

University of the Sunshine Coast

With planned cuts in IT administration, USC wanted to meet audit requirements and provide open access to information for staff and students—without compromising security. USC is using NetIQ® Sentinel™ to improve security and meet audit requirements for monitoring access to its core finance systems. Sentinel provides simpler access to network resources without compromising security.



Overview

Founded in 1994, the University of the Sunshine Coast (USC) in Queensland, Australia, has more than 6,300 students and 500 staff. The institution offers undergraduate and postgraduate degree programs in arts and social sciences; business; and science, health and education.

Challenge

As an educational institution, University of the Sunshine Coast (USC) aims to be open and inclusive, and this ethos extends to its computing and network resources. Without sacrificing security or exposing confidential information, the university aims to make it easy for staff and students to access the information and resources they need.

With plans to reduce the number of times users needed to enter their credentials and to cut IT

“With [Sentinel] we could both meet the audit requirements and create a number of new solutions to improve security.”

PETER HENDERSON

Enterprise Architect
University of the Sunshine Coast

administration, USC was looking for a solution that could aggregate and monitor logs and events from various systems. The financial enablement for the project came when Queensland Audit Office (QAO) asked the university to monitor its PeopleSoft and TechnologyOne enterprise finance systems for failed login attempts.

“The recommendation from the QAO helped us to secure the internal funding for a broader log monitoring solution,” said Peter Henderson, Enterprise Architect, USC. “We knew that with the right software we could both meet the audit requirements and create a number of new solutions to improve security, enhance access and reduce administration.”

Solution

USC selected Sentinel as the most cost-effective solution, largely because it already had support for connecting to the required applications, parsing the data, and producing detailed reports. USC worked with Sentinel solution partner, Directory Concepts, to implement the solution on a single server running SUSE® Linux Enterprise Server.

“Directory Concepts deployed the custom collector for PeopleSoft—and the process was so straightforward that they were able to add the TechnologyOne collector at the same time,” said Henderson. Sentinel aggregates information



At a Glance

■ Industry

Education

■ Location

Queensland, Australia

■ Challenge

Without sacrificing security or exposing confidential information, the university aims to make it easy for staff and students to access the information and resources they need.

■ Solution

Use Sentinel to aggregate information from system logs and enable sophisticated monitoring and reporting.

■ Results

- + Enables companies to meet their audit requirements
- + Provides a flexible platform to build new automation solutions

“This has enabled us to reduce complexity and effort for users without compromising network security.”

PETER HENDERSON

Enterprise Architect
University of the Sunshine Coast

www.netiq.com

from system logs and enables sophisticated monitoring and reporting. The solution includes rules-driven alerts to automatically flag suspicious events. By monitoring numerous systems and devices and presenting real-time network security information in tailored reports, Sentinel significantly reduces manual administration and helps improve security.

“For our key corporate applications, Sentinel alerts us to predefined activities or events,” said Henderson. “We can immediately see repeated failed login attempts and where they are originating. The insight that Sentinel provides would be impossible to gain manually in real time: there’s simply too much data, and from too many different systems.”

Sentinel enables USC to meet or exceed the audit standards expected by the QAO—without occupying valuable staff in manual administration. More important, the technology is highly extensible, and USC is now building or planning a further six related solutions over the next twelve months.

“By using Sentinel to monitor activity on our Squid Internet proxies and match it with other network logs, we have been able to eliminate the need for users to re-enter their internal network credentials to use the web,” said Henderson. “This has enabled us to reduce

complexity and effort for users without compromising network security.”

Results

The Sentinel deployment has enabled USC to meet its audit requirements, and has given the university a flexible platform to build new automation solutions. In the past, the IT team spent approximately two man-days each month manually reviewing system logs. Sentinel automates the process, freeing up staff and enabling them to focus on analysing and fixing problems.

“Sentinel doesn’t just help with security—it also enables us to see where an authorised user is having a problem with logging in and may require assistance or education,” said Henderson. “With Sentinel, it’s much easier to spot patterns and anomalies in log files because the data is already filtered and normalised. This reduces risk and enables our skilled technical staff to focus on more valuable tasks.”

USC is now building a solution using Sentinel that will monitor provisioning requests and ensure that they are correctly executed.

“There are often exceptions to rules that cause errors in the automated provisioning process,” said Henderson. “Sentinel will help us proactively fix issues before users need to contact the helpdesk.”



Australia

+ 61 3 9825 2300

China

+ 86 10 6533 9000

Hong Kong

+852 2588 5288

India

+ 91 80 4002 2300

Japan

+ 81 3 5413 4800

Malaysia

+ 60 3761 00214

New Zealand

+ 61 2 9904 6111

Singapore

+ 65 6510 4200

South Korea

+ 822 2008 4690

Taiwan

+ 866 2 2376 0036

NetIQ

Worldwide Headquarters

Houston, Texas
713 548 1700
888 323 6768

www.netiq.com