Ensure PCI Data Security Standards Compliance with Quest InTrust Solutions

Companies that process, issue or acquire transactions made with Visa or MasterCard credit cards must be aware of the Payment Card Industry Data Security Standards (PCI). As millions of transactions are made daily with credit cards, the event data generated by these activities can grow very quickly to Gigabyte-level, causing concern for the IT security department tasked with managing this important data.

The majority of the auditing requirement comes in Section 10 of the Payment Card Industry Data Security Standard: Track and monitor all access to network resources and cardholder data. The logging mechanisms and ability to track user activities are critical. Relevant to this discussion, a company must:

- Have access to all audit trails
- Track all actions taken by a root or employee with administrative level privileges
- Track creation and deletion of objects
- Limit the views to those with a job-related need
- Back up logs to a centralized server
- Review logs daily
- Retain audit trail history that is consistent with its effective use, as well as legal regulations. (An audit history usually covers a period of at least one year, with a minimum of 3 months available online.)

Companies are looking for solutions that will automate the collection of this event data, store the logs inexpensively, and provide easy-to-read reports to corporate data security personnel. The bottom line is that companies must audit all relevant servers. The audit logs must be collected, stored, monitored and assessed on a routine basis. The authenticity of the logs must be verified at all times.

The Quest InTrust family of products (including InTrust and InTrust for Active Directory) help by enabling organizations to collect audit log data from a heterogeneous network in an automated, network-friendly configuration. Compressing the data at a 40:1 ratio, InTrust provides organizations a way to collect the logs in a timely fashion and store them for an extended period of time at a reduced cost. The compression occurs while retaining the native state of the log and in such a manner as to allow for recreation for forensic purposes.

Each InTrust report provides information such as the date/time, identity of affected user, system component and server, the account performing the action and the origination of the event.

InTrust solutions provide flexible, easy-to-read reports. These reports can be delegated out to only those individuals who are on a need-to-know basis. The reports can be scheduled to run throughout the day or on an ad-hoc basis. Reports can be modified and/or created to reflect the exact information required by the organization.

Quest InTrust solutions are helping companies around the world meet the requirements as defined by PCI by automating the collection of audit logs, preservation of logs and output of the information in a readable format. For more information on how InTrust solutions can help, visit http://wm.quest.com/products/intrust/.

©2006 Quest Software, Inc. All rights reserved. Quest and Quest Software are trademarks or registered trademarks of Quest Software. All other brand or product names are trademarks or registered trademarks of their respective holders.