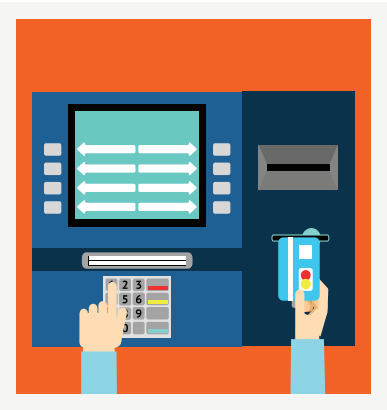
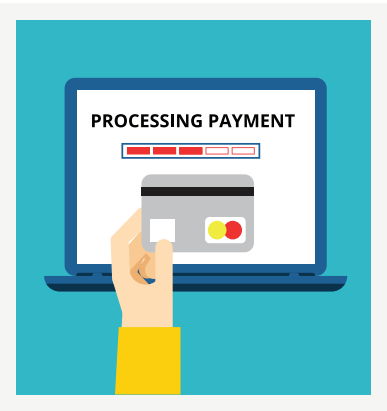
cimtrak
detecting change throughout the enterprise

cimcor.com

FILE INTEGRITY MONITORING FOR PCI-DSS COMPLIANCE IN 3 EASY STEPS

Two Payment Card Industry Digital Security Standards (PCI-DSS) requirements specifically call for the use of file integrity monitoring in order to detect changes to critical files and logs associated with your PCI environment.





SECTION 10.5.5

"Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)"

SECTION 11.5

"Deploy a change detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly."

CimTrak is an advanced file integrity monitoring tool running on proprietary technology which offers its "truly real-time" change detection capabilities. Many PCI environments lack file integrity monitoring because it is often perceived as being too expensive, too hard to install, and produces too much "noise." CimTrak breaks through all these familiar objections, offering a tool that is simple to configure and allows users to differentiate good change from bad, cutting down on the dreaded "noise." What's more, it comes at a price that won't bust your budget.

CIMTRAK MAKES FILE INTEGRITY MONITORING EASY:

1. INSTALL

First, install CimTrak on the endpoints you wish to monitor. CimTrak quickly and easily installs on servers, workstations and POS systems and supports a wide variety of operating systems including Windows, Linux, Mac OSX and UNIX

2. SET UP

Next, set up policies for what you want to monitor. Don't worry though, it's quite simple. CimTrak includes base operating system templates, which you can apply to instantly monitor the underlying critical system files. This means with a few clicks, you can be meeting 50% of section 11.5. From there, pick the other files on your systems that are critical to monitor. These are generally files associated with your payment card application and log files from the PCI environment.

3. CONFIGURE/CONNECT

Finally, configure any alerts you would like to receive when changes occur, and optionally, connect CimTrak to any log management or SIEM solution that you may utilize. With granular user control, you can also set up user permissions to restrict certain operations and/or viewing certain systems or files.

That's it, all finished. You are now detecting changes to critical files and logs as required by PCI-DSS!

WANT TO LEARN MORE?

Visit www.cimcor.com and request a demo or free trial.

CIMCOR