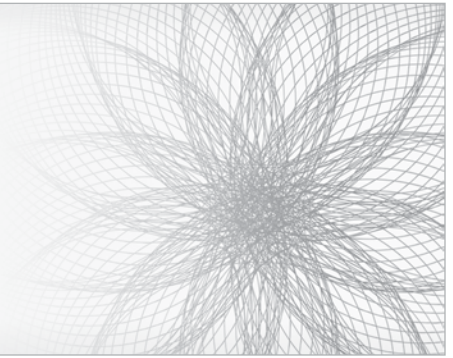


CASE STUDY

MAJOR EASTERN US UNIVERSITY



CUSTOMER SNAPSHOT

Large Eastern
University in the U.S.

Industry:
Education

Location:
United States

Solutions:
Three Solera DS Appliances

- Results:**
- A complete historical record of all network traffic to be used by a number of open source and commercial analysis tools
 - Quick resolution to network issues
 - Evidentiary proof of policy compliance



With the Solera DS Appliances in place the CSO and his team are able to see what happened on their network.



A major university located on the east coast of the U.S. recently implemented a network monitoring and security solution that includes the world's fastest deep packet capture and stream-to-storage solution from Solera Networks. Combined with numerous open source and proprietary network forensics tools, the university now has complete visibility into all network activity.

OVERVIEW

The Chief Security Officer of a major eastern U.S. university is responsible for developing the network security strategy to protect the university's 15,000 students and 2,000 employees.

(The case presented below is based on an actual client. The challenges, situation, and outcomes are all real. Individual and organization names have been omitted to maintain confidentiality).

CHALLENGE

At this particular university, there is a serious expectation of privacy. The network security team is prohibited from actively watching network traffic without approval. They rely on several open source and proprietary tools to alert them when something is wrong. The CSO compares the process to obtaining a warrant—when they obtain permission, they then leverage other tools to further uncover evidence to support their claim that something has gone wrong and needs attention.

With this privacy policy in place, the CSO and his team were often looking at the aftermath of a breach, and would have to run through a complete forensic analysis to determine how it specifically happened. Even with a complete analysis, the result might only be a best guess.

As such, the CSO was interested in a “lockbox for digital information.” He needed a way to track problems and then go “back in time” to see what happened, how it happened, where it happened and the consequences that followed. The solution needed to provide actionable data while also respecting the individual privacy of students and employees.

SOLUTION

The CSO turned to Solera Networks to solve the “lockbox” issue using the Solera Networks DS series. The university implemented three full-feature deep packet capture and stream-to-storage appliances.

Solera Networks appliances continuously capture and store all network traffic at unprecedented speeds (full line rate on 10Gb networks). The system the university implemented has 32 terabytes of data storage. This capability delivers the power for the CSO to have about 30 days worth of recorded traffic at any given time.

University policy mandates that the CSO can't analyze traffic that has been recorded with the Solera Networks solution unless the university council provides permission. Once approved, his team moves forward with active, real-time monitoring coupled with the unabridged historical record provided by the Solera DS appliance. In fact, because the solution is so exacting and comprehensive, the security team is audited to ensure it is being used according to policy.

As with most universities, it was a priority to keep costs down, yet maintain a high degree of value from the solutions they implement. The team therefore uses a mix of open source and proprietary technologies and solutions, including:

Snort®: an open source network Intrusion Detection System (IDS) that excels at traffic analysis and packet logging on IP networks. The university leverages the Solera Networks' appliance by pointing Snort to the complete historical record.

Wireshark: the most popular open source packet analysis tool available today. The Solera DS appliances deliver complete historical packet traffic (header and payload) to Wireshark, which decodes, analyzes and displays information about the packets.

Observer: Network Instruments Observer® was built for real-time analysis, monitoring, and reporting of full-duplex network links. The university uses only the software of this proprietary solution, instead of using Network Instruments' expensive and limited packet capture solution. The university chose the more cost-effective Solera Networks appliance instead.

Other open source tools: Argus, Ntop TCPdump, TCPStat, TCPFlow, and more.

The CSO felt it was important for the university to leverage open source, not just for the cost savings, but also because most of the tools they use are very well documented in higher education environments. "There are experts who have tested, used and proven the effectiveness of the open source tools, not to mention the fact that they work seamlessly with Solera Networks," said the CSO.

RESULT

The university now has its "lockbox" in place. For example, the security team recently received several alerts from Snort. Specifically, they received an alert that a hacker tool was being used to take over machines and gain remote access. The CSO used the Solera DS appliances to pull entire sessions out to see exactly how they got in and what they did. This capability allowed them to obtain the full context (what tool they used to get in, the path, and history of how events transpired) before any serious damage was caused.

"Without a Solera Networks appliance, I wouldn't have been able to see what actually happened," said the CSO. "I would have had to pull the offending machine, and look at the tracks. That would have taken us 15-20 hours to do a forensics evaluation of the machine. Even with the actual machine, we might not have the full picture, as many hacker tools clean themselves up following an attack. The Solera appliances elegantly provide the evidence, and do it in a fraction of the time."



"There are experts who have tested, used and proven the effectiveness of the open source tools, not to mention the fact that they work seamlessly with Solera Networks."

University CSO
Major US University

"Without a Solera Networks appliance, I wouldn't have been able to see what actually happened. I would have had to pull the machine, and look at the tracks. That would have taken us 15-20 hours to do a forensics evaluation of the machine. The Solera appliances elegantly provide the evidence, and do it in a fraction of the time."

University CSO
Major US University

