

INDUSTRY CHECKLIST

- **Ensure reliable security**
- **Address PCI DSS compliance**
- **Integrate the right-sized solution**
- **Differentiate services to customers**



Maximizing Return When Processing Credit Card Data

Companies accepting credit or debit cards in exchange for goods or services must already be compliant with the PCI DSS (Payment Card Industry Data Security Standard) requirements. Any merchant that does not comply with PCI DSS is at risk of extensive fines from Visa and other card brand companies. To ensure that a PCI-compliant merchant is able to incorporate new technologies and to protect against new ways of hacking personal data, continuous auditing is required to retain PCI DSS compliance.

The cost of data compromise can be astronomical. Consider the class-action lawsuit against TJX Companies Inc., which operates TJ Maxx, Marshalls, and other retail stores. Hackers accessed at least 45 million credit or debit cards and about 450,000 driver's licenses, and military or state identification data stored on TJX computers. This breach is considered to be the largest computer theft of personal data in U.S. history with overall cost in damages, reputation, and legal fees in the billions.

However it is not only the large, household-name companies that face malicious network attacks. Smaller franchises and retailers are under constant threat of theft or damage as they typically do not focus investment in IT resources, cardholder data monitoring, and preventative network security solutions.

For PCI DSS compliance, it is important to design a network with appropriate physical and logical boundaries to segregate the PCI-compliant operating environment. The PCI DSS monitoring scope must also be manageable. To this end, the strong segregation and detailed traffic control capability available with the application proxy technology of the WatchGuard® Firebox® X family of threat management appliances is ideally suited to meeting these requirements.

See the free *Meeting PCI DSS Merchant Requirements with a WatchGuard® Firebox®* white paper for an extensive PCI DSS Requirements comparison with WatchGuard solutions (available through the *White Paper* link on www.watchguard.com).

Challenges retail customers face include

- **PCI DSS Compliance** - The effort to meet current and annual PCI DSS compliance requirements for controlling, monitoring, logging, and auditing cardholder data.
- **Operational Improvements** - Servicing more customers quickly during peak times without purchasing additional POS stations, such as queue-busting solutions to mitigate customer wait times, all while ensuring WLAN security.
- **New Revenue Opportunities** - In the highly competitive realm of retail, customer loyalty and repeat business is key. To continue winning customers, savvy retailers introduce differentiated services such as wireless guest access for buyer convenience.
- **Protect, Protect, Protect** - Ensuring company data and reputation and protecting customer data are at the forefront of executives' and IT management's thoughts every day.

PCI Security Standards Council

As a network security pioneer and visionary, WatchGuard® Technologies is a member of the PCI Security Standards Council, collaborating on standards development. For more information on the PCI Security Standards Council, visit www.pcisecuritystandards.org/



Extensible Threat Management for Retail

Extensible threat management (XTM) security solutions from WatchGuard aggregate multiple security measures into a single, easily configurable solution. Choose from a family of these devices, which can be deployed everywhere from physical retail locations to data centers to POS web sites and call centers. XTM protects customer cardholder data while delivering reliable management, monitoring, logging, and reporting.

Address PCI Compliance and Ensure Reliable Security

Security is not an event, it is a process. No firewall product can be "certified PCI DSS compliant." This is just a myth. Any network firewall or threat management appliance that combines a network firewall with other features – such as anti-virus and intrusion prevention services – can be a part of becoming compliant.

With WatchGuard's proxy firewall architecture, detailed network traffic control, intuitive management interface, extensive logging and reporting, standard encryption mechanisms (including WPA2, IPSec, and SSL VPN), and gateway anti-virus support, along with WatchGuard LiveSecurity® Service, merchants can quickly optimize WatchGuard technology for achieving compliance and reliable security.

Integrate Right-Sized Solutions

There are a number of different data sources that may be active at any given time of day from retail locations, franchises, the Web and call centers. And each may have its own topology to consider. Whether you are increasing protection at the data store while decreasing data storage at the retail site, or converting older, standalone POS systems to a new integrated system, highly reputable, easily upgradable and extensible WatchGuard network security solutions fit the bill.

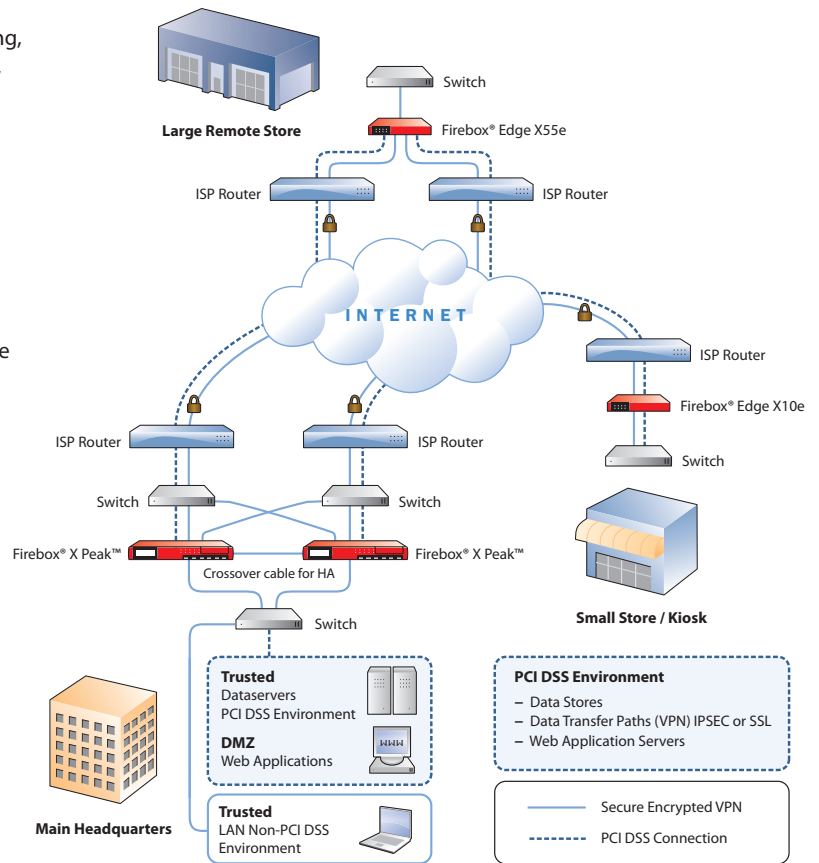
Each merchant requires a unique recipe for data security. Build the appropriate network environment, knowing the data is safe when integrating any WatchGuard network security solution.

Physical retail locations, franchises, POS web sites, and call centers pass encrypted cardholder data to data stores for ensuring customer information security.

Differentiate Services to Customers

The ability to provide quicker service to customers is at your fingertips. Queue-busting techniques and offering free wireless Internet access (wireless guest services) allow retailers to increase spend-per-transaction, the customer base, and customer loyalty.

Retailers who want to service customers quickly during peak times without purchasing more POS stations have an excellent option with WatchGuard. One solution is to reuse existing handheld mobile computers to perform POS applications – such as adding SKUs, viewing inventory, and checking out customers faster – via the wireless local area network (WLAN). Don't hesitate to go wireless for customer convenience while maintaining customer trust. WatchGuard provides Mobile VPN clients and Firebox® appliances to support handheld mobile computers from Motorola, Datalogic, NCR, Honeywell, and others.



WatchGuard® offers a family of interoperable, centrally managed devices that easily integrate into retail networks complying with PCI DSS requirements.

For more information about WatchGuard Retail Security Solutions, contact your reseller, visit www.watchguard.com, or call the number below.

Address: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 • **Web:** www.watchguard.com • **U.S. Sales:** 1.800.734.9905 • **International Sales:** +1.206.613.0895

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Firebox, and Peak are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners. Part No. WGCE66572_090308

