



Denmark's Novo Nordisk IT (NNIT) has high aspirations to be the leading IT firm in Europe. Since 1999, the 700-person company has provided IT consulting, development, and operations across a number of business areas—from IT management consulting and SAP solutions deployment to web-enabled solutions and outsourcing. NNIT also boasts an exceptional track record in information management for the pharmaceutical industry. This comes as no surprise, given that the company is a subsidiary of Novo Nordisk, a leading pharmaceutical product manufacturing and marketing company. Novo Nordisk's innovations in diabetes care, hormone therapy, and homeostasis management are world renown.

According to Arne Liebe Kristensen, NNIT network consultant and 30-year networking veteran, NNIT's greatest networking challenge is ensuring continual network availability from every workstation to every application. The company has tried a number of log analysis and reporting products designed to improve network stability and security, but nothing has met its expectations.

Last year, NNIT came across the LogLogic LX 1000 analyzer, a secure appliance for realtime log analysis. The LX 1000 analyzer not only offers visibility into what is happening across network devices, but offers insightful details about what is happening. "We were impressed with LogLogic's purpose-built appliance as it was far more secure than server or software-based solutions and offered a higher level of network protection," said Kristensen.

One year later, NNIT's LX 1000 appliance supports more than 15,000 desktops and 150 firewalls across 120 of its offices worldwide, all reporting into the Copenhagen headquarters. Another redundant appliance runs in parallel in the event of fail over.

RESULTS

Provided instant responsiveness to virus attacks

Delivered greater value and insight from network device logs

Allowed proactive network management

Significantly increased network stability

Enabled compliance with government reporting requirements

LX 1000 Appliance Enables Compliance with National Security Requirements

Complying with national security measures is one of NNIT's most pressing networking objectives. Danish government bodies and police agencies have the right to audit a company's log files at any time in the interest of national security. In fact, at any moment, the authorities can demand up to one year's worth of log records of who traversed the company's firewall both from inside and outside of the organization. This represents a tremendous amount of traffic—roughly 600 firewall log messages per second and 3 gigabytes of data per day.

Reports can be set up to run automatically at specific time intervals, or sent automatically to key individuals throughout the organization. The LX appliance can also consolidate log reports from multiple devices, simplifying the task of reviewing and comparing log data from different sources. Administrators can run device-specific reports to zero in on the activity of a particular box, as well. Using the LX appliance's auto-alerting feature, administrators can pre-configure a network device to send an email to key individuals if certain threshold filters are exceeded, so that they know immediately if the network is experiencing abnormal activity. Auto alerting provides even greater, more instantaneous visibility into firewall traffic. Prior to installing the LogLogic analyzer, NNIT could only maintain logs for three to four days, because the company was forced to use regular expression in a UNIX environment—an inefficient approach at best. "When the authorities wanted information, we couldn't deliver it and there wasn't anything we could do about it," said Kristensen. "Since, all firewall log traffic is monitored by the LX appliance now, we can quickly and easily produce the information officials require, allowing us to be confident that we can comply with national security laws without disruption to operations."

“Whenever a virus hits, the LX appliance gives us the critical information we need to isolate and fix the problem,” said Kristensen. “Instead of dealing with the aftermath of a full-blown virus attack, the IT staff can work proactively to repair infected PCs and thwart the virus before it spreads.”

— **Arne Liebe Kristensen,**
Novo Nordisk IT Network Consultant

Auto Alerting Thwarts Virus Attacks

NNIT discovered an unexpected benefit of the LogLogic appliance when the Code Red computer virus struck worldwide. The virus initially made it through the firewall to infect a handful of PCs, but the LX appliance’s alert feature quickly notified NNIT of the problem. With the help of the appliance, the NNIT team was able to immediately identify which PCs had been attacked so the company could quickly resolve the problem and stop the Code Red worm from spreading any further. In situations where every minute counts, the appliance gave Kristensen exactly what he needed to avert disaster. “We were probably the only company in Denmark not affected by the virus,” said Kristensen. “Many businesses were brought to their knees, but most of our users didn’t even know the attack was taking place.” He added that the company avoided significant losses by containing the virus so effectively.

According to Kristensen, none of the threatening viruses have affected the company since installing the LX 1000 appliance. “Whenever a virus hits, the LX appliance gives us the critical information we need to isolate and fix the problem,” said Kristensen. “Instead of dealing with the aftermath of a full-blown virus attack, the IT staff can work proactively to repair infected PCs and thwart the virus before it spreads.” Kristensen added that the ability to act quickly makes containing the virus easier. “If you can’t act fast, however, a virus can crush the organization,” he said.

Better Visibility Into Network Security

With the LX appliance, NNIT has realized greater value from its network device logs by making them more actionable and more insightful. “We are especially pleased with the appliance’s dynamic and intuitive reports,” said Kristensen. “These reports capture all system log information without filtering for more accurate reporting, and they are modeled on how security and network managers actually work. The tool’s distributed data-gathering allows network administrators to get at the information they need quickly and also keep the network from being overloaded.”

Kristensen said the LogLogic analyzer helps NNIT’s firewalls work smarter IT staff has been able to move out of its reactive posture and stay in a more strategic and proactive mode. “With the LX 1000 appliance, we can keep track of our network trends at any given time interval,” he said. “Such insight keeps us abreast of what’s happening in our network at all times, so that we’re never caught off guard.”

LogLogic, Inc.
3061-B Zanker Road
San Jose, CA 95134
United States
US Toll Free: 888 347 3883
Tel: +1 408 215 5900
Fax: +1 408 321 8717

LogLogic EMEA
Albany House
Market Street
Maidenhead, Berkshire SL6 8BE
United Kingdom
Tel: +44 870 351 7594
Fax: +44 870 351 7595

LogLogic APAC
Suite 303, Tower B, Beijing Kelun Building
12A, Guang Hwa Lu
Chaoyang District
Beijing 100020, China
Office: +8610 6581 3298
Fax: +8610 6581 3299

loglogic.com
blog.loglogic.com
info@loglogic.com

