

BACKGROUND AND VALIDATION

Q. Is this the product that was originally developed by Raytheon?

A. Yes the product was sold from Raytheon to Computer Associates in 2003. Then the product was renamed to eTrust Network Forensics. In September 2008, AccessData purchased the rights to the product and also took the original name back.

Q. Is this court credible evidence?

A. Yes, all data is captured and stored in a forensically sound manner.

Q. Is SR currently deployed in any federal or large corporate entities?

A. Yes SilentRunner is deployed in multiple federal and large corporate organizations worldwide.

LEGAL COMPLIANCE ISSUES (Corporate & Law Enforcement)

Q. What specific regulatory compliance is SR designed to demonstrate? PCI? HIPAA?

A. SilentRunner has alerting modules that are targeted towards the following regulatory requirements: HIPAA, PCI, Sarbanes Oxley

Q. The demo and features mention that silent runner collects *all* data across the wire. Can the scope be reduced to fall within the limitations of a narrower warrant?

A. *Absolutely* the SR collector has the ability to filter and target specific IP addresses, MAC addresses and protocols.

Q. Can this product be used on networks in countries other than the U.S., particularly EU nations, in which the privacy laws are far more complex and stringent?

A. SilentRunner, can be successfully used to assist corporations without violating the privacy laws. Utilizing the product in a post-real-time mode to analyze the logs of other security tools to determine what occurred or to monitor the network without being able to view personally identifiable information (PII) is permitted in most countries. There is a white paper available on our website, which more clearly explains the use of SR within EU compliance in more detail. It can be downloaded from the SilentRunner product page on our website at <http://www.accessdata.com/silentrunner.html>.

COMPATIBILITY / CAPABILITIES / FUNCTIONALITY

Q. What are the network speed limitations of this product?

A. There are two options available for SilentRunner. The mobile edition can capture all communications on a 100MB network segment. The enterprise edition can capture all communications on a gigabit network segment.

Q. Does it work with IPv6 ?

A. SilentRunner currently only supports IPv4. The next generation of SilentRunner, due out later this year, will be fully IPv6 compliant.

Q. Will this tool interface with a notification system or a firewall to block known bad host (internal or external to the network).

A. SilentRunner does not interact with the network at all, hence the name SilentRunner. It passively records all the network packets to be used for analysis and investigations. This is used to confirm alerts generated by notification systems.

SR does have contextual alerting abilities that can be sent to security information management systems (SIM) or the upcoming AccessData Information Assurance product.

Q. How long and much data can it capture?

A. There is no limit to how much data SilentRunner can capture. All the data captured is stored in a database. The duration of how long the data is retained is dependent on how much storage is allocated to the database.

MORE ...

Q. Could you use SR to monitor DSL & Analog lines traffic?

A. SilentRunner is designed to capture and record any and all TCPIP communications that are seen by the collector's interface.

Q. Could you monitor if there is someone else that is not authorized monitoring the network traffic?

A. SilentRunner captures and records every packet that is sent across its interface. If there is a user that is sniffing/monitoring the network and is generating network packets then SR will show you who they are.

Q. Can SR also block known data from leaving the network?

A. SR is not a Data Leakage Prevention tool. It is a forensic investigation and network analysis technology. It can alert you that specific data is leaving, and show you who is moving it, as well as where they got the data from and where they are sending it to. It will also show you everything else that the user is doing while he or she is on the network.

DLP technologies will only provide you with the ability to stop the data leaving, but you need to clearly define which data it should be blocking. Its functionality ends there...

Q. How are encrypted communications handled?

A. SilentRunner captures and records every packet that is sent across its interface, therefore any and all encrypted files or sessions will be captured. As far as the encrypted files, SR will capture those files and the user will be able to utilize AccessData's decryption tools to crack the data.

Q. Can captured data be re-played over the network by the capture machine/device via SilentRunner?

A. SilentRunner has the ability to record tcpdump files that can be replayed at any time for additional analysis

Q. How does the network mapping work?

A. The SilentRunner analysis engine uses 25 proprietary algorithms to sort and analyze all data in preparation to handoff to the one-of-a-kind, 2-D visualization engine.