

Case Study

Manufacturing

CUSTOMER SUCCESS

Resolve bandwidth issues by prioritizing and blocking content

CUSTOMER:

Time-Cap Labs New York,
USA
(200 users, 1 location)

CYMPHONIX PRODUCT:

Network Composer DC30



Situation

Time-Cap Labs has established itself as one of the premier and most innovative generic pharmaceutical manufacturing companies in the state of New York. Primarily an over-the-counter drug manufacturing company specializing in delayed and sustained release dosages, the lab's tablet coating processes have helped set new industry standards.

Time-Cap Labs maintains 80 PCs on a standard T1 circuit and operates within its network using Active Directory and group policies. Due to the mandatory regulations imposed by the FDA and other government agencies, as well as the quality demands of customers, the company must ensure that all proprietary and customer confidential information is protected in order to maintain regulatory and contractual compliance. The majority of the organization's computers are located in individual offices with a select number of PCs in public function areas that provide access to a number of lab employees.

Challenge

Time-Cap Labs had been relying on its SonicWall Firewall and software-based Browse Control to filter content and protect the company's information as well as its computer network. However, Ken Broggelwirth, Director of Information Systems and Technology for Time-Cap Labs, Inc. recognized that his current solution did not provide complete visibility into his network and user activity.

"We were experiencing lagging network speeds even after bandwidth improvements and just assumed it was due in part to users streaming media while at work or running unapproved applications, but unfortunately, since we didn't have the ability to see who was generating the traffic and with which sites, so we were essentially limited to building our content filtering policies after we happened by a user who was visiting inappropriate content. It really was not a time-efficient procedure and could have left us open to any number of threats," says Broggelwirth.

Even if an employee was caught visiting bandwidth intensive sites like MySpace or YouTube, the company's filtering solution wasn't robust enough to protect against anonymous proxies or prevent other forms of user bypass.

"There is a never ending selection of websites and ways to bypass filters so even if we blacklisted certain sites, we could not be certain that our users were not getting around our security measures," Broggelwirth continued. "I felt like our previous solution was simply not up to the job and was better suited for a smaller organization with

Reveal.
Optimize.
Protect.



fewer users.”

Additionally, the exposure of employees accidentally or deliberately downloading any of the various executables, scripts, objects, etc. that can be the source for a malware or viral outbreak was very high and in fact repairing the damage from the existing exposure was both time consuming and costly. The risk to our productivity as well as our intellectual property was very high.”

Solution

Ken Broggelwirth had seen a demonstration of the Cymphonix Network Composer and was confident that the product would address his organization’s bandwidth issues and could ultimately provide the required visibility into his user’s online activity. The installation of the Network Composer took Broggelwirth a half hour to complete and once the device was in place, Time-Cap Labs began to see, in real-time, what events were taking place on the network.

“It was nice to have something work right out of the box and have it integrate quickly and easily into my existing network structure,” commented Broggelwirth. “The Network Composer DC30C gives me unmatched visibility into my network and as a result, I have been able to weed out a lot of unnecessary and problematic traffic - even block viruses and spyware at the gateway, and prevent unauthorized executable applications from being downloaded from the web”

The Network Composer revealed that there were certain employees who had been spending an excessive amount of time streaming movies at their desk and were responsible for the slowed network speeds and lack of available bandwidth. Broggelwirth added, “We found that there were some people who had been trying to set up a P2P network but Network Composer allowed me to completely block that type of file transfer through P2P clients as well as through Instant Messaging. Its been great to have this kind of information at our finger tips and Cymphonix makes it easy to present data through a high level overview or pull more granular reports specific to an individual user.” The Network Composer also helped

Broggelwirth locate a computer that had been infected with spyware prior to the installation of the Cymphonix box.

“I noticed that we had a computer generating traffic on our network and it turned out that it had been infected with spyware. We were able to trace the computer and clean it before it morphed into a more complex issue. Before, we would have only found the problem when the computer’s owner had complaints that their machine was running slower than normal,” Broggelwirth finished.



“It was nice to have something work right out of the box and have it integrate quickly and easily into my existing network structure. The Network Composer DC30C gives me unmatched visibility into my network and as a result, I have been able to weed out a lot of unnecessary and problematic traffic - even block viruses and spyware at the gateway, and prevent unauthorized executable applications from being downloaded from the web”

Ken Broggelwirth,
Director of IS and Technology
Time-Cap Labs



Success

The Cymphonix Network Composer provided Time-Cap Labs with the granular visibility needed to allow IT administrators to set policy and ultimately maximize bandwidth availability for critical applications. With the real-time information, Time-Cap Labs was able to put a stop to lagging employee productivity by eliminating the staff’s ability to stream media and share files through P2P networking or through Instant Messaging. Cymphonix has also helped Time-Cap Labs locate and clean computers that had been infected with spyware and ultimately circumvent future issues or information loss. prioritize bandwidth consumption, Cymphonix has allowed Corpus

Christi Public Libraries to optimize its Internet connection so that public browsing does not negatively impact the business-necessary ILS. Finally, by automating the libraries’ Internet policies, Cymphonix ensured that the productivity of administrators, employees and visitors is never affected by lagging network speeds.

See for Yourself

See how Network Composer delivers visibility, security, and performance in one reliable package. Contact your Authorized Cymphonix Reseller for an online demonstration or call or email Cymphonix at 866-511-1155 or sales@cymphonix.com



About Cymphonix

Cymphonix Corporation, headquartered in Sandy, Utah, uses patentpending Cross-Layer Intelligence™ (XLI™) technology to provide unmatched network threat protection and resource optimization. With the powerful XLI engine, Cymphonix products seamlessly integrate network protection, application performance, and traffic visibility into a single, easily managed solution. Leading the Cymphonix product line is Network Composer, a smart gateway appliance that helps organizations understand at a glance who is abusing network resources and with what applications - enabling problems to be corrected instantly through a clear, easy-to-manage interface.



Cymphonix Corporation
8871 S. Sandy Parkway, Suite 150
Sandy, Utah 84070-6408

801-938-1500 Tel
801-938-1501 Fax
866-511-1155 Sales

www.cymphonix.com