



CASE STUDY



For any security team to stay on top of a global network, it is critical to know what is happening and “has happened” on the network. Tahitian Noni International is able to keep the juices flowing through capture and playback of all network traffic using a solution from Solera Networks.

Customer Snapshot

Leading provider of noni-based products

Industry: Consumer health products

Location: Provo, Utah
United States

Solution: One Solera DS Appliance

Results: Ability to capture 3 weeks worth of complete network traffic

Provides context to Snort® intrusion detection alerts

Fits seamlessly with their many analysis tools

Can now quickly find the source of network problems

“We were interested in the device because it has deep packet capture and playback capabilities and fits so seamlessly with our analysis tools.”

DOUG JAMES

Information Security Engineer
Tahitian Noni International

Overview

Founded in 1995, Tahitian Noni International has experienced explosive growth as the leader in the discovery, development, manufacturing, and marketing of noni-based products including beverages, beauty and spa products, weight management lines, and animal nutrition. Headquartered in Provo, Utah, Tahitian Noni International has manufacturing facilities in the United States, Germany, Tahiti, Japan, and China; and sales offices in more than 30 countries worldwide.

Challenge

With offices spread across the globe, Tahitian Noni International (TNI) has worked to create a network security and management strategy to meet the challenges that are akin to some of the world’s largest corporations. With such a diverse network, the company’s impressive data center acts as a hub with spokes that link to all the foreign offices. It was critical that the network security team know what is happening on all their varied networks and be able to manage security strategies accordingly.

Communication and uptime is critical to business continuity. With network traffic being generated by http, file servers, print services and several proprietary applications that are developed in house to communicate with databases housed in the data center, it was important to know exactly what was happening on the network.

Doug James, Information Security Engineer for TNI and his team rely on several applications designed to bolster security, including Snort, Wireshark and others. “We have systems in place that tell us when something is happening and we wanted the ability to know the ‘why’s and how’s,” said James. “We also wanted to be able to identify any trends in weak areas on our network. It’s impossible to know what is coming down the road. We have a busy IT staff, if we can strengthen and enhance what we know, we can free up our resources to deal with other critical activities.”

Solution

TNI needed to address a fundamental challenge with today’s network security. Without the ability to look “back in time” to watch events unfold, they were trying to solve problems using only slices of incomplete information. Consider a crime



record.



replay.



relax.™



SOLERA
NETWORKS

See everything. Know everything.™

scene investigation. How much more valuable is video to an investigator than a mere snapshot? James found his solution from Solera Networks and its DS Series of deep packet capture and stream-to-storage appliances.

Solera Networks appliances fit into any Ethernet network, attaching via a mirror (SPAN port) or network tap. Unlike other limited options, Solera Networks DS Appliances provide a complete historical record of network traffic (including header and payload), enable complete regeneration, filtering, and analysis using any commercial, custom, or open source analysis and forensic tools.

With TNI's current setup, the DS appliance can store more than 3 weeks of traffic. An unabridged historical record is important because it is imperative to know what happened and why. "When we have an alert from Snort, our intrusion detection system we can usually stop the intruder and clean up the mess, but we also want to go back and find out how it happened and where it came from—Solera Networks enables us to do just that," said James

The Solera DS appliance is used primarily to monitor internal policy violations and "interesting" or threatening traffic that the team considers outside the norm. "We were interested in the device because it has deep packet capture and playback capabilities and fits so seamlessly with our analysis tools," James continues. "Everything that goes in or out on our networks gets recorded on the Solera Networks Appliance. The data is then piped out to various monitoring systems where it is examined for suspect items and applications we don't want on our network. For instance, we've used it to track down spyware and to see who is installing desktop applications that are against policy. It has been a very useful tool."

Result

Recently, James received a call late one night about a serious virus infection in their office in Japan, which is the second largest office in the company. "We first had to disconnect the Japan network from headquarters, and then we turned to the Solera Networks box to replay several hours of network traffic to try to pinpoint the source of the virus," James said. "Half a world away we were able to track down the source of the virus infection, then disconnected the computer and all the other infected computers that were broadcasting. That functionality alone has been a great help to us."

James said that without Solera, it would have been much more difficult to determine which computer was the first to be infected, when it started broadcasting, how quickly it spread from one system to another, and what other systems were affected.

The company takes security very seriously. The team is able to show a return on investment using the DS appliance to gather evidence, troubleshoot network problems, and test performance using actual traffic loads as opposed to simulated traffic. "One of the complaints our engineering staff used to have was that they couldn't simulate production network traffic in our QA environment. Now we can be replaying a day's traffic back through any system and see what happens."

"Customer support has been outstanding," James said. "We have found Solera Networks to be very responsive—they patiently listened to our challenges, and have been very forthcoming in solving our problems. Everyone has been on time when they have set appointments, which for as busy as we are, that is very important. There have been some vendors who have lost our business because they have been late; our time is too valuable for anyone to not be prompt or responsive."

"Customer support has been outstanding. We have found Solera Networks to be very responsive—they patiently listened to our challenges, and have been very forthcoming in solving our problems."

DOUG JAMES

Information Security Engineer
Tahitian Noni International

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

Web: 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

Web: 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.



See everything. Know everything.™