NOWELL
DEVELOPMENT

Securing Financial Transaction, Credit Card Data against Internal Security Risks

Shalom ESX Platform helps Visa CISP and PCI Security Standards for Financial Service Providers

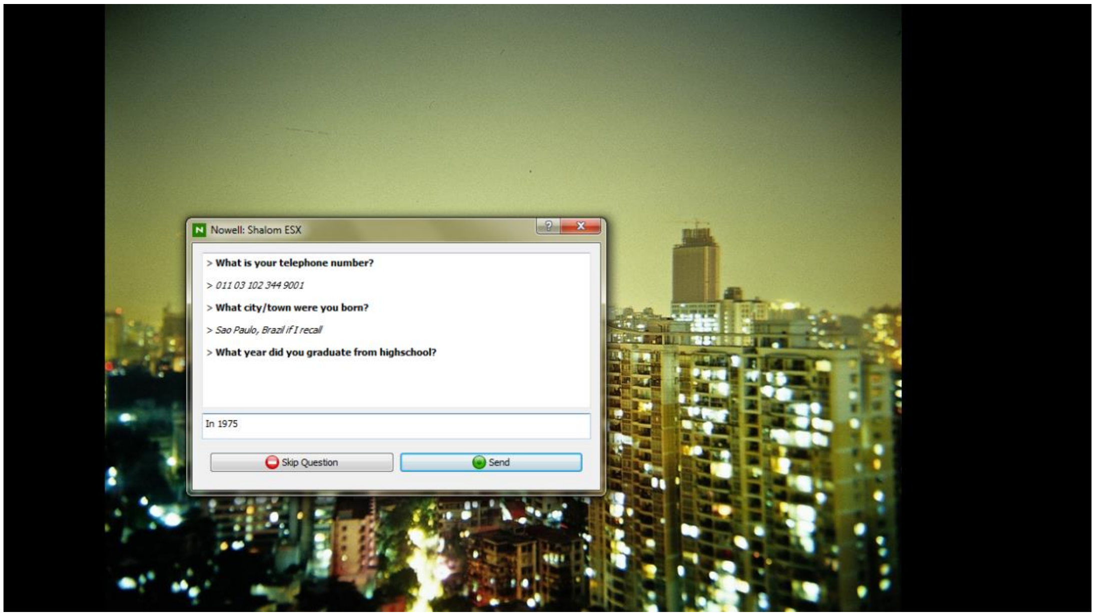
Industry Focus: Financial Services, Payment processors automated clearing houses (ACHs), merchants, service providers, retailers, credit and debit card issuers, and e-commerce

The *PCI Security Standard and the Visa USA Cardholder Information Security Program (CISP)* defines a basic standard for securing cardholder data in transit and in storage. Required for all business 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 DSS, Visa's CISP establishes a set of information security goals and requirements that include:

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

TRUSTED INSIDERS POSE A RISK TO CARDHOLDER DATA SECURITY - DUE TO ERROR OR BREACH

Although most enterprises maintain secure networks that are shielded from external attacks, today's risk to cardholder data lies on the inside, among insiders and those with access to the financial data. Impostors and malicious insiders with access rights to cardholder data are sometimes the root causes of stolen credit card information from computers. While most insiders are trustworthy and honest, occasionally a few fall to misusing their liberty to information access for illegitimate activity such as undisclosed unauthorized self-profiting or gross financial fraud, or divulging login credentials to outsiders via virus, social engineering etc.



> **What is your telephone number?**

> *011 03 102 344 9001*

> **What city/town were you born?**

> *Sao Paulo, Brazil if I recall*

> **What year did you graduate from highschool?**

In 1975

To address this insider risk problem, all computer systems that hold or transmit cardholder data should be continuously monitored and authenticated for *suspicious user activity.* An effective internal security solution should authenticate and report suspicious insiders and prevent unauthorized entities.

In addition, a solution should provide a historic audit trail around the data, for full accountability of who accessed the data, where data went, what it was used for and when it was accessed. Nowell's Shalom ESX Platform meets some of these requirements by monitoring, and authenticating the systems that hold the data, and coupled with other security tools, like database security auditing and forensics tools, SIEM, we provide a comprehensive solution to these challenges.

SHALOM ESX PLATFORM 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 ESX Platform, the minute they behave erratically – *during an anomaly*— they are *authenticated* and reported in real time. This act of authenticating and reporting malicious insiders at the very minute they behave suspiciously deters from stealing or misusing cardholder data. Shalom ESX software integrates with LDAP directory services to improve the security and risk monitoring of security sensitive environments

SHALOM ESX PLATFORM REPORTS SUSPICIOUS UNAUTHORIZED ACCOUNTS

Sometimes intruders steal log on credentials of legitimate insiders (admin accounts, employees) who have access to sensitive data. Using hijacked accounts, intruders behave suspiciously, logging in at odd times and/or running suspicious applications from odd workstations. Shalom ESX detects such suspicious behavior, and authenticates for identity verification. Implanted automated scripts and secretly created backdoor accounts are also identified and reported. In conclusion, malicious insiders and intruders disguised as legitimate insiders pose the greatest risk to cardholder information. With Shalom ESX Platform, cardholder information is protected from insider risks ensuring highest security standards and PCI-DSS & Visa CISP compliance for merchants and service providers.

NOWELL
Integrity Above Profits

Contact Us Today:

Nowell Development, Inc
11152 Westheimer Road # 956
Houston, Texas 77042
United States of America
Web: http://www.nowellgroup.com
E-mail: support@nowellgroup.com
http://linkedin.com/company/nowell-inc