

The logo for Technology Pathways is centered at the top of the page. It consists of a black rectangular background. The word "Technology" is written in a red, sans-serif font, and the word "Pathways" is written in a white, serif font below it.

Technology Pathways

For Immediate Release:

Technology Pathways introduces ProDiscover IR, a powerful new tool for improving System Audits and Incident Response at Websec show in San Francisco

ProDiscover IR is the only tool available today that allows IT Managers to reliably determine if a system has been compromised without taking the system down

Coronado, Ca, July 14, 2003, Technology Pathways, LLC announces today the unveiling of ProDiscover[®] IR, a new product in its powerful ProDiscover family of security products, at Websec in Booth 101. ProDiscover IR empowers System Managers to detect any changes made to their computers by intruders and to gather the evidentiary quality information needed to help identify and prosecute the intruders.

The new ProDiscover IR product uses a read-only CD containing trusted binaries which is loaded on the system to be examined. Then, using a standard PC as the console, the System Administrator can examine all files on the suspect system for any evidence of tampering by an intruder. This examination can be done on a live system without disrupting other processes operating on the system and can be done locally or remotely. ProDiscover IR accesses the suspect disk at the lowest level in the operating system and circumvents its file system to find all files, even if they have been deleted or hidden by user or kernel level rootkits typically employed by hackers to cover their tracks.

ProDiscover IR also takes hash signatures of all files and compares these to signatures from the National Drug Intelligence Center "Hashkeeper" database of known system files to assure that none of these files have been altered. If any altered or hidden files are detected, ProDiscover IR can be used to create a bit-stream image of the corrupted system disk for complete forensic analysis. The corrupted files can then be replaced, restoring the system to operation quickly while further investigation continues "off-line" utilizing the bit-stream image copy. Utilizing ProDiscover IR with this bit-stream copy enables evidence to be gathered which can be used by law enforcement agencies and the courts to catch and prosecute the intruders.

ProDiscover IR may be used remotely to analyze systems, eliminating the need for expensive staff at remote facilities. It can also operate in "stealth" mode. Stealth mode can be used to investigate internal policy compliance or during internal investigations

where the System Administrator does not wish to alert the user that the system is being analyzed. All communications between the remote system and ProDiscover IR may be encrypted to prevent any compromise of the system or data being analyzed.

“The ability to have a reliable method to verify whether a system has (or has not) been compromised without taking the system off-line will significantly improve network integrity and productivity,” stated Christopher Brown, President of Technology Pathways. “As hackers get more sophisticated, the tools to detect them must improve. Existing tools such as Trojan and virus scanners rely on the file system which may be compromised and therefore cannot be trusted. Today, System Administrators can spend hours or days examining files and system logs in an attempt to determine if a system has been compromised, and even then they may miss a Trojan or kernel rootkit if the intruder covers their tracks. ProDiscover IR empowers administrators to get the job done quickly and reliably. With ProDiscover IR, a live system can be checked without taking it out of service, and if compromised, can be corrected and put back in service immediately.”

ProDiscover IR is priced at \$995 and is available immediately. In addition to the product being demonstrated at Websec, ProDiscover IR will be used to analyze the results of the “Ultimate Hack Challenge” competition sponsored by the Websec show. ProDiscover IR will enable attendees to see exactly how the winner succeeded in compromising the system.

Technology Pathways, LLC is a leading edge provider of computer and network security tools and services for the Corporate IT, government and legal communities. Our CISSP certified consultants have provided forensic and discovery services to major corporations. The ProDiscover family of security products combines high quality, high performance, and ease of use at affordable prices. Its premier computer forensic solution, ProDiscover DFT, is being utilized nationally by corporations and government agencies.

For more information please contact:
Chris Brown at Technology Pathways
(619) 435-0906 or marketing@TechPathways.com