

Nevada Office of Veterans Services



The Nevada Office of Veterans Services deployed SecureWave Sanctuary to make sure that its systems and sensitive information were protected as their employees were becoming more technologically advanced

Background

The Nevada Office of Veterans Services (NOVS) is a state government agency with seven locations, including headquarters in Reno, NV. NOVS provides assistance and services to veterans, their family members and residents of Nevada serving in the U.S. armed forces. The agency has six programs: Veterans' Benefit Representation, Veterans' Cemeteries, Veterans' Nursing Home, Veteran Guardianship Program, Veteran Legislative Issues and Veteran Information Clearinghouse. NOVS serves as a liaison between veterans and the U.S. Department of Veterans Affairs.

Challenge

In the past four years, NOVS has experienced significant changes to its IT environment. Most notably, its staff was becoming more computer savvy. In early 2005, Jeff Fuhler, information security officer at NOVS, realized that he needed to conduct a risk assessment on the agency's IT security infrastructure.

"It used to be that people only knew how to use one or two programs

depending on their specific job function," said Fuhler. "In the past few years, however, people have become more familiar with computers and understand how to do much more. While this created many positive opportunities for the agency to grow and expand its services, it has also introduced security risks that were not there before. We needed to make sure that our systems and sensitive information were protected as our employees were becoming more technologically advanced."

After evaluating the agency's security posture, Fuhler recognized that removable storage media—including external hard drives and USB memory sticks—represented a serious threat. NOVS had a policy in place that defined how employees could use their work machines, but enforcement was limited to the capabilities of Active Directory. Fuhler had no way of prohibiting employees from removing information via portable storage devices.

"Active Directory allows us to effectively block access to certain information and applications based on job description. However, it does not prevent authorized users to download that information to a device," said Fuhler. "What was perhaps even more of a concern was malicious intrusion. With no control over USB access, someone—whether it was a disgruntled employee or a guest—could easily plug in a device and potentially install a malicious application or virus. This was a serious issue because much of the information we have on file is medical records, so we needed to do whatever was necessary to comply with HIPAA and keep that data safe."

Solution and Benefits

After researching potential solutions, Fuhler elected to deploy SecureWave's Sanctuary endpoint security software on all the agency's workstations. Sanctuary enables IT administrators to create a whitelist of allowed devices, denying all others by default. Sanctuary allows for flexible enforcement of device control policies through granular parameters. Administrations can assign permissions at a high level or allow particular user groups or individual machines to access certain devices at specific times. Policies can also be enforced by specific models of media, such as those with automatic encryption, and by time constraints, encryption, volume of data, data transfer or other criteria.

"Sanctuary is the perfect solution for our situation. We wanted a technology that controls what removable storage media can work on our machines, and Sanctuary does just that," said Fuhler. "I'm not worried about the threats posed by these devices because we know exactly what media is being used, by whom and for what purpose. The granular permissions that I can set using Sanctuary also make it a much more practical approach than removing all USB ports or CD drives. For example, we allow employees to play music CDs but we do not allow them to copy anything onto data CDs."

Occasionally, a NOVS employee will want to bring work home via a USB stick or other removable media. The agency's policy states that no employee can use a device for this purpose, so by not making any exceptions, this becomes a business decision rather than an IT decision.

“If you have a solution in place that secures your network, then you can make business decisions about any allowed exceptions,” said Fuhler. “If someone needs to remove information, there is a procedure in place and I will typically copy the data for them. This changes a security risk into a business function. There’s no reason for most of the staff to take information off of the network, so we can make this our default policy and address potential exceptions on a one-off basis.”

In addition to effectively enforcing the agency’s device use policies, Sanctuary also requires very little maintenance. The NOVS IT staff consists of two people, so using products that require a great deal of administrative overhead is not feasible regardless of how effective they are.

“We’ve never had a security breach and we never intend to,” said Fuhler. “It blows me away that Windows is designed so that users cannot install a local printer but they can use any

removable storage media they want. Sanctuary allows us to proactively address this security risk and keep the proprietary information contained in our systems safe from data theft and other malicious activity.”



SecureWave
Safeguarding Tomorrow

www.securewave.com
info@securewave.com

North America

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America
+1 (703) 713 - 3960 Phone
+1 (703) 793 - 7007 Fax

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom
+44 (0) 1908 357 897 Phone
+44 (0) 1908 357 600 Fax

Continental Europe and Rest of World

Atrium Business Park
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg
+352 265 364-11 Phone
+352 265 364-12 Fax

© 2007 SecureWave SA. SecureWave and Sanctuary are registered trademarks of SecureWave SA. All third party trademarks are the property of their respective owners.