



C A S E S T U D Y

Golden State Water Company

How a major California utility protects the health and security of IBM Power Systems

Rigorously monitoring and managing the health and security of your systems has always been a prudent practice, but for some companies it has become much more than that. With the advent of stringent business accountability regulations such as Sarbanes-Oxley (SOX), many auditors now insist on the aggressive protection of systems and data. Golden State Water Company is well cognizant of that fact and, being proactive, the company took action before being required to do so by its auditors. The solution? Golden State Water and its auditors rest easy knowing that StandGuard Network Security, StandGuard Anti-Virus, MessengerPlus, and PeekPlus, all from Bytware, Inc., are monitoring and protecting the company's IT environment.

San Dimas, California-based Golden State Water is the flagship subsidiary of American States Water Company, which also owns American States Utility Services, Inc. and Chaparral City Water Company. Through its subsidiaries, American States Water serves more than 255,000 customers throughout California and more than 13,000 customers in Fountain Hills, Arizona. In addition to providing life's most vital commodity, water, the company also generates and distributes electricity to more than 23,000 customers in Big Bear, California. In 2007, publicly trad-

an eye on what commands are being used by whom," explained Alan Carroll, senior systems programmer at Golden State Water. "We are very proactive about monitoring system services and the use of various commands that we think are crucial to watch. For example, I can see when an 'end subsystem' command is issued and who issued it. As a result, when our auditors came in they were very impressed with our aggressive monitoring of our systems."

StandGuard Network Security also helps to guarantee that employees adhere to the stated policies for the management of system data. A case in point: Application support personnel have been told that they are not supposed to create user profiles. To validate that this policy is being followed, StandGuard Network Security will send real-time notifications of violation attempts to the IT administration group. In fact, StandGuard Network Security notifies IT administrators of any user profile activity that falls outside of the company's normal protocols.

In addition to notifying administrators of any protocol violations, StandGuard Network Security also logs all critical events, such as user profile changes, whether or not they fall within the company's policies. This function is indispensable because SOX

“I can see when an ‘end subsystem’ command is issued and who used it. As a result, when our auditors came in they were very impressed.”

ed American States Water Company (NYSE: AWR) earned a net income of approximately \$28 million on operating revenues of more than \$301 million.

Enforce and Audit Policies

The establishment of meticulous business and system data update policies is a critical component of an effective security plan. Nonetheless, creating rules that define who can change what data is one thing, but enforcing those policies, auditing actions taken under them, and tracking violation attempts is something else. StandGuard Network Security makes it easy for Golden State Water to do just that by providing a supplemental layer of public and private authorities to access and update resources, with a focus on users and groups, and their relationship to databases, applications, and objects.

Golden State Water employs StandGuard Network Security not only to control and audit the use of system services, but also to monitor the execution of specific commands. "We like to keep

requires that the company monitor those changes and report on them weekly.

Thwart Infections

What they say is true. IBM i (like its predecessors OS/400 and i5/OS) is exceptionally resistant to viruses, but "exceptionally resistant" and "immune" are not synonyms. There have only been a few confirmed viruses that affect IBM i, but the problem goes deeper than that. With the Integrated File System (IFS) hosting data and applications for a variety of operating systems in addition to IBM i, the opportunities for viruses to sneak onto the IFS are rife. And viruses on the IFS can spread to other computers on your network.

StandGuard Anti-Virus is built specifically for IBM i, but it is powered by McAfee's industry-leading virus scanning engine. Golden State Water has been using it since 2005 to protect the company's systems from the threat of viruses. "Other than the test virus [EICAR test file] that Bytware sends to make sure ev-

everything is working, I have not, knock on wood, personally come across a virus on our system,” noted Carroll, “but, that having been said, at COMMON I have talked to folks who have run into IFS infections. If you think about it, it’s probably very common for somebody to connect to a Net server or ODBC and accidentally plant something on the IFS. And, again, using StandGuard Anti-Virus is something that the auditors love. It’s a proactive approach to making sure your system is clean.”

Ensure Reliable Availability

Golden State Water runs its business on an IBM System i model 570 server located in San Dimas. To facilitate high availability, the company uses MIMIX from Vision Solutions to maintain a real-time replica of its production server on a System i Model 520 server located in Fountain Hills. The model 520 server contains two partitions. One partition serves as a test and development environment, while the other serves as a backup for the production 570 server. Should the server in San Dimas go down or need to be taken offline for maintenance, the replica in Fountain Hills stands ready to take over at a moment’s notice.

In theory, this geographically distant replication strategy provides a way to ensure that the company will be able to continue

MessengerPlus has proven itself in the real-world. As just one example, Golden State Water has had situations where queries ran out of control and continued to build temporary files that crashed the system. MessengerPlus sent out notifications of the problems, allowing the IT staff to address them immediately. And, “it has really put the auditors’ minds at ease knowing that, whether we are present or not, we are monitoring our environment 24x7x365,” added Carroll.

Keep a Watchful and Helpful Eye

Bytware’s PeekPlus has also given the IT department an eye on its users’ world. When authorized IT personnel call up PeekPlus it shows them a list of all users who are logged on at that moment. The IT staff can then use PeekPlus to view a user’s screen, chat with the user, enter data into fields on the user’s screen and, if the user is having a problem, send a command to or take control of his or her screen.

This functionality provides a valuable way to support users, but it also offers a means for authorized IT personnel to scrutinize activity and make sure that security policies are not being breached. “It lets you go in and look over the shoulder of the user and make sure they aren’t doing anything they shouldn’t be do-

“I have talked to folks who have run into IFS infections... Using StandGuard Anti-Virus is something that the auditors love.”

to operate should a disaster strike the main data center. However, as Carroll learned while working at another company, theory and practice sometimes diverge. His former employer also used high availability software to maintain replica servers, but one weekend the communications link between the two servers went down and, unbeknownst to the IT staff until Monday, remained down most of the weekend. During that time, system recoverability was jeopardized. Carroll was determined to ensure that Golden State Water would never be caught off-guard like that.

The solution was MessengerPlus. Beyond merely ensuring that the link between the replica servers is available, it eliminates a variety of critical production system exposures by constantly monitoring the status and stability of each of the servers. What’s more, a ping monitor also checks to make sure that the company’s Exchange Server is running. If a problem arises, MessengerPlus automatically sends a message to the appropriate IT staff member’s BlackBerry. That person can then log onto the system remotely to resolve the issue.

ing,” said Carroll. “We primarily use it for professional contractors who are either in-house or dialed into our system. We just like to keep an eye on them and make sure they are behaving.”

The Choice

The results that Golden State Water has received from Bytware’s solutions been very positive, but why did the company choose Bytware in the first place? Actually, the decision was easy. “We didn’t look at any other solutions,” declared Carroll. “It’s a small, small world in the AS/400 arena and Bytware has a very good reputation out there, so why spin your wheels when you know they’ve got a solution that’s going to work? Their reputation for support is excellent and the product is really rock solid. Right there are two really good reasons to go with them.” ●

For a free, fully-functional trial of StandGuard Network Security, StandGuard Anti-Virus, MessengerPlus, and PeekPlus, contact Bytware at 1.800.932.5557 or visit www.bytware.com today!

