



Need IBM i Training?
Click here for the only site you'll ever need.

[THE FOUR HUNDRED](#)[SUBSCRIBE](#)[MEDIA KIT](#)[CONTRIBUTORS](#)[ABOUT US](#)[CONTACT](#)

THE FOUR HUNDRED

Power Systems & IBM i Insight

COUNTERPANE BRINGS OS/400 INTO ITS MANAGED SECURITY FOLD

March 1, 2005 Alex Woodie

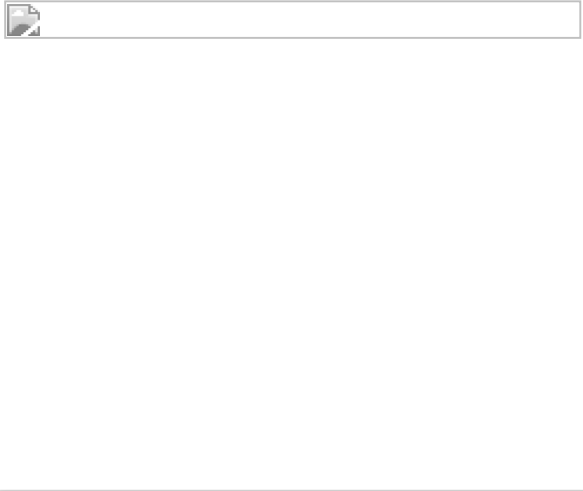
OS/400 shops looking to outsource their network and server security monitoring may want to check out Counterpane Internet Security, a managed security service provider (MSSP) that introduced a new OS/400 monitoring agent with the launch of Enterprise Protection Suite 2.0 last month. Inclusion of OS/400 event logs provides another piece in the security puzzle that Counterpane's security analysts are trying to put together for its customers, 24 hours a day, seven days a week.



Volume 5, Number 9 -- March 1, 2005

THIS ISSUE SPONSORED BY:

Vision Solutions
Aldon
COMMON
looksoftware
Affirmative Computer



Founded in Silicon Valley six years ago by noted cryptologist Bruce Schneier, Counterpane today is one of a growing number of MSSPs that are taking over the tedious job of continuously monitoring networks and servers, looking for signs of overt attacks or security policy violations. Analysts say new federal regulations like Sarbanes-Oxley are driving growth in the use of MSSPs, which they say will be used by 90 percent of enterprises by 2010.

In most cases, Counterpane is called on only to monitor its customers' server and firewall logs, using an appliance called the Sentry. Log data from assorted agents is gathered by the Sentry and sent to Counterpane, where a program called Socrates filters out the chaff. The refined event data is then displayed for customers on a secure Web portal. In other cases, customers pay Counterpane to install and manage its firewalls and other security appliances, and make changes to the servers to keep them safe. Antivirus, antispam, content control, and protection from denial of service attacks are other options on its services menu.

Whatever choices customers make, the real value that Counterpane has to add comes in the form of the expertise of its three teams of security analysts—one in Mountain View, one on the East Coast, and another in Belgium—which keep a watchful eye on 500 networks in 38 countries. "What customers are looking for is for us to be the leading authority" on network security, says Toby Weir-Jones, Counterpane's manager of field engineering.

"We're looking at raw data from traditional devices, firewalls, databases, and servers," Weir-Jones says. "We're capturing messages from logs and looking for messages with security relevance . . . and the net result is a huge feed of disparate sources from customers, which may span different devices and times."



TABLE OF CONTENTS

Counterpane Brings OS/400 Into Its Managed Security Fold
GST Unveils Line of Affordable Memory for i5 Servers
Informatica Unveils 18-Month Roadmap for Enterprise ETL
Linoma Boosts Security and Automation of Data Transfer Tool

With hundreds of networks under its watch, Counterpane is able to spot trends that a single network administrator has no way to see. This size advantage is bolstered by the fact that Counterpane's reputation as a security expert is staked on it keeping up-to-date with the latest security threats, software vulnerabilities, and associated events.

And it has been successful. Counterpane claims that, in 2003, it processed 523 billion messages, detected more than 70,000 attacks, and directly notified customers 21,000 times. In 2004, Counterpane successfully defended over 400,000 attacks without one of its customers suffering a financial loss, according to Counterpane CEO, Paul Stich.

A New 'Target'

But security threat signatures are constantly changing these days, and it can take a discerning eye to tell an inconsequential event from a potentially harmful one. "We're looking for a much more ephemeral event," Weir-Jones says. "A failed login in the CEO's office at 3 a.m. looks no different in the log message than a failed login at 3 p.m. But the contextual message is, he's probably not in his office at 3 a.m. It's probably somebody else."

This is where OS/400 support comes into play. Counterpane was providing network monitoring for the Unix and Windows servers (or "targets" in Counterpane's parlance) of some very large, Fortune 100 customers. Of course, these customers also had OS/400 and mainframe servers in their data centers, so Counterpane decided to roll-out support for these targets as well, which it did with the release of its Enterprise Security Suite version 2.0 in late February.

"We saw an opportunity to take a leading role in the MSSP market. Nobody else was doing this with OS/400," Weir-Jones says. "As far as we know, we're the only managed security provider who can do this" with the OS/400 server.

Counterpane bought two iSeries servers for development and began writing its own program to monitor OS/400 logs. The Counterpane "AS/400 Security Agent" looks for 72 different system events, ranging from invalid passwords and change of authority to changes made to objects and attempts to access network resources.

By themselves, these events may or may not alert Counterpane to an attack underway, or a violation of security policy. The value comes with Counterpane's ability to correlate different events, such as an FTP exploit making the rounds. "It becomes a piece of the puzzle," Weir-Jones says. "We would expect an OS/400 customer to have a large and complex network of other devices we're monitoring."

Security Solutions for the modern era of IBM i

[Learn More](#)

NEXT40

 **kisco**

CONTENT ARCHIVE

The Four Hundred
Four Hundred Stuff
Four Hundred Guru



So far, Counterpane has several OS/400 clients, including two contracts it won from a rival Silicon Valley antivirus and security firm that claimed it could provide OS/400 event logging, but in fact could not, Weir-Jones says.

Counterpane supports OS/400 V4R5 and higher. The AS/400 Security Agent itself is free; customers pay for monitoring according to the number and type of device that Counterpane is monitoring. The average customer is paying about \$7,000 to \$8,000 per month to have Counterpane monitor 70 to 80 devices. Of that number, 15 to 20 percent are typically dedicated security appliances like firewalls, and the rest are considered targets.

It will cost from \$500 to \$1,500 per device per month to have Counterpane remotely manage your security appliances and server settings. Counterpane does not offer OS/400 security management at this time. For more information, visit www.counterpane.com.

Tags:

Sponsored by
Manta Technologies

The Leader in IBM i Education!

Need training on anything i?

Manta is all you need.

130 courses and competency exams on:

- IBM i operations
- System Management and Security
- IBM i Programming Tools
- Programming in RPG, COBOL, CL, Java
- Web Development

SQL, DB2, QueryProduct features:

- Runs in every popular browser
- Available 24/7/365
- Free Student Reference Guides
- Free Student Administration
- Concurrent User License
- Built-In IBM i Simulator

You can download our 200-page catalog and take sample sessions at MantaTech.com

Admin Alert: Configuring Output
Queues to Print Multi-Copy
Spooled Files on Remote Printers

Embedding SQL in /free

LEAVE A REPLY

RECENT POSTS

The State Of The Power Systems
Base 2024: The Systems
IBM Retired Db2 Web Query; It's
Time You Did, Too
2024 IBM i Predictions Part 3 – The
Final Chapter

SUBSCRIBE

To get news from IT Jungle sent to
your inbox every week, subscribe
to our newsletter.

IBM i Shops Are Still Getting Their
Generative AI Acts Together
IBM i PTF Guide, Volume 26,
Number 5
Power Systems Grows For The
Second Year In A Row
The IBM i Base Is Ready To Keep
Investing In The Future
New IBM Champion Class Grows
Nearly 40 Percent
As I See It: The Other Eight Hours
IBM i PTF Guide, Volume 26,
Number 4

PAGES

About Us
Contact
Contributors
Four Hundred Monitor
IBM i PTF Guide
Media Kit
Subscribe

SEARCH

