

Capture Volatile Data With SnapShot

Capture, analyze and preserve volatile data from servers and workstations on multiple operating systems across the enterprise

“Coupled with the right training, EnCase Enterprise has the potential to bring accurate closure to every intrusion alarm. As regulatory pressure increases to protect consumer data, due diligence can come in the form of EnCase Enterprise.”

Infoworld

With Snapshot, expand the power of EnCase Enterprise to achieve a deeper level of network visibility...

- Enables Windows DLL enumeration that identifies injected and rogue DLLs mapped to processes.
- View live and physical Windows® registry information and compare the two for malicious entries, such as autostart hacking tools.
- View all user accounts with last logged-on time and SID information, and mark all current logged on users.
- Map open files to processes and PID.
- Enable network interface enumeration to reveal MAC address, IP address and brand information.

* SnapShot capability available for Windows NT, 2000, XP, 2003 Server and Vista; Linux kernel 2.4 and above, designed for Red Hat, SuSE & Mandrake; Sun Solaris 8 & 9, both 32- and 64-bit processors, AIX 4.3, 5.1, 5.2 & 5.3, NetWare 5.1 SP8, 6.0 SP4 and 6.5, MAC OSX version 10.2-10.5 and MAC Intel platforms.



©2007 Guidance Software, Inc. All rights reserved. Guidance Software, the Guidance Software logo and EnCase are trademarks or registered trademarks of Guidance Software, Inc. All names may be trademarks of their respective owners.

The SnapShot add-on for EnCase® software provides the critical ability to immediately capture and analyze volatile data rapidly across thousands of machines, enabling investigators and computer incident response teams to quickly identify the scope, magnitude and status of suspected incidents across multiple operating systems*. Security analysts can quickly confirm whether an event took place and understand the impact on servers and workstations to determine if any anomalous or malicious activity has occurred. This capability, along with the ability to quickly preview and validate static files on system media, gives investigators the power to quickly isolate, identify, assess and remediate both internal and external security breaches.

- Capture, analyze and preserve volatile data from servers and workstations on multiple operating systems* across the enterprise with a single tool
- Identify all running processes on your network and detect unapproved or unknown processes using machine profiles
- Analyze up to 30,000 computers an hour for suspicious or malicious activity
- Conduct incident impact analysis to identify the difference between machine states across time
- Have the unique ability to identify rootkits, hidden registry keys, hidden processes, hidden ports and malicious, injected DLLs
- Exactly match the technical requirements of the NIST Computer Security Incident Handling Guide and GLBA 501b Operational Incident Response Capabilities
- Be armed with a practical incident response solution that enables repeatable processes with consistent results
- Preserve SnapShot data in EnCase Logical Evidence Files for evidentiary purposes
- View all TCP/UDP port information associated with processes

SnapShot delivers deep system analysis

DEPTH OF ANALYSIS COMPARISON	EnCase Enterprise SnapShot	Typical Auditing Tools
Detect Running Processes	✓	✓
Detect Hidden Processes	✓	⊘
Detect Renamed Processes or Drivers	✓	⊘
Detect Running Services	✓	✓
Detect Injected DLLs	✓	⊘
Detect Rootkits	✓	⊘
Identify Current Logged-on User	✓	✓
Enumerate Autostart Registry Keys	✓	⊘
Detect Hidden Ports	✓	⊘
Identify Hidden Registry Keys	✓	⊘
Port-to-Process Mapping	✓	⊘
Provide Detailed Reporting	✓	✓