



## CASE STUDY

# MAJOR US UNIVERSITY

To secure their network for 35,000 students and 10,000 employees, a major private US university deploys a Solera Networks solution. They are now able to record, playback, and analyze all their network activity and respond to attacks, performance bottlenecks, malware or any other issue they might face.

### Customer Snapshot

Large private university in the U.S.

Industry: Education

Location: United States

Solutions: Two Solera DS Appliances

Results: Complete network monitoring capabilities

Ability to capture up to 30 days of actual network traffic

Playback of any "time slice" of recorded network traffic

Fast resolution of network security-related issues

*"This is the most valuable tool we have seen for network forensics. ... We have an 'all-seeing-eye' into our network. We know what has happened and what is happening."*

**Security Analyst**  
Major US University

### Overview

The security analysts at a major US university are responsible for keeping the network secure for 35,000 students and 10,000 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 for confidentiality reasons.)*

### Challenge

A large organization like this with a complex network inherently creates many possibilities for hackers to infiltrate and cause havoc. This was exactly the problem the security analysts faced several years ago after a malicious hack of their website.

The team continuously analyzes and monitors the state of the network, creates optimization strategies based on traffic flows and analyzes any past or present security breaches to insure the network is locked down and performing well.

Like security analysts at most large enterprises, the team implemented intrusion detection software. After evaluating several commercial offerings, they selected Snort®, an open source solution, capable of performing real-time traffic analysis and packet logging on IP networks. Snort uses a detection engine in conjunction with a flexible rules language to describe whether traffic should be collected or passed. While Snort was a great solution for intermittent scanning of traffic analysis, the university found a major challenge with its implementation.

"Snort works with rules to search for certain items that are suspect or items that demand attention, especially if there was evidence of an attack, said a university security analyst. "The servers would quickly fill up and would begin to drop the traffic. It simply wasn't possible to see everything."

The security analyst goes on to say, "What we had was an OK indicator of general trends, but we knew Internet traffic would continue to grow, and we needed something more powerful and comprehensive. Bottom line, we needed to see the whole picture."



record.



replay.



relax.™



**SOLERA**  
NETWORKS

See everything. Know everything.™

## Solution

The answer came from Solera Networks and its product line of deep packet capture and stream-to-storage appliances. Using two Solera DS appliances, they were able to integrate, out-of-the-box, with Snort. Instead of sampling or polling or worse, dropping packets, the university now captures the complete view of network activity—every packet (header and payload).

“This is the most valuable tool we have for network forensics. It gives us the ability to look at the past in the minutest detail,” said the security analyst.

Unlike other capture devices, The Solera DS appliance provides for seamless implementation with no visible network presence. Sustained line-rate gigabit capture, storage, intelligent access to the data via virtual Ethernet adapters, and real-time regeneration all ease the integration to existing analysis frameworks. This enables hundreds of commercial, custom, or open source network forensics applications to process all data on the network, rather than a mere sampling.

For instance, the university once encountered a situation where a student employee put some key loggers on some of the lab systems. They ended up having to scour the drives to find out who purchased the software, where they purchased it and so on. It required a tremendous amount of work. They eventually discovered the offending party, but it took weeks. If they had a Solera DS appliance in place when it happened, they know they would have caught the perpetrator in a fraction of the time.

A common problem they face concerns someone from the outside saying that one of his IP addresses is scanning an outside entity on port 22 and trying to infiltrate their system. The team can go in and look to see if that system is actually scanning them or not, or if they are getting spoofed. Now, if someone is doing something at the moment or in the past that was against policy, they almost instantly see it and can easily take the necessary corrective measures.

## Result

With the introduction of the Solera DS appliances, this major university is now in control of what is happening on their network and can take appropriate measures to ensure its security. Since they can capture and playback an exact record, they can investigate specific time slices to analyze specific traffic. This is extremely valuable to their security strategy. They can effectively respond more quickly and they now have a comprehensive forensic record that helps provide aid for law enforcement agencies when necessary.

The main benefit of having this solution is they have an “all-seeing eye” into the network. They know what has happened and what is happening. With the intrusion prevention system, they partially had this ability, but it was not enough. Now they have the power to be completely accurate with no guesswork. When they recently had some Web pages that were compromised, they were able to “go back in time” to see exactly how it happened and were able to quickly close up the breach. That would have been impossible without Solera Networks.

Life as a security analyst is never easy, but with Solera Networks DS appliances in place, the team now knows that there is nothing that can escape their view.

*“What we had was an OK indicator of general trends, but we knew Internet traffic would continue to grow, and we needed something more powerful and comprehensive. Bottom line, we needed to see the whole picture.”*

**Security Analyst**  
Major US University

Contact a Solera Networks solution provider, or call Solera Networks at:

Solera Networks Headquarters  
355 South 520 West  
Suite 225  
Lindon, Utah 84042  
1 877-5SOLERA (877-576-5372)  
1+ 801-623-5705  
1+ 801-623-5706 fax

Email: [info@soleranetworks.com](mailto:info@soleranetworks.com)

Web: [www.soleranetworks.com](http://www.soleranetworks.com)

Solera Networks Japan, Inc.  
Shinjuku Park Tower N30F  
3-7-1, Nishi-Shinjuku  
Shinjuku-ku, Tokyo 163-1030  
1+ 81-3-5326-3367  
1+ 81-3-5326-3001 fax

Email: [info@soleranetworks.co.jp](mailto:info@soleranetworks.co.jp)

Web: [www.soleranetworks.co.jp](http://www.soleranetworks.co.jp)

© 2008 Solera Networks. All rights reserved. Solera Networks, Solera DS Series, DeepSee, Solera V2P Tap, DS 1150, DS 3150, DS 5150, and See everything. Know everything. are registered trademarks of Solera Networks. All other company names, brand names and product names are the property and/or trademarks of their respective companies.

 **SOLERA**  
NETWORKS  
See everything. Know everything.™