

Swiss Police Aargau

Fighting Data Thieves: Swiss Police Department in Aargau trusts Sanctuary Device Control



Trespassers have a hard time, indeed, in Switzerland's region of Aargau. As part of a network of municipal, regional and county police stations, an overall number of 550 officers ensure public security. However, without the deployment of modern IT systems, it would be unthinkable to effectively protect the 575,000 inhabitants of this Swiss county consisting of eleven districts. Fighting data thieves within its computer network, Aargau police's IT department trusts Sanctuary Device Control, a software developed by Lumension Security leveraging whitelist technology to proactively control the use of portable media and endpoint devices within business environments.

At Aargau police, Bernhard Wernli and his team of eight IT experts faced the challenge of fulfilling upcoming security and data privacy regulations by the Swiss government in the year 2007. Considering the steady flow of visitors every day, they had to deal with the realistic risk of unsolicited users stealing sensitive data or causing malware and spyware attacks within the internal network through USB memory sticks, mobile devices, and port access at unprotected PCs. The primary goal of a fundamental network redesign was to immunize more than 650 PC workstations at Aargau police, and protect the internal computer network against malware and virus infections "behind the central firewall's back". At the same time, a limited number of mobile devices still had to be accessible in order to perform everyday police tasks at headquarters and its twelve additional field offices.

IBV Informatik AG, located in Urdorf, took up the role of service partner during the entire consulting and implementation process. Developing and distributing a product portfolio for OS/400, Windows, .NET, Linux and Unix operating systems, the company was founded in 1981 and special-

izes in comprehensive solutions for automation, customer relationship management, database management, system management, and security. After having thoroughly surveyed the market, Aargau police selected Sanctuary Device Control, the software's whitelist technology enforcing central security policies for mobile devices and port access to effectively stop data leakage, malware and spyware attacks.

Sanctuary Device Control's Whitelist Technology

Deployed at kernel layer of the client's operating system, Lumension Security software utilizes whitelist technology to enforce company security policies and block unauthorized scripts. Installed on every single computer within the network, Sanctuary Device Control limits user activities to selected functionality, preventing the execution of unauthorized commands. Unlike traditional security solutions that take a reactive approach to symptoms after a threat has already propagated, Sanctuary proactively protects against data leakage, malware and spyware by denying everything by default. Whitelist technology creates digital fingerprints of selected programs and activities that are allowed, instead of wrestling with the huge variety of ever-changing applications wreaking havoc in today's IT environments. After an initial scanning process of services within company networks, only whitelisted devices are allowed.

Through its Positive Security Model, Lumension enables Aargau police to maintain a desired security posture, ensuring full control of a PC's activities. Users logging into their computers are authorized by security server identification based on the individual PC, user, and user group. Hash and authorization lists allow for communication with Active Directory and eDirectory databases to align access rights of end devices with user

activities. In the event of users attempting to install a new program, the security program “hits the brakes” until the network team has given approval. Executable code like VBScript, Microsoft Office VBA, and JavaScript have to comply with security configuration and policy, and Sanctuary blocks any other attempt of the operating system to establish links. In this way, malware and hacker attacks are stopped before harming the company network infrastructure.

Project History

“We had to deal with the situation that data was being exchanged between network and stand-alone computers,” Bernhard Wernli, head of the IT department at Aargau police, explained. “In such a scenario, there is constant danger of sensitive information stored on USB memory sticks leaving the network, or alternatively, malware bypassing the central firewall system.” Now, it is possible to allocate individual user rights, and configure and survey different access rights for every police station. Depending on whether security personnel works with mobile memory devices, CD-ROM drives, floppy disks, or digital cameras, there are different user groups with corresponding user rights. Police officers simply fill out the request forms to determine which services they need to access, and then, they are placed within one of six current Active Directory groups. “Daily administrative work for this is really low,” says Wernli. “All we had to do is configure the user groups with different access rights once, and now users can be placed within these groups by every member of our IT department – even temporarily.”

“Every Computer Is Shut Down”

The quest for the right security solution proved to be more difficult, though. “At first, we had tested a product by a competitor which, as we found out, didn’t work at all within our network,” adds Aargau police’s head of the IT department. “However, when we installed Sanctuary Device Control, we were pleasantly surprised.” Before the actual rollout, Aargau police’s IT experts tested as part of a pilot project, whether all of the functionalities worked without defect, and set up the individual user groups with specific access rights. Due to the fact that Aargau district consists of a multitude of small police stations with completely diverse IT requirements, gradually more computer networks were equipped with Sanctuary technology. “This could not be done simultaneously,” Wernli points out in retrospect. “All in all, there were more than 650 computers, but only five of them caused problems which is a really low percentage rate considering such a large number of PCs.” Other criteria such as the software’s price-performance ratio as well as its functionality and user-friendly design played an important role, too, when Aargau police selected Lumension Security. Bernhard Wernli’s summarizes: “With Sanctuary Device Control every computer is shut down and protected against unsolicited access.”



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.