CSP
COMPUTER SECURITY PRODUCTS, INC.

Alert-Plus®

Real-time Intrusion Detection

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

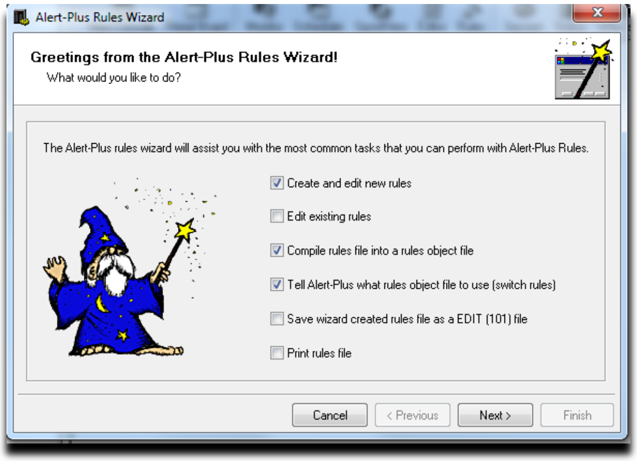
What's new!

- Support for BASE24 messages
- Real-time data feeds to data warehouse
- Support for OSS filesystem events
- OSS file browsing from the Alert-Plus GUI
- Support for CSP PassPort®, CRM and FIC Audit Trails

Building rules is easy!

Alert-Plus makes it easy to build rules. The Rules Wizard will create the necessary detection criteria and actions for most requirements.

Rules Wizard:



Alert-Plus Rules Wizard

Greetings from the Alert-Plus Rules Wizard!

What would you like to do?

The Alert-Plus rules wizard will assist you with the most common tasks that you can perform with Alert-Plus Rules.

☑ Create and edit new rules
□ Edit existing rules
☑ Compile rules file into a rules object file
☑ Tell Alert-Plus what rules object file to use (switch rules)
□ Save wizard created rules file as a EDIT (101) file
□ Print rules file

For more complex requirements, Alert-Plus provides:

- Simple scripting language
- Built-in routines
- Easy-to-use built-in text editor

Get Alerted!

Alert-Plus actions can include audible alarms, email alerts, EMS messages, or even freezing a user – which can stop an intrusion or password attack in its tracks.

Integrated Enterprise Security

Alert-Plus reads events from CSP's other security products, including Passport (for full session control and audit), CRM (compliance reports) and FIC (file integrity checker.

The Alert-Plus GUI is also integrated into Protect, CSP's Nonstop security management console.

COMPUTER SECURITY PRODUCTS,INC.

Alert-Plus®

Real-time Intrusion Detection

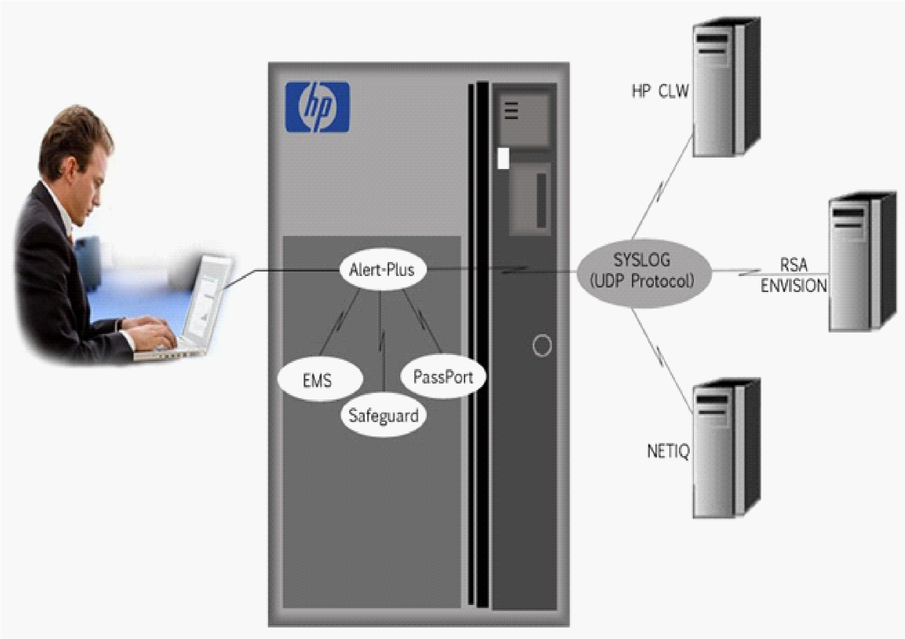
Merged Audit and SIEM

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

Alert-Plus supports the merging of several sources of audit information into a central data warehouse or SIEM.

Alert-Plus can 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. Alert-Plus receives data from Safeguard Audit, CSP PassPort Audit, EMS messages, 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.



Hewlett Packard Enterprise
Silver Partner
Technology Partner

Contact Computer Security Products for more information

Tel: 1-800-565-0415 or 1-905-568-8900
Email us at: Sales-csp@cspsecurity.com
Visit us at: www.cspsecurity.com