

Salvation Army

Salvation Army finds Sanctuary
in Whitelisting Software



Background

As the second largest provider of social care in the UK apart from the Government, The Salvation Army provides a vital service to homeless people, the elderly and other vulnerable groups. It is both a church and a charity, served by 7,000 employees, comprising 1,500 Salvation Army officers who are ordained ministers of religion, and civilian staff including care workers, drug counselors and social workers.

The Territorial Headquarters (THQ) of the organization is based in Elephant and Castle, London and staffed by 350 people, including 21 IT staff who manage and support the networking and communications requirements for The Salvation Army's 18 divisional headquarters, social services centers, and corps (churches and community centers), covering the whole of the UK.

Organizational Challenges

"The Salvation Army's IT is extremely centralized" explains Martyn Croft, Head of Corporate Systems. "We have a dispersed workforce, made up lay people and church staff, providing care and support in a variety of environments including drug addiction centers, elderly care homes and the familiar Salvation Army centers."

Croft estimates that there are 2,000 endpoints, with 2,500 users: "If you overlay IT on this sort of organizational structure, it has to be a very controlled environment. The care workers can't be expected to be looking after the security of PCs in the centers, they are there to deliver care, not manage IT. So we have to ensure that this is centrally managed," he says.

While the organization already uses thin client technology in its social centers, the issue of endpoint security became more pertinent when the Salvation Army migrated from NT4 to XP across the whole organization. This meant that Martyn Croft and his team needed to find a way to enable The Salvation Army to benefit from the flexibility of 'plug and play', while mitigating the risk of data leakage via USB storage devices, such as flash keys. "We have data that we have an obligation to protect and so we wanted to establish a man-

aged desktop environment before we rolled out XP."

Initially, The Salvation Army used an endpoint security product which, although it enabled the IT team to close all USB ports by default, did not enable the team to carry out auditing and reporting on the device usage across the organization.

As this reporting and auditing requirement became more critical, Martyn Croft and his team began to look for an alternative solution that could deliver the functionality and visibility that they required to centrally manage USB device usage throughout this diverse organization.

The Solution

Martyn Croft's boss is David Clayden, the Chairman of the Charities Consortium IT Directors' Group (CCITDG www.ccitdg.org.uk), which involves 85 of the premier charities in the UK. Each year the CCITDG members can opt in to a benchmark of best practice in IT, which measures key indicators such as cost per user and IT spend as a percentage of turnover and these are useful parameters to keep in mind when looking for cost-effective solutions.

Croft looked into alternative products that would still meet budgetary and performance criteria while enabling the functionality and reporting that he required to centrally manage USB device usage at The Salvation Army. He chose Lumension Security's Sanctuary, which is endpoint security software that enables central management of all removable storage media and applications that run on corporate networks. Sanctuary works on a "whitelist" model, whereby only the devices and applications that are specifically authorized by the IT department are able to connect to or run on the corporate network. Nothing else is permitted to connect or run on the network. This enforces acceptable use policies throughout the organization by simply blocking the use of any device or application that has not been authorized by the IT department.

Sanctuary is even granular enough to permit use of specific brands of USB key by named individuals

at certain times of day. So, for example, John could use a Lexar stick at 9am - 5.30pm Monday to Friday, but be blocked from using this device on Saturday afternoons. His colleague Peter would be blocked from using a USB device at all and John would be blocked from using a U3 stick, unless this device was on the authorized list.

Increasing Visibility

Croft reports that The Salvation Army is already using System Management Server (SMS) so that his team has an overview of every PC that's on the network and is able to deploy software to every PC on the network without having to physically visit each site. The ability to install Sanctuary using SMS was a critical factor in its deployment at The Salvation Army.

Sanctuary also has the advantage of auditing all data that is downloaded or uploaded from authorized USB devices. This means that IT managers can create an audit trail for data protection, compliance, or simply to gain greater visibility of what data is being transferred via USB ports throughout the organization. It was this strong auditing and reporting functionality that convinced Croft and his team to trial the Sanctuary software alongside the existing device control software in use at the Salvation Army. To date, Sanctuary has been rolled out to protect the PCs of The Salvation Army headquarter offices and it is anticipated that all 2,000 endpoints will be protected eventually.

“The great thing is that you can run Sanctuary in logging mode so that you can test it. Sanctuary also gives us much more granularity than the product we were using before, which we found a little too cumbersome. Sanctuary is a piece of cake to install”, reports Croft. “Once you’ve got XP, enabling the use of USB storage media, these are foreign devices that you’ve added to your network. So you have to be able to have visibility of what’s going out on those devices. If we allow our people to use USB sticks, then I want to be able to audit this, so that if we suffer a data breach (in or out), it’s very easy for me to track who has perpetrated that breach.”

While recognising the inherent risk of enabling removable storage media to connect to the network, Croft and his team also recognise the value that USB storage devices offer across the organization. He explains that he wants to enable his colleagues to use USB memory sticks, for example to download PowerPoint presentations to help Salvation Army officers in their Christian ministry, but he wants to ensure that this is done without any associated risk to the data.

“We want to be able to create a policy whereby if you do store data on a USB device, you have a duty of care to that data. So we advise our staff to use an encrypted USB stick – so that if the stick gets lost or left on the bus, the information won’t fall into the wrong hands. Using Sanctuary, we can open the USB port to encrypted devices, but block USB watches, or personal devices such as digital cameras from connecting to the network, to remove the risk of data being downloaded to less secure devices,” he explains.

Croft also warns: “It’s not just what people take from the network that has to be monitored, these days it’s what they leave behind too. The crossover between corporate and lifestyle computing means that employees seem to think it’s okay to bring their digital devices such as cameras, iPods and memory sticks into the workplace. You don’t want to find that someone has plugged in a device and left you with copyright images or MP3 files on your company server. The only way to control this is to monitor the network and block anything that’s not authorized.”

About Lumension Security™, Inc.

Lumension Security, a company formed by the combination of PatchLink® Corporation and SecureWave® S.A., is a recognized, global security management company, providing unified protection and control of enterprise endpoints for more than 5,100 customers and 14 million nodes worldwide. Leveraging its proven Positive Security Model, Lumension enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions that simplify the entire security management lifecycle. This includes automated asset discovery, vulnerability assessment, remediation and validation; application and device control; extensive policy compliance reporting; and integration with leading network access control solutions. Headquartered in Scottsdale, Arizona, Lumension has offices worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, Hong Kong and Singapore.



Lumension Security
15880 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260
480.970.1025 / www.lumension.com

©2007 Lumension Security. All rights reserved. Lumension Security, the Lumension Security logo, and the PatchLink and Sanctuary product names and logos are either registered trademarks or trademarks of Lumension Security. In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.