



Computer Security Products Inc.

www.cspsecurity.com

Alert-Plus®

Real-Time NonStop® Security and Merged Audit

Intrusion Detection and Prevention

PCI DSS and other legislation require system managers to take measures to prevent intrusions and unauthorized access into their computer systems.

Alert-Plus® provides real-time intrusion detection on HP NonStop® systems. Using powerful customized rules to evaluate events from many sources, including Safeguard Audit, Alert-Plus® takes immediate action when an event of interest occurs in real-time. Alert-Plus® not only detects intrusion attempts in real-time but can help block them.

Alert-Plus® monitors reside on multiple HP NonStop® systems and use sophisticated rules to monitor and evaluate hundreds of different events.

From a TACL script or using the Windows® based graphical user interface (GUI), you can:

- Create, edit and compile event rules
- Observe events from the monitors in real-time
- Define actions to be carried out in response to events
- Control the NonStop® based monitors
- Configure log files
- List users currently logged on
- Access and print reports from the spooler

Rules creation and maintenance

To facilitate rules creation and maintenance, Security Administrators can use the Alert-Plus® scripting language, by means of an NSK text editor integrated within the Windows® Interface.

Rules Wizard



In order to simplify many of the most common rule-building and event reaction tasks that are possible with the product, CSP has created the Alert-Plus® rules wizard which guides you through the entire rules creation and implementation process. This simplifies these tasks for you, thereby reducing your workload and training costs.

Built-ins

Built-ins are code-routines that allow you to define complex rules without knowing any special syntax.

They allow you to monitor up to 20 different security vectors and invoke up to 20 different actions, including audible alarms, e-mail alerts, EMS messages, freezing a user ID, etc. Security vectors include events such as suspicious logon activity or intrusion access attempts.



Computer Security Products Inc.

www.cspsecurity.com

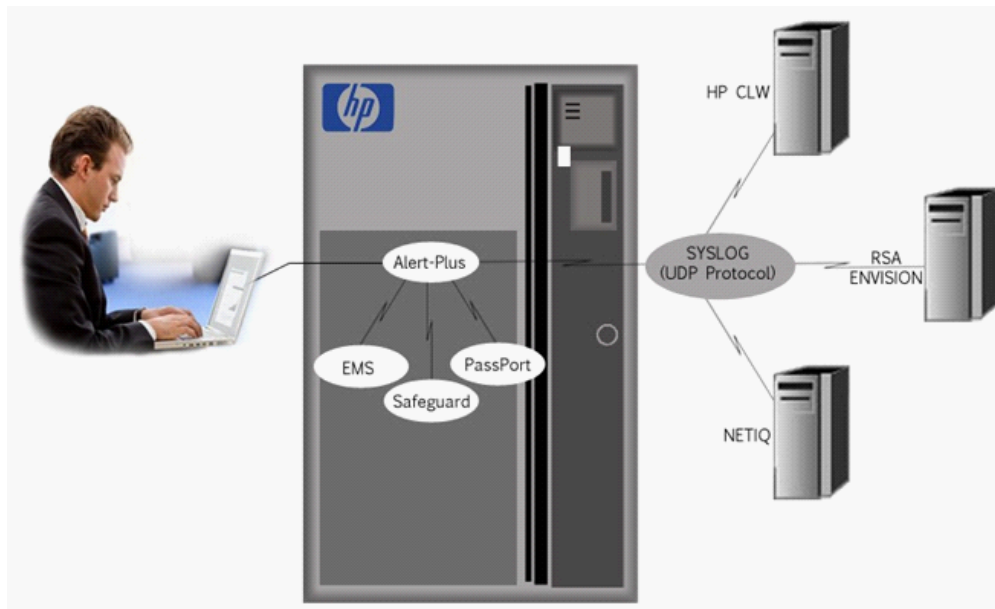
Alert-Plus®

Real-Time NonStop® Security and Merged Audit

NEW features

- Real-time data feeds to data warehouse.
- Significant Performance enhancements.
- Alert-Plus® now supports OSS files and directories such as:
 - Create
 - Open
 - Execute
 - Purge
- OSS file browsing from the Alert-Plus® GUI.
- Support for CSP PassPort® Audit Trails.

Alert-Plus® receives data from Safeguard Audit, CSP PassPort Audit, EMS messages (including ACI's BASE24 messages) and audit from CSP's own Compliance Reporting Module and File Integrity Checker. Messages that pass the pre-defined criteria are forwarded to the central data log solution of choice using a standard (SYSLOG) message format.



Merged audit event feed to central log server.

Merged Audit

As the need to implement strict security and audit compliance criteria expands, more and more companies are implementing central data log warehouse solutions to collect, correlate and analyze audit data from many sources.

Beginning with release 2.40 Alert-Plus® now supports the merging of several sources of audit information into a central data warehouse. Alert-Plus® can now extract events in real-time, evaluate the events against any user-defined rules to see if they are of interest and then forward them to any number of data warehouse products such as HP's Compliance Warehouse, RSA Envision and NETIQ Log Management.

Summary

Alert-Plus® allows you to monitor attempts at unauthorized access to your HP NonStop® systems as they occur and to take pre-defined corrective actions. Alert-Plus® also allows you to capture many sources of audit data on your NonStop systems and forward them to a central log server for offline analysis.

Contact Computer Security Products for more information

Tel: 800-565-0415 or 1-905-568-8900

For sales information: sales@CSPSecurity.com

Visit our website at: www.CSPSecurity.com