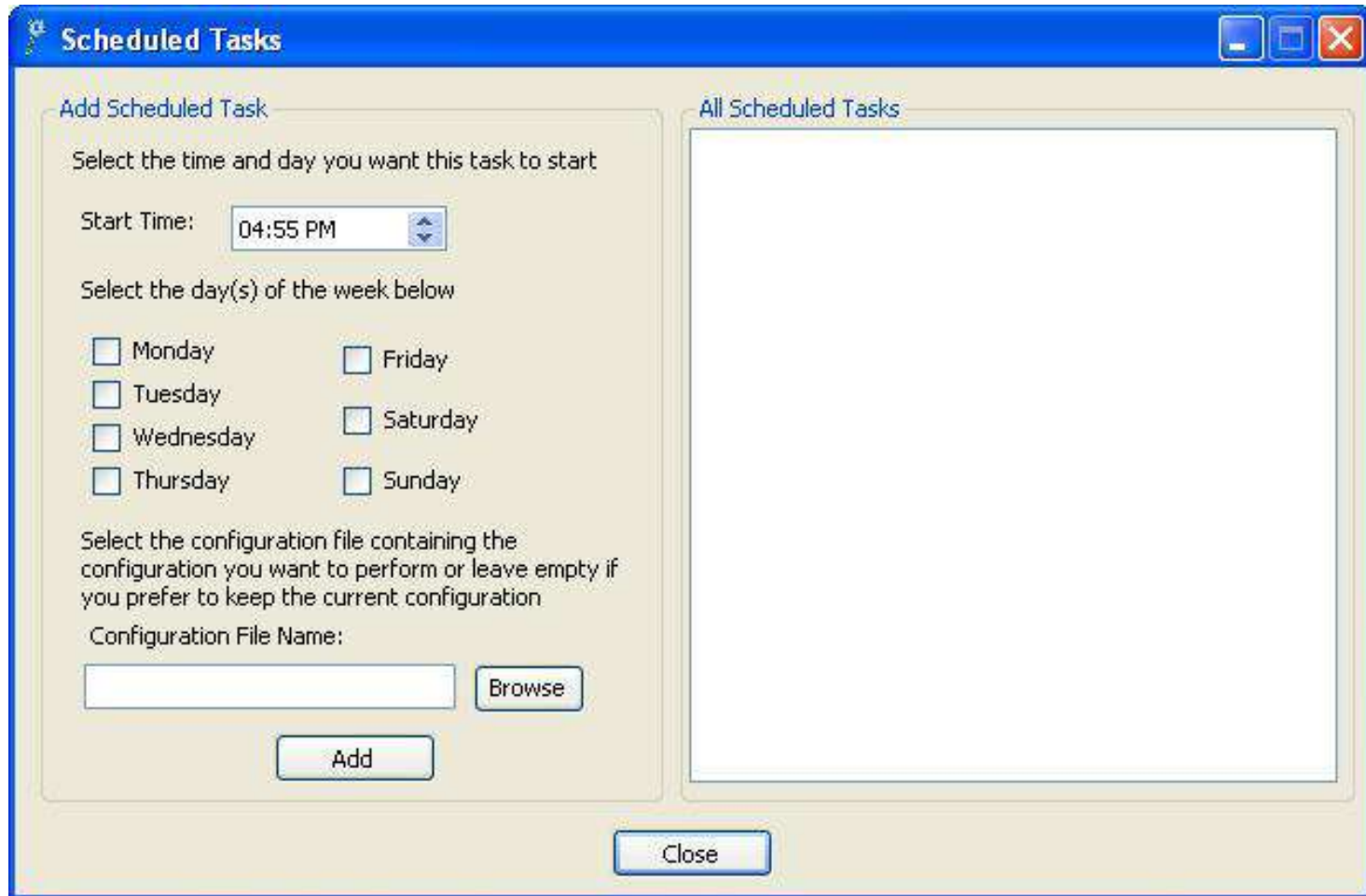
| Host Name | IP Address | Last Logged-On User | Object | Status | Details |
|-----------|---------------|---------------------|----------------------------|-----------|--|
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | Elvish | Installed | |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | Windows Messenger | Installed | Evidence for this item was found. How |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | GoToMeeting | Installed | Evidence for this item was found, but |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | Virtual Network Computing | Installed | Evidence for this item was found, but |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | More Than One Network Card | Installed | Active: Broadcom 440x 10/100 Integr |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | More Than One Network Card | Installed | Active: Dell Wireless 1370 WLAN Mini |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | Storage | Installed | Kingston DataTraveler II USB Device |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | Service Pack 2 | Installed | Service Pack 2 (Evidence for this item |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | Podcast022706.mp3 | Exists | |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | Podcast1.mp3 | Exists | |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | HigherValue1.mp3 | Exists | |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | pes101.mp3 | Exists | |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | pes102.mp3 | Exists | |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | test.avi | Exists | |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | network.GIF | Exists | |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | sig.jpg | Exists | |
| XPPROSP2 | 192.168.0.102 | XPPROSP2\Owner | network.WS | Exists | |

Promisec Spectator Professional

Easily Report On or Mass Change Registry Entries



Schedule a Spectator Job to Run at Any Time



Spectator – Easy to use Reports

Compliance report

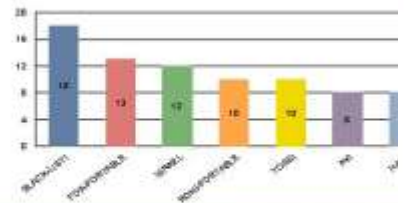
Total number of hosts inspected: 40
 Report Score based on number: 433

Score Broken down by alert

| Severity level | Number of alerts |
|----------------|------------------|
| High (4) | 13 |
| Medium (3) | 121 |
| Low (2) | 8 |
| Warning (1) | 2 |

Alerts broken down by host

Host alert c



| Host Name | IP Address | High | Medium |
|------------|----------------|------|--------|
| PROMISE-DC | 192.168.12.101 | 0 | 0 |
| LIAT | 192.168.13.4 | 0 | 1 |
| AVI | 192.168.13.13 | 3 | 3 |

Previous Spectator Professional Inventory report

Chatting

| Name | IpAddress | OS | MacAddress |
|-------------|--------------|-----|-------------------|
| HADM | 192.168.13.5 | 5.1 | 00-50-8A-08-08-08 |
| BLACK-LIST1 | 192.168.14.2 | 5.1 | 00-0C-29-72-3D-01 |

Google Talk

| Name | IpAddress | OS | MacAddress |
|-------------|--------------|-----|-------------------|
| BLACK-LIST1 | 192.168.14.2 | 5.1 | 00-0C-29-72-3D-01 |

ICQ

| Name | IpAddress | OS | MacAddress |
|-------------|---------------|-----|-------------------|
| AVI | 192.168.13.13 | 5.1 | 00-13-20-11-1C-D8 |
| YOSSEI | 192.168.13.3 | 5.1 | 00-18-F3-50-3F-09 |
| RAH1 | 192.168.15.10 | 5.1 | 00-0C-29-45-87-44 |
| BLACK-LIST1 | 192.168.14.2 | 5.1 | 00-0C-29-72-3D-01 |

ICQ Lite

| Name | IpAddress | OS | MacAddress |
|-------------|---------------|-----|-------------------|
| AVI | 192.168.13.13 | 5.1 | 00-13-20-11-1C-D8 |
| YOSSEI | 192.168.13.3 | 5.1 | 00-18-F3-50-3F-09 |
| RAH1 | 192.168.15.10 | 5.1 | 00-0C-29-45-87-44 |
| BLACK-LIST1 | 192.168.14.2 | 5.1 | 00-0C-29-72-3D-01 |

Microsoft Comic Chat

| Name | IpAddress | OS | MacAddress |
|-------------|--------------|-----|-------------------|
| BLACK-LIST1 | 192.168.14.2 | 5.1 | 00-0C-29-72-3D-01 |

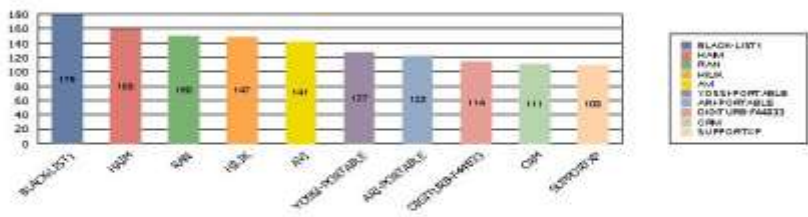
Miranda

| Name | IpAddress | OS | MacAddress |
|-------------|--------------|-----|-------------------|
| BLACK-LIST1 | 192.168.14.2 | 5.1 | 00-0C-29-72-3D-01 |

Top Hosts

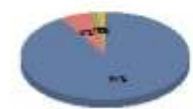
Report data:

Report date: 1/14/2008
 Total number of hosts: 512
 Hosts inspected: 21
 No responses: 19
 Unknown hosts: 442



Host name: BLACK-LIST1

Total Objects: 179
 IP Address: 192.168.14.9
 MAC Address:
 OS type: Microsoft Windows XP
 Last user: PROMISE-C-DOMAIN\jaim



■ Network
 ■ Chatting
 ■ Removable Media
 ■ Process

A Real World Example

At one company, Spectator's initial inspection of the company's 9,900 endpoints revealed that:

19% of the endpoints showed one violation of the baseline security policy (anti-virus issues, out-of-date service packs, P2P applications, unauthorized shares, USB devices, remote control software, *etc.*)

77% endpoints showed at least two violations

Only 4% of the endpoints inspected showed no violations

Administrators had been completely unaware of the scope of their problems until Spectator revealed just how exposed their network and PCs really were.

Free Memory Stick!

- 1 Gb Memory Stick with 64Mb encrypted using Check Point's Encryption Policy Manager
- No Client to Install on non-protected PC
- All JCS & Associates, Inc. products, and many of our product demos/evaluations are included in the encrypted area of the memory stick
- Front-end program (jcsinc.com) allows reading of text file that contains password, execution of decryption program (unlock.exe) and accessing of www.jcsinc.com web site
- This presentation is also included on the memory stick in the encrypted area

We're Here To Help!

If you would like us to come in and perform a Threat Inspector or Promisec Spectator Professional scan on your network, we're available to do so free of charge.

We'll even leave behind a report of all the anomalies that we find!

The complete process will take less than an hour, and you'll be amazed at what we discover.

If you're not ready to have us come on-site, we'll show you how a real scan of a live network looks through a live webcast. Sign up for your webcast with us after the presentation.

And don't forget to stop by and trade us your business card for your free 1gb USB memory stick.

For More Information on
Threat Inspector or
Promisec's Spectator Professional

Contact:

Jim Shaeffer

JCS & Associates, Inc.

Phone 800-968-9527

E-Mail: jcs@jcsinc.com

Web Site: <http://www.jcsinc.com>