# VERTICAL BRIEF

## Novell Payment Card Industry

Sponsored by: Novell

Sally Hudson
February 2008

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

## PAYMENT CARD INDUSTRY AND DIGITAL SIGNATURES

On September 7, 2006, Payment Card Industry (PCI) vendors officially joined together to form the PCI Security Standards Council. This council, which comprises American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International, tackled its first initiative: to update the PCI Data Security Standard (PCI DSS) and introduce v1.1 of this standard. First introduced in January 2005, the PCI DSS provides a single global security standard that offers specific technical guidance for protecting cardholder interests. PCI DSS presents the framework and standard for protecting cardholder and sensitive authentication data with the ultimate goals of limiting access, controlling fraud, and providing financial benefits to organizations that are in compliance. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.

The PCI Data Security Standard defines 12 high-level requirements in the following six categories:

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

IDC believes that much of PCI compliance can be achieved through a strong identity and security management (ISM) implementation. Identity and access management (IAM) enterprise strategies are being widely adopted as a way to create a more reliable and cost-effective security infrastructure driven by economic and compliance considerations. IAM automates and simplifies the process of enabling access to trusted network resources, activating and deactivating (provisioning) of accounts, and creating and managing access rights policies, cards, and other privileges from across the enterprise. These IAM capabilities, coupled with security information and event management (SIEM) software, provide a formidable combination in PCI security implementations. SIEM solutions include software designed to aggregate data from multiple sources to identify patterns of events that might signify attacks, intrusions, misuse, or failure. Event correlation simplifies and speeds the monitoring of network events by consolidating alerts and error logs into a short, easy-to-understand package. SIEM also includes activities that collect and disseminate threat intelligence, provides early warning threat services, and can provide information on countermeasures.

## Novell and Identity and Security Management Solutions

Novell Inc., based in Waltham, Massachusetts, has consistently been a leader in the IAM market space. The company is one of a small number of vendors in the market today offering a full and comprehensive suite of compliance and security software and a wide range of individual products in IAM, SIEM, and security management, which can be effectively combined to create solutions to solve PCI-related compliance issues. Novell solutions include secure user access, provisioning, secure single sign-on, and automated event monitoring coupled with the appropriate systems management capabilities. By viewing these solution combinations in context of the business problem they are solving, companies realize that this approach can be very effective in meeting regulatory compliance demands (see Table 1).

TABLE 1

PCI Challenges and Solutions

| Requirement | IDC Best Practice | Novell Solution Feature(s) |
|---|---|---|
| Protect stored data | Locate and encrypt data | Secure data at rest and in transit, combine network encryption, transparent data encryption of all data types and complete table spaces, and strong authentication; Novell Storage Manager, Novell Identity Manager |
| Regularly test security systems and processes | Conduct regular scans and testing of applications | Automated user/resource discovery; Novell Sentinel; Novell ZENworks |
| Assign a unique ID to each person with computer access | Train employees to improve security awareness, track unusual employee behavior | Password and profile management, personalized user interface, automated user/resource discovery; Novell Identity Manager, Novell SecureLogin, Novell ZENworks |
| Install and maintain a firewall configuration to protect data | Segment credit card networks and control access to them | Workflow, audit, and reporting with real-time alerts; Novell Sentinel, Novell Access Manager, Novell ZENworks |

Source: IDC, 2008

## Copyright Notice