

Aqua Finance, Inc

CUSTOMER:

Aqua Finance, Inc

LOCATION:

Wausau, WI

INDUSTRY:

Financial services

PRODUCT:

iPrism



“Before iPrism, we frequently had to tend to computers clogged with adware and spyware, which not only slowed down our staff but also put a strain on the IT team’s time and resources. Since iPrism’s installation, we almost never have to respond to an infected PC, allowing us to put our time to better use for long-term projects. Now, we are confident our work environment supports productivity while reducing the risk of corrupted computers.”

Brett YirkovskyNetwork technical analyst and
telecom administrator at Aqua Finance

Objective

Located in Wausau, Wis., Aqua Finance has a staff of 275 that provide financing and account servicing for the water treatment industry. As the company operates in a deadline-oriented environment, it wanted to ensure its employees were using the Internet for work-related purposes only, and also wanted to prevent liability issues associated with inappropriate Web surfing during work hours.

Furthermore, management had noticed an increasing uptick in corporate computers infected with viruses. Staffed with limited IT resources, Aqua Finance needed a solution to reduce time spent on burdensome tasks, such as removing spyware and malware from computers, and ensuring workers adhere to the company’s Acceptable Usage Policy.

Challenge

With only three IT personnel available to respond to the immediate needs of nearly 300 workers, Aqua Finance’s Network Technical Analyst and Telecom Administrator, Brett Yirkovsky, estimated his team spent a minimum of four hours a week removing malware, spyware and adware from corporate computers. In addition, nearly 20 percent of PCs on the network were plagued with hazardous pop-ups and viruses.

Because of these ongoing issues, Aqua Finance also suspected its employees were visiting Web sites unrelated to work, but had no way of preventing this activity. In order to free up time for more critical projects, and maintain a high level of productivity, the company needed a powerful Web filtering solution that was easy to implement and maintain.

About St. Bernard Software

St. Bernard Software, Inc. (OTCBB: SBSW) is a global provider of security appliances and hosted solutions, including secure content management and archiving. The company's award-winning products deliver innovative security solutions that offer the best combination of ease-of-use, performance and value. Established in 1995 with headquarters in San Diego, CA, St. Bernard sells and supports its products directly and through solution partners worldwide. For more information, please visit www.stbernard.com.



Solution

After researching several hardware and software solutions, Aqua Finance chose St. Bernard's iPrism for its Web filtering needs.

As a dedicated appliance, iPrism does not require any additional hardware or software and is easy to configure and administer. Brett found these self-contained properties appealing as it did not require him to purchase another server or install and maintain any software. iPrism's proprietary, kernel-level filtering technology also protects against threats in HTTP, IM and P2P traffic, such as spyware, malware and phishing. Since its deployment, Brett has noticed a much faster computer processing efficiency as computers are no longer slowed down with malware.

Aqua Finance is also assured its employees are more focused and productive thanks to iGuard™, the 100% human-reviewed URL database that powers iPrism. It receives automatic updates, ensuring all inappropriate Web sites are filtered accordingly. The detailed reporting and real-time monitoring features offered by iPrism further assist Brett with overseeing employee Internet use and the network, quickly illustrating what sites have been visited, as well as which ones have been blocked.

Result

Since deploying iPrism, Aqua Finance has removed all of the hazardous pop-ups and viruses that previously plagued the network. In addition, the company now experiences faster computer processing, and the IT team is able to focus on business continuity while operating more proactively.

