



Securing Credit Cardholder Information against Internal Threats

How Shalom Security Enforces Visa CISP and PCI Security Standards for Financial Service Providers

Industry Focus: Payment processors, Automated Clearing Houses (ACHs), merchants, service providers, retailers, and e-commerce.

The PCI Security Standard and the Visa USA Cardholder Information Security Program (CISP) define a basic standard for securing cardholder data in transit and in storage. Required for all entities storing, processing, or transmitting cardholder data, it was developed to ensure that credit card merchants and service providers maintain highest information security standards. In conjunction with the PCI Data Security Standard, Visa's CISP establishes a set of information security requirements that include:

1. Build and maintain a secure network
2. Protect cardholder data - from outside and inside threats
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

FRAUDULENT INSIDERS POSE A THREAT TO CARDHOLDER DATA SECURITY

Although most enterprises maintain secure networks that are shielded from external attacks, today's threat to cardholder data lies on the inside, among insiders. Impostors and malicious insiders with access rights to cardholder data are root causes of stolen card information from computers.

To address this insider problem, all computer systems that hold or transmit cardholder data should be continuously monitored for suspicious user activity. An effective internal security solution should authenticate and report suspicious insiders and lock out intruders.

SHALOM SECURITY AUTHENTICATES AND REPORTS SUSPICIOUS INSIDERS

Without copying, pasting, or transferring files, some malicious insiders steal data by simply viewing cardholder data through secure enterprise applications.

With Shalom Security, the minute they behave erratically, they are AUTHENTICATED and reported in real time. This act of questioning and reporting malicious insiders at the very minute they behave suspiciously deters them from stealing cardholder data.

SHALOM SECURITY LOCKS OUT INTRUDERS AND REPORTS UNAUTHORIZED BACKDOORS ACCOUNTS
Sometimes hackers steal log on credentials of legitimate insiders (admin accounts, employees) who have access to sensitive data. Using hijacked accounts, intruders always behave suspiciously, logging in at odd times and running suspicious commands from odd workstations.

Shalom Security detects their suspicious behavior, questions them, and locks them out when they fail the identity verification. Implanted automated scripts and secretly created backdoor accounts are also reported.

In conclusion, malicious insiders and intruders disguised as legitimate insiders pose the greatest risk to cardholder information. With Shalom Security, cardholder information is protected from insider threats ensuring highest security standards and Visa CISP compliance for merchants and service providers.