



Alert-Plus®

Alert-Plus provides real-time intrusion detection on HPE 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 also help block them.

What benefits does it provide?

- Intrusion Detection
- Identify vulnerabilities
- Stop cyber-attacks in real time
- Instant notifications for security events
- Continuously monitor for unauthorized events
- Forward logs to SIEM for security event analysis
- Address PCI and other compliance requirements

Key features

- Read and notify based on Safeguard audit and logs from various CSP products
- Support for BASE24 OMF messages
- Forward logs to SIEM via Syslog for further analysis
- Support for Guardian and OSS events
- Support for CSP PassPort® audit (user access and session control) and Verify Elite (file monitoring)
- Setup immediate automated actions on critical notifications
- Create, edit and compile customized event rules
- Correlate events for intelligent analysis
- Define automatic actions to be carried out in response to events
- Access and print reports from the spooler
- Use Built-in routines
- Rules wizard for easy rules creation
- Stop intrusions immediately using audible alarms, email alerts, EMS messages, or freezing users
- Quick and easy installation



PCI and Alert-Plus

Alert-Plus helps address key PCI requirements:

- Req. 6 - Develop and maintain secure systems and applications (change control)
- Req. 10 - Track and monitor all access to network resources and cardholder data (instant notifications)
- Req. 11 – Regularly test security systems and processes (monitor unauthorized events)





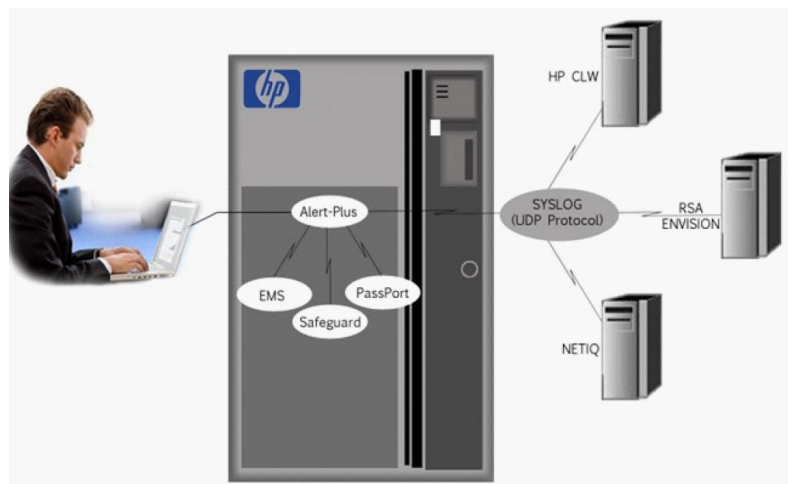
As the need to implement strict security and audit compliance criteria expands, more companies are implementing central data log warehouse, security information, and event management (SIEM) solutions to collect, correlate, and analyze audit data from many sources.

Receive Alerts

Alert-Plus actions can include audible alarms, email alerts, EMS messages, or even freezing a user. These alerts can stop an intrusion or password attack as it happens.

Merged Audit and SIEM Key Features

- Supports the merging of several sources of audit information into a central data warehouse or SIEM
- Provides the ability to extract, evaluate and forward events in real time to any number of data warehouse products
- Receives data from Safeguard Audit, CSP PassPort Audit, EMS messages, ACI's BASE24 messages, and other sources
- Messages that pass the predefined criteria are forwarded to the central data log solution of choice using a standard (SYSLOG) message format



Integrated Enterprise Security

Alert-Plus reads events from CSP's other security products, including CSP Passport (session control and audit) and Verify Elite (compliance reports and file Integrity checks). The Alert-Plus GUI is also integrated into Protect, CSP's Nonstop security management console.

Learn more about how enterprise data protection can benefit your organization here or contact us to discuss your data protection requirements: www.comforte.com. Follow us on social media:

