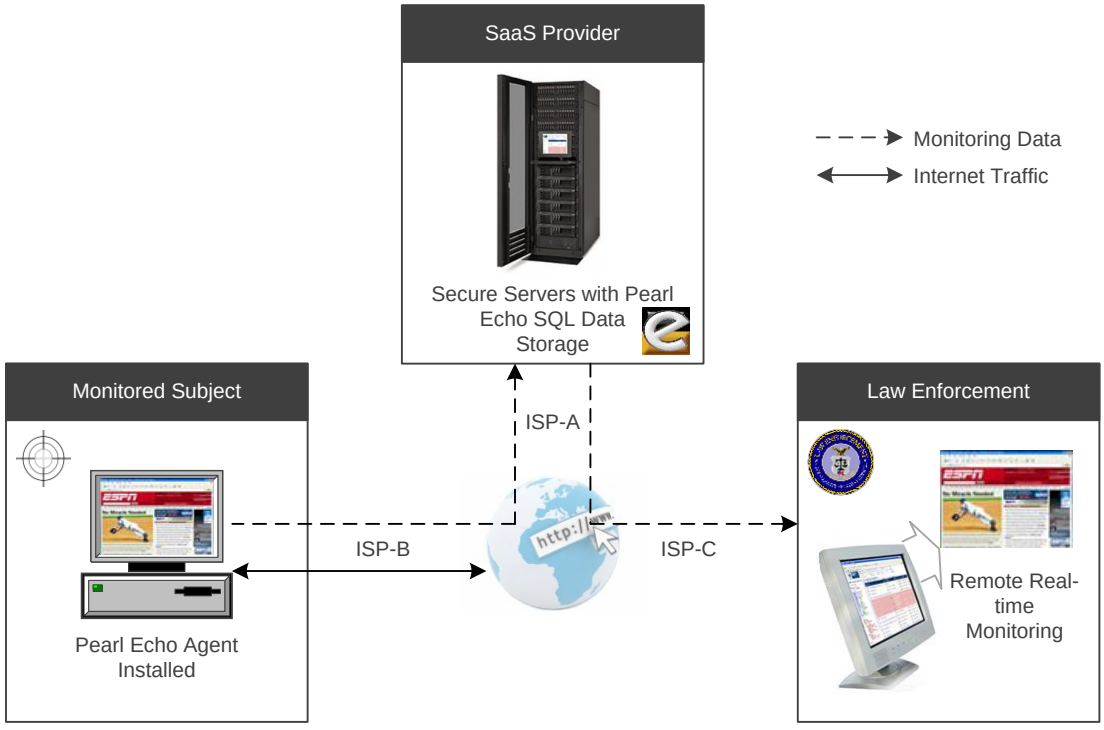
Problem Case Study || Law Enforcement

US Law Enforcement requires real-time capability to monitor subjects and supervise offenders and defendants who have access to technology. The solution must consist of a highly secure technology that is designed to comply with existing case law and Federal legal opinions rendered as well as withstand rigorous judicial scrutiny. Proof of data integrity must be built into the solution and separation of government powers must be respected in all aspects of the design.

The Solution

Pearl Echo.Suite is the cyber component to LE's SaaS offering which includes real-time monitoring and control of remote users' internet communications[1]. The SaaS solution provides Law Enforcement access to the subjects' raw data as well as LE's proprietary predictive analytics engine for reporting, threat assessment display and subsequent intervention.



[1] Partner's company name and branding omitted for confidentiality.

Based on Pearl Software's patented cybersecurity technology, LE's SaaS product is highly scalable and enables real-time monitoring and control of remote and mobile subjects using their existing Internet provider without re-routing communications through LE's environment. Because the Pearl Echo agent is resident on subjects' computers, the solution is indifferent to the method of Internet access (hotspot, on network, off network, etc.) and cannot be circumvented via endpoint encryption. Additional layers of endpoint security are built-in to prevent subjects from removing the Pearl Echo agent from the subjects' computers. By nature of its design, data is hierarchically stored by LE in order to be viewed securely, demonstrate data integrity as well as maintain data segregation. As processing is distributed, subjects' notice no performance degradation in their online-experience should LE's SaaS solution be required to be implemented in a stealth configuration.

Success in the Field

Law Enforcement continues to be enthusiastic about the use of LE's SaaS solution and its effectiveness. From their perspective, the system is relatively straightforward to use in comparison with more traditional computer forensics and management systems. LE's SaaS solution does not require time-consuming analysis of the computer's hard drive, nor does it require deep knowledge of computer operating systems, hands-on access to the subjects' home or office computer, or access to computer forensics laboratory resources. Officers appreciate the fact that LE's SaaS solution provides access to information that reflects the subjects' activities in real-time and includes safeguards against the subjects' devising methods to defeat the system, all while improving officer safety.

According to one officer: "I had a pretrial diversion case where community service was imposed and the individual was dishonest with the amount of hours he completed. I discovered his dishonesty when I reviewed his monitored computer and Internet activities revealed that he was at home and could not have completed the hours he indicated on his time sheet. Although the reality is that he is not going to prison for this activity, it does reinforce that this is no joke and that these are activities that will not go unnoticed."

Another officer commented: "The goal of any type of supervision is to reduce the likelihood of a re-offense and to enhance the safety of the community." LE's SaaS solution assists in ensuring individuals arrested on bond are not reoffending. "On a separate pretrial diversion case, I learned of unauthorized communication with a codefendant through an email which revealed they had been communicating all along despite the Court's directives not to."

Limited resources and tight funding make prioritizing cases a necessity. One officer stated, "I review the data to get valuable insight into my cases' risk. If I see things that concern me about a particular case, I shuffle my field visits such that I make certain I get to that case first."