SAFEPOINT/KSL

Sophisticated Keystroke Logging and Reporting

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The Payment Card Industry Data Security Standard (PCI DSS) requires that all access to network resources and cardholder data is tracked and monitored. Specifically, it requires that "All actions taken by any individual with root or administrative privileges" are logged. Organizations are required to establish a process for linking all access to system components to each individual user and to implement automated audit trails for all system components. This can be achieved on HPE NonStop systems by implementing keystroke logging which records all keyboard activity of a user on the HPE NonStop. SafePoint/KSL (Keystroke Logging) allows security administrators to automatically log all keyboard activity of all users and to create customized event reports.

Purpose

SafePoint/KSL provides organizations with the right tools to be able to record and to report on all user keyboard activity on HPE NonStop systems. SafePoint/KSL can be configured based on individual users or groups. SafePoint/KSL is tightly integrated into the following comForte or HPE products: SecurSH, SecurTN, and NonStop SSH. By being integrated with a component which fully replaces TELSERV, SafePoint/KSL 'sees' all keystrokes right at the source and does not rely on having to configure a 'substitution TACL object'.

Features

Keystroke Logging:

▶ Easy installation and configuration.

▶ Level of detail for logging (input only, only first few lines of output etc.) and criteria (which users and/or Aliases to log) are highly configurable.

▶ Works with any terminal emulator. Even more log information (e.g., remote Windows user names, DNS names, IP addresses) can be attained when used with comForte emulators (e.g., MR-Win6530).

▶ Keystroke logging cannot be bypassed by starting separate TACL processes with different IN, OUT and TERM.

Reporting:

▶ Reports provide integration between keystrokes and Safeguard audit log.

▶ Define reports to cover distinct time periods, sets of users and objects, types of events, particular terminals and more.

▶ Run reports on all HPE NonStop systems from a centralized node and have data from multiple HPE NonStop systems automatically merged into single reports.

▶ Schedule reports to run automatically, for instance during off-peak load hours.

▶ Automatically download any reports to the PC in order to analyze and work with data in Excel worksheets, Word documents and virtually any other application.

▶ Automatically Email reports or have them sent to a central repository (e.g., SIEM)

System Requirements

- ▶ Easy installation and configuration
- ▶ Flexible configuration of logging details
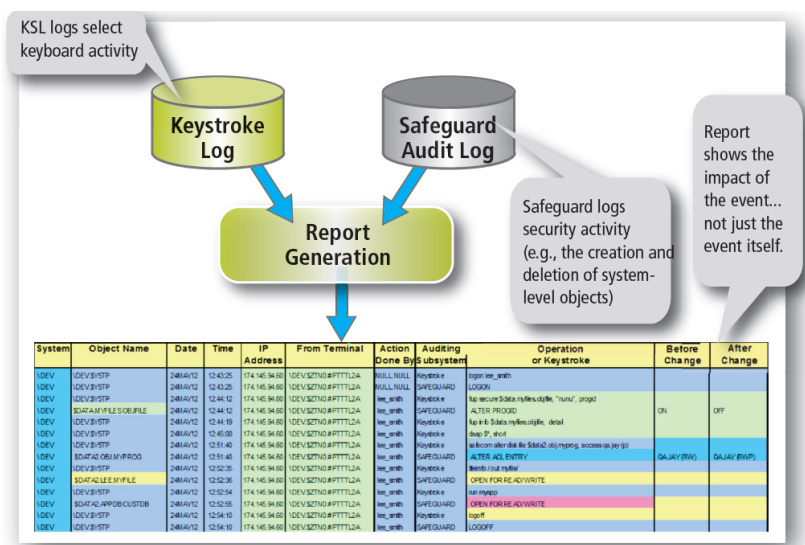- ▶ Comprehensive reporting facility
- ▶ Integrates with SIEM

comforte AG, Germany
phone +49 (0) 611 93199-00
sales@comforte.com

comforte, Inc., USA
phone +1 646 438 5716
ussales@comforte.com

comforte Asia Pte. Ltd., Singapore
phone +65 6808 5507
asiasales@comforte.com

comforte Pty Ltd, Australia
phone +61 2 8197 0272
aussales@comforte.com

www.comforte.com

Benefits

- ▶ **PCI DSS compliance**
  SafePoint/KSL enables organizations to track and monitor all access to network resources and card holder data. Consequently, SafePoint/KSL helps to achieve PCI DSS compliance.
- ▶ **Integration of KSL and Safeguard audit logs**
  SafePoint/KSL combines the KSL log and the Safeguard audit log into one meaningful report.
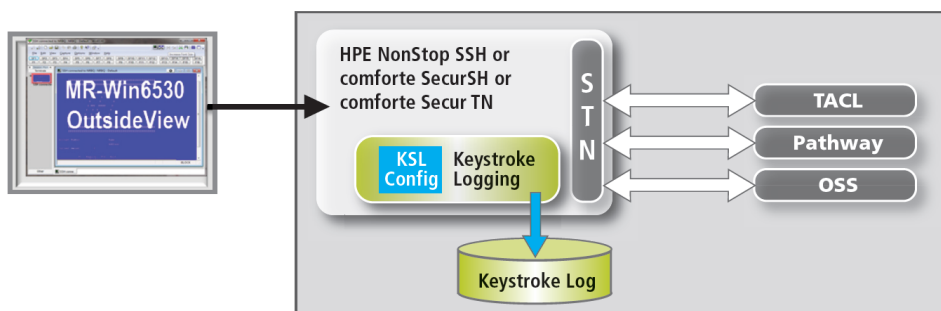
Keystroke logging integrated with SSH
The keystroke log reports can be integrated with the Safeguard Audit Log reports to provide meaningful cause and effect conditions which can either be emailed on a regular basis or can be sent to a central facility (e.g., SIEM).

Reports merged from KSL and Safeguard Audit Log