netPrefect & HIPAA

Creating an Enterprise-wide Audit Trail Log

Executive Summary

Since 1997, Cyclone's infrastructure management software has been used in some of the world's largest datacenters, improving system availability and performance, and reducing the cost of maintaining non-stop computing environments.

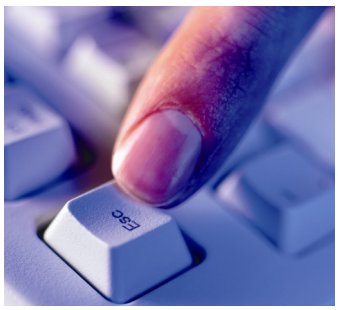
The challenge has always been how to centralize the management of all critical IT systems and devices across a distributed environment.

In recent years, government regulations such as Sarbanes-Oxley and HIPAA have been introduced, and with them entirely new headaches for IT professionals. Security requirements are now defined by law. Comprehensive and complete logs of all user activity and security events are now needed, not only to enforce security policy, but to provide accountability and audit trail for adherence to agencies such as the Department of Health and Human Services.

The new challenge is collecting user activity logs and security event notifications from all critical IT systems and devices across a distributed environment. This is nothing new to Cyclone. We've been doing it for years. That is why so many healthcare providers have chosen Cyclone's technology to both manage their mission critical systems, and to create a proactive and comprehensive security audit trail and event notification system.

What is HIPAA?

HIPAA was introduced originally in 1996 as a means to improve the effective delivery of the Medicare program by reducing waste and fraud, assuring continuance of healthcare service to all people, while at the same time protecting the individual's right to privacy.



Security Standards Rule

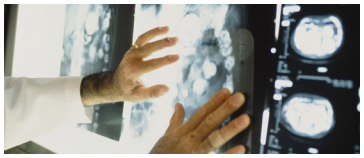
Such an enormous undertaking was bound to be complicated, and it came as no surprise when it was five years before the final Privacy rule was published, and two years following that when the Security Standards were at long last defined. Even though the healthcare industry has had a long time to prepare for these security requirements, organizations are still struggling to comply with the final rule which has been in effect since April 21st, 2003 .

Real Time Event Detection

Most operating systems and network devices include complete functionality for capturing security events, but provide little or nothing in the way of analysis, archiving, and real-time monitoring capabilities. Cryptic event descriptions compound the problem, as does the fact that each computer maintains a separate security log. Yet to comply with the Security Standards rule in today's networked business environment, it is essential to track security activity and to respond immediately to intrusion attempts. **netPrefect** manages both In-Band and Out-Of-Band access to managed devices, by collecting user access and security information in real time. In addition, using **netPrefect's** token replacement feature, unintelligible ASCII text messages can be transformed into meaningful events. **netPrefect** uses advanced algorithms to filter out the background noise, and create events based on simple-to-create rules and pattern matching, which eliminates false positives in the alert process.

Event Logging

netPrefect maintains a comprehensive log of events by severity, system, and frequency. This event log can be viewed in real-time, using the **netPrefect** GUI, and a simple to understand dashboard is available to show an up to the minute accounting of all events. The **netPrefect** rules wizard makes it simple to create reusable rules, which filter captured data and trigger events when specific criteria is met or patterns matched. These rules can be applied to multiple systems, or system groups, reducing the amount of time required to configure the system, and also ensuring that the same security standards are applied to all systems across the entire enterprise.



Use file-access auditing for internal security

With **netPrefect**, administrators can enable auditing on selected files, for specific types of access. This is most useful for monitoring how users are accessing documents, such as Microsoft Excel and Microsoft Word files. However, this type of auditing can also be used to monitor for such things as changes to folders that contain executables, or unauthorized attempts to access database files. Administrators can audit failed or successful attempts to open a given file or folder for read, write, delete, and other types of access (to monitor changes to an object, enable auditing for successful writes. To monitor users who try to read files they aren't authorized to read, enable auditing for failed reads).

Administrator Accountability

One of the problems inherent in most security logging is a lack of administrator accountability. Although most systems record administrator activity (e.g., account maintenance, privilege use), the Security log itself is always vulnerable to an administrator who decides to clear the log, disable auditing, or shut down the system and tamper directly with the log file by booting from a floppy disk. **netPrefect** can address those problems, and enforce accountability by simply creating events that recognize log clearing and audit policy changes as critical events and triggers the appropriate notification and response.

Satisfy Long-Term Audit Trail Requirements

In addition to event logging, **netPrefect** creates a separate log for every system or device under management in a single log-file repository. This log information includes date-stamps, system name and the ASCII text that was collected by the **netPrefect** server. **netPrefect** can be configured to save a specific number of log entries or amount of data collected. All of this log data can also be exported in XML or .csv format so that it can be used for reporting purposes with third party applications. It is recommended that administrators have a comprehensive back-up strategy in place that allows for long-term data availability in the event that it is required for audit trail purposes.

Next Steps

Cyclone have been the choice of many blue chip companies, as the most simple and cost effective way to collect and act on security information across the entire enterprise in real time, while at the same time aggregating logs of all security events by severity and type, and lastly creating a long term audit trail.

To learn more about how Cyclone's infrastructure management software can assist you, or to arrange a no obligation time limited evaluation of the software, email sales@cyclone-technology.com or telephone us on 01584 811467.