StoreGazer Integration with Existing PCI Solutions

StoreGazer is one of the leading system monitoring and management tools for the Toshiba 4690 operating system for retail. Originally designed to centralize the 4690 events logs into a single enterprise console, StoreGazer has continued to evolve to meet the needs of our clients, particularly in the areas of security management and monitoring to meet the ever-changing requirements set forth by PCI.

Active Monitoring and Immediate Notifications

Included in the StoreGazer solution is a resident background agent on the POS controller that monitors the 4690 event logs, actively running processes, and specific files stored on the hard drive. If the background agent detects something unusual in any of these areas, an immediate notification is sent to a StoreGazer Server application on the enterprise server. That notification can take several different forms, including logging the condition to a database for monitoring and reporting purposes, sending a customized email to a specific recipient list, or generating an SNMP trap or Windows Event Log entry for integration with third party trouble ticket and enterprise monitoring solutions.

SYSLOG Integration

In 2014, StoreGazer was enhanced with the ability to transform any of these notifications into a SYSLOG message, which can then be sent to a Security Information & Event Management (SIEM) product, enabling customers to include their 4690 controllers in their enterprise monitoring solution. The data in these SYSLOG messages is entirely customizable, so you can change the message into whatever format works best for your environment, using all of the available data fields that are relevant to the event (who, what, where, when, etc.)

The StoreGazer Advantage

One of the key features of StoreGazer is the use of a database backend to store all notifications. By centralizing these notifications and maintaining a history of prior notifications, customers have the power to generate audit trails for the events leading up to and following any single condition or situation that is encountered. Centralization also simplifies the task of determining if a condition is isolated to a single location, related to a specific hardware or software characteristic at the store, or indicative of a more serious enterprise-wide problem.

Web-Enabled Client Interface

In addition to integrating with third party trouble ticket and enterprise management solutions, StoreGazer includes a client interface for reviewing the event notifications, inventory data, and security-related alerts through a web browser. The web client also enables users to take a variety of actions on one or more controllers, either in response to a reported condition or as part of the day-to-day management of the 4690 environment. Some of the more common actions include starting and stopping processes, transferring files, reloading registers, adding or removing users from the store security files, or performing system-wide password changes for enterprise-level staff.

4690 Authorization Management

StoreGazer is a valuable addition to any PCI toolbox, providing functionality and insight specific to the security of the 4690 POS system.

As a functional tool, StoreGazer enables customers to manage the store-level authorization files, controlling who has access to the POS controller and terminal, and what level of access those users have. By providing a password management tool, enterprise users can change their password on every store controller from a single screen, making it possible for helpdesks to transition from using a shared master account to a PCI-compliant environment where everyone has their own login - complete with password expiration and complexity requirements.

As a reporting tool, StoreGazer monitors those same user authorization records and reports any changes that occur – not only users being added or removed, but also any changes to permissions or passwords for already defined users. By tracking password changes, StoreGazer can quickly identify any logins that are not actively being used and provide recommendations that will close these potential security holes. By tracking permissions, customers can quickly produce reports for auditors to display every active user with command-line access to their stores, or other sensitive permissions of concern.

Additional PCI Reporting Tools

Command Logs

The 4690 operating system maintains logs of any commands issued from the command line or an FTP session. These logs, along with notifications of files being opened and edited in the 4690 file editing tools, are monitored and transferred off the controller automatically by StoreGazer. Stored in the database, these logs can now be searched and reviewed from an enterprise level, providing not just the command that was run, but the "who", "where" and "when" associated with that command as well as any related activity by the operator, at the location, or in the timeframe as the command in question.

PIN Pad Inventory (with Serial Number Tracking)

Toshiba has recently provided access to pin pad inventory, including the PIN pad's model and serial number, as part of the ACE V7R5 EPS solution. As a result, StoreGazer now has the ability to retrieve this pin pad inventory and provide immediate notifications of any changes to the pin pads installed on the store registers. StoreGazer tracks this information historically - when a new pin pad shows up at a register, it takes just a single click to find out if that pin pad came from another register or if it was recently introduced to your store environment.

WhiteListing

StoreGazer includes a 4690 process monitoring tool that employs a user-defined whitelist to control which applications are allowed to run on the controller and which ones are not. While monitoring the actively running processes, if StoreGazer detects any process that is not on the whitelist, an alert is raised, which can then be acted upon automatically by stopping the process, or sending out a notification (email, syslog, etc.) to alert a security response team about the unidentified process being run.