

SilentRunner: VoIP Investigations

Frequently Asked Questions...



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 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. Although the content of the packets are data, these are also voice communications. Are you aware of any legal challenges to intercepting VoIP traffic asserting a violation of the Telecommunications Act?
A. If the interception is being done by a law enforcement agency, then a court order would be required. However, if an organization is investigating its own VoIP network and its own employee's use of that resource, that would be governed by an individual organization's internal policies and its own legal advisors. We are not able to provide any legal advice on the use of this technology in the workplace.
- Q. Is this court credible evidence?
A. Yes, all data is captured and stored in a forensically sound manner.
- Q. From an evidence perspective, is there hashing and chain of evidence features.
A. Yes!
- Q. Is there some sort of template for a court order for this information?
A. We are not in a position to provide any information that could be construed as legal advice. In the future, we will discuss caselaw with regard to this issue in our legal journal, *The Rules of Evidence and AccessData Technology*. This document can be found on our website. However, any discussion of legal challenges and caselaw should not be construed as legal advice.

COMPATIBILITY / CAPABILITIES / FUNCTIONALITY

- Q. Is there a list for the VOIP providers you support?
A. Currently we support any VoIP transmissions that communicate over the SIP and H323 protocols. We are adding more in the future.
- Q. Can you get successful packet capture on Vonage, and can you replay the call?
A. Currently we support any VoIP transmissions that communicate over the SIP and H323 protocols. We are adding more in the future.
- Q. How would this work with commercial VoIP like Skype, Packet8, etc.?
A. There isn't any technology available today that can intercept Skype communications. Packet8 uses standard VoIP communication protocols so this works fine.
- Q. Could you explain the sensors?
A. The sensors are our collection products that get connected to a mirror port on the network switch and passively record all the packets — not just VoIP.
- Q. How long are the phone calls stored?
A. The phone calls can be retained as long as the customer wants to keep them. They are all stored in a database and standard data retention methods apply.
- Q. Does SilentRunner transcend through all network gateways?
A. SilentRunner can be placed at any gateway from which the user requires collection, whether it's the internet gateway, the VoIP gateway or any other network switch.

[MORE ...](#)

- Q. Do you have to do the capture real time?**
A. No, if you have collected the packets with other devices, such as a sniffer, they can be loaded into the SilentRunner collector at any time, as long as the capture is in a pcap format.
- Q. This information comes from the suspects network correct? And if so, does this have to be at the ISP, or where does this reside?**
A. It depends on the collection. It can be on the internal government or corporate network (organizations must be responsible to ensure their legal compliance), or put in at the ISP (court order would be required).
- Q. The protocols were always listed as VOIP. Can SilentRunner break them out as say SIP or iAX32? Also can it do VoIP within an application, such as Jabber?**
A. Yes, we can break them apart by specific udp/tcp protocols. We are working on all the VoIP transmissions within other applications.(currently we do not).
- Q. What is the cost of this solution?**
A. Please contact your local sales executive for the pricing models.
- Q. What storage is required for this solution?**
A. Storage requirements vary by organization and depend on how the organization wishes to utilize the solution. To find out what your specific storage requirements might be, please contact AccessData Sales at 800.574.5199 (US) or +1.801.377.5410 (International).
- Q. Are calls compressed and how much space is used per hour?**
A. All data captured is compressed and saved into a database. Storage requirements are variable, depending on the organization.
- Q. How do we identify that a user is using a VOIP?**
A. All communications are identified by doing a packet inspection.
- Q. Is this a stand-alone product or do you need to have the other Access Data products?**
A. It is a stand-alone solution that can be integrated with the other AccessData products, allowing you to achieve 360-degree visibility into all data across your enterprise through one vendor.
- Q. Is it just a software, or is there hardware as well?**
A. It is just software, but the user would be required to meet hardware requirements.