ServerGuard

ADMINUX®

Fact: More security breaches are from internal than external sources.

Fact: You cannot have Unix or Linux operating system security without automated system administration.

ServerGuard is a server-based intrusion detection system that provides around-the-clock detection of server security breaches.

Your servers are regularly scanned for a wide variety of security issues and a daily security diary is created so that review of potential security issues can be accomplished quickly and easily.

ServerGuard automatically:

- Scans for Trojan Horse violations
- Scans for backdoor violations
- Scans for changes in checksums, ownership and permissions to sensitive files, directories, devices and programs
- Scans for suspicious failed login attempts
- Scans for suspicious failed su attempts
- Scans root's PATH variable for security concerns
- Scans for any new world writeable files
- Scans for any new user writeable files
- Scans for any new rogue (misplaced) devices
- Scans for any new SGID files
- Scans for any new SUID files
- Determines if a file has lost its stickybit
- Logs deletion of system owned files
- Logs deletion of user owned files
- Scans for potential problems in /etc/passwd file, such as:
  - no matching entry in NIS
  - group ID not in /etc/group
  - invalid home directory
  - duplicate logins
  - duplicate UIDs
  - root entry missing
  - root entry is not the first entry
  - unexpected value for shell
  - invalid shell
  - shell is Set UID
  - shell is Set GID
- Detects possible file name spoofing
- Determines if the last boot expected
- Creates a daily security diary
- Monitors tcp and udp ports
- Determines if an inactive port has become active
- Determines if an active port has become inactive
- Determines if a URL exists
- Determines if the URL changed
- Stores a copy of the URL web page locally
- Notifies the designated personnel (on-site or off-site) via pager, fax, email, or other methods if it determines there is a possibility that system security has been compromised.