

# Protect Your Network with StandGuard Network Security

Clover Stornetta Farm (*cloverstornetta.com*) is a locally owned and operated dairy processor specializing in organic and conventional dairy products from the bucolic fields of the North Coast of California. To keep up with increasing demand for its high-quality, sustainable, free-farmed dairy products, Clover recently expanded its milk processing facility at the Lakeville Petaluma location. The processing center extension forced Clover to move its business offices offsite to a second location, and Clover's network was also expanded to link the two sites with Voice over IP (VOIP) and a wide area network (WAN) on the company's System i. As the company grew, Ken Kuhn, Clover's IT director, began to think about how he could best secure his company's systems and data from unauthorized access.

After testing lots of different software and techniques, Kuhn chose Bytware, Inc.'s (*bytware.com*) StandGuard Network Security solution to protect Clover's network. StandGuard Network Security is a real-time System i security solution that lets system administrators easily and quickly set enforceable security policies across a network of multiple systems. By controlling access to, and functionality within, key services running on a company's server, StandGuard Network Security protects system data from accidental or intentional data loss. StandGuard Network Security secures, monitors, and audits access to objects, network services, and resources on your System i using an object-based design that is consistent with i5/OS object-level security.

By spending about 15 minutes a day over the course of a month, Kuhn was able to look at all the activities that were taking place on Clover's network and approve or disprove the various actions Clover's users were taking. This phased approach to implementation let Kuhn build a highly effective network security policy that was perfectly adapted to Clover's business environment. By building a security policy in this manner and defining security rules based on what users needed, there were no user interruptions when the network security policy was finally locked into place, Kuhn says. The implementation of the new policy was absolutely painless, and once the rules were set up, Clover's team could sit back and let StandGuard do the heavy lifting. "StandGuard sits and watches our environment 24 hours a day, seven days a week. The tool runs itself," Kuhn says.



Clover also uses Bytware's MessengerPlus, a fully integrated System i messaging solution, to monitor its network. MessengerPlus provides essential monitoring, message management, notification, and statistical reporting features essential for reducing the high cost of operational management and downtime and for improving systems productivity and reliability. In case of a problem, MessengerPlus is configured to send Clover's team e-mails or text messages notifying them of the problem so action can be taken quickly to reduce downtime, Kuhn says.

Clover also uses StandGuard Anti-Virus to keep its System i and network free of malicious code. The solution's nightly updates and weekly IFS scans let Kuhn rest assured that Clover's network is protected.

**The implementation of the new policy was absolutely painless, and once the rules were set up, Clover's team could sit back and let StandGuard do the heavy lifting.**

Bytware's portfolio of network security, anti-virus, and messaging products has been a "slam dunk," Kuhn says. StandGuard Network Security has helped Clover painlessly develop a network security policy personalized to meet the company's needs, and Bytware's MessengerPlus and StandGuard Anti-Virus continue to help Kuhn and his team protect Clover against malicious code and unexpected downtime. ■

**BYTWARE, INC.**

**Monitoring & Securing a Connected World.™**

**Bytware, Inc.**  
775-851-2900  
[bytware.com](http://bytware.com)