clearswift

Sunshine Coast COUNCIL

# Sunshine Coast Regional Council

Case Study – Local Government

> We are confident in the ability of the Clearswift solution and the next logical step for us is to think how we can be always - ready for the changing IT landscape.

## Sunshine Coast Regional Council prepares for changing IT landscape with critical information protection

**OVERVIEW**

The Sunshine Coast Regional Council was formed following the amalgamation of Caloundra, Maroochy and Noosa Councils in 2008. At the time, the merging of the three individual local government bodies created the fourth largest local government authority in Australia. Despite the Shire of Noosa reestablishing itself as independent from the Sunshine Coast Regional Council in December 2013, the Council remains one of Australia's largest and most advanced constituencies, covering 2,291,000 square meters.

Headquartered in Nambour, the Council is focused on planning and providing services to more than 278,000 people, building a region like no other in Australia. To deliver on this, it is supported by a strong, agile organisation with energy, enthusiasm and innovation, as well as a commitment to responsible governance, service delivery and valuing staff. A key focus since its amalgamation has been to adjust to the ever changing IT landscape; this is to ensure operational efficiency and the protection of its citizens from the increased threat of cyber-attacks and unauthorised sharing of critical information.

When the initial amalgamation took place, there were three distinct IT networks in operation, meaning there was a need to combine these to create one overarching network. For the Sunshine Coast Regional Council's IT department, an industry leading, robust and flexible web and email filtering solution was central to the development of a new IT infrastructure.

"We started with three internet access points that needed to merge, so the immediate challenge was to establish a uniform policy across all environments in order to build a single one," said Robert Grandcourt, Information Technology Security Analyst for the Sunshine Coast Regional Council. "As a local government body, we were also mindful of the need to use technology in a way that delivered value, not just for us, but also for our ratepayers and constituents."

## About Clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations to have 100% visibility of their critical information 100% of the time.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific and the United States. Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at **www.clearswift.com**


**UK - International HQ**
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

**Australia**
Clearswift (Asia/Pacific) Pty Ltd
5th Floor
165 Walker Street, North Sydney
New South Wales, 2060
Australia

Tel: +61 2 9424 1200
Technical Support: +61 2 9424 1210
Email: info@clearswift.com.au

**Germany**
Clearswift GmbH
Landsberger Straße 302
D-80 687 Munich
Germany

Tel: +49 (0)89 904 05 206
Technical Support: +49 (0)800 1800556
Email: info@clearswift.de

**Japan**
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
Japan

Tel: +81 (3)5326 3470
Technical Support: 0800 100 0006
Email: info.jp@clearswift.com

**United States**
Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

Tel: +1 856-359-2360
Technical Support: +1 856 359 2170
Email: info@us.clearswift.com


The decision was made by the IT team that the most suitable approach was to adopt the best operating environment to implement across all three councils, and adhere to a 'best of breed' usage policy. At the time of amalgamation, Maroochy Council, the largest council network of the three, had been successfully using Clearswift for almost a decade, including the Clearswift SECURE Email Gateway and Clearswift SECURE Web Gateway. After evaluating these solutions in operation, Robert and his team decided to administer the appliances across the complete newly formed network.

The benefits the Council received from the implementation included increased access for staff across all communication channels (web 2.0, email and Internet) than previously, whilst ensuring the highest levels of security across the organisation, centralised management and technical support benefits.

Being a local council, the IT team were under increasing pressures to continuously achieve cost savings, as well as ensuring the business was operating with proven and robust technology in order to prepare for the anticipated future requirements of the council and the requisite critical information protection.

When Noosa left the Council group, and the number of users dropped to 1,500 from 2,500, Robert and his team decided it would be an opportunity to reassess the architecture embedded across the network. In order to assess if both Clearswift and other vendors' technology, which already existed within their infrastructure, still met their needs a decision was made to pilot a software blade approach for web security in order to make a like for like comparison.

Throughout the pilot, it was evident that the potential alternative to Clearswift wasn't operating at a level that the Council required, or at the level they were previously receiving from the Clearswift solution.

*"The main red flag for us was that the anti-virus filtering and malware blocking capabilities weren't operating effectively, which is something you would expect from a leading security vendor. With the growth in malware attacks we have been experiencing across our networks, any reduction in costs is heavily outweighed if we have to compromise on the protection of our staff, ratepayers, supply chain partners and increased resources to manage content filtering policies. As a result of the pilot, and the vendor's inability to meet the council's established security governance policies, a decision was made to revert back to the Clearswift solution due to the high level of information protection that had already been demonstrated."*

As soon as the Clearswift SECURE Web Gateway was re-instated across the network, the Council noticed the instant improvement in the levels of protection its staff were experiencing.

Clearswift's SECURE Email and Web Gateways provide the Sunshine Coast Regional Council with centralised network security protection, underpinned with the industry's most advanced Deep Content Inspection engine to combat advanced malware detection, delivering bi-directional content-aware data loss prevention that is integrated into the architecture. The Gateways operate a centralised granular policy management interface that is 'resource-lite' for ease of configuration, and ongoing operations.

Businesses in today's challenging environment are required to maintain an agile IT infrastructure, in order to remain efficient and cost effective. New technologies like the National Broadband Network (NBN) and cloud solutions have been key considerations for the Council and how these new trends in IT will make an impact. With the support of Clearswift, the Sunshine Coast Regional Council continues to have robust security in place for web and email, meaning its focus has moved towards future organisational needs.

*"Like most businesses today, our IT environment is changing all the time. We have more mobile applications and mobile devices coming into the network and the core infrastructure is changing to open up and embrace the mobile movement. With this collaboration shift in mind, security has once again become a concern."*

To embrace the proliferation of mobile devices, the Council has adopted a basic BYOD strategy. This includes adjusted internal policies to allow employees to access the network via their mobile devices and applications, as well as external VPN access. The Council also has other applications running to allow file sharing and Wi-Fi access for non-network devices.

Following the success of the Clearswift SECURE Web Gateway and the Clearswift SECURE Email Gateway, the Council is looking to consider the implementation of the Clearswift Critical Information Protection (CIP) Management Server and Agent. This would provide endpoint protection for mobile workers including device control, deep content inspection, remediation actions, encryption and comprehensive auditing.

*"We are confident in the ability of the Clearswift solution and the next logical step for us is to think how we can be always-ready for the changing IT landscape. The Clearswift CIP Management Server and Agent is a solution that will support the strategies we already have in place, advancing our content-aware Data Loss Prevention strategy and really put the Council on the right path to enhance our operational agility and provide greater efficiencies for the Council in the future,"* concluded Grandcourt.