



Welcome to the San Jose Tech-Security Conference

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

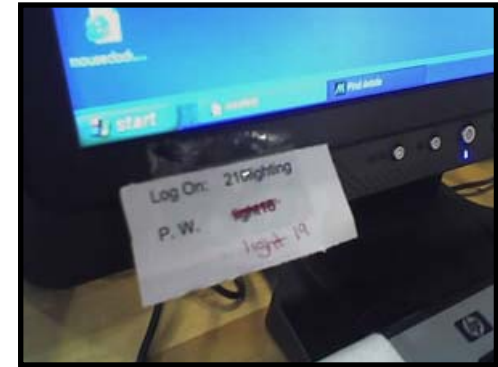
The Password Challenge

Static passwords are an organization's weakest security link

- Easy to Steal
- Easy to Guess
- Easy to Crack
- Not Auditable
- Regularly Written Down
- Expensive to Manage
- Hard to Remember



Hacking remotely...



Written passwords ...

“The weakest link only involves easily getting your password!”

- Jason Hart (World Renowned IT Security Specialist)

The Password Challenge

Every employee holds the keys to your business!

Your information is now held in a virtual office
...and your users are coming and going 24x7

Your firewalls, VPN's or SSL/VPN's
...create the walls and doors of your virtual office

Your users' digital identities
...are the keys to your front door

It only takes one user to be careless with their key
...and you don't know who is going to walk in!



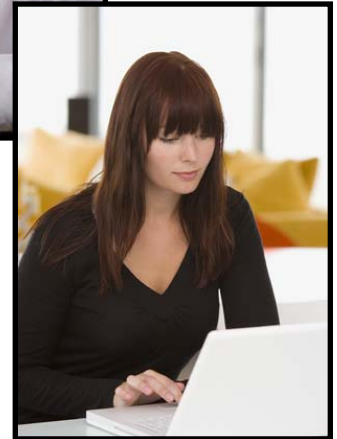
The Password Challenge

User Productivity still requires **Simple, Flexible** and **Secure** Access to information

- Programs & Applications
- Digital Assets & IP
- Portal / Enterprise Management
- e-Business & e-Commerce
- Customer & Partner Info
- Internal and External Networks
- Web Site
- Outlook Web Access (OWA)



Network access at the office...



or remote access from your home or while travelling.

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

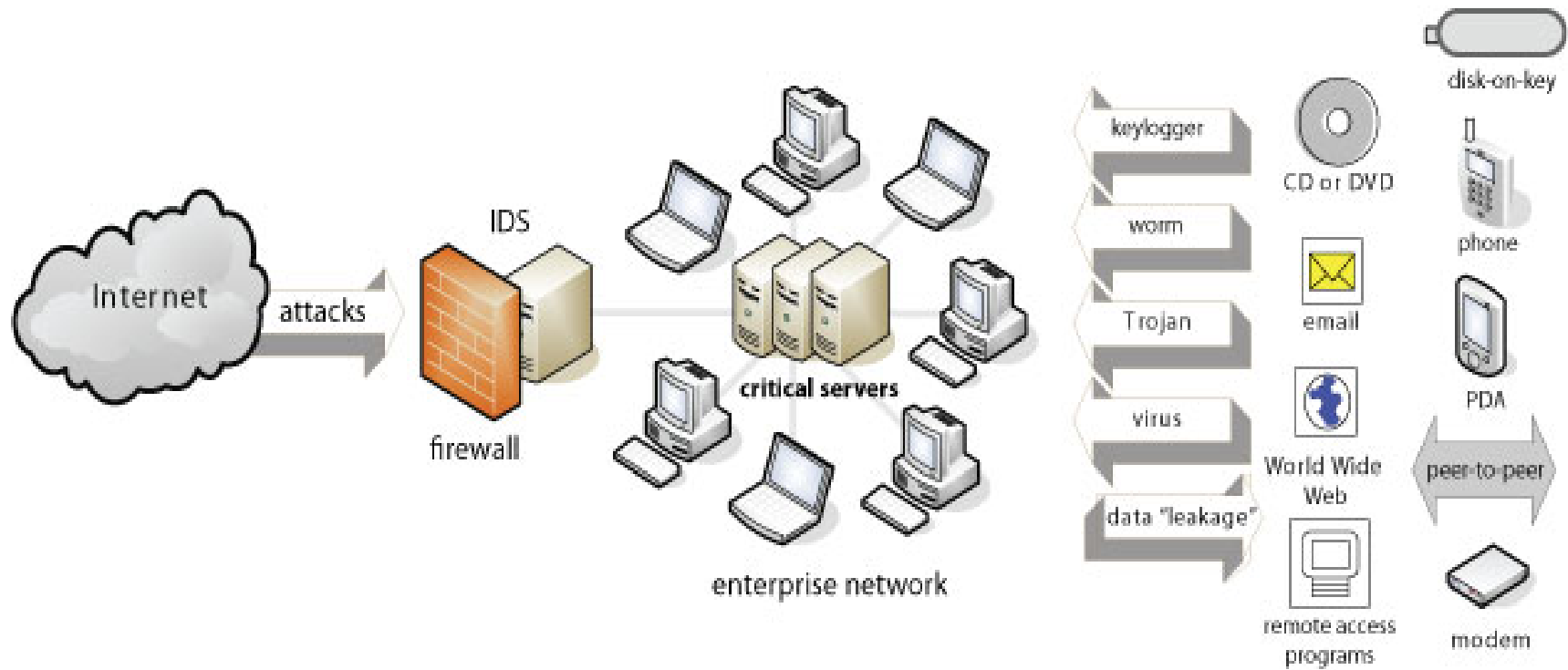
The Endpoint Challenge

- ▶ 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 issues 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



CRYPTOCARD: The Solution to The Password Challenge

CRYPTOCARD

A unique identity for every user – every time they log-in.

Normal login procedure.

Step 1: Enter your user name...

Something You Know (Factor #1).

Step 2: Enter your Personal PIN in the password area...

Something You Have (Factor #2).

Step 3: Generate with a one-time password and type it right after your PIN.



CRYPTOCARD

A unique identity for every user – every time they log-in.



Generated by a simple to use *Token*

- Press the button for a One-Time Password!!

Enables *Two Factor Authentication (2FA)*

- Something You Know (PIN)

- Something You Have (Token)

123456 + U=YnxKs1

- If You Are Using Passwords, You Are Vulnerable!
- Act Today To Amend Your Security Policy
- CRYPTOCARD Provides You With:
 - 2FA With The Highest Security Possible
 - Meeting Your Budget Requirements
(Capital Expenditure vs. Operational Expenditure through CRYPTOMas Managed Service Option).
 - Best Total Cost of Ownership
(Price, Low Support Costs, Long Warranty, Perpetual Licenses vs. RSA where you get the pleasure of purchasing tokens every 3, 4 or 5 years!).



Threat Inspector: The Solution to The Network and Communications Challenges

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



Threat Inspector®

Affordable Security Information Management



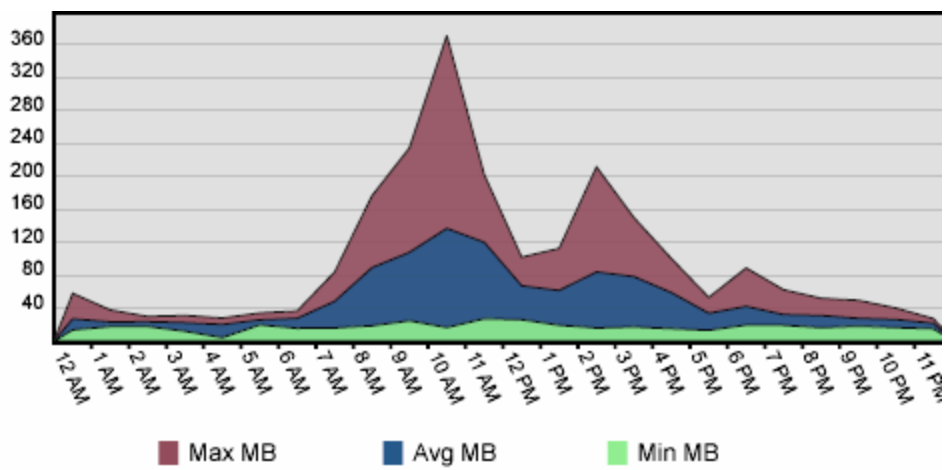
What's Normal?

Trust, But Verify...

Security Information Management (SIM)

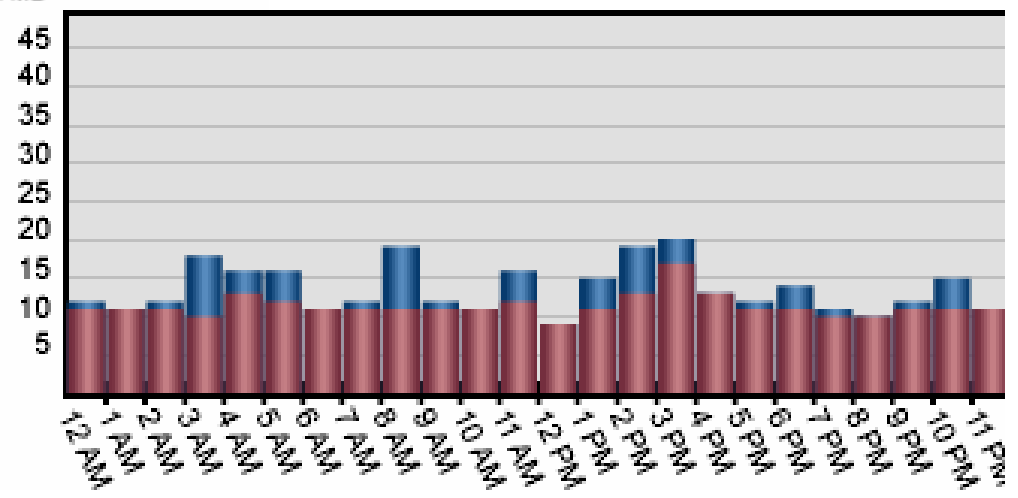
- Centralized Security Console
- Easy one-click operation
- Full accounting, comprehensive usage profile
- Documents key controls, policy & performance status
- Simplifies troubleshooting
- Proactive security management reduces IT costs

Threat Inspector

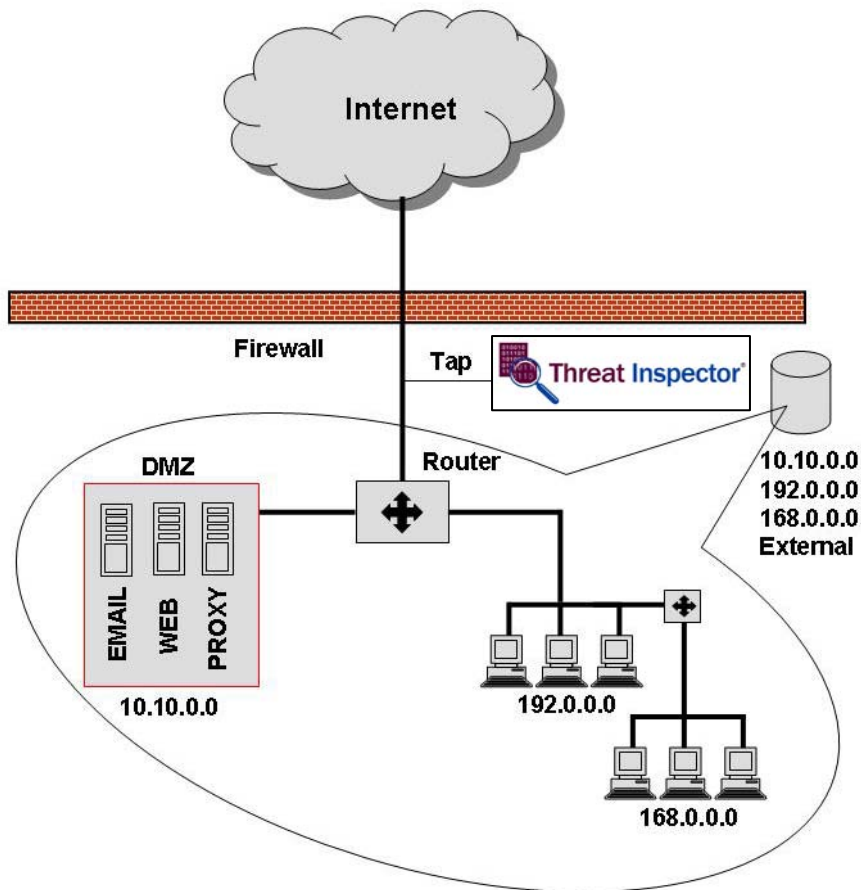


Normal Network Trend

Abnormal Trend



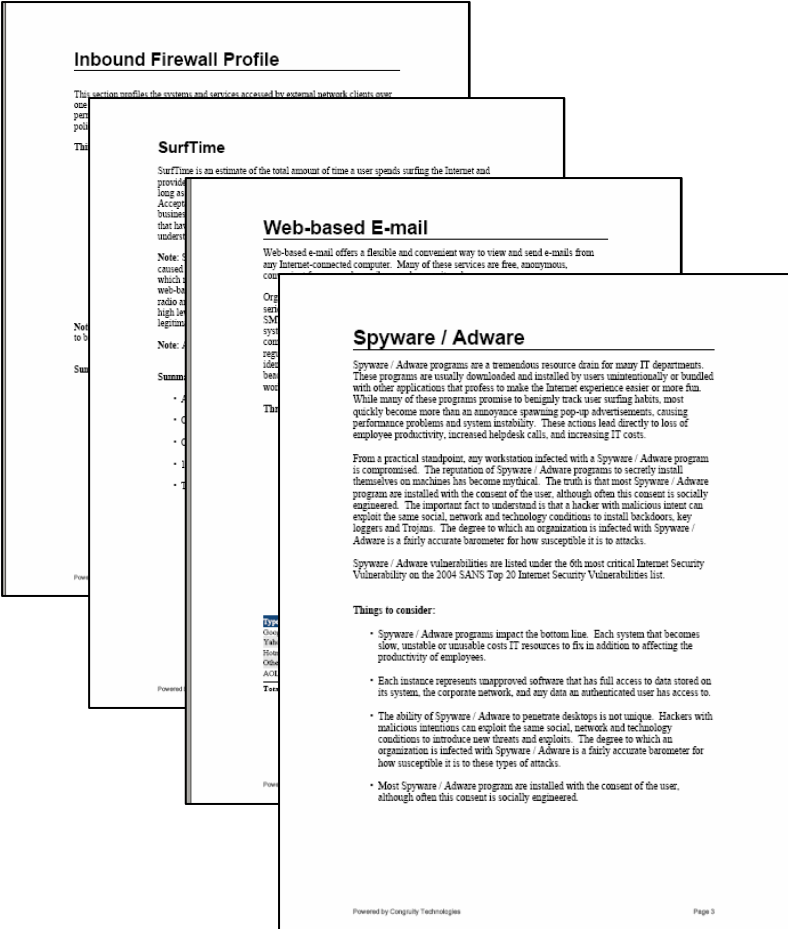
Threat Inspector



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

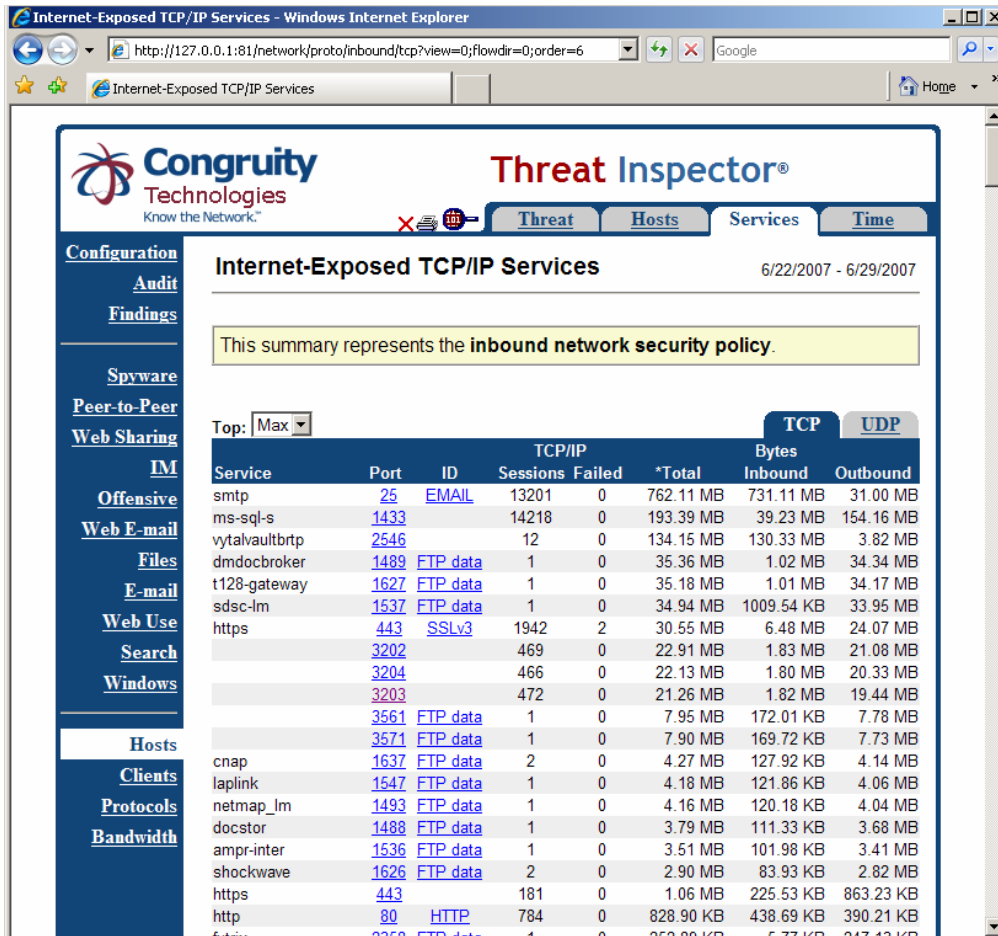
Reports



- 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 - Windows Internet Explorer

http://127.0.0.1:81/network/proto/inbound/tcp?view=0;flowdir=0;order=6

Congruity Technologies Know the Network.® Threat Inspector®

Configuration Audit Findings Spyware Peer-to-Peer Web Sharing IM Offensive Web E-mail Files E-mail Web Use Search Windows Hosts Clients Protocols Bandwidth

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

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

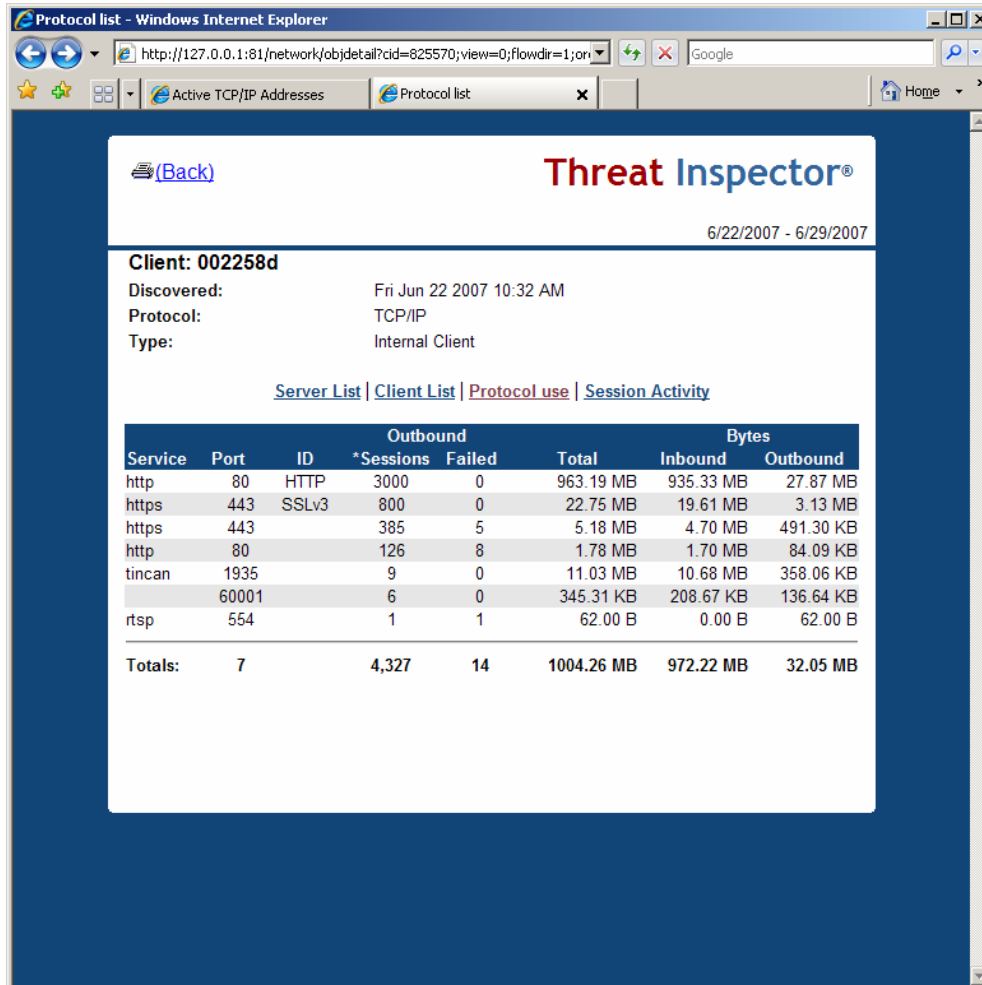
Top: Max

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
vtalvaultbrtp	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	1537	FTP_data	1	0	34.94 MB	1009.54 KB	33.95 MB
https	443	SSLv3	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 URL is "http://127.0.0.1:81/network/jobdetail?cid=825570;view=0;flowdir=1;ori...". The page content includes a "(Back)" link, the "Threat Inspector" logo, and the date range "6/22/2007 - 6/29/2007". The client information is "Client: 002258d", discovered on "Fri Jun 22 2007 10:32 AM", using "TCP/IP" protocol, and is an "Internal Client". There are links for "Server List", "Client List", "Protocol use", and "Session Activity". Below this is a table with columns for Service, Port, ID, Outbound Sessions, Outbound Failed, Total, Inbound Bytes, and Outbound Bytes.

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 100 Endpoints \$1,995
 - Up to 250 Endpoints \$2,995
 - Up to 500 Endpoints \$3,995
 - Up to 1,000 Endpoints \$4,995
 - 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

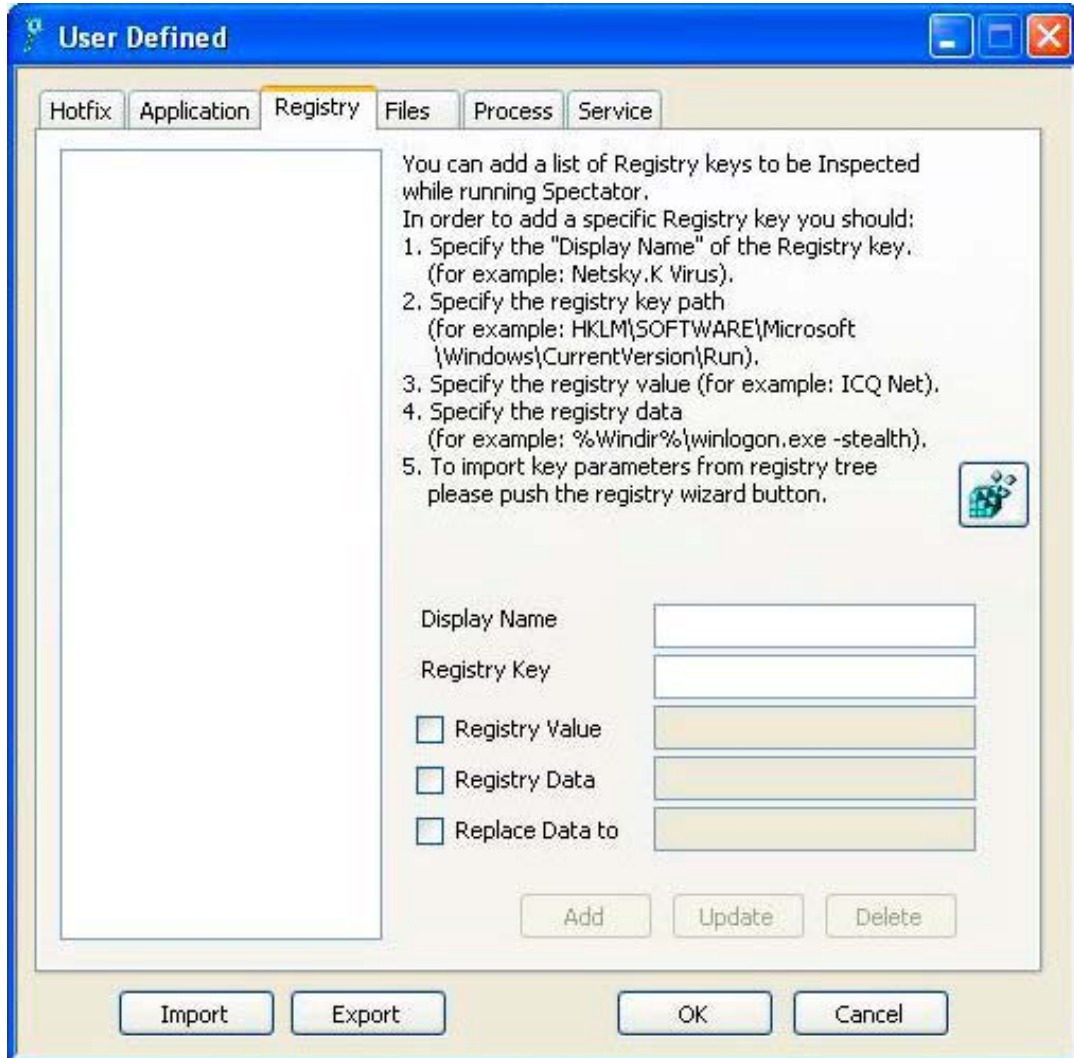
Define a baseline endpoint security policy

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

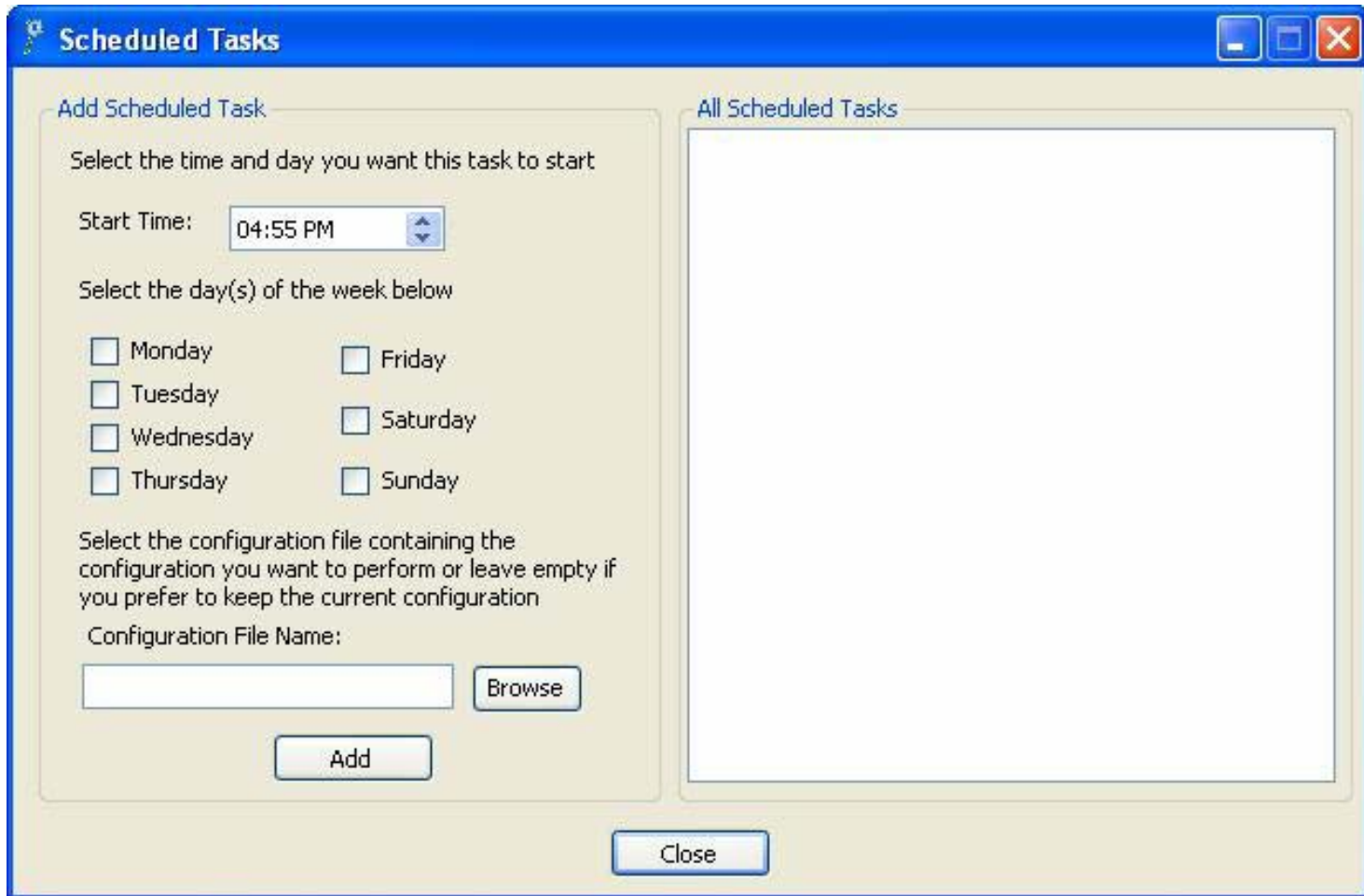
Promisec Spectator Professional

Easily Report On or Mass Change Registry Entries



Promisec Spectator Professional

Schedule a Spectator Job to Run at Any Time



Promisec Spectator Professional

Easy to Use Report Writer Interface

Spectator(tm) Report Viewer

Report view:

Host name	IP A...	Application	Logged-on user	Status	Additional Information	Scanning Computer	Configuration
COMP4423	192....	USB Removable Storage	ORG-DOMAIN\user4423	Detected as Installed	I-Stick2 IntelligentStick ...	SpectatorInspector1	Marketing Department
COMP1933	192....	Kazaa	ORG-DOMAIN\user1933	Multiple occurrences detected		SpectatorInspector1	Marketing Department
COMP1933	192....	Modem	ORG-DOMAIN\user1933	Multiple occurrences detected	IR Modem	SpectatorInspector1	Marketing Department
COMP1933	192....	Startup Monitor	ORG-DOMAIN\user1933	Multiple occurrences detected	Dot.Net.Update: c:\win...	SpectatorInspector1	Marketing Department
COMP1933	192....	Application Monitor	ORG-DOMAIN\user1933	No further indication after mult...	FIFA 2005	SpectatorInspector1	Marketing Department
COMP1933	192....	eDonkey	ORG-DOMAIN\user1933	Multiple occurrences detected ...		SpectatorInspector1	Marketing Department
COMP3442	192....	Skype	ORG-DOMAIN\user3442	Multiple occurrences detected		SpectatorInspector1	Marketing Department
COMP3442	192....	Modem	ORG-DOMAIN\user3442	Multiple occurrences detected	IR Modem	SpectatorInspector1	Marketing Department
COMP3442	192....	More Than One Network Card	ORG-DOMAIN\user3442	Multiple occurrences detected	Intel(R) PRO/Wireless ...	SpectatorInspector1	Marketing Department
COMP3442	192....	More Than One Network Card	ORG-DOMAIN\user3442	Multiple occurrences detected	Intel(R) PRO/100 VE N...	SpectatorInspector1	Marketing Department
COMP1233	192....	Service Pack 2	ORG-DOMAIN\user1233	No further indication after mult...	Service Pack 1	SpectatorInspector1	Marketing Department
COMP1233	192....	Trillian	ORG-DOMAIN\user1233	No further indication after mult...		SpectatorInspector1	Marketing Department
COMP1233	192....	Everyone Share	ORG-DOMAIN\user1233	Multiple occurrences detected	D	SpectatorInspector1	Marketing Department
COMP8812	192....	Everyone Share	ORG-DOMAIN\user8812	Multiple occurrences detected	Documents	SpectatorInspector1	Marketing Department
COMP8812	192....	Anti Virus	ORG-DOMAIN\user8812	Multiple occurrences detected	Anti Virus is not installe...	SpectatorInspector1	Marketing Department
COMP1245	192....	USB Removable Storage	ORG-DOMAIN\user1245	Multiple occurrences detected	USB Flash Drive USB De...	SpectatorInspector1	Marketing Department
COMP6642	192....	Anti Virus	ORG-DOMAIN\user6642	Multiple occurrences detected	Anti Virus is not installe...	SpectatorInspector1	Marketing Department
COMP6642	192....	iTunes	ORG-DOMAIN\user6642	Multiple occurrences detected		SpectatorInspector1	Marketing Department
COMP6642	192....	PodService	ORG-DOMAIN\user6642	Multiple occurrences detected		SpectatorInspector1	Marketing Department
COMP2422	192....	USB Removable Storage	ORG-DOMAIN\user2422	Multiple occurrences detected	USB2.0 (FS) FLASH DIS...	SpectatorInspector1	Marketing Department
COMP2422	192....	Skype	ORG-DOMAIN\user2422	Multiple occurrences detected ...		SpectatorInspector1	Marketing Department
COMP2422	192....	Everyone Share	ORG-DOMAIN\user2422	Multiple occurrences detected	Shared	SpectatorInspector1	Marketing Department
COMP4623	192....	VNC	ORG-DOMAIN\user4623	Multiple occurrences detected		SpectatorInspector1	Marketing Department
COMP4233	192....	Anti Virus	ORG-DOMAIN\user4233	Multiple occurrences detected	Stopped	SpectatorInspector1	Marketing Department
COMP8832	192....	Process Monitor	ORG-DOMAIN\user8832	Multiple occurrences detected	qdsqds	SpectatorInspector1	Marketing Department

Additional information:

Detection history:

13-02-2006 22:28:51

Indication timeframe: 13-02-2006 22:28:51
 Indication type: Detected as Installed
 Last user logged on: ORG-DOMAIN\user4423
 Details: I-Stick2 IntelligentStick USB Device

Custom Query Auto report mode

Query start date: 13/02/2006 10:36 PM

Query end date: 13/02/2006 10:36 PM

Go!



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.

Selected Customer List



Free Memory Stick!

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
CRYPTOCARD, 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>