

ViewTrust
TECHNOLOGY



simplifying
**Log
Management**

**Enterprise Log Management with
Analysis and Compliance Reporting**

LogVision is a comprehensive Log Analysis and a reporting system that collects, analyses and reports on information derived from security logs, system logs and alerts. Both raw and

processed information is stored in a relational database system, for dynamic query and reporting. The reports are dynamically generated and viewed on a web-based customer portal.

LogVision Features

Anytime, Anywhere Customer Portal based Access	Features the browser-based Portal allowing secure anytime, anywhere access to the organization's critical network and security information.
Enterprise-Wide Reporting	Allows the generation of security reports across single or multiple Network, Security, Application and Database devices within an enterprise.
Scheduled Reporting	Permits the scheduling of select security reports, saving substantial time and effort for IT managers that are currently using Check Point's Firewall-1 Management Module and Cisco PIX Platform.
Log Archive Management	Automatically archives all firewall log files.
Custom Query Reporting	Permits the creation of reports using flexible queries, so data of a specified type and timeframe can be isolated for analysis.
Centralized Information Repository	Keeping track of documentation is easy with the web-based access to any documentation
RDBMS database for storage of log data	The collected log data is stored in a relational database system for easy access and custom queries.

Problem Scenario

Today, ensuring that an enterprise's network perimeter remains secure is one of the most critical tasks

undertaken by an organization's IT staff. To guarantee that no breaches of an organization's security policies occur, Firewall and VPN log files must be continuously scrutinized by experienced

security experts. However, budget constraints, increased responsibilities, and high employee turnover make this sensitive IT task nearly impossible to perform.

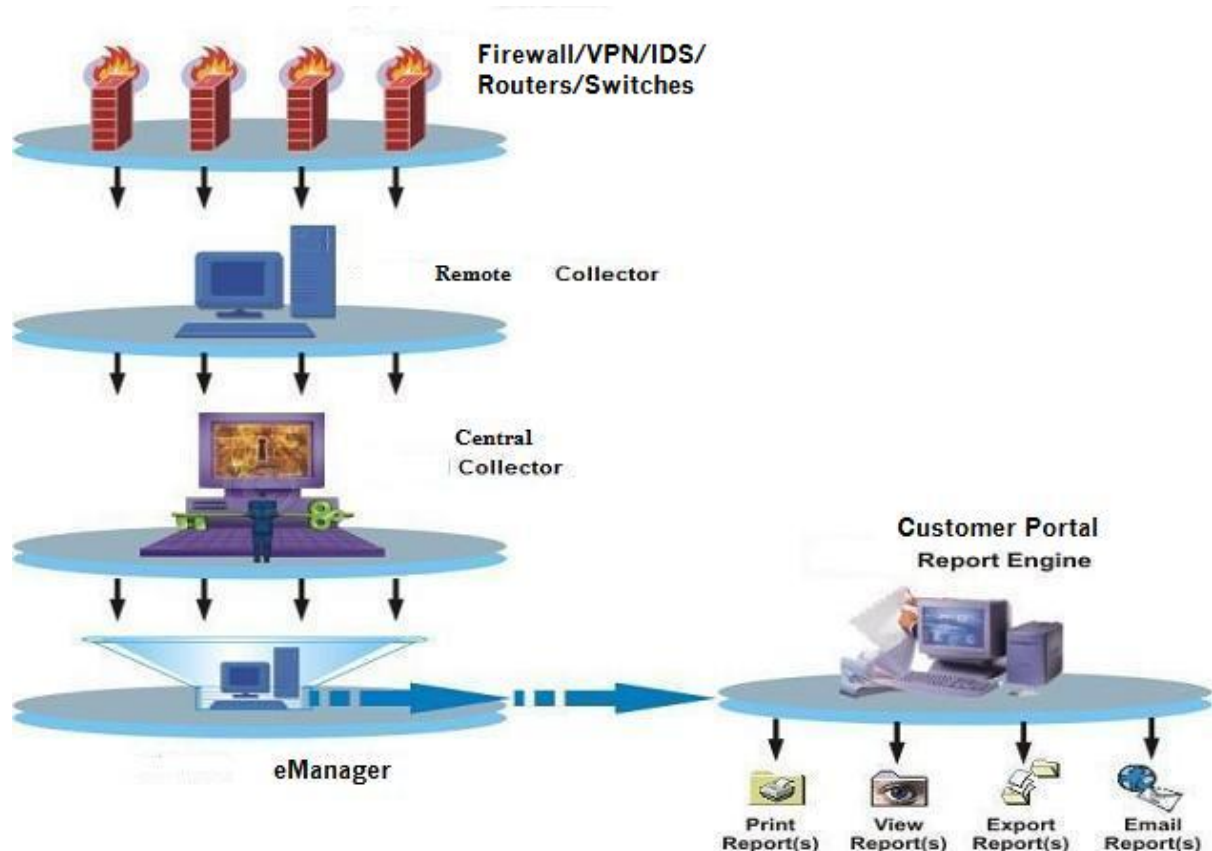
Firewall/VPN appliances protect the network and in the process generate massive quantities of security log files for review and analysis. Managing and monitoring these log files is a huge burden on any organization's information technology staff and information systems, especially in an enterprise environment with multiple distributed Firewalls and VPNs.

LogVision Solution

LogVision solution provides invaluable information about firewall and VPN activities that help IT personnel to optimize their organization's network security and efficiently manage their network operations. By facilitating the detection and analysis of network security breaches, ViewTrust LogVision solution aids in the assurance of sound network security.

LogVision provides a web-based graphical analysis and reporting of the log data. Customers can run custom reports of their own or utilize the pre-defined reports.

LogVision Architecture



LogVision solution offers protection against rapidly changing information security threats by unifying the threat information from multiple devices in a centralized database and providing detailed reporting through a web-portal.

LogVision collectors collect log information from enterprise log sources and forward it to the 'eManager' for data processing. Once the data is processed, the information is stored in a Relational Database Management System (RDBMS). The web-based customer portal site then provides access to the predefined reports or allows 'dynamic' queries to the database for customized reports.

Customer Portal

LogVision Customer Portal provides a dynamic web-based view of the log reports and customer specific information based on the data collected from various log sources.

Custom Query

LogVision 'Custom Query Report' represents one of the most powerful features in the industry.

The custom query feature allows customers the complete freedom to create their own customized reports with twenty-two (22) variables. Customer can choose a specific firewall at a site, with start and end date/time, specify source of destination IP

addresses and select standard or custom services, to create customized reports from the log data stored in the database.

Relational Database Storage

LogVision stores all the collected log data in a relational database system. The Database of choice is Microsoft SQL server. The data received from the collector is normalized and stored in the database. Once in the database, the data can be queried for custom reports or the data can be trended to create Trend Reports.

Customizable Pre-Processors

LogVision provides pre-processors specific to the log source. Each pre-processor can be customized through the web interface. No coding or scripting skills are needed.

For More Information on ComplyVision and ThreatVision solutions, visit www.viewtrust.com/Products or please contact:

ViewTrust Technology, Inc.

6311 Cardinal Hill Place
Springfield, Virginia 22152
Tel: 703.627.7539
Fax: 703.995.4649
info@viewtrust.com