Log Management:

Simplifying Compliance, Auditing and Security.

netiQ

Knowing.

‘Because of both the rising cost of security incidents and a host of recent regulatory changes, enterprises can no longer afford to overlook the value of their log files.’

IDC: The Growing Importance of Log Files, www.cio.com, July 2004

Keeping track of a dangerous world

Today's business environment is filled with security risks. Data, systems and networks have become the lifeblood of the organisation, yet with increasing network speeds, higher degrees of connectivity, more advanced mobile devices, and more prevalent wireless connectivity, organisations are more at risk than ever before.

In the fight against infiltration, system logs are the most under-utilised sources of security, event and performance information in organisations today. Yet their value is immense.

Clean system logs are the best proof that there's been no system or data compromise, and are a vital source of information for effective network management. What's more, an audit trail of logs can be critical in proving compliance with the growing volume of standards and regulations that affect every business operating today. Indeed, many regulations refer specifically to logs.

The importance of log management

With effective analysis of system logs, you have access to a wealth of information that empowers you to:

Comply with regulations. PCI DSS, ISO 17799, Basel II, Sarbanes-Oxley… all require logs to be retained and regularly reviewed.

Respond to security events. If something goes wrong, logs are an obvious tool for identifying the problem so you can fix it.

Carry out forensic investigations of events. Logs also help you conduct a post-event analysis of why and how things went wrong.

Manage IT risk. Prevention is better than cure, and logs record activity (such as increased firewall activity or degraded system performance) that can be used to reveal potential problems.

Maximise network uptime and per formance. Early warnings of per formance problems, such as drives running low on space, let you be proactive in maintaining optimum levels of uptime and performance.

Ensure accountability. Managers need the means to monitor systems and data integrity for compliance and good business. They also need to be able to prove that log files have not been tampered with.

Knowing.

The log management challenge

Quite simply, you can't afford not to collect, review and analyse logs regularly. You also need to retain them for a specified period, and prove that they have not been tampered with.

The problem is that, no matter what size or complexity your infrastructure, it's difficult, if not impossible, to maintain and manage your logs manually. This is attributable to:

Sheer volume of logs. Nearly every technology today is capable of creating a log file, including operating systems, web servers, database management systems, switches, firewalls, routers and intrusion-detection systems. Simply capturing this data can require huge storage resources, and can even affect network performance. Analysing logs and maintaining logging systems often requires significant amounts of manpower.

No consistent format. Every device has its own way of recording events, making it difficult and time-consuming to compare or extract trends across your entire infrastructure.

Difficulty extracting meaningful, actionable information. With so much raw data to choose from, and so little visibility and control over how it changes, it can seem impossible to select and process data to reveal valuable insights in a useful timescale.

Take control of your infrastructure with NetIQ Log Manager

NetIQ Log Manager is designed to be easy to use and offers comprehensive functionality, without impacting system performance. It automates the process of collecting and centralising log files, collecting events from the host operating system, or from common stream-based protocols such as SNMP or syslog.

What's more, as an integral part of NetIQ Security Manager, it gives you the power to use your logs for managing intrusions, monitoring security devices and more.

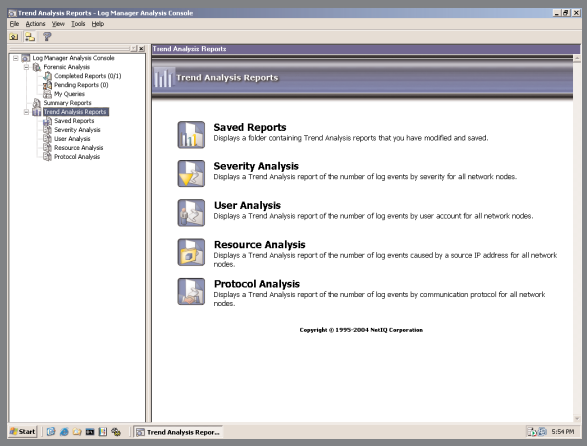

Fig1:
Log Manager Analysis Console - Trend Analysis Report

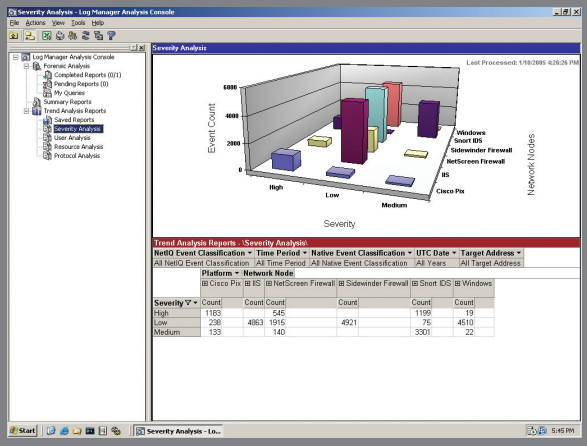

Fig2:
Log Manager Analysis Console - Severity Analysis

Knowing.

NetIQ Log Manager key features and benefits

Collect only the information you need and want.

Consolidate logs from all devices into one secure repository, where they can quickly and easily be accessed.

Control your logs by normalising their data into a common format, for automatic analysis of information drawn from different platforms and devices.

Analyse trends to identify ongoing security issues and integrate different kinds of information in an interactive, graphical view. Drill down to get more detail.

Summarise as often as you need to report on security status and to demonstrate compliance.

Investigate with powerful forensic analysis that lets you understand the meaning of log information collected during security incidents.

Respond to events fast with a sophisticated, built-in incident work flow engine.

Comply by retaining and protecting raw log data offline, optimising the use of storage for log files and preserving complete, secure audit trails.

Monitor access to log files and secure collection, processing and storage for authenticity and non-repudiation.

So easy to use

The full suite of Log Manager functionality is easily managed from a single console. What's more, the system features a fault-tolerant design that's not only scalable, but compatible with Windows, Linux, UNIX and iSeries platforms, as well as hundreds of network appliances and security devices. This minimises risk and disruption as you integrate log management into your infrastructure.

Quite simply, Log Manager helps you get the most from your log data, not just for compliance, but to reduce business risk and enhance IT security, as these issues become ever more important in business today.

Find out how you can achieve fast, effective visibility of your systems with NetIQ Log Manager.

Visit netiq.com today or call us on 01784 454500.

NetIQ Limited
Mallard Court
Market Square
Staines, Middlesex
TW18 4RH United Kingdom

Tel: +44 (0) 1784 454 500
Fax: +44 (0) 1784 416 900

Email: info-emea@netiq.com

netiq.com/go/logmanagement