Case Study: Northwestern Memorial Hospital

LogLogic Improves Prognosis for Risk Management at Northwestern Memorial Hospital

About the Hospital

A premier academic medical center in the heart of downtown Chicago, Northwestern Memorial Hospital is recognized for its outstanding clinical and surgical advancements in such areas as cardiothoracic and vascular care, gastroenterology, neurology and neurosurgery, oncology, organ and bone marrow transplantation, and women's health As a major referral center, patients have access to advanced diagnostic and therapeutic modalities, such as medical imaging and laser technology. Northwestern Memorial is the primary teaching hospital for Northwestern University's Feinberg School of Medicine; many physicians serve on the faculty and participate in both medical education and research programs.

Northwestern Memorial received the prestigious 2005 National Quality Health Care Award and is listed in eight specialties in this year's US News & World Report's issue of "America's Best Hospitals." The hospital is also cited as one of the "100 Best Companies for Working Mothers" by Working Mother magazine for the past six years and has been chosen by Chicagoans for a decade as their "most preferred hospital" in National Research Corporation's annual survey.

The Problem

Federal legislation through the Healthcare Insurance Portability Accountability Act (HIPPA) of 1996 provided incentives for healthcare organizations like Northwestern Memorial to standardize processes for log collection, analysis and retention to better protect patient data confidentiality. To comply with HIPAA regulations and gain greater insight into the IT infrastructure, Northwestern Memorial searched for a log management solution that provided 100 percent log data collection and aggregation, as well as reporting and management features that would save time and reduce costs, while providing a high degree of security, scalability, and data accessibility.

The Northwestern Memorial IT department maintains more than 12,000 IP devices to run its numerous programs and to support its staff. All of these devices are monitored by firewalls IDS systems and other Security Controls that produce massive amounts of raw log data. Security of this network is crucial because it contains confidential patient data. It is of primary importance to the hospital to maintain that data's confidentiality and integrity on the network while securing this campus network with hospitals, affiliates and partners IP devices.

The Evaluation of Log Management Software:

Northwestern Memorial needed a complete Log Management solution with intelligence built-in so it could take advantage of this solution to put intelligence into the collected raw data from hundreds of IP devices. It was looking for a log management solution that addressed the following challenges:

- Collect security data from multiple VPNs, firewalls, and other network gear and keep it in a centralized repository.
- Access the data through fast searches and create meaningful [security] reports
- Generate alerts on data to improve insight into user activity and possible threats to the IT infrastructure.
- Store the data and access it later, with drill down capabilities to pinpoint network issues and threats.
- Seamlessly interoperate a heterogeneous network environment with different vendor devices and applications.

After evaluating a number of options, Northwestern Memorial selected the LogLogic solution. Using LogLogic's Log Management solution Northwestern Memorial was successfully able to conclude the activities of 12,000+ IP devices on their network that were generating large volumes of raw log data.

CHALLENGE

- Premier medical center in Chicago seeks log management solution for 12,000 IP devices for security and compliance.

SOLUTION

- LogLogic LX appliance for decision support and problem remediation.
- Early warnings of device misuse and unusual behavior.

RESULTS

- Real time analysis and targeted queries.
- Early warnings of device misuse and unusual behavior.
- Reduced log analysis time 95%.

"In the past, to analyze logs manually after getting the data from our former database would take 180 to 240 minutes. The same job can now be done in less than 10 minutes."

Asad Syed
Senior Security Analyst,
Northwestern Memorial Hospital

About LogLogic

LogLogic is an intelligent appliance based Log Management solution that processes all syslog messages from connected devices, servers and applications in real time, including the highest volume informational-level messages. LogLogic's LX appliance stores a parsed and summarized copy of the data for up to 90 days for instant analysis or for decision support and problem remediation purpose. Users can pinpoint the locations of threats or other network problems and miss-configurations.

It can create graphical or text-based reports in minutes. The solution reliably aggregates high volumes of data and provides fast search and drill-down capabilities essential for risk mitigation. Proof of compliance and policy management is enabled with easy-to-use templates that generate up to 13,000 custom reports. Northwestern Memorial's IT department can now create management reports as evidence of access and Change-Control for security policy and compliance, audits or more general-use analysis.

LogLogic's powerful alerting capabilities are based on Log Learning technology that can be set by device, group of devices. Network and Security Managers can monitor log data and/or receive early warning of insider misuse or unusual behavior. Adaptive baseline alerts, network policy alerts and ratio-based alerts are all powered by the machine learning technology built into the solution. "If I see an alert, I can immediately connect the dots and investigate further to stop the damage in its initial stages," said Asad Syed, Senior Security Analyst at Northwestern Memorial Hospital.

Northwestern Memorial can perform real-time analysis with targeted queries that make log data instantly searchable and insightful. "With so many devices and applications to manage, time is of the essence," said Syed. "LogLogic puts our eyes and ears on the network and gives us the transparency to see what is happening in the electronic frontiers. For example we can now see

- Virus infected devices that are trying to go out of our perimeter.
- Traffic denied by the firewall, in different formats.
- Active connection in our VPN concentrator.

Previously, the logs were there, but were obscure or hidden somewhere below the bilog data. Now we can access the data quickly and take action when necessary," he said.

Analysis has become faster, continues Syed. "In the past, to analyze logs manually after getting the data from our former database would take us anywhere from 180 to 240 minutes. The same job could now be done in less than 10 minutes," he said.

"The ability to process log data from different Network Security Controls [Firewalls, IDS, Routers, Switches, VPN Concentrators, etc] and to produce security reports allows us to keep our eyes and ears on the network."

Asad Syed
Northwestern Memorial Hospital

Conclusion

Since implementing LogLogic, Northwestern Memorial Hospital's IT department has gained insight into critical network log data that was previously extremely challenging. "Our end objective was to be able to identify threats in real time, as they are happening," said Syed. "The ability to process log data from different Network Security Controls [Firewalls, IDS, Routers, Switches, VPN Concentrators, etc] and to produce security reports allows us to keep our eyes and ears on the network. Ultimately, these capabilities along with carefully crafted processes help us mitigate risk and meet HIPAA requirements in its true sense, while providing a secure, reliable IT infrastructure to serve our hospital goals," he said.

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 China
Suite 303, Tower B, Beijing Kelun Building
12A, Guang Hwa Lu
Chaoyang District
Beijing 100020, China
Tel : (8610) 6581-3298
Fax : (8610) 6581-3299

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