Faronics™

Intelligent Utilities for ABSOLUTE Control

Deep Freeze, Faronics Anti-Executable, and the Los Angeles Police Department

CASE STUDY

Last modified: February, 2006

Faronics
Toll Free Tel: 800-943-6422
Toll Free Fax: 800-943-6488
International Tel: +1 604-637-3333
International Fax: +1 604-637-8188

www.faronics.com

History

The City of Los Angeles, California is the second most populous city in the United States with a current estimated population of nearly 4 million people. Los Angeles is the principal city in a very large metropolitan region. With its 470 square miles, the City represents 11.5% of the area and 38.8% of the population of the County of Los Angeles. Founded in 1781, the City has grown from a provincial outpost under a succession of Spanish, Mexican, and American rule to consistent and dramatic population increases ranging from 50,000 in 1890, to 1.5 million in 1940, to 2.4 million in 1960, to 3,864,400 in 2003, and nearly 4 million today.

The Los Angeles Police Department (LAPD) is the second largest Police Department in the nation and is one of the most innovative and certainly recognizable law enforcement agencies in the world. The population size and density, the large geographical area, and the cultural diversity of the City of Los Angeles provides challenging complexities for policing by the LAPD. Information technology plays a significant role in facilitating those complexities and in improving the overall efficiency of the Department.

As of August 2005, the LAPD has 9,214 sworn officers, 3,046 civilian employees, and serves a population base of 3,819,951 (2003) in a territory of 468 square miles.

Situation

The LAPD patrol cars are currently set up with Mobile Data Terminals (MDTs). The terminals have both software and hardware limitations; they run Windows 95 and have only a single application installed on them — a CAD (computer aided dispatch) application used as a tool for law enforcement. The MDTs use a Motorola proprietary communication system with very low bandwidth; therefore, if a terminal has problems, it is replaced and the affected device is usually re-imaged, rather than troubleshooting a very specific configuration issue. When a terminal does need to be brought in for maintenance and re-imaging, this means downtime for the terminal as well as the patrol car it services.

However, the LAPD is changing the make-up of its technological resources in both hardware and software. They are switching from the terminal model to a computer model by replacing the MDTs with what are known as Mobile Data Computers (MDCs). These new MDCs are Dell D610 laptops and come with the Windows XP operating system with Service Pack 2, 1 GB of RAM, a DVD drive, and an 80 GB hard disk. The Department will be using 1,586 of these laptops for the Department's patrol cars.

Because of the new software and hardware that is being introduced into the computing environment at the LAPD, the Department was concerned about new threats and possible software configuration issues on the machines. The new operating systems are susceptible to external threats such as spyware, viruses, and other malware, and the department was looking for a solution to prevent any damage that might be caused by these threats.

Initial Deployment Process

Tim Riley, CIO and Bureau Chief of the LAPD's Information and Communication Services Bureau, was familiar with Deep Freeze from his tenure as a Police Captain with the Newport Beach Police Department where he oversaw the implementation of Deep Freeze on all their MDCs. He decided to implement this proven technology at the LAPD as a way to dedicate fewer resources fixing machines in such a data sensitive environment. Anti-Executable was seen as a good complement to Deep Freeze's reboot-to-restore technology.

"Deep Freeze and Anti-Executable are crucial to preserving an image determined for mission critical law enforcement systems used 24x7 to ensure reliability and security with minimal downtime and with the least reliance on IT personnel," said Chief Riley.

The LAPD recently decided to deploy Anti-Executable and Deep Freeze as a comprehensive solution on the 1,586 new patrol car MDC laptops. Without Deep Freeze, any problems on the new systems would produce downtime that would need to be solved in the same way as the MDTs — re-imaging or replacing the laptops. Deep Freeze lets the user quickly reboot the laptop to return it to its original configuration every single time, eliminating the need for the laptop to be brought in or replaced. Anti-Executable's whitelist technology standardizes any environment by preventing all unauthorized or unwanted programs from being installed, regardless of whether they are downloaded from the Internet or introduced via any removable media.

"This configuration setup with Anti-Executable and Deep Freeze will cut down the amount of staff needed to manage the laptops while still keeping them up and running," said Tom Hsieh, Senior Network and Systems Analyst at the LAPD. "I have seen all the problems that can occur in a workstation environment, but in a mobile environment, it is completely different because we have less time, staff, and resources to work with — and the service level is very important. We are pretty sure Deep Freeze and Anti-Executable will help accomplish our task of having the laptops up and running without requiring any antivirus definition file or windows updates."

"We currently have a policy that prohibits unauthorized installation of non-Department sanctioned/owned software on any Department computer," said Mr. Riley. "Anti-Executable will serve to increase a user's productivity by blocking the installation of non-business and harmful files that could prevent the use of a mission critical system." Because Anti-Executable proactively protects machines by only allowing authorized executables to run, tasks that are often performed to avoid software compliance problems, such as constant routine software audits, are not necessary when Anti-Executable is installed.

"I see this laptop security concept just taking off in every mobile environment because I see no point in dealing with updates where there is a bandwidth limitation," said Mr. Hsieh. "It is better to invest the time defining and stabilizing one laptop image with the configuration settings and applications needed or required, and determine what needs to run in order to avoid configuration updates. This way you protect the time when the user is logged in, and you are able to restore the computer to its original configuration, down to the last bit, every time the computer reboots. This will let us service the users better and more efficiently."